Signals and Communication Technology

Branislav Jovic

Synchronization Techniques for Chaotic Communication Systems

Springer

Signals and Communication Technology

For further volumes:
http://www.springer.com/series/4748

Branislav Jovic

Synchronization Techniques for Chaotic Communication Systems

Springer

Author

Dr. Branislav Jovic
4/87 Lake Road
Belmont 0622
Auckland
New Zealand
E-mail: bjov001@gmail.com

ISBN 978-3-642-21848-4 e-ISBN 978-3-642-21849-1

DOI 10.1007/978-3-642-21849-1

Library of Congress Control Number: 2011931874

Typeset & Cover Design: Scientific Publishing Services Pvt. Ltd., Chennai, India.

Printed on acid-free paper

9 8 7 6 5 4 3 2 1

springer.com

I dedicate this book to my parents, Vera and Zelimir,
and my brother Vedran.

Preface

Since the early 1990s, when synchronization of chaotic communication systems became a popular research subject, a vast number of scientific papers have been published. However, most of today's books on chaotic communication systems deal exclusively with the systems where perfect synchronization is assumed, an assumption which separates theoretical from practical, real world, systems.

This book is the first of its kind dealing exclusively with the synchronization techniques for chaotic communication systems. It describes a number of novel robust synchronization techniques for single and multi-user chaotic communication systems published in world's leading journals in the area. In particular, it presents a solution to the problem of robust chaotic synchronization by presenting the first fully synchronized, highly secure, chaos based DS-CDMA system. The book fills a gap in the existing literature where a number of books exist that deal with chaos and chaotic communications but not with synchronization of chaotic communication systems. It also acts as a bridge between communication system theory and chaotic synchronization by carefully explaining the two concepts and demonstrating how they link into chaotic communication systems. The book also presents a detailed literature review on the topic of synchronization of chaotic communication systems. Furthermore, it presents the literature review on the general topic of chaotic synchronization and how those ideas led to the application of chaotic signals to secure chaotic communication systems. It therefore, in addition to presenting the state of the art systems, also presents a detailed history of chaotic communication systems.

Summary

In this book, sequence synchronization techniques for single and multiple-access chaotic communication systems are investigated. In particular, the techniques of sequence synchronization studied include those based on the principles of Pecora-Carroll (PC) chaotic synchronization and those based on the principles of traditional direct sequence code division multiple access (DS-CDMA) synchronization.

Based on the principles of PC chaotic synchronization, novel approaches to chaotic synchronization are proposed and used to design new single-user chaotic communication systems. These new chaotic communication systems include those based on the chaotic parameter modulation (CPM) and the initial condition modulation (ICM) techniques. Furthermore, the principles of time division multiplexing (TDM) are used to obtain the CPM and ICM based multi-user TDM systems. The performance of all of the proposed and the existing systems is evaluated in terms

of the bit error rate (BER) in the additive white Gaussian noise (AWGN) and the Rayleigh fading channels. Furthermore, it is shown that by implementing certain linear and wavelet filters, one can improve the BER performance of the ICM based systems in the AWGN channel.

The sequence synchronization of chaotic communication systems based on the DS-CDMA principles is then proposed. Both phases of the sequence synchronization process, namely the code acquisition and the code tracking, are proposed and investigated. It is shown that in terms of BER the chaos based DS-CDMA systems outperform the CPM and ICM based TDM systems for low number of users in the AWGN channel and vice-versa for large number of users. In addition, it is found that the chaos based DS-CDMA systems outperform the ICM and CPM based TDM systems in the Rayleigh fading channel. However, in the Rayleigh fading channel, they all fail to satisfy the adopted highest acceptable BER level of 10^{-3}.

In addition to the CPM and ICM based TDM systems and the chaos based DS-CDMA systems, the chaos based TDM system with the DS-CDMA correlator receiver is also proposed. It is shown that this system outperforms the CPM and ICM based TDM systems for any number of users. However, the system is outperformed by the chaos based DS-CDMA systems for low number of users and vice-versa for large number of users.

In order to mutually exploit the DS-CDMA and TDM benefits, a generalized chaos based TDM communication system with more than one DS-CDMA user per TDM branch is proposed and evaluated in the AWGN channel. In this way, the bandwidth efficiency of a DS-CDMA system is combined with the inter-user interference immunity of a TDM system, to allow for an increased number of users in the system while improving the BER performance.

In general, it is shown that the multi-user chaotic communication systems based on the acquisition and tracking synchronization scheme, are more robust to AWGN and Rayleigh fading than those based on the principles of chaotic synchronization.

Finally, the security of the proposed, as well as of the existing chaotic communication systems, is evaluated in terms of the newly proposed measures termed the 'Bit Power Parameter Spectrum' (BPPS) and the 'Bit Power Initial Condition Spectrum' (BPICS). Using these measures, it is shown that chaotic communication systems can be optimized in terms of security.

Outline

The book is organized into eleven chapters and an appendix. Chapter 1 gives a thorough introduction to multi-user communication systems and presents methods for their modeling and performance evaluation. It states the motivation of the book by demonstrating the importance of synchronization among the transmitter and the receiver. In chapter 2, chaotic signals and their synchronization methods within secure communication systems are introduced. Chapters 3 and 4 investigate synchronization of flows and maps, respectively, using tools from nonlinear control theory and propose novel methods of achieving synchronization. In chapter 5, a

novel mathematical analysis for predicting master-slave synchronization of chaotic systems is proposed and demonstrated on three different systems. Chapter 6 proposes a number of single user chaotic communications systems based on the synchronization techniques of chapters 3-5. In chapter 7, the traditional DS-CDMA synchronization technique is implemented within the multi-user chaos based DS-CDMA (CBDS-CDMA) communication scheme proposing three highly secure and robust PRBS and chaotic pilot based CBDS-CDMA systems. Chapter 8 proposes a chaos based TDM multi-user system based on the DS-CDMA synchronization technique while chapter 9 proposes the chaotic synchronization based multi-user TDM systems. Chapter 10 proposes techniques for the optimization of security within chaotic communication systems. In chapter 11, the conclusions and the future directions are outlined. Finally, the methods of de-noising chaotic communication systems and thus improving their BER performance are proposed and investigated in the appendix.

Acknowledgements

I would firstly like to acknowledge the help of Dr. Charles Unsworth. Without his positive attitude toward any problem, this book, which is based on my PhD thesis, would not have been possible.

Furthermore, I would like to acknowledge the financial support provided to me by the Faculty of Engineering Guaranteed Financial Support Scheme (GFSS), the Graduate Research Fund (GRF) and the Department of Electrical and Computer Engineering of the University of Auckland, New Zealand.

Finally, I would like to acknowledge the help and support of my family, my mother Vera, father Zelimir and brother Vedran. Synchronization with them was a necessary requirement for the completion of this book!

Contents

Chapter 1
Introduction to Multi-user Mobile Communication Systems

In this chapter, the brief history and the main categories of the multi-user (multiple access) mobile communication systems, as well as some of their hybrids, are introduced. Furthermore, the disturbances encountered within the physical transmission channel, such as noise and fading, are presented. The concept of the bit error rate (BER), which is used to measure the effects of the channel imperfections on the transmitted signal, is then outlined. The procedure of evaluating the bit error rate is then demonstrated when noise and fading are present in the channel. Finally, the motivation of the book is stated by demonstrating the importance of synchronization among the transmitter and the receiver through its effect on the BER performance of the system.

The three basic categories of multiple access techniques include those based on frequency division multiplexing (FDM), time division multiplexing (TDM) and code division multiplexing (CDM), that is, frequency division multiple access (FDMA), time division multiple access (TDMA) and code division multiple access (CDMA). These three basic techniques can be combined to form hybrid systems such as the combined frequency division and time division (FD/TDMA), combined frequency division and code division (FD/CDMA), combined time division and code division (TD/CDMA) and the combined frequency division, time division, and code division (FD/TD/CDMA) [1,2]. Figure 1.1 illustrates the three basic techniques and their relationship to the aforementioned hybrids. The hybrids can then be further subdivided [1].

The concept of mobile communication systems for general use by the public was introduced in the 1960s and 1970s by AT&T Bell Laboratories [3]. This concept was based on dividing the operational area or coverage zone of the system into small cells which could be reused by different users of the system. Accordingly, such systems have also been termed cellular systems. Due to the lack of technology these mobile cellular systems could not be developed until the late 1970s. The world's first cellular system was implemented in Japan in 1979 by the Nippon Telephone and Telegraph company (NTT) [3]. In 1983, Ameritech of Chicago U.S.A., deployed the first U.S. cellular system, termed the Advanced Mobile Phone System (AMPS) [3]. NTT and AMPS used the concepts of FDMA to transfer information among users. In the U.S.A., AMPS was gradually phased

B. Jovic: Synchronization Techniques for Chaotic Commun. Syst., SCT 5, pp. 1–30.
springerlink.com

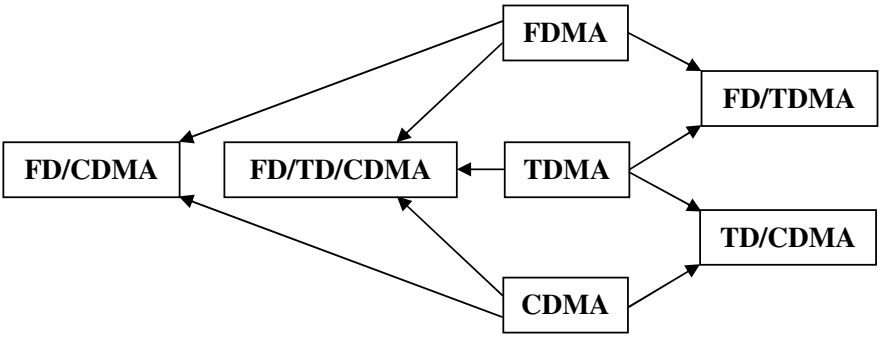


Fig. 1.1 The three basic categories of multiple access communication techniques and their hybrids

out by the introduction of the U.S. Digital Cellular (USDC) system in 1991. USDC implemented TDMA principles and offered three times the capacity of the AMPS. A cellular system based on the principles of CDMA was developed by Qualcomm, Inc. in 1993. It became standardized by the Telecommunications Industry Association (TIA) as an Interim Standard known as IS-95 [3]. The operation and the characteristics of the IS-95 mobile system have been described in detail in [2]. Today, the most advanced CDMA based mobile communication systems implement technologies such as CDMA2000 and Wideband CDMA (W-CDMA) [2].

1.1 Frequency Division Multiple Access (FDMA)

In FDMA, individual frequency bands, or channels, are assigned to individual users during the transmission time. The frequency axis of a certain available bandwidth is divided up into *M* discrete channels, as illustrated in Figure 1.2 [3].

Such division of the available bandwidth, denoted by B_t, allows each user in the system to be allocated a unique frequency band. The available frequency

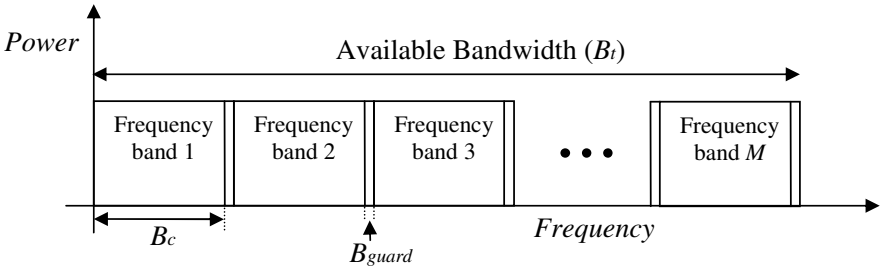


Fig. 1.2 The available frequency bands (channels) within an FDMA communication system

bands are assigned on demand to users who request service. Once a user has been assigned the particular frequency band, no other user can access this frequency band for the duration of the call. Furthermore, any frequency band which is not in use cannot be used by other users to increase or share capacity [3]. An example of a system which implements FDMA is the Advanced Mobile Phone System (AMPS) [3]. In order to allow for the simultaneous two way conversation among the users of the system, (ie. to be able to talk and listen simultaneously) AMPS implements frequency division duplexing (FDD). In this scheme a user is allocated a frequency band which is separated from the other user's frequency band by 45 MHz. Furthermore, in AMPS the guard bands separating the frequency bands (channels) from each other typically have a value of $B_{guard} = 10\,\text{kHz}$, while the channel bandwidth is equal to $B_c = 30\,\text{kHz}$.

1.2 Time Division Multiple Access (TDMA)

Before describing a typical TDMA system, the general principles of time division multiplexing (TDM) are first explained. Time division multiplexing involves sampling a number of different waveforms and interleaving them into a single waveform before transmission across the channel takes place. Within the channel, disturbances such as noise and fading, affect the transmitted signal. The input signals are sampled and interleaved by employing a multiplexing switch which samples the input signals sequentially, as illustrated in Figure 1.3a. The multiplexing switch samples each of the *M* message signals *m*(*t*) from 1 to *M*. Once all the signals are sampled, the switch returns back to sample the user 1 again and repeat the cycle. A waveform *c*(*t*), produced by sampling some arbitrary message signals *m*(*t*), is shown in Figure 1.3b. The received signal *r*(*t*) is decomposed into the separate signals using a de-multiplexing switch.

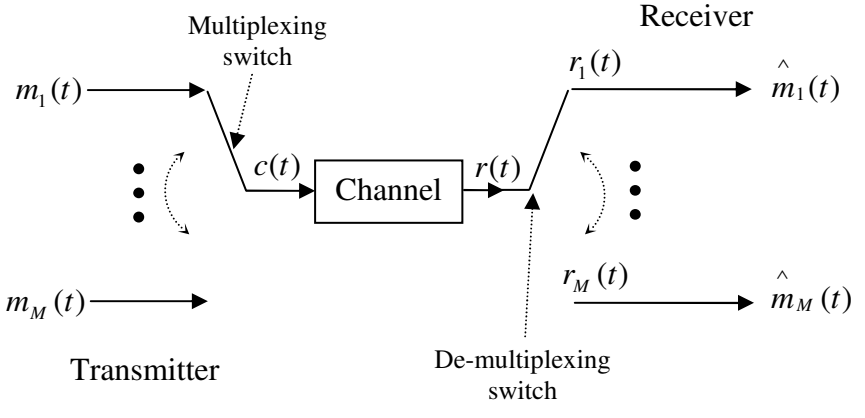


Fig. 1.3a A simplified block diagram showing the TDM principle. The message signals *m*(*t*) are transmitted across the channel and are received in the form of $\hat{m}(t)$.

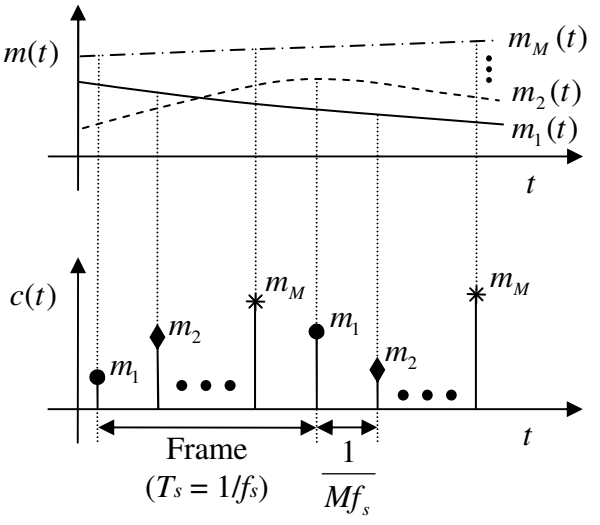


Fig. 1.3b The sampling procedure of some arbitrary message signals $m(t)$ and the transmitted signal $c(t)$.

Provided that all the input signals have the same message bandwidth W, the inputs should be multiplexed at the rate $f_s \geq 2W$. This results in the time separation between the successive samples of $T_s = 1/f_s \leq 1/2W$. In the TDM system, the time interval T_s containing one sample from each input is called a frame [4]. The multiplexing and de-multiplexing switches of Figure 1.3a are most often realised using electronic switching [4]. Their synchronization is of crucial importance because each sample must be distributed to the correct output at the appropriate time. A way of synchronizing the multiplexer and de-multiplexer is to devote one time slot per frame to a distinctive marker sample which is known and expected by the receiver. The drawback of the synchronization using markers is that an extra time slot is required per frame to accommodate them. Other synchronization methods involve auxiliary pilot tone or the statistical properties of the TDM signal itself [4].

Furthermore, for different TDM systems the transmitted signal may consist of bursts of samples for each user rather than a single sample. The bursts can then be ordered into frames with one burst for each active user.

In a typical TDMA system the users are allocated into M time slots which comprise one frame. On top of the time slots, the frame also consists of the preamble and trail bits. These are used for the synchronization purposes and to eliminate any possible interference among adjacent frames and time slots. They may also be used for channel estimation and training of the data equalizer. A particular user is allocated a particular time slot. Therefore, each user has access to the channel for the duration of a time slot. Furthermore, each time slot contains the information bits as well as the trail, synchronization and the guard bits. The composition of a TDMA frame is shown in Figure 1.4 [3].

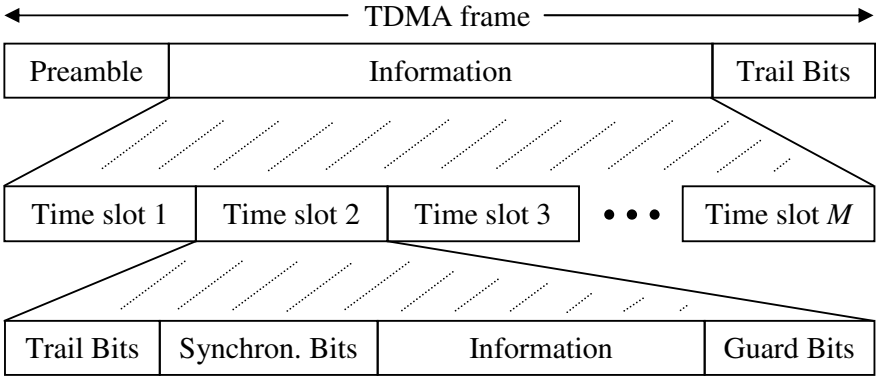


Fig. 1.4 The general representation of one TDMA frame

An example of a system which implements TDMA is the Global System for Mobile (GSM) [5,3]. In GSM, each frame consists of eight time slots. Each time slot contains 156.25 bits and lasts for 0.577 ms [3]. Furthermore, in each time slot there are two traffic bursts of 58 bits of data (information), while the remaining 40.25 bits are used as trail, synchronization and guard bits. In order to allow for the simultaneous two way conversation among users of the system, GSM implements FDD.

1.3 Code Division Multiple Access (CDMA)

Unlike FDMA and TDMA systems, a CDMA system offers a certain level of security. This is achieved by spreading the spectrum of the message beyond its minimum required transmission bandwidth. Therefore, the CDMA system is not bandwidth efficient for a single user in the system. However, a CDMA system becomes bandwidth efficient in a multi-user environment as the available bandwidth can be shared among the users. There are two main kinds of CDMA, that is, multi-user spread spectrum communication systems [3]. These are called frequency hopped multiple access (FHMA) and the direct sequence code division multiple access (DS-CDMA) systems.

1.3.1 Frequency Hopped Multiple Access (FHMA)

In an FHMA system a particular user is constantly assigned different frequency bands during the duration of the transmission, as illustrated for a 3 user system in Figure 1.5 [6].

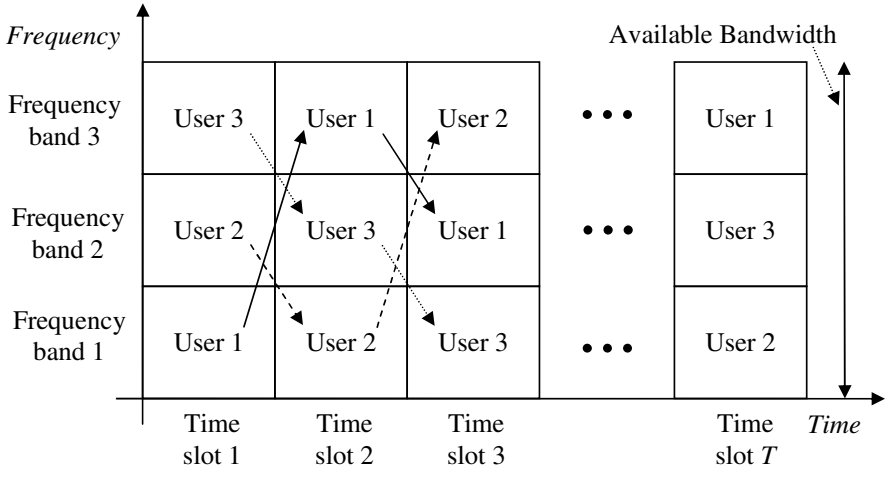


Fig. 1.5 A possible frequency hopping pattern within a 3 user FHMA system

It can be observed from Figure 1.5 that a particular user is assigned a particular frequency band for a fixed amount of time, before being allocated a different frequency band. For instance, at the end of time slot 1, user 1 hops from the frequency band 1 into frequency band 3, while at the end of time slot 2 it hops from the frequency band 3 into the frequency band 2. The order in which the user is "hopped" across the frequency bands is determined by a pseudo random binary sequence (PRBS) [6]. Therefore, for the successful communication of the message across the channel, both, the transmitting and receiving parties, must have the knowledge of the particular PRBS used. This pseudo randomness of the hopping pattern provides for the increased security of transmission, as one must know the exact initial conditions of the particular PRBS to accurately reproduce it.

Therefore, a FHMA system can be viewed as a hybrid combination of FDMA and TDMA systems [6]. Like a FDMA system, FHMA system has frequency bands. However, unlike a FDMA system, FHMA system does not continuously transmit the information of one user using a single frequency band, but spreads it all over the available bandwidth by hopping between frequency bands.

1.3.2 Direct Sequence Code Division Multiple Access (DS-CDMA)

In a DS-CDMA system [2] a binary message is multiplied by a particular signal whose bandwidth is a few magnitudes larger than the bandwidth of a message. This process of multiplication spreads the spectrum of the binary message. Therefore, the multiplying signal is termed the spreading signal. The spreading signal is in general of a pseudo random nature, such as the PRBS. The PRBS time series is generated by means of a feedback shift register, as illustrated in Figure 1.6. At the start of operation the flip flops of the shift register are initialized to some arbitrary

values (initial conditions). At every clock cycle a value in each of the flip flops is shifted to the right with the first flip flop being assigned a new value generated by the logic unit. In order to generate a pseudo random sequence, the feedbacks into the logic unit must be precisely chosen for a given shift register length [6].

Thus, due to the pseudo random nature of PRBS time series, spreading introduces security into the system. Each user in the system possesses its own distinct PRBS code which is approximately orthogonal to every other PRBS code used to spread other message signals. The fundamental property of the PRBS sequences generated by the generator of Figure 1.6 is that they are periodic with a maximum

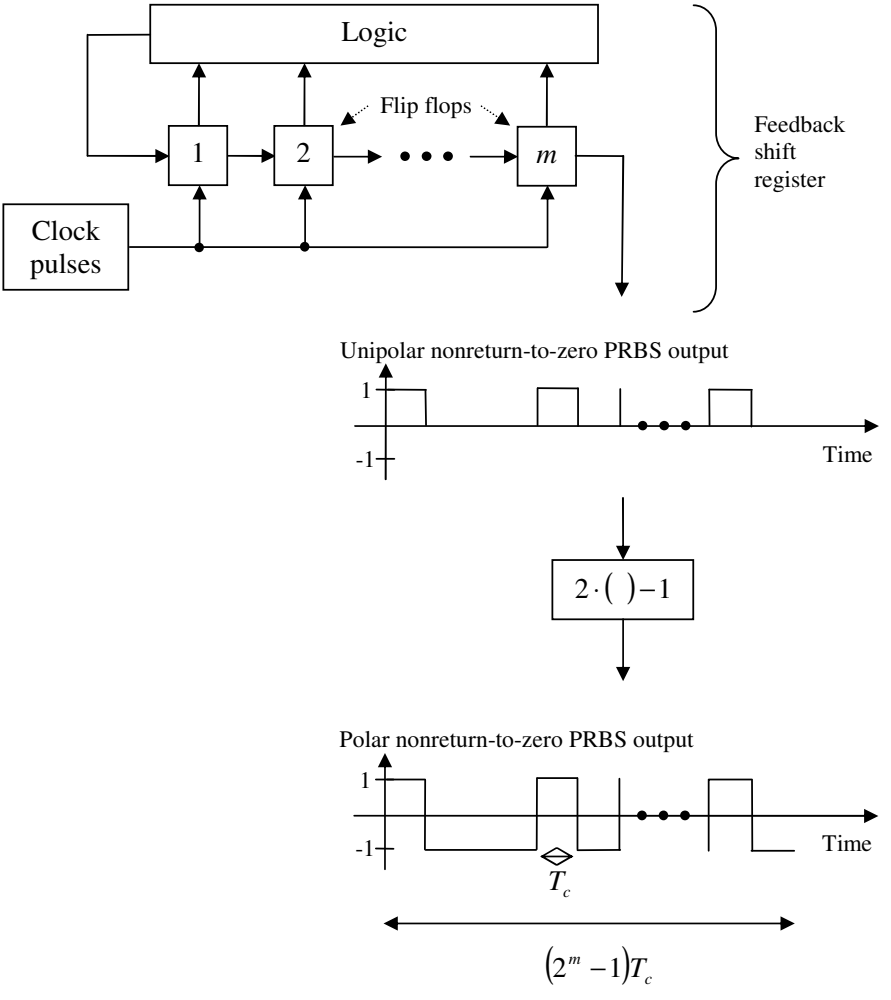


Fig. 1.6 The pseudo random binary sequence (PRBS) generator

period of $2^m - 1$, where m denotes the number of flip-flops in the shift register. In any given period of the maximum length sequence the number of ones always exceeds the number of zeros by one. A single point of the PRBS sequence is termed a chip and its period is denoted by T_c. Therefore, a period of a maximum length sequence is equal to $(2^m - 1)T_c$ seconds.

The approximately orthogonal nature of the spreading PRBS codes is demonstrated by low cross correlation of Figure 1.7a. The autocorrelation function of the PRBS is presented in Figure 1.7b showing the dominant peak [6]. The length of the PRBS used to produce Figures 1.7a and 1.7b is equal to 511 points (chips). In Figures 1.7a and 1.7b t denotes the time delay. Note that the correlation functions have been normalized to the peak of the autocorrelation function, that is, to $2^m - 1$.

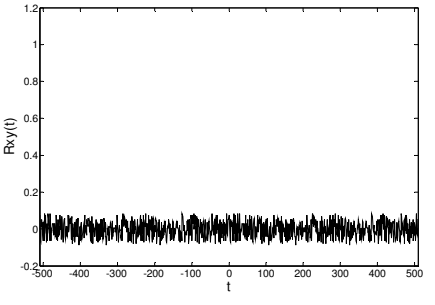


Fig. 1.7a Cross-correlation of PRBS time series

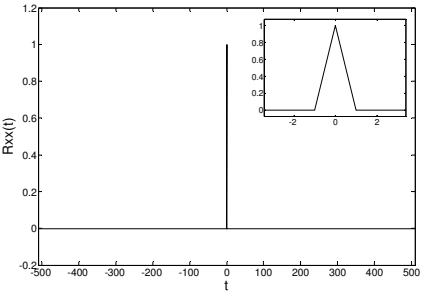


Fig. 1.7b Autocorrelation of PRBS time series. The close up is shown in the top right hand corner

The orthogonal property of the spreading signals allows the receiver to decode the transmitted message of each of the users by correlating the received signal by the local copies of the spreading signals. Figure 1.8 shows the block diagram of a DS-CDMA communication system. Within a DS-CDMA system different modulation architectures can be implemented, such as the binary phase shift keying (BPSK) [2] and quadrature phase shift keying (QPSK) [2] architectures. In Figure 1.8, the most basic architecture, namely BPSK, is shown.

In Figure 1.8, $x(t)$ denotes the spreading signals and A their amplitudes. The spreading signals are multiplied by the binary message signals $m(t)$ and their products then summed up to produce the signal $c(t)$ which is transmitted through the channel. The received signal $r(t)$ is correlated with the punctual despreading codes. The process of correlation involves despreading, that is multiplying, the received signal by the locally generated replica of the spreading sequence at the receiver and then integrating the product over the bit period. Provided that the power of the noise in the system is comparatively low to the power of the signal, the correlation value produced at the output of each correlator is positive if the bit 1 is transmitted and negative if the bit 0 is transmitted. A way of synchronizing the

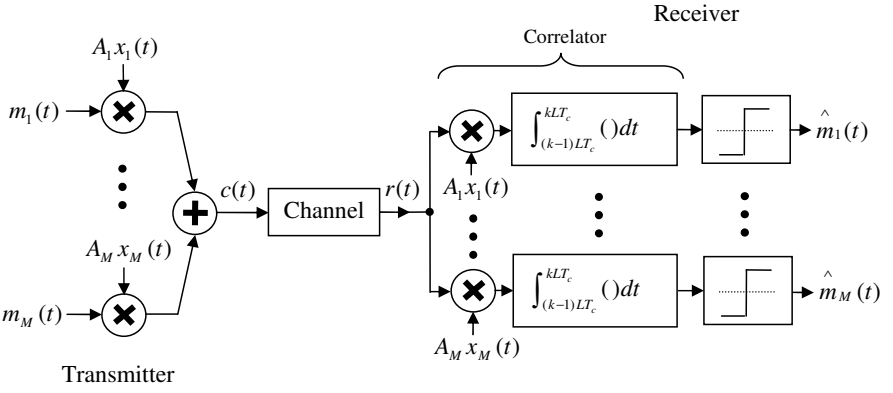


Fig. 1.8 A DS-CDMA communication system, where the bit duration $T_b = LT_c$ and L denotes the spreading factor, that is, the number of chips representing a single bit

spreading and despreading sequences is through the process of acquisition and tracking [7,8,2,9-16]. The code acquisition [7,2,9,10,13,15,16], or the initial synchronization phase, involves determining the time offset amidst the incoming signal and the basis function copy at the receiver to within a specified range known as the pull-in region of the tracking loop [7,8,2,11,12,14]. Upon the successful completion of the acquisition phase, the code tracking phase starts with the fine alignment followed by the process of maintaining synchronization of the two signals. This type of synchronization, where the incoming and the local sequences are synchronized, is known as the sequence synchronization and is the primary subject of this book. Sequence synchronization may be achieved using techniques other than acquisition and tracking, as shown in the subsequent chapters. Furthermore, two other types of synchronization are required within a system such as that of Figure 1.8. These are known as carrier and clock synchronization and are briefly discussed in the last two sections of this chapter.

An example of a system which implements DS-CDMA is the IS-95 system [2]. In order to achieve further spreading, the IS-95 system implements the so called Walsh functions which are perfectly orthogonal to each other. The IS-95 system implements both the BPSK and QPSK modulation architectures. The bit duration can be either 0.1042 ms or 0.0694 ms. In order to allow for the simultaneous two way conversation among users of the system, IS-95 implements FDD.

1.4 The Hybrid Systems

In this section two hybrid spread spectrum multiple access techniques are described. These are the hybrid FDMA/CDMA (FD/CDMA) system and the hybrid TDMA/CDMA (TD/CDMA) system.

1.4.1 The Hybrid FDMA/CDMA (FD/CDMA) System

In a FD/CDMA system the wide bandwidth of a DS-CDMA system is divided into a number of narrower bandwidths, with each of the narrower bandwidths implementing the DS-CDMA technique. The signals of the narrower bandwidths are transmitted in one and only one sub-spectrum. All of the narrow bandwidths are assumed equal [17], as shown in Figure 1.9.

The advantage of the FD/CDMA hybrid system over a wideband DS-CDMA system is that the required bandwidth does not need to be contiguous and different users can be assigned different narrow bandwidths.

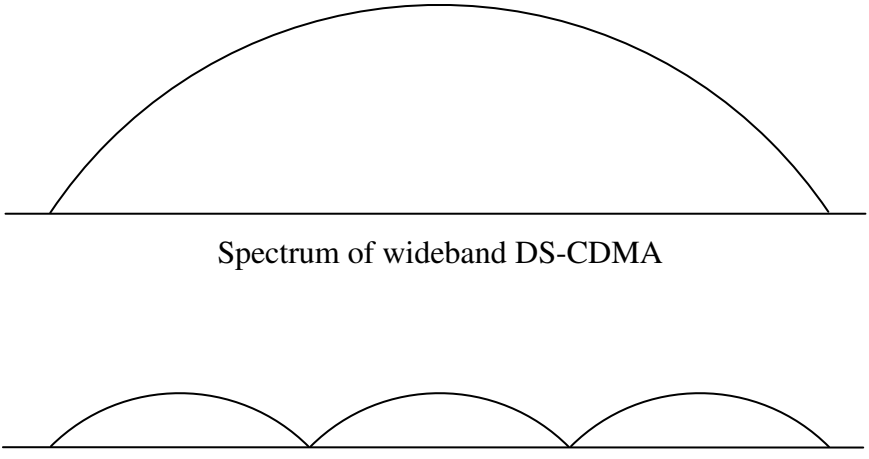


Fig. 1.9 Schematic of a spectrum of wideband DS-CDMA system compared to a spectrum of a frequency divided narrowband FD/CDMA hybrid system

1.4.2 The Hybrid TDMA/CDMA (TD/CDMA) System

In a TDMA/CDMA hybrid system the data of each of the users is spread in a DS-CDMA fashion, however, the signals are then delayed in time instead of being immediately summed. In this way the interuser interference is eliminated or minimized [18], as compared to a DS-CDMA scheme, as the users' data is transmitted in different time slots. The general block diagram of a hybrid TDMA/CDMA system is shown in Figure 1.10. The delay units of Figure 1.10 have a similar function to that of the multiplexing switch of Figure 1.3 in that they both separate user signals in time to avoid interuser interference. A number of different hybrid systems combining the advantages of TDMA and CDMA schemes exist [19-21]. An example of a system which uses the TD/CDMA hybrid, while implementing time division duplexing (TDD), is the Universal Mobile Telecommunications System (UMTS) [18].

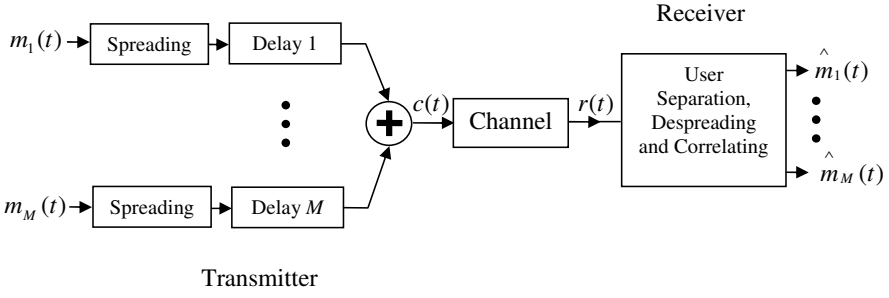


Fig. 1.10 A simplified block diagram showing a TD/CDMA hybrid system. The message signals $m(t)$ are transmitted across the channel and are received in the form of $\hat{m}(t)$.

1.5 The Channel

In every communications channel noise is always present. Furthermore, other disturbances which cause the transmitted signal to change, such as fading, may also be present. In this section, additive white Gaussian noise (AWGN) and Rayleigh flat fading are introduced. These two disturbances are used in subsequent chapters to model the channel and evaluate the performance of the communication systems.

1.5.1 Additive White Gaussian Noise (AWGN)

In most cases, AWGN is used to evaluate the performance of a communication system in a noisy channel. This is an idealized form of noise where the term additive refers to the fact that noise is added directly onto the transmitted signal. The term white, denotes the fact that this type of noise is of theoretically infinite bandwidth, with power spectral density of:

$$S_W(f) = \frac{N_o}{2}, \tag{1.5.1}$$

as illustrated in Figure 1.11a. The dimension of the parameter N_o of equation 1.5.1 is watts per Hertz. N_o is usually referenced to the input stage of the receiver, and is expressed as:

$$N_o = kT_e, \tag{1.5.2}$$

where k is Boltzmann's constant and T_e is the equivalent noise temperature of the receiver.

The equivalent noise temperature of a system is defined as '*the temperature at which a noisy resistor has to be maintained such that, by connecting the resistor*

to the input of a noiseless version of the system, it produces the same available noise power at the output of the system as that produced by all the sources of noise in the actual system' [6]. Finally, the term Gaussian refers to the fact that the noise time series is of Gaussian distribution, as illustrated in Figure 1.12. Noting that the autocorrelation function is obtained by taking the inverse Fourier transform of the power spectral density, it is readily verifiable that the autocorrelation function of AWGN is [6]:

$$R_W(t) = \frac{N_o}{2}\delta(t) \tag{1.5.3}$$

where t is a time delay and $\delta(t)$ denotes the impulse function.

The autocorrelation function of AWNG is graphically illustrated in Figure 1.11b. It can be observed from Figure 1.11b that the autocorrelation function of AWGN is an impulse function weighed by the factor $N_o/2$. This implies that any two different samples of white noise are uncorrelated regardless of how close in time they are taken [6].

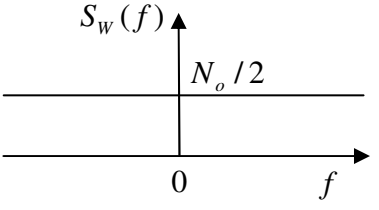


Fig. 1.11a Power spectral density of AWGN

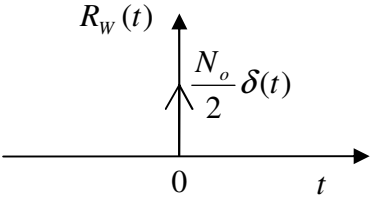


Fig. 1.11b Autocorrelation function of AWGN

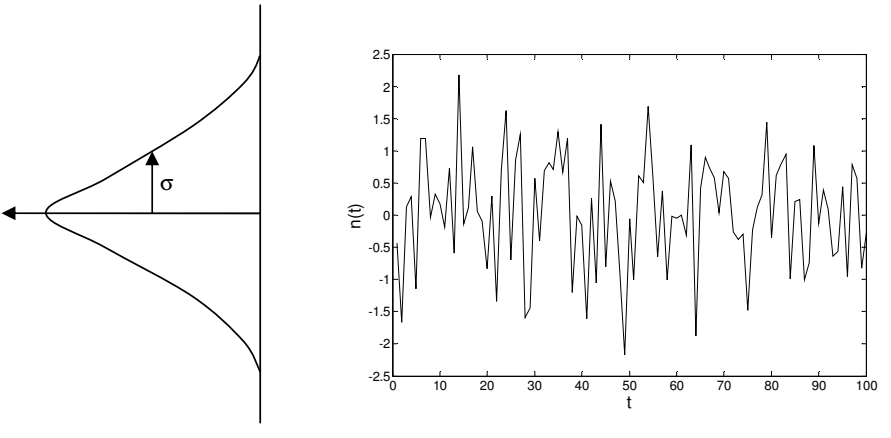


Fig. 1.12 The Gaussian distribution of AWGN, where σ denotes the standard deviation

There are different methods which can be used to model AWGN, such as the Box-Muller method [22,23], as well as a number of other methods [23].

1.5.2 Rayleigh Flat Fading

Different mechanisms of fading can be present in a mobile channel, such as the long term, short term, frequency selective, time selective, and flat fading mechanism [2]. In a flat fading channel [24-27] there are no dominant fading mechanisms, but fading occurs from the random channel fluctuations. In order to evaluate the performance of the communication systems in a fading environment the Clarke and Gans flat fading model has been developed. The method of implementing this model has been outlined in [24-26] and used to simulate a multipath Rayleigh fading channel. This method is now briefly described. The technique used to obtain the simulation of multipath propagation is achieved by appropriately shaping the two independent Gaussian low-pass noise sources [24,26]. The shaping filter used is given by equation 1.5.4 [24]:

$$S(f) = \begin{cases} \dfrac{P_r}{\pi f_m \sqrt{1 - \left(\dfrac{f - f_c}{f_m} \right)^2}} & |f - f_c| \le f_m \\ 0 & otherwise \end{cases} \tag{1.5.4}$$

In equation 1.5.4, f_m denotes the maximum Doppler frequency shift caused by the movement of the receiver with the respect to the transmitter, and vice versa. The f_c denotes the carrier frequency and the P_r denotes the average received power of the Rayleigh fading envelope. The maximum Doppler frequency shift, f_m, depends on the speed of the receiver, *v*, relative to the transmitter, as well as the carrier frequency f_c. This relation is given by equation 1.5.5:

$$f_m = \frac{v f_c}{c} \tag{1.5.5}$$

where *c* denotes the speed of light.

Upon shaping the random Gaussian noise sources the inverse fast Fourier transform (IFFT) is performed on each of the shaped waveforms. The Rayleigh fading envelope is then obtained from the two band limited noise sources, as shown in equation 1.5.6 [24]:

$$r_E(t) = \sqrt{\left|r_I(t)\right|^2 + \left|r_Q(t)\right|^2} \tag{1.5.6}$$

In equation 1.5.6, $r_I(t)$ and $r_Q(t)$ denote the in phase and quadrature components of the Rayleigh envelope $r_E(t)$.

In Figure 1.13, the algorithm for the frequency domain implementation of the Rayleigh fading envelope at baseband is outlined. It should be noted that the Fourier transform of the Gaussian noise does not exist mathematically and thus most often noise and fading generators are modelled in the time domain. However, it is also possible by way of [24] to model fading using a frequency domain represenatation. The steps used to implement the simulator are now briefly described [24]:

(1) Specify the number of points over which the fading envelope, *N*, is to be produced.
(2) According to a given *v* and f_c, calculate f_m, and thus determine the frequency spacing between adjacent spectral lines as $\Delta f = 2f_m/(N-1)$.
(3) Generate the frequency vector $f = -f_m : \Delta f : f_m$.
(4) Produce the positive frequency components of the complex Gaussian line spectra by generating a set of *N*/2 complex random numbers with Gaussian distribution. Store those in a vector g_{p1}. Conjugate the vector g_{p1} and flip the conjugated vector left to right to obtain a vector of negative frequency components g_{n1}. Finally create the vector $g_1 = [g_{n1}, g_{p1}]$ containing the frequency components of the complex Gaussian line spectra.
(5) Generate the second set of *N*/2 complex random numbers with Gaussian distribution. Repeat step 4 to obtain the output of the second Complex Gaussian noise source: $g_2 = [g_{n2}, g_{p2}]$, of Figure 1.13.
(6) Generate the fading spectrum $S(f)$ of size *N*, using the components of the vector *f*.
(7) Take the square root of $S(f)$ and multiply the square rooted value by each of the complex Gaussian line spectra $g_1(f)$ and $g_2(f)$.
(8) Take the IFFT of both products.
(9) Introduce a 90 degree phase shift into the second product. The two resulting time domain signals are the in phase, $r_I(t)$, and quadrature, $r_Q(t)$, components of the Rayleigh fading signal $r_E(t)$.

(10) Obtain the magnitude of $r_I(t)$ and $r_Q(t)$ signals, square the magnitudes, and add them together. Take the root of the sum to obtain the Rayleigh fading envelope $r_E(t)$.

(11) Normalize the resulting Rayleigh envelope to $\sqrt{r_E^{\,2}}$ [25]. This results in the envelope of the average power of 1W. Finally adjust the average power to the required average power P_r, by multiplying $r_E(t)$ by $\sqrt{P_r}$. The final result is the Rayleigh fading envelope, $r_n(t)$.

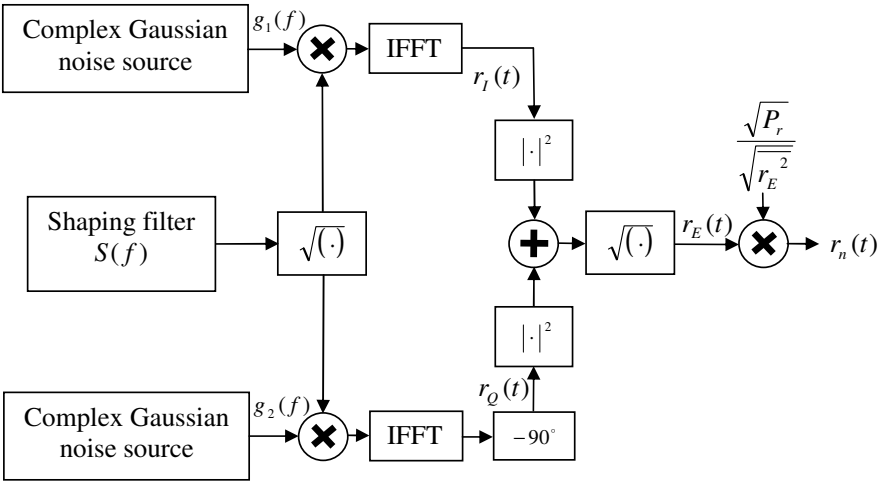


Fig. 1.13 The baseband implementation of a Rayleigh fading simulator

The impact of flat fading on the transmitted signal is determined by simply multiplying the transmitted signal by the fading envelope [24].

1.6 The System Performance Analysis Using the Bit Error Rate (BER)

In order to analyse the performance of the communication systems an evaluation of the average probability of symbol error, or the bit error rate (BER), is often used. In this section, the concept of BER is introduced and the method used to obtain it described.

The average probability of symbol error is defined as 'the probability that the reconstructed symbol at the receiver output differs from the transmitted binary symbol, on the average' [6]. The bit error rate of a system is obtained by counting the number of incorrectly received bits and dividing this number by the total

number of bits transmitted. By incorrectly received bits it is meant that bit 1 was received when bit 0 should have been received and vice versa. Therefore, the more incorrectly received bits, the higher the bit error rate. When measuring the bit error rate, it is assumed throughout the book that all the bits in the original binary message are of equal importance.

In every communication system it is the aim of a designer to minimise the bit error rate as much as possible. The main causes of incorrectly received bits are the channel disturbances, such as noise and fading. Therefore, the bit error rate can be reduced, and thus the system optimized, by minimizing the effects of the channel disturbances on the transmitted signal. A way of presenting the bit error rate is to plot it against the signal energy to noise power spectral density ratio (E_b / N_o). A typical shape of the bit error rate curve, when plotted against the E_b / N_o ratio, resembles a "waterfall" curve [6], as illustrated in Figure 1.14.

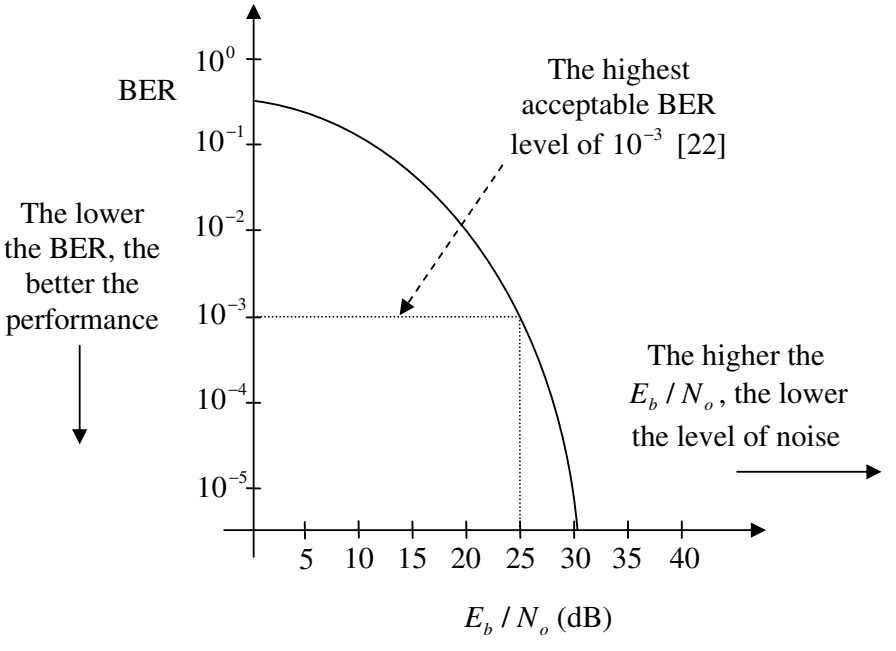


Fig. 1.14 A typical shape of a BER curve of a communication system plotted against the E_b / N_o ratio

It can be observed from Figure 1.14 that the higher the E_b / N_o is, the lower the BER of a system. When a sufficiently low E_b / N_o level is reached, the receiver can no longer successfully decode the message, resulting in the BER level of 0.5. For a system to have a satisfactory performance it is often required that the

BER level not exceed 10^{-3} [28,29]. In the example in Figure 1.14, the BER level of 10^{-3} is reached when the E_b / N_o ratio is equal to 25 dB.

In order to demonstrate the BER evaluation of a communication system, the performance of the simplest form of a binary phase shift keying (BPSK) system, shown in Figure 1.15, is evaluated in noisy and Rayleigh fading channels.

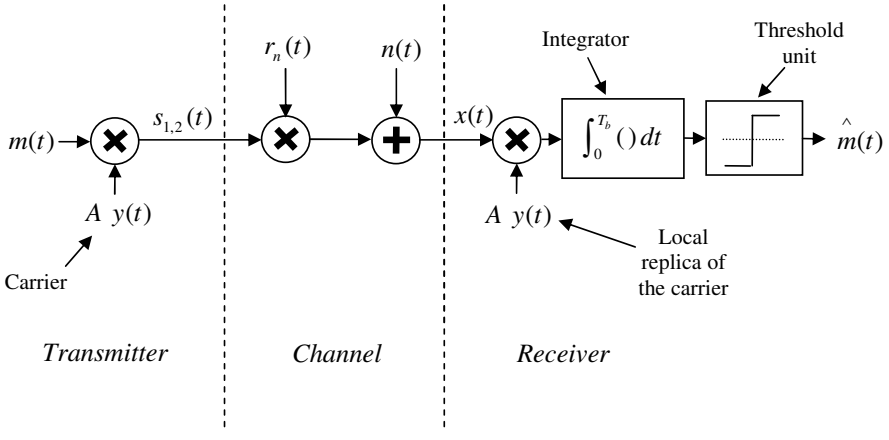


Fig. 1.15 A bandpass BPSK communication system in a Rayleigh fading and AWGN channel, where: $A = \sqrt{2E_b / T_b}$ and $y(t) = \cos(2\pi f_c t)$

In Figure 1.15, A represents the amplitude of the sinusoidal carrier $y(t)$. The sinusoidal carrier is of frequency much higher than that of the message signal and is used to up-convert the message signal to a higher frequency for the transmission across the channel. Depending on the polarity of the binary message symbol $m(t)$, which takes on the values of 1 or -1, the sinusoidal carrier is modulated to produce two possible outcomes:

$$s_1(t) = \sqrt{\frac{2E_b}{T_b}} \cos(2\pi f_c t) \tag{1.6.1a}$$

$$s_2(t) = -\sqrt{\frac{2E_b}{T_b}} \cos(2\pi f_c t) \tag{1.6.1b}$$

where E_b and T_b denote the energy and time duration of one bit, respectively. f_c denotes the carrier frequency.

Note that equations 1.6.1a and 1.6.1b are orthogonal to each other. It should be observed from equations 1.6.1a and 1.6.1b that there is only one basis function of unit energy, expressed by equation 1.6.2:

$$\phi_1(t) = \sqrt{\frac{2}{T_b}} \cos(2\pi f_c t) \tag{1.6.2}$$

In terms of equation 1.6.2, equations 1.6.1a and 1.6.1b can be expressed in the form of equations 1.6.3a and 1.6.3b:

$$s_1(t) = \sqrt{E_b}\phi_1(t), \qquad 0 \le t < T_b \tag{1.6.3a}$$

$$s_2(t) = -\sqrt{E_b}\phi_1(t), \qquad 0 \le t < T_b \tag{1.6.3b}$$

In this one-dimensional symbol space, shown in Figure 1.16, the coordinates of the message points are represented by equations 1.6.4a and 1.6.4b:

$$s_{11} = \int_0^{T_b} s_1(t)\phi_1(t)\,dt = +\sqrt{E_b} \tag{1.6.4a}$$

$$s_{21} = \int_0^{T_b} s_2(t)\phi_1(t)\,dt = -\sqrt{E_b} \tag{1.6.4b}$$

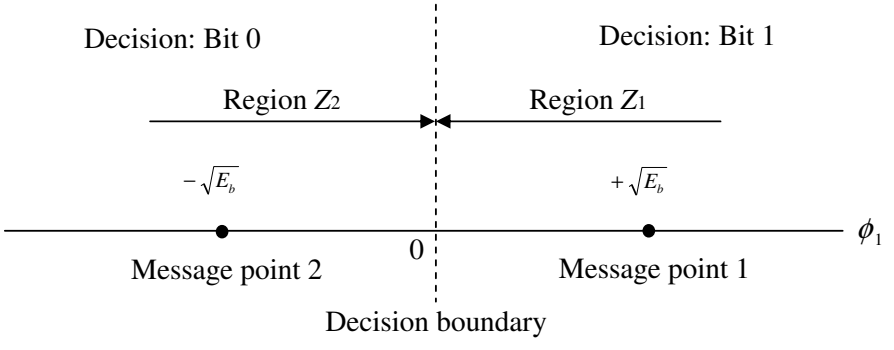


Fig. 1.16 The symbol space of the system of Figure 1.15

If the received signal point falls in the region Z_2 of Figure 1.16, the decision is made that bit 0 was sent. Alternatively, the decision is made that bit 1 was sent if the received signal point falls in the region Z_1. If, however, bit 0 is sent but the received signal point falls in the region Z_1, due to the noise in the system, the receiver will incorrectly decide in favour of bit 1, thus causing an error of first kind.

The incorrect decision of second kind is made if bit 1 is sent but the received signal point falls in the region Z_2. In order to optimize the performance of the system in the AWGN channel, it is important to separate the message points as far apart as possible in their symbol space. In case of the system of Figure 1.15, the decision boundary, or threshold, is at zero. It is often the case, however, that the threshold is not at zero, and furthermore, is not fixed, but varies with the E_b / N_o ratio [30,6].

The mathematical procedure of obtaining the theoretical BER curve for the system of Figure 1.15, but without fading in the channel, is now briefly demonstrated [6]. The probability that the error of the first kind is made, is calculated in the following manner. Consider the decision region associated with bit 1 described by

$$Z_1 : \ 0 < x_1 < \infty$$

where x_1 is related to the received signal $x(t)$ by equation 6:

$$x_1 = \int_0^{T_b} x(t)\,\phi_1(t)\,dt \tag{1.6.5}$$

The conditional probability density function of random variable X_1, given that bit 0 was transmitted, is defined by equation 1.6.6:

$$\begin{aligned} f_{X_1}(x_1 \mid 0) &= \frac{1}{\sqrt{\pi N_o}} \exp\left[-\frac{1}{N_o}(x_1 - s_{21})^2 \right] \\ &= \frac{1}{\sqrt{\pi N_o}} \exp\left[-\frac{1}{N_o}\left(x_1 + \sqrt{E_b}\right)^2 \right] \end{aligned} \tag{1.6.6}$$

The conditional probability that the receiver decides in favour of bit 1, given that bit 0 was transmitted, is expressed by equation 1.6.7:

$$\begin{aligned} p_{10} &= \int_0^{\infty} f_{X_1}(x_1 \mid 0)\,dx_1 \\ &= \frac{1}{\sqrt{\pi N_o}} \int_0^{\infty} \exp\left[-\frac{1}{N_o}\left(x_1 + \sqrt{E_b}\right)^2 \right] dx_1 \end{aligned} \tag{1.6.7}$$

Let the variable z be defined by equation 1.6.8:

$$z = \frac{1}{\sqrt{N_o}}\left(x_1 + \sqrt{E_b}\right) \tag{1.6.8}$$

Differentiating equation 1.6.8 with respect to x_1, and making x_1 the subject of the formula, equation 1.6.9 is obtained:

$$dx_1 = \sqrt{N_o}\, dz \tag{1.6.9}$$

Equation 1.6.7 can now be written in the compact form of equation 1.6.10 by changing the variable of integration from x_1 to z.

$$p_{10} = \frac{1}{\sqrt{\pi}} \int_{\sqrt{E_b / N_o}}^{\infty} \exp\left[- z^2\right] dz \tag{1.6.10}$$

Note the so-called 'complementary error function' defined by equation 1.6.11 [6]:

$$\operatorname{erfc}(u) = \frac{2}{\sqrt{\pi}} \int_{u}^{\infty} \exp(-z^2)\, dz \tag{1.6.11}$$

Equation 1.6.10 can now be put into the form of equation 1.6.11, and expressed by equation 1.6.12:

$$p_{10} = \frac{1}{2} \operatorname{erfc}\left(\sqrt{\frac{E_b}{N_o}} \right) \tag{1.6.12}$$

Due to the fact that the symbol space of Figure 1.16 is symmetrical about the origin, it follows that the expression for the incorrect decision of the second kind is also described by equation 1.6.12, as shown by equation 1.6.13:

$$p_{01} = \frac{1}{2} \operatorname{erfc}\left(\sqrt{\frac{E_b}{N_o}} \right) \tag{1.6.13}$$

Averaging the conditional probabilities p_{10} and p_{01}, equation 1.6.14 is obtained. Equation 1.6.14 represents the worst case probability of error, that is, the worst case bit error rate for coherent BPSK in an AWGN channel when perfect synchronization is assumed.

$$P_e = \frac{1}{2} \operatorname{erfc}\left(\sqrt{\frac{E_b}{N_o}} \right) \tag{1.6.14}$$

Furthermore, it is readily verifiable that in the Rayleigh fading channel, the theoretical expression for the bit error rate is given by equation 1.6.15 [7]:

$$BER = \overline{P_e} = \frac{1}{2}\left(1 - \sqrt{\frac{\gamma_o}{1+\gamma_o}}\right) \tag{1.6.15}$$

where $\gamma_o = E\{\alpha^2\} \cdot (E_b / N_o) = P_r \cdot (E_b / N_o)$ and α is a Rayleigh random variable [7].

The empirical and theoretical BER curves for the system of Figure 1.15, under the influence of AWGN and Rayleigh fading, are presented in Figure 1.17. The theoretical BER curves are obtained by evaluating equations 1.6.14 and 1.6.15. From Figure 1.17, one can see a very close match between the empirical and theoretical curves in the presence of AWGN alone, as well as in the AWGN and Rayleigh fading channel. This fact indicates that the AWGN and Rayleigh fading simulators work correctly. Note that the speed of the receiver with respect to the transmitter has been chosen to be $v = 55$ km/h, and the carrier frequency $f_c = 900$ MHz. Substituting these values into equation 1.5.5, it is readily verifiable that in this case the maximum Doppler frequency shift $f_m = 45.83$ Hz. It can be observed from Figure 1.17 that the highest acceptable BER level of 10^{-3} is reached at the E_b / N_o of approximately 7 dB for the system in the AWGN channel only and at 24 dB for the system in the Rayleigh fading and AWGN channel.

The system of Figure 1.15 has been analyzed at bandpass, meaning that the transmitted data has first been up-converted to a higher frequency using a sinusoidal carrier. It should be noted that the performance of the baseband systems, where carrier is not included, is equivalent to those of the bandpass systems. However the simulations performed at baseband are more economical on computing resources than simulations performed at bandpass [31]. Therefore, in most of the analysis in the following chapters, unless otherwise specified, systems will be analysed at baseband.

It is of crucial importance for the accurate retrieval of the bits transmitted at the receiver that the carrier at the transmitter and its replica at the receiver are synchronized. The standard techniques used to achieve carrier synchronization exist [32-34]. Therefore, in case of Figure 1.15, the synchronization among the carrier at the transmitter and its replica at the receiver has been assumed. In addition to the carrier synchronization, clock synchronization, also known as timing/clock recovery, must be achieved and maintained [32-34]. Clock synchronization involves adjusting the clock of the receiver, which controls the integrator and the sampling of the threshold unit of Figure 1.15, to the clock of the transmitter. In the following section, the effect of inaccurate synchronization is investigated at baseband and its adverse effect on the BER curve demonstrated.

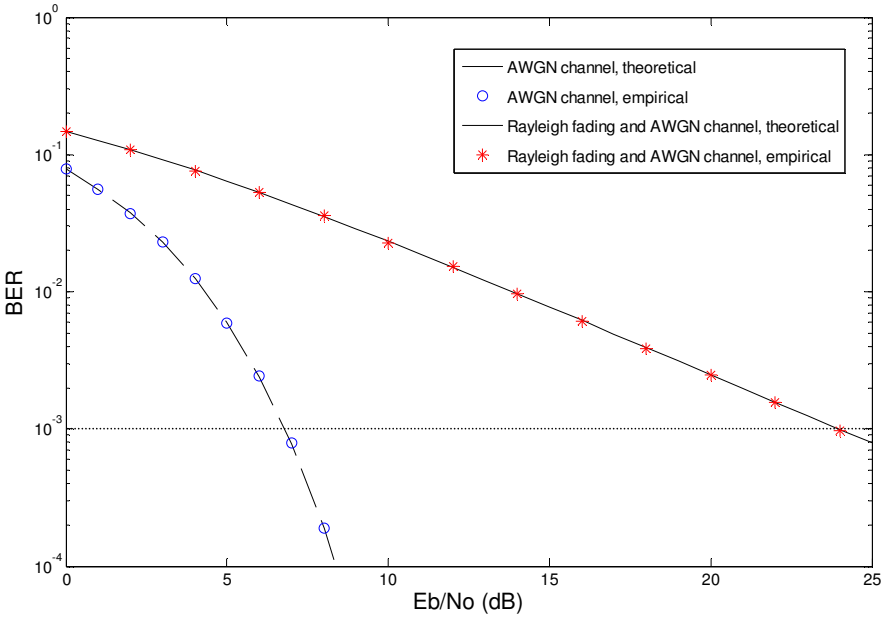


Fig. 1.17 The BPSK BER curves: (a) the dashed line is for the theoretical BPSK in AWGN channel only; (b) the open circles are for the empirical BPSK in AWGN channel only; (c) the solid line is for the theoretical BPSK in Rayleigh fading and AWGN channel; (d) the asterisks are for the empirical BPSK in Rayleigh fading and AWGN channel.

1.7 The Synchronization Problem

In this section, the effect of synchronization error on the bit error rate of a BPSK system is shown. The crucial importance of the accurate synchronization within a coherent communication system is thus demonstrated. A coherent communication system is a system which requires synchronization at the receiver in order to successfully decode the information transmitted. In contrast to coherent systems, non-coherent systems do not require synchronization at the receiver. However, these systems are not the topic of this book and will therefore not be considered any further.

The analysis is performed at baseband in an AWGN channel only. Figure 1.18 shows the equivalent system to the one of Figure 1.15 but at baseband and with no Rayleigh fading.

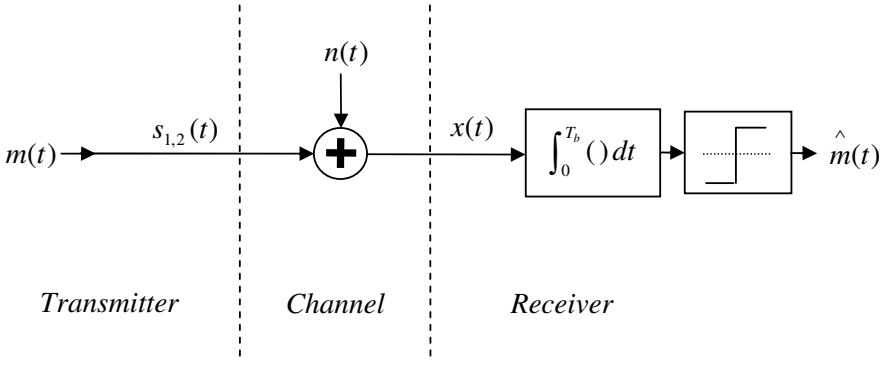


Fig. 1.18 A baseband BPSK communication system in an AWGN channel

With non-ideal synchronization, the worst scenario probability of error of the BPSK communication system of Figure 1.18 is expressed by equation 1.7.1. In equation 1.7.1, T_b is the bit period and τ is the signal time shift, that is, the offset due to the non-ideal synchronization.

$$P_e = \frac{1}{2} erfc\left(\frac{(T_b - 2\tau)}{T_b} \sqrt{\frac{E_b}{N_o}} \right) \tag{1.7.1}$$

where: $0 \le \tau < \frac{T_b}{2}$.

Equation 1.7.1 is plotted in Figure 1.19 for the time shifts of $\tau = 0$, $\tau = 1$, $\tau = 2$, $\tau = 3$ and $\tau = 4$ time units. The corresponding empirical curves are also plotted for comparison. In the case of Figure 1.19, the duration of one bit has been chosen to be 8 chips long, that is $T_b = nT_c = 8T_c$ seconds, where T_c is the time duration of a single chip.

It should be observed from Figure 1.19 that the BER curves degrade ever more significantly as the time delay τ increases. Finally, at the time delay τ equal to half of the bit duration, the bit error rate reaches its maximum value of 0.5 and remains there for any E_b / N_o. Therefore, it is most important to obtain, and maintain, synchronization within the system.

The mathematical procedure, similar to that of section 1.6, of obtaining equation 1.7.1 is now briefly demonstrated [6]. Assuming non-ideal synchronization, the coordinates of the message points are now represented by equations 1.7.2a and 1.7.2b:

$$s_{11} = \frac{(T_b - 2\tau)}{T_b}\int_0^{T_b} s_1(t)\,\phi_1(t)\,dt = +\frac{(T_b - 2\tau)}{T_b}\sqrt{E_b} \tag{1.7.2a}$$

$$s_{21} = \frac{(T_b - 2\tau)}{T_b}\int_0^{T_b} s_2(t)\,\phi_1(t)\,dt = -\frac{(T_b - 2\tau)}{T_b}\sqrt{E_b} \tag{1.7.2b}$$

where $s_1(t)$, $s_2(t)$ and $\phi_1(t)$ are as defined in equations 1.6.1a, 1.6.1b and 1.6.2, respectively.

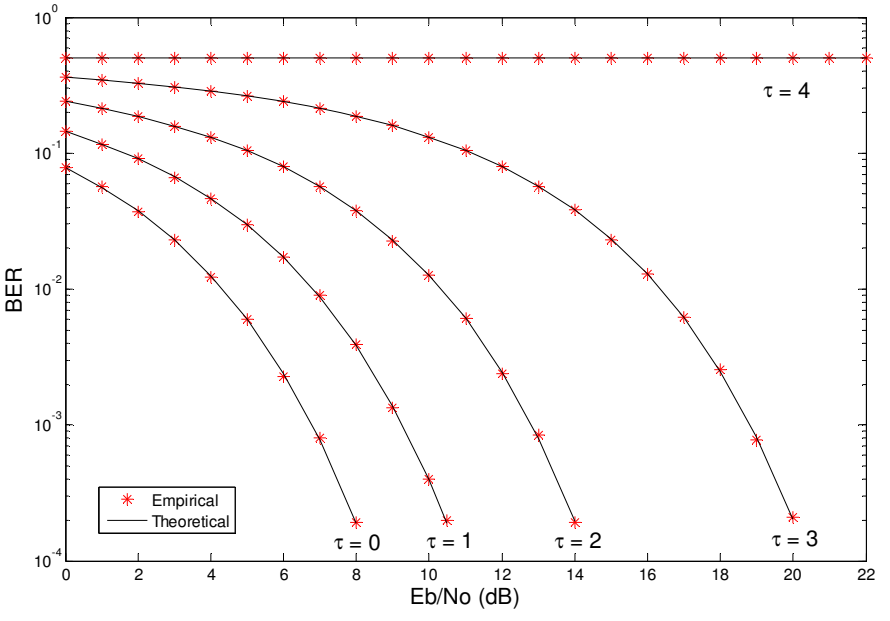


Fig. 1.19 Theoretical (solid line) and empirical (asterisks) BPSK BER curves for different synchronization errors in an AWGN channel

Note that when $\tau = 0$ equations 1.7.2a and 1.7.2b reduce to $+\sqrt{E_b}$ and $-\sqrt{E_b}$, respectively. The conditional probability density function of random variable X_1, given that bit 0 was transmitted, is now defined by equation 1.7.3:

$$f_{X_1}(x_1 \mid 0) = \frac{1}{\sqrt{\pi N_o}} \exp\left[-\frac{1}{N_o}(x_1 - s_{21})^2 \right]$$
$$= \frac{1}{\sqrt{\pi N_o}} \exp\left[-\frac{1}{N_o}\left(x_1 + \frac{(T_b - 2\tau)}{T_b}\sqrt{E_b} \right)^2 \right] \tag{1.7.3}$$

The conditional probability that the receiver decides in favour of bit 1, given that bit 0 was transmitted, is then expressed by equation 1.7.4:

$$p_{10} = \int_0^\infty f_{X_1}(x_1 \mid 0)\, dx_1$$
$$= \frac{1}{\sqrt{\pi N_o}} \int_0^\infty \exp\left[-\frac{1}{N_o}\left(x_1 + \frac{(T_b - 2\tau)}{T_b}\sqrt{E_b} \right)^2 \right] dx_1 \tag{1.7.4}$$

Let the variable z now be defined by equation 1.7.5:

$$z = \frac{1}{\sqrt{N_o}}\left(x_1 + \frac{(T_b - 2\tau)}{T_b}\sqrt{E_b} \right) \tag{1.7.5}$$

Differentiating equation 1.7.5 with respect to x_1, and again making x_1 the subject of the formula, equation 1.7.6 is obtained.

$$dx_1 = \sqrt{N_o}\, dz \tag{1.7.6}$$

Equation 1.7.4 can now be written in the compact form of equation 1.7.7 by changing the variable of integration from x_1 to z:

$$p_{10} = \frac{1}{\sqrt{\pi}} \int_{(T_b - 2\tau)\sqrt{E_b / N_o}/T_b}^\infty \exp\left[-z^2 \right] dz \tag{1.7.7}$$

Keeping in mind that the complementary error function is defined by equation 1.6.11 [6], it is then readily verifiable that the worst case bit error rate, when synchronization is not assumed, is expressed by equation 1.7.8:

$$P_e = \frac{1}{2}\operatorname{erfc}\left(\frac{(T_b - 2\tau)}{T_b}\sqrt{\frac{E_b}{N_o}} \right) \tag{1.7.8}$$

The existence of the factor $(T_b - 2\tau)/T_b$ of equations 1.7.2a and 1.7.2b is now explained by considering, for simplicity, the baseband case of Figure 1.19. Assuming ideal synchronization, the integrator at the receiver, sums up along a single bit as shown in Figure 1.20, case 1. In case 1, the integration result (sum) is therefore $+A$. However in case 2, when the receiver is out of synchronization, the sum is $+\frac{3}{4}A$. Therefore, the shift of one discrete point results in the reduction of a bit by 25 %. Similarly, a shift of two discrete points results in the bit reduction of 50 %. This behaviour is represented by the term $(T_b - 2\tau)/T_b$ of equations 1.7.2a and 1.7.2b. It has thus been demonstrated that the separation of symbols in their symbol space, when $\tau \neq 0$, is reduced from its full potential as compared to the situation when $\tau = 0$ and $(T_b - 2\tau)/T_b = 1$. The scenario of Figure 1.20 is the worst case as every new bit transmitted has been assumed to be different from the one preceding it, so that the bits follow the pattern: [0 1 0 1 0 1 0…]. In this case equations 1.7.2a and 1.7.2b strictly hold. However, had the bit pattern involved the stream of bits where the new bit can be the same as the one preceding it, equations 1.7.2a and 1.7.2b and thus equation 1.7.1 (1.7.8), would not be accurate.

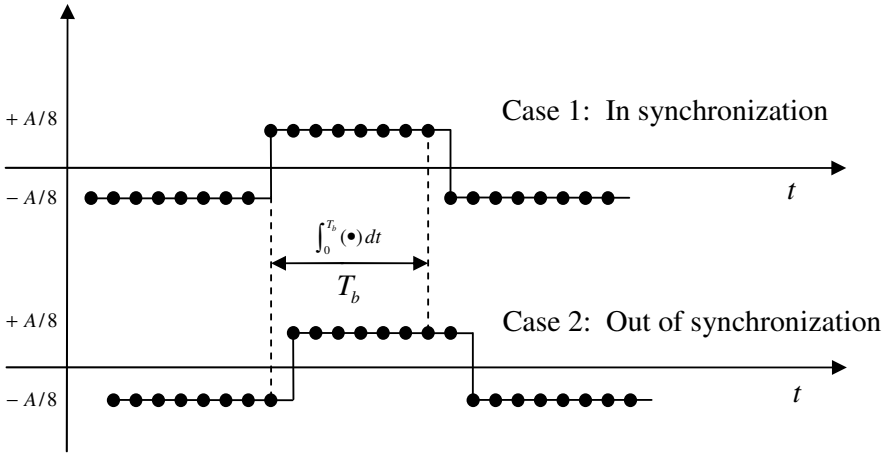


Fig. 1.20 The 'in' synchronization and 'out of' synchronization cases for the baseband BPSK communication system of Figure 1.18

The one-dimensional symbol space, with the synchronization factor $(T_b - 2\tau)/T_b$, is shown in Figure 1.21. Clearly, the symbol space is reduced for any value of τ that is greater than 0, thus causing the degradation in the bit error rate performance.

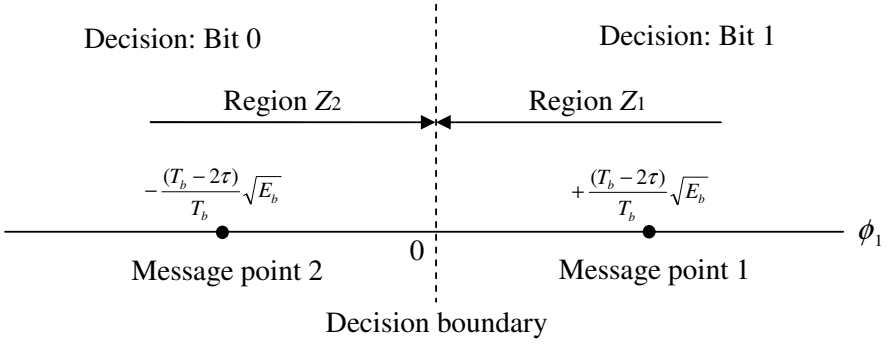


Fig. 1.21 The symbol space of the system of Figure 1.18 with the synchronization error factor: $(T_b - 2\tau)/T_b$

The three main types of synchronization introduced in this chapter, namely clock, carrier and sequence synchronization, are summarised within a general structure of a digital communication system of Figure 1.22. The clock and carrier synchronization techniques have been extensively studied [32-34] and are always assumed within this book. The motivation of the book is to investigate the sequence synchronization properties of chaotic systems and their application to single and multiple-access secure communications. The inherent properties of chaotic systems, discussed in the next chapter, make them of prime interest in secure communications. However, in order to implement chaotic systems within coherent communication systems, one must be able to synchronize them.

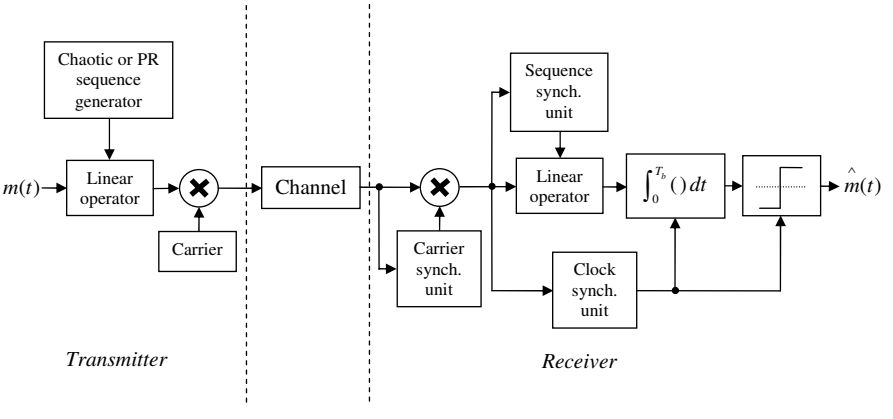


Fig. 1.22 General structure of a digital communication system showing three different types of synchronization. PR stands for pseudo random. The 'Linear operator' denotes either an addition or multiplication operation.

1.8 Conclusion and Book Organization

In this chapter, the three main categories of the multi-user (multiple access) mobile communication systems, namely FDMA, TDMA and CDMA, as well as some of their hybrids, have been introduced. Following this, the disturbances encountered within the physical transmission channel, namely the AWGN and the Rayleigh fading have been presented. Furthermore, the concept of the BER, which is used to measure the effects of the channel imperfections on the transmitted signal, has been described. Finally, the effect of synchronization error on the BER performance has been demonstrated.

The remainder of the book is organized in the following manner. In chapter 2, chaotic signals and their synchronization methods within secure communication systems are introduced. In chapters 3-5 and 7 the concept of synchronization within chaotic systems is studied and the novel methods of achieving it proposed. In particular, chapters 3 and 4 investigate the synchronization of flows and maps, respectively, using tools from nonlinear control theory and propose novel methods of achieving synchronization. In chapter 5, a novel mathematical analysis for predicting master-slave synchronization of chaotic systems is proposed and demonstrated on three different systems. Chapters 6-9 investigate synchronization of chaotic signals within the single and multiple access chaotic communication systems and evaluate their performance in terms of BER. A number of novel chaotic communication systems based on the principles of synchronization of chapters 3-5 and 7, are proposed in chapters 6-9. In particular, in chapter 6 single user systems based on the synchronization techniques of chapters 3-5 are proposed whereas in chapter 9 these are extended to TDM multiuser systems. In contrast to this, in chapter 7, the traditional DS-CDMA synchronization technique is implemented within the multi-user DS-CDMA chaotic communication scheme. In addition, chapter 8 proposes a chaos based TDM multiuser system based on the DS-CDMA synchronization technique. Furthermore, chapter 10 proposes techniques for the optimization of security within chaotic communication systems. In chapter 11, the conclusions and the future directions are outlined. Finally, the methods of denoising chaotic communication systems and thus improving their BER performance are proposed and investigated in the appendix.

References

[1] Wittman, J.H.: Categorization of Multiple-Access/Random-Access Modulation Techniques. IEEE Transactions on Communications Technology 15(5), 724–725 (1967)

[2] Lee, J.S., Miller, L.E.: CDMA Systems Engineering Handbook, pp. 18–837. Artech House Publishers, Boston (1998)

[3] Rappaport, T.S.: Wireless Communications Principles and Practice, 2nd edn., pp. 447–461. Prentice Hall, Inc., Upper Saddle River (2002)

[4] Carlson, A.B.: Communication Systems An Introduction to Signals and Noise in Electrical Communication, 3rd edn., pp. 363–365. McGraw-Hill Book Company, New York (1986)

[5] Hanzo, L., Stefanov, J.: Global System of Mobile Communications – known as GSM. In: Steele, R., Hanzo, L. (eds.) Mobile Radio Communications Second and Third Generation Cellular and WATM Systems, 2nd edn., pp. 661–775. Wiley, West Sussex (1999)
[6] Haykin, S.: Communication systems, 4th edn., pp. 61–514. Wiley, New York (2001)
[7] Peterson, R.L., Ziemer, R.E., Borth, D.E.: Introduction to Spread Spectrum Communications, pp. 149–495. Prentice Hall, Inc., Upper Saddle River (1995)
[8] Ziemer, R.E., Peterson, R.L.: Introduction to Digital Communication, 2nd edn., pp. 611–615. Prentice Hall, Inc., Upper Saddle River (2001)
[9] Polydoros, A., Weber, C.L.: A Unified Approach to Serial Search Spread-Spectrum Code Acquisition – Part I: General Theory. IEEE Transactions on Communications Com-32(5), 542–549 (1984)
[10] Polydoros, A., Weber, C.L.: A Unified Approach to Serial Search Spread-Spectrum Code Acquisition – Part II: A Matched – Filter Receiver. IEEE Transactions on Communications Com-32(5), 550–560 (1984)
[11] Hurd, W.J., Anderson, T.O.: Digital Transition Tracking Symbol Synchronizer for LOW SNR Coded Systems. IEEE Transactions on Communications Technology COM-18(2), 141–147 (1970)
[12] Spilker, J.J., Magill, D.T.: The Delay-Lock Discriminator – An Optimum Tracking Device. In: Proceedings of the IRE, vol. 49(9), pp. 1403–1416 (1961)
[13] Nielsen, P.T.: On the Acquisition Behaviour of Binary Delay-Lock Loops. IEEE Transactions on Aerospace and Electronic Systems AES-11(3), 415–418 (1975)
[14] Jovic, B., Unsworth, C.P.: Performance comparison of a multi-user chaos based DS-CDMA synchronisation unit within an AWGN and a Rayleigh fading channel. IET Electronics Letters 43(18), 988–989 (2007)
[15] Davidovici, S., Milstein, L.B., Schilling, D.L.: A New Rapid Acquisition Technique for Direct Sequence Spread-Spectrum Communications. IEEE Transactions on Communications COM-32(11), 1161–1168 (1984)
[16] Polydoros, A., Simon, M.K.: Generalized Serial Search Code Acquisition: The Equivalent Circular State Diagram Approach. IEEE Transactions on Communications COM-32(12), 1260–1268 (1984)
[17] Eng, T., Milstein, L.B.: Capacities of Hybrid FDMA/CDMA Systems in Multipath Fading. In: Proceedings of the IEEE Military Communications Conference (MILCOM 1993), Boston (MA), October 11-14, pp. 753–757 (1993)
[18] Haas, H., McLaughlin, S.: A Dynamic Channel Assignment Algorithm for a Hybrid TDMA/CDMA-TDD Interface Using the Novel TS-Opposing Technique. IEEE Journal on Selected Areas in Communications 19(10), 1831–1846 (2001)
[19] Zhang, Z., Seifert, F., Weigel, R.: A time code division multiple access (TCDMA) system proposal for indoor wireless communications. In: Proceedings of the 1996 International Conference on Communication Technology (ICCT 1996), Beijing, China, May 5-7, vol. 2, pp. 1094–1097 (1996)
[20] Ruprecht, J., Neeser, F.D., Hufschmid, R.: Code time division multiple access: an indoor cellular system. In: Proceedings of the 42nd IEEE Conference on Vehicular Technology (VTC 1992), Denver (CO), May 10-13, vol. 2, pp. 736–739 (1992)
[21] Leppanen, P.A., Pirinen, P.O.: Code time division multiple access: an indoor cellular system. In: Proceedings of the 1997 IEEE International Conference on Personal Wireless Communications (PWC 1997), Mumbai, India, December 17-19, pp. 419–423 (1997)

[22] Jeruchim, M.C., Balaban, P., Shanmugan, K.S.: Simulation of Communication Systems: Modeling, Methodology and Techniques, 2nd edn., p. 384. Kluwer Academic/Plenum Publishers, New York (2000)
[23] Sprott, J.C.: Chaos and Time-Series Analysis, pp. 230–440. Oxford University Press, Oxford (2003)
[24] Rappaport, T.S.: Wireless Communications Principles and Practice, pp. 172–188. Prentice Hall, Inc., Upper Saddle River (1996)
[25] Smith, J.I.: A Computer Generated Multipath Fading Simulation for Mobile Radio. IEEE Transactions on Vehicular Technology VT-24(3), 39–40 (1975)
[26] Arredondo, G.A., Chriss, W.H., Walker, E.H.: A Multipath Fading Simulator for Mobile Radio. IEEE Transactions on Communications COM-21(11), 1325–1328 (1973)
[27] Prabhu, G.S., Shankar, P.M.: Simulation of Flat Fading Using MATLAB for Classroom Instruction. IEEE Transactions on Education 45(1), 19–25 (2002)
[28] Giger, A.J., Barnett, W.T.: Effects of Multipath Propagation on Digital Radio. IEEE Transactions on Communications COM-29(9), 1345–1352 (1981)
[29] Wehinger, J., Mecklenbrauker, C.F.: Iterative CDMA Multiuser Receiver With Soft Decision-Directed Channel Estimation. IEEE Transactions on Signal Processing 54(10), 3922–3934 (2006)
[30] Kennedy, M.P., Kolumban, G.: Digital Communications Using Chaos. In: Chen, G. (ed.) Controlling Chaos and Bifurcations in Engineering Systems, pp. 477–500. CRC Press LLC, Boca Raton (1999)
[31] Hanzo, L., Yang, L.-L., Kuan, E.-L., Yen, K.: Single – and Multi – Carrier DS – CDMA Multi – User Detection, Space – Time Spreading, Synchronisation and Standards, pp. 754–772. IEEE press and Wiley, Chichester (2003)
[32] Meyr, H., Ascheid, G.: Synchronization in Digital Communications, pp. 3–17. Wiley Interscience, New York (1990)
[33] Mengali, U., D'Andrea, A.N.: Synchronization Techniques for Digital Receivers. Plenum Press, New York (1997)
[34] Barry, J.R., Lee, E.A., Messerschmitt, D.G.: Digital Communication, 3rd edn., pp. 727–761. Kluwer Academic Publishers, Boston (2004)

Chapter 2
Chaotic Signals and Their Use in Secure Communications

This chapter introduces nonlinear dynamical systems known as chaotic systems and describes their suitability for application to secure communications. A nonlinear or chaotic signal is characterised by its high sensitivity to parameter and initial condition perturbations, the random like nature and broadband spectrum [1]. From a nonlinear dynamical perspective, chaotic motion is a motion which possesses at least one positive Lyapunov exponent. Furthermore, for a given set of parameters and initial conditions chaotic motion is highly deterministic. Among other applications, these properties make chaotic systems suitable for the application in secure communications [2-9]. One of the main reasons for the increased security of communication provided by the chaotic signals is their broadband nature. In many cases the broadband nature of a chaotic system allows for the effective spectral cover up of the message by the chaotic carrier. In addition, the high sensitivity of chaotic signals to parameter and initial condition perturbations often can act as the encryption keys. In this chapter, the distinguishing features of chaotic systems are first presented and some approaches, used to identify chaotic behavior, are introduced. Furthermore, the approaches and the suitability of chaotic systems to the implementation within secure communication systems are examined. Finally, some of the noise reduction techniques, used to filter chaotic communication systems, are introduced.

2.1 Chaotic Systems

One of the earliest observations of nonlinear behaviour was made in 1961 by the Japanese electrical engineer, Yoshisuke Ueda. The observation occurred when Ueda conducted analog computer simulations of the Duffing/Van der Pol mixed type equation:

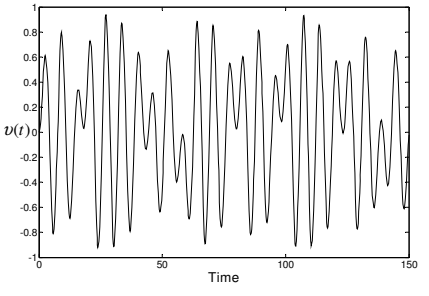
$$\frac{d^2\upsilon}{dt^2} - \mu(1-\gamma\upsilon^2)\frac{d\upsilon}{dt} + \upsilon^3 = B\cos(vt) \tag{2.1.1}$$

where: $\mu = 0.2$, $\gamma = 8$, $B = 0.35$ and $v = 1.02$.

B. Jovic: Synchronization Techniques for Chaotic Commun. Syst., SCT 5, pp. 31–47.
springerlink.com

The phenomenon output by the computer subsequently became known as chaos [10]. At around the same time American meteorologist, Edward Lorenz, independently discovered chaos in a third order autonomous system. Since then, a large number of chaotic systems have appeared in the literature [1].

Chaotic systems can be divided into those described by differential equations, known as flows, and those described by difference equations, known as maps [1,11]. The dynamics of a chaotic system can be represented in the time domain as time series or in phase space as a strange attractor [1,11]. The time series and the corresponding "broken-egg" strange attractor, obtained by numerically integrating equation 2.1.1, are shown in Figure 2.1a and Figure 2.1b, respectively.



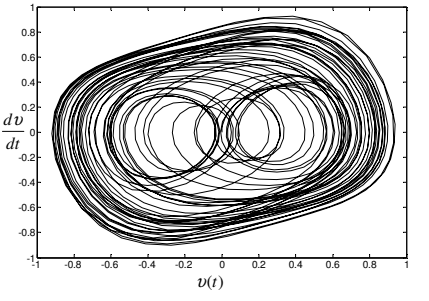


Fig. 2.1a The broken egg chaotic time series, **Fig. 2.1b** The broken egg strange attractor $\upsilon(t)$

The time series graph of Figure 2.1a is obtained by simply plotting the amplitude of the signal against time. On the other hand, the strange attractor is obtained by plotting two or more of the state variables of the system against each other. The state variables of the system are most often defined as the first or the second derivative of the time series, or a combination of those. It is readily verifiable that the system of equation 2.1.1 can also be represented in the state-space form of equation 2.1.2:

$$\begin{aligned} \dot{x} &= y \\ \dot{y} &= \mu y - \mu \gamma x^2 y - x^3 + B\cos(vz) \\ \dot{z} &= 1 \end{aligned} \tag{2.1.2}$$

where $x = \upsilon$, $y = \dot{\upsilon}$ and $z = t$ are the state variables of the system.

2.1.1 Chaotic Flows

The chaotic system of equation 2.1.1 (2.1.2) is an example of a chaotic flow. The Lorenz chaotic flow, which is an example of another well known flow, is now presented and its broadband nature and high sensitivity to parameter perturbations demonstrated. Further examples of some of the well known flows, such as the Rossler [12] and the Rucklidge flow [13], can be found in [1,12,13].

The dynamics of the Lorenz chaotic system, described by equation 2.1.3:

$$\begin{aligned} \dot{x} &= \sigma(y - x) \\ \dot{y} &= rx - y - xz, \\ \dot{z} &= -b\,z + xy \end{aligned} \tag{2.1.3}$$

are shown in Figure 2.2 when the parameter $\sigma = 10$, $r = 28$ and $b = 8/3$.

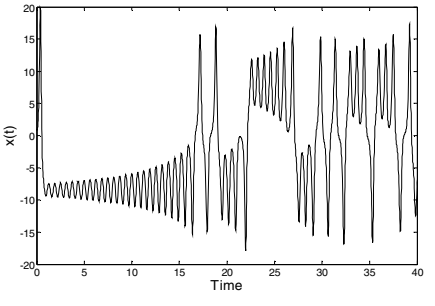


Fig. 2.2a The Lorenz chaotic time series, $x(t)$

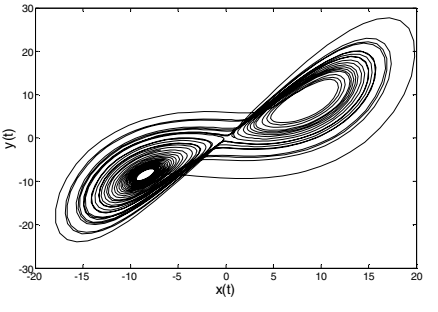


Fig. 2.2b The Lorenz strange attractor

The dynamics of the strange attractor of a chaotic flow are referred to as a trajectory [1]. The trajectory of a chaotic flow is characterised by a smooth, continuous nature. An example of a chaotic flow is a turbulent flow of water from a pipe [1].

The broadband nature of the Lorenz chaotic flow can be observed from Figure 2.3 where the power spectral density of the Lorenz x signal has been plotted against the normalized frequency. Furthermore, the high sensitivity of the Lorenz chaotic flow to parameter perturbations is demonstrated in Figure 2.4. It can be observed from Figure 2.4 that a small alteration to a parameter of the system causes the system to generate an entirely different chaotic signal. It is shown in chapter 6 how this property of chaotic signals can be used in the design of secure chaotic communication systems.

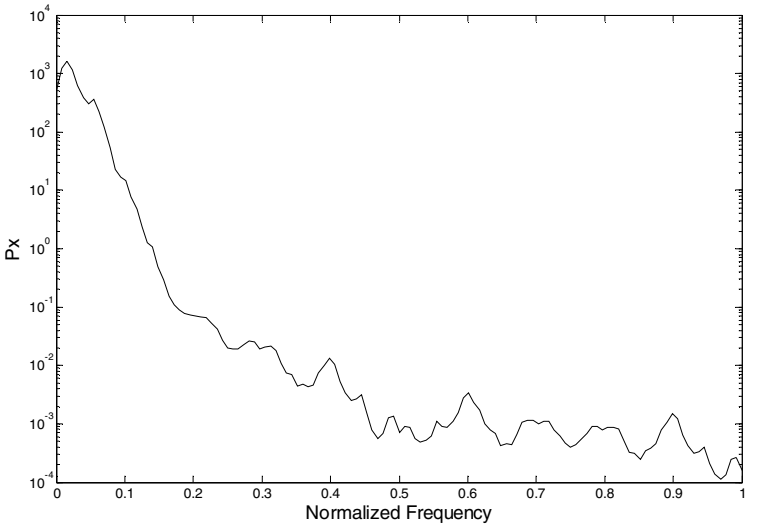


Fig. 2.3 The power spectral density (P*x*) of the Lorenz *x* signal versus the normalized frequency

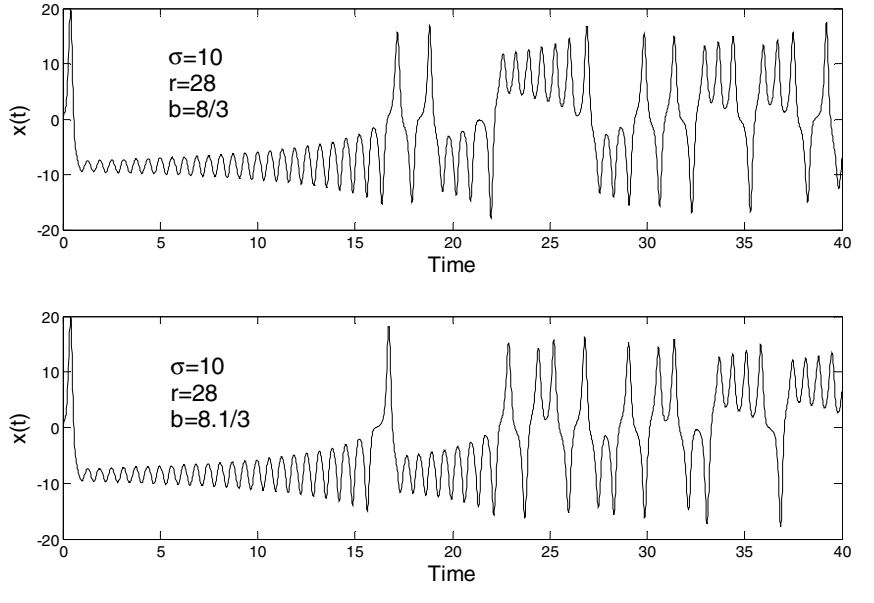


Fig. 2.4 Sensitive dependence on the parameter perturbations within the Lorenz chaotic flow

2.1.2 Chaotic Maps

The dynamics of one of the most well known chaotic maps, the Hénon map:

$$\begin{aligned} X_{n+1} &= 1 - aX_n^2 + bY_n \\ Y_{n+1} &= X_n \end{aligned} \tag{2.1.4}$$

are shown in Figure 2.5 when the parameter $a = 1.4$ and $b = 0.3$.

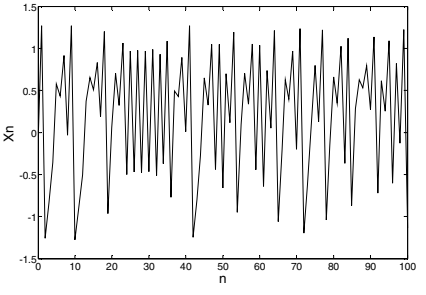


Fig. 2.5a The Hénon chaotic time series, X_n

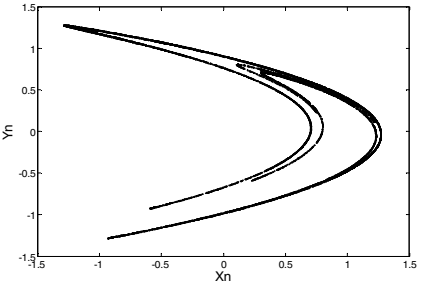


Fig. 2.5b The Hénon map

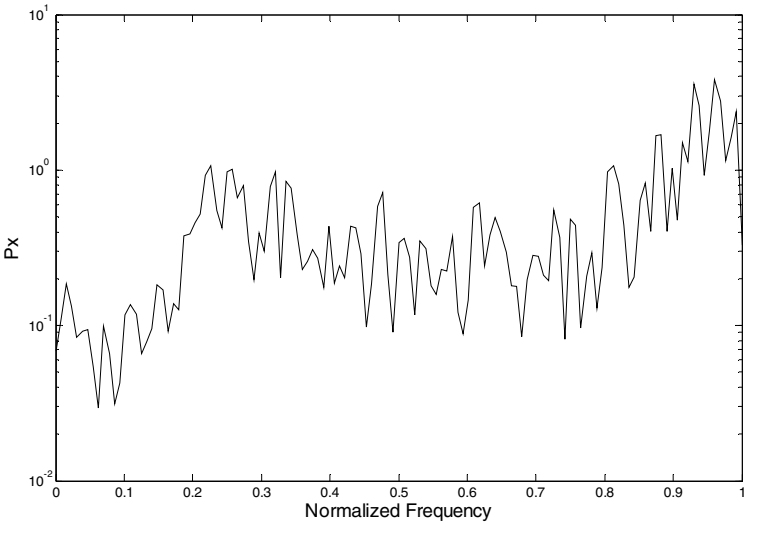


Fig. 2.6 The power spectral density (P*x*) of the Hénon X_n signal versus normalized frequency.

The broadband nature of the Hénon chaotic map can be observed from Figure 2.6 where the power spectral density of the Hénon X_n signal has been plotted. Furthermore, the high sensitivity of the Hénon chaotic map to parameter perturbations is demonstrated in Figure 2.7. As for the Lorenz chaotic flow, it can be observed from Figure 2.7 that a small alteration to the parameter of the Hénon map causes the system to generate an entirely different chaotic signal.

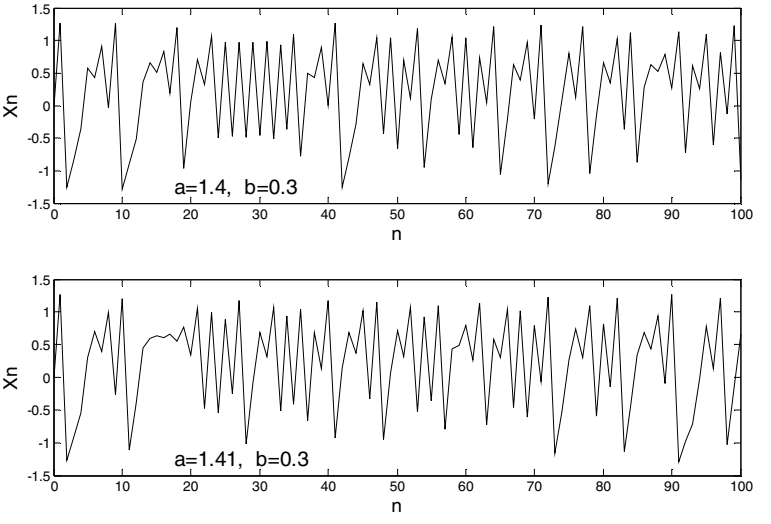


Fig. 2.7 Sensitive dependence on the parameter perturbations within the Hénon chaotic map

The logistic map is an example of another well known chaotic map. The logistic map time series are generated using equation 2.1.5 [14].

$$X_{n+1} = 1 - 2X_n^2 \tag{2.1.5}$$

The dynamics of the logistic map are shown in Figure 2.8 [15]. Furthermore, the dynamics of some of the other well known maps, such as the cusp, Lozi and Chirikov chaotic map, can be found in [1].

The dynamics of the chaotic map are referred to as an orbit [1]. In contrast to the trajectory of chaotic flows, the orbit of a chaotic map is characterised by a non-smooth, discontinuous motion. It can be observed from Figures 2.5 and 2.8, that each chaotic system has its own signature in phase space, that is, a unique attractor characterising it. An example of a chaotic map is the non-periodic dropping of water from a pipe [1].

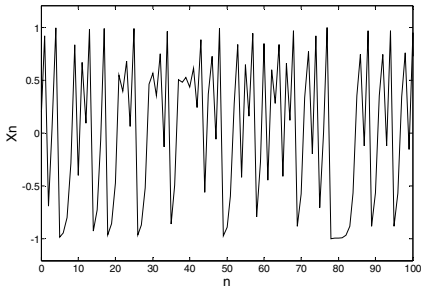


Fig. 2.8a The logistic chaotic time series, X_n

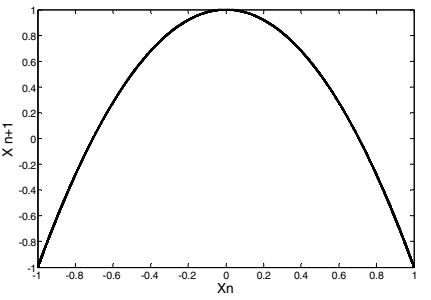


Fig. 2.8b The logistic map

2.2 Lyapunov Exponents

One of the main characteristics of chaotic systems is that they are deterministic, but extremely sensitive to the starting points, that is, their initial conditions. By high sensitivity to the initial conditions it is meant that the two trajectories (orbits), starting from infinitesimally close initial conditions, quickly diverge in phase space. This phenomenon is illustrated in Figures 2.9 and 2.10 on the Lorenz chaotic flow and the Hénon chaotic map time series, respectively. However, given the knowledge of the exact initial conditions, chaotic systems are predictable. It is shown in the next section how this property of chaotic signals can be used to hide (encrypt) messages within a communication system.

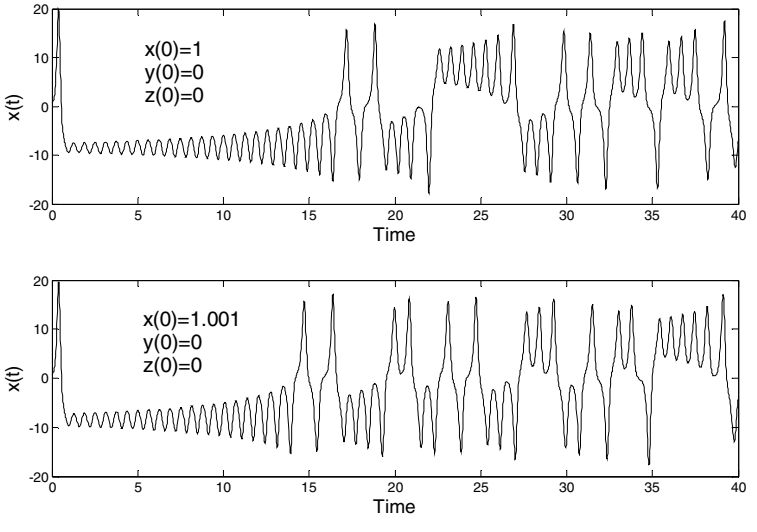


Fig. 2.9 Sensitive dependence on the initial conditions, denoted by $x(0)$, $y(0)$ and $z(0)$, within the Lorenz chaotic flow

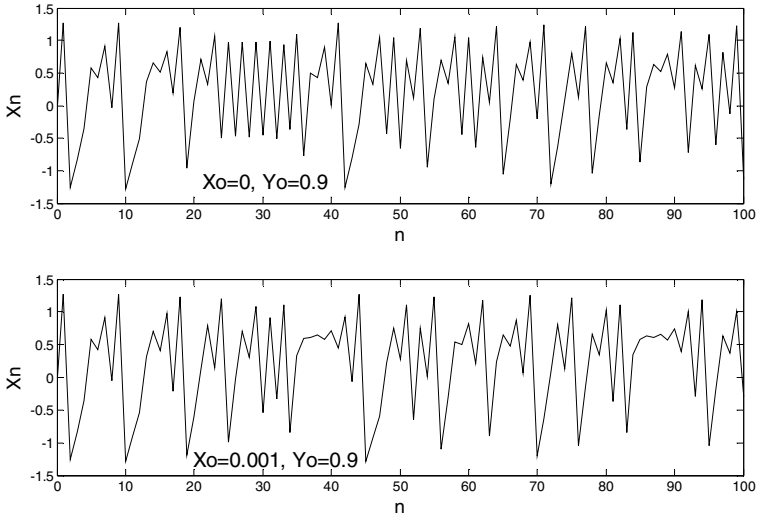


Fig. 2.10 Sensitive dependence on the initial conditions, denoted by X_0 and Y_0, within the Hénon chaotic map

The Lyapunov exponents of a system under consideration characterise the nature of that particular system. They are perhaps the most powerful diagnostic in determining whether the system is chaotic or not. Furthermore, Lyapunov exponents are not only used to determine whether the system is chaotic or not, but also to determine how chaotic it is. They are named after the Russian mathematician, Aleksandr Mikhailovich Lyapunov, who introduced the idea around the turn of the 19th to the 20th century [16,1]. The Lyapunov exponents characterise the system in the following manner. Suppose that d_0 is a measure of the distance among two initial conditions of the two structurally identical chaotic systems. Then, after some small amount of time the new distance is:

$$d(t) = d_0 2^{\lambda t}, \tag{2.2.1}$$

where λ denotes the Lyapunov exponent.

For chaotic maps, equation 2.2.1, is rewritten in the form of equation 2.2.2:

$$d_n = d_0 2^{\Lambda t}, \tag{2.2.2}$$

where Λ denotes the Lyapunov exponent and *n* a single iteration of a map.

The choice of base 2 in equations 2.2.1 and 2.2.2 is arbitrary [16]. The Lyapunov exponents of equations 2.2.1 and 2.2.2 are known as local Lyapunov exponents as they measure the divergence at one point on a trajectory (orbit). In order to obtain a global Lyapunov exponent the exponential growth at many points

along a trajectory (orbit) must be measured and averaged [16]. Therefore, the global, or the largest, Lyapunov exponent is represented by equation 2.2.3:

$$\lambda = \frac{1}{t_N - t_0} \sum_{k=1}^{N} \log_2 \frac{d(t_k)}{d_0(t_{k-1})} \tag{2.2.3}$$

Similarly, for chaotic maps, the global Lyapunov exponent is defined by equation 2.2.4:

$$\Lambda = \lim_{n \to \infty} \frac{1}{N} \sum_{k \to \infty}^{N} \log_2 \left| \frac{d f(X_n)}{dX} \right| \tag{2.2.4}$$

where $f(X_n) = X_{n+1}$.

A motion is said to be chaotic if the global Lyapunov exponent is greater than zero [16,1]. A motion with a negative global Lyapunov exponent implies a fixed point or a periodic cycle [1]. In certain cases it is possible to analytically evaluate Lyapunov exponents of the system [1]. If, however, analytical evaluation is not possible, one must resort to the numerical evaluation [16,1].

A chaotic system has as many Lyapunov exponents as it has dimensions. However, the global (largest) Lyapunov exponent is the most important one as its evaluation determines whether the system is chaotic or not. For instance, the one-dimensional logistic map of equation 2.1.5 (Figure 2.8) has a single positive Lyapunov exponent. The two-dimensional Henon map of equation 2.1.4 (Figure 2.5) has two Lyapunov exponents, one negative and the other positive. Furthermore, the Lorenz chaotic flow of equation 2.1.3 (Figure 2.2) has three Lyapunov exponents, one positive, one negative and one equal to zero.

Beside Lyapunov exponents, there are other techniques used to determine whether a system under consideration is chaotic or not, such as the correlation dimension [1] and the Kaplan-Yorke (or Lyapunov) dimension [1]. Unlike the Lyapunov exponent, which measures the attractor's average predictability, the dimension of an attractor measures its complexity. The attractor dimension is less than but not equal to the number of variables of a chaotic system. Furthermore, it is not an integer, but a fraction. Thus the attractor dimension is also called the fractal dimension.

2.3 Application of Chaos to Communications

Unlike pseudo random signals, which are limited in number and are periodic, chaotic systems can theoretically produce infinite numbers of chaotic signals which are non-periodic. This property and the broadband nature of chaotic signals make them of particular interest in secure communications. In this book, two approaches to chaotic communication systems are investigated. The first approach, investigated in the sixth chapter, is that based on the principles of chaotic

synchronization [17]. The second approach, investigated in the seventh chapter, is that based on the classical synchronization techniques used within DS-CDMA systems.

2.3.1 Chaotic Communication Systems Based on the Principles of Chaotic Synchronization

The general block diagram which demonstrates the principles of chaotic synchronization is presented in Figure 2.11. In Figure 2.11, the master chaotic system transmits one or more of its signals to the slave system. The slave system is another chaotic system, which in general, can be entirely different from the master system. Depending on the nature of the master signal supplied to the slave system, the slave system may or may not synchronize to the master system. If the master-slave system does not synchronize for a given master signal(s), it is possible to design a controller at the slave side which enforces synchronization. The principles of chaotic synchronization are thoroughly discussed in the next chapter.

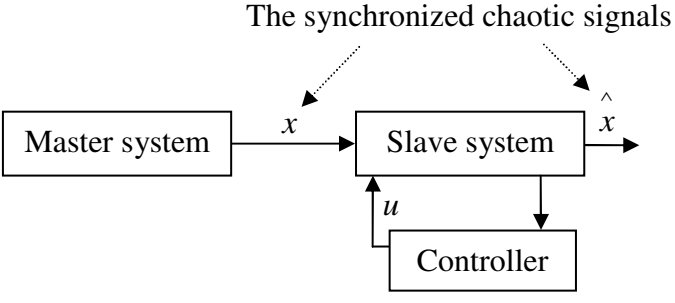


Fig. 2.11 General block diagram demonstrating the principles of chaotic synchronization, where x denotes the master and $\hat{x}$ the slave signal

Once the master-slave synchronization has been achieved, it is possible to design a communication system based on the principles of chaotic synchronization. The general block diagram of such a communication system is illustrated in Figure 2.12. The communication system of Figure 2.12 is therefore entirely based on the principles of chaotic synchronization and an ideal synchronization within it cannot be assumed. This is in contrast to DS-CDMA based systems where one can assume perfect synchronization in order to evaluate the benchmark performance, as was explained in the first chapter. In Figure 2.12, the sequence synchronization unit and the linear operator have been specifically highlighted to clarify the relation of this chaotic synchronization based system to the general system of Figure 1.22. As will be shown in chapter 6, the message m of Figure 2.12 can be encrypted within the chaotic carrier x via the parameter or the initial condition perturbations, or by simply adding it directly onto the chaotic carrier.

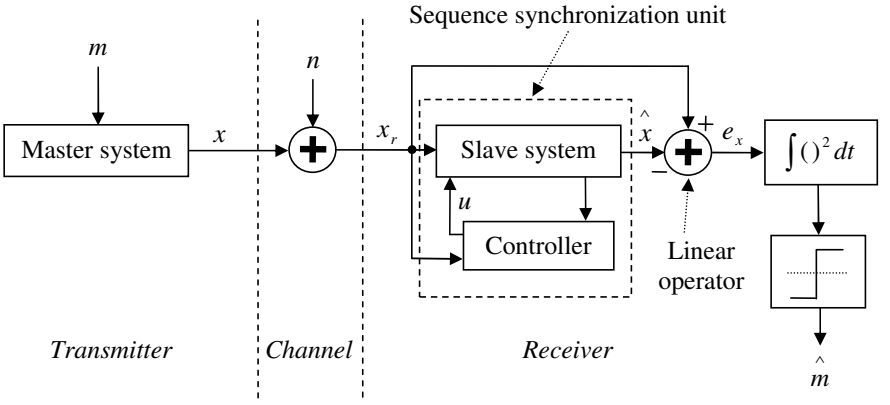


Fig. 2.12 General block diagram of the chaotic communication system based on the concept of chaotic synchronization

2.3.2 *Chaotic Communication Systems Based on the DS-CDMA Principle*

The implementation of chaotic signals within chaos based DS-CDMA systems is possible due to the fact that the chaotic signals are approximately mutually orthogonal. In particular, this property is more dominant within signals generated by chaotic maps than chaotic flows.

For instance, consider the logistic map, whose time series is generated using equation 2.1.5 [14] and whose dynamics are shown in Figure 2.8 [15]. The two different chaotic time series generated by the same logistic map, but with different initial conditions, are highly orthogonal as is demonstrated in Figure 2.13a by the cross-correlation function with no dominant peaks. The autocorrelation function of the logistic map time series is presented in Figure 2.13b showing the dominant peak. The length of the logistic map time series used to produce Figures 2.13a and 2.13b is equal to 511 points (chips). In Figures 2.13a and 2.13b t denotes the time delay. Also, note that the correlation functions have been normalized to the peak of the autocorrelation function.

As opposed to the logistic map of equation 2.1.5, the Lorenz chaotic flow of equation 2.1.3, for instance, has the correlation properties illustrated in Figures 2.14a and 2.14b. The length of the Lorenz flow time series used to produce Figures 2.14a and 2.14b is equal to 2001 points (chips). In contrast to Figure 2.13a, it can be observed from Figure 2.14a that the cross correlation function of the Lorenz flow contains dominant peaks which are strongly pronounced. Furthermore, whereas the autocorrelation function of the logistic map resembles an impulse function, with a single dominant peak at $t = 0$, the autocorrelation function of the Lorenz flow does not. This can in particular be observed by comparing the close ups of Figures 2.13b and 2.14b and observing that the logistic map autocorrelation function has a sharp falloff from 1 to 0 at $t = 0$ and $t = \pm 1$, whereas the Lorenz

flow does not. This indicates that the logistic map time series is more orthogonal to itself than the Lorenz flow time series. Therefore, in this book, only the logistic map time series will be used within a DS-CDMA system for spreading.

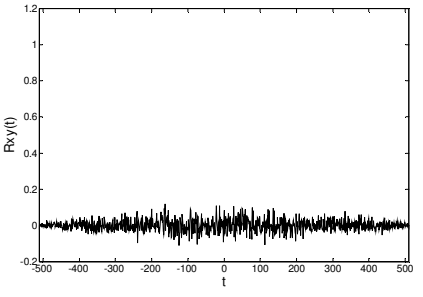


Fig. 2.13a Cross-correlation of logistic map time series

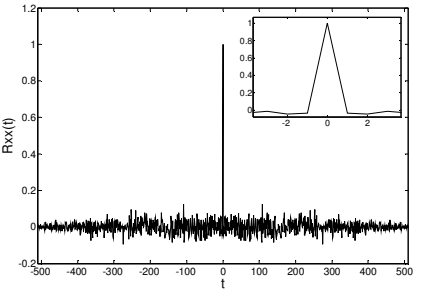


Fig. 2.13b Autocorrelation of logistic map time series. The close up is shown in the top right hand corner

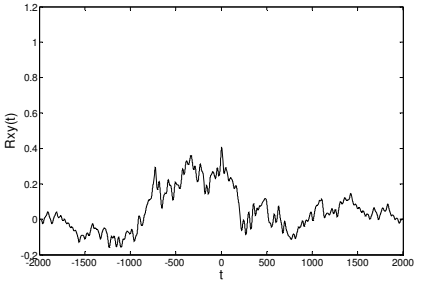


Fig. 2.14a Cross-correlation of Lorenz flow time series

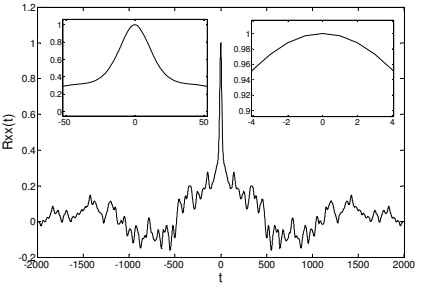


Fig. 2.14b Autocorrelation of Lorenz flow time series. The close ups are shown in the top right and left hand corners

A DS-CDMA system where chaotic signals are used to spread data is termed chaos based DS-CDMA system. A chaos based DS-CDMA communication system with perfect sequence synchronization assumed is shown in Figure 2.15 [18].

In Figure 2.15, $x(t)$ denotes the chaotic spreading signals which are multiplied by the binary message signals $m(t)$. The products are then summed to produce the signal $c(t)$ which is transmitted through the channel:

$$c(t) = \sum_{i=1}^{M} m_i(t)\, A_i\, x_i(t) \tag{2.3.1}$$

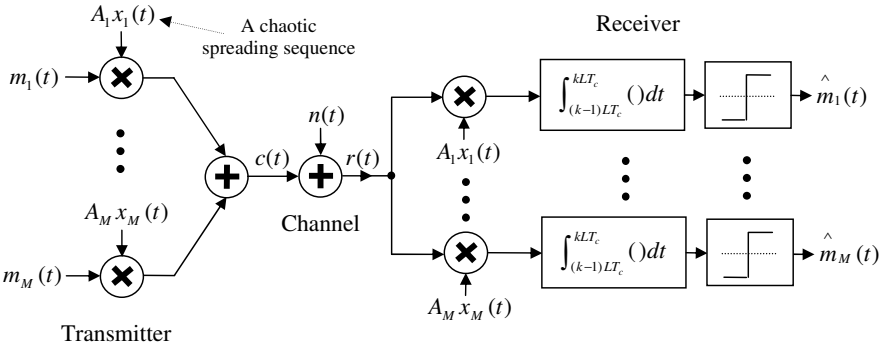


Fig. 2.15 The chaos based DS-CDMA system with perfect sequence synchronization assumed

The received signal $r(t) = c(t) + n(t)$ is despread and correlated with the punctual despreading codes to recover the message $\hat{m}_q(t)$ of each of the *M* users in the system:

$$\begin{aligned}
\hat{m}_q(t) &= \mathrm{T_h}\left[\int_{(k-1)LT_c}^{kLT_c} r(t)\, A_q x_q(t)\, dt\right] \\
&= \mathrm{T_h}\left[\int_{(k-1)LT_c}^{kLT_c} \left\{\sum_{i=1}^{M} m_i(t)\, A_i\, x_i(t) + n(t)\right\} \cdot A_q x_q(t)\, dt\right] \\
&= \mathrm{T_h}\left[\begin{array}{l} \displaystyle\int_{(k-1)LT_c}^{kLT_c} m_q(t)\, A_q^2 x_q^2(t)\, dt \\ \displaystyle + \int_{(k-1)LT_c}^{kLT_c} \sum_{\substack{i=1 \\ i\neq q}}^{M} m_i(t)\, A_i A_q\, x_i(t)\, x_q(t)\, dt + \int_{(k-1)LT_c}^{kLT_c} n(t) A_q x_q(t)\, dt \end{array}\right]
\end{aligned} \tag{2.3.2}$$

where, $\mathrm{T_h}[\ ]$ is the signum function which denotes the thresholding operation and assigns either a -1 or a 1 depending on whether the value in the brackets is negative or positive, respectively [19]. It is assumed that all the received signals have the same average power.

Due to the mutually orthogonal properties of the chaotic spreading sequences produced by the logistic map with different initial conditions, as demonstrated in Figures 2.13a and 2.13b, equations 2.3.3a and 2.3.3b are expected to hold:

$$\int_{(k-1)LT_c}^{kLT_c} m_q(t)\, A_q^2 x_q^2(t)\, dt > 0 \qquad if \quad m_q(t) = 1 \tag{2.3.3a}$$

$$\int_{(k-1)LT_c}^{kLT_c} m_q(t)\, A_q^2 x_q^2(t)\, dt < 0 \qquad if \quad m_q(t) = -1 \tag{2.3.3b}$$

Provided that the power of noise in the system and the interferences among different users are comparatively low to the power of the signal, the noise and the interferences terms of equation 2.3.2 are expected to be approximately equal to zero, that is: $\int_{(k-1)LT_c}^{kLT_c} n(t) A_q x_q(t)\, dt \approx 0$ and $\int_{(k-1)LT_c}^{kLT_c} \sum_{\substack{i=1 \\ i \neq q}}^{M} m_i(t)\, A_i A_q\, x_i(t)\, x_q(t)\, dt \approx 0$, so that equation 2.3.2 takes on the form of equations 2.3.4a and 2.3.4b:

$$\hat{m}_q(t) = 1 \qquad if \quad m_q(t) = 1 \tag{2.3.4a}$$

$$\hat{m}_q(t) = -1 \qquad if \quad m_q(t) = -1 \tag{2.3.4b}$$

Therefore, by assigning the unique initial conditions to each of the *M* users provides for the increased security of transmission as only the users with the same initial conditions can decrypt the message at the receiver.

2.4 Noise Reduction within Chaotic Communication Systems

In the previous section, the two main approaches to the implementation of chaotic systems to secure communications have been described. In this section, the techniques of noise reduction by means of de-noising (or filtering) are now briefly introduced.

Noise removal from chaotic time series has been attempted by a number of researchers [20-27], among others, and is still an active area of research. Filtering methods include linear filters [20,22] and different wavelet techniques [20,21,23-25], among other. A potential application of chaotic filtering techniques lies in chaotic communication systems [20,26,27]. In this book, the linear and wavelet techniques have been developed and used to filter a newly proposed chaotic communication system based on the principles of chaotic synchronization [20]. While the general block diagram of a chaotic communication system with the filter embedded inside the receiver is shown in Figure 2.16, the complete results are presented in the appendix. The appendix should be read only after reading chapters 3-6.

In Figure 2.16, the filter unit processes the received signal x_r and produces its filtered version x_f. The filtered signal x_f is then fed into the slave system. In this book, three different kinds of filtering techniques have been developed and

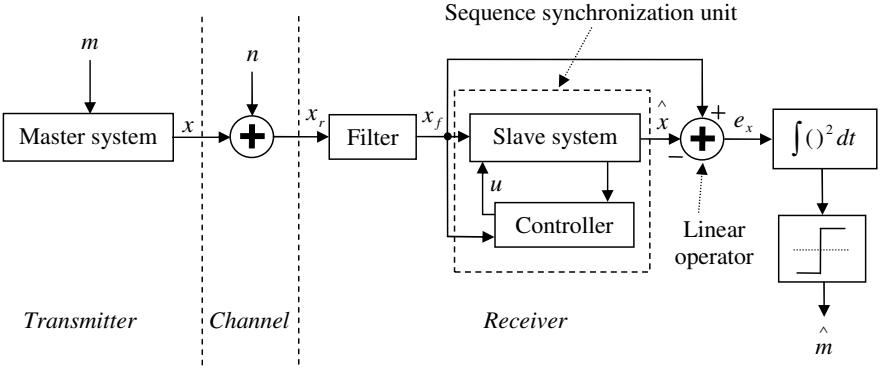


Fig. 2.16 General block diagram of a chaotic communication system based on the concept of chaotic synchronization with the filter unit incorporated

implemented within the chaotic communication system. The filtering techniques include those based on the running average finite impulse response (FIR) filter [1] and those within the Haar wavelet [28] and the Daubechies wavelet domain [28]. It has been shown, in terms of the bit error rate, that both linear and wavelet filters significantly improve the noise performance of the system [20].

2.5 Conclusion

In this chapter, nonlinear dynamical systems, known as chaotic systems, have been introduced and their suitability to the application to secure communication systems outlined. Chaotic behaviour was recognised by the scientific community in the early sixties. It was characterized by apparent random behaviour, high sensitivity to parameter and initial condition perturbations and broadband spectrum. These were some of the properties that led to the belief that chaotic signals could be used within secure communications. Here, two different types of chaotic systems, known as flows and maps, have first been introduced and their broadband nature and high sensitivity to parameter and initial condition perturbations demonstrated. The Lyapunov exponents which are used to diagnose and characterize the system have then been presented. Furthermore, the two different approaches of implementing chaotic systems within secure communication systems have been outlined. These include chaotic communication systems based on the principles of chaotic synchronization and those based on the DS-CDMA principle. Finally, some of the filtering techniques that can be used within chaotic communication systems have been briefly introduced.

References

[1] Sprott, J.C.: Chaos and Time-Series Analysis, pp. 230–440. Oxford University Press, Oxford (2003)
[2] Stavroulakis, P.: Introduction. In: Stavroulakis, P. (ed.) Chaos Applications in Telecommunications, pp. 1–12. CRC Press LLC, Boca Raton (2006)
[3] Kennedy, M.P., Kolumban, G., Jako, Z.: Chaotic Modulation Schemes. In: Kennedy, M.P., Rovatti, R., Setti, G. (eds.) Chaotic Electronics in Telecommunications, pp. 163–175. CRC Press LLC, Boca Raton (2000)
[4] Chen, G., Dong, X.: From chaos to order: Methodologies, Perspectives and Applications, pp. 598–614. World Scientific Publishing Co. Pte. Ltd., Singapore (1998)
[5] Lau, F.C.M., Tse, C.K.: Chaos-Based Digital Communication Systems, ch. 1, pp. 1–20. Springer, Berlin (2004)
[6] Kolumban, G., Kennedy, M.P.: Correlator-Based Chaotic Communications: Attainable Noise and Multipath Performance. In: Chen, G., Ueta, T. (eds.) Chaos in Circuits and Systems, pp. 443–485. World Scientific Publishing Co. Pte. Ltd., New Jersey (2002)
[7] Kennedy, M.P., Kolumban, G.: Digital Communications Using Chaos. In: Chen, G. (ed.) Controlling Chaos and Bifurcations in Engineering Systems, pp. 477–500. CRC Press LLC, Boca Raton (1999)
[8] Wu, C.W.: Synchronization in coupled chaotic circuits and systems, pp. 13–33. World Scientific Publishing Co. Pte. Ltd., New Jersey (2002)
[9] Setti, G., Rovatti, R., Mazzini, G.: Control of Chaos Statistics for Optimization of DS-CDMA Systems. In: Chen, G., Yu, X. (eds.) Chaos Control Theory and Applications, pp. 295–319. Springer, Berlin (2003)
[10] Abraham, R., Ueda, Y.: The chaos avant – garde memories of the early days of chaos theory, pp. 23–80. World Scientific Publishing Co. Pte. Ltd., Singapore (2000)
[11] Moon, F.C.: Chaotic Vibrations - An Introduction for Applied Scientists and Engineers, pp. 24–36. Wiley Interscience, New York (1987)
[12] Rossler, O.E.: An equation for continuous chaos. Physics Letters A 57A(5), 397–398 (1976)
[13] Rucklidge, A.M.: Chaos in models of double convection. Journal of Fluid Mechanics 237, 209–229 (1992)
[14] Parlitz, U., Ergezinger, S.: Robust communication based on chaotic spreading sequences. Physics Letters A 188(2), 146–150 (1994)
[15] Zhou, C.S., Chen, T.L.: Extracting information masked by chaos and contaminated with noise: Some considerations on the security of communication approaches using chaos. Physics Letters A 234(6), 429–435 (1997)
[16] Moon, F.C.: Chaotic and Fractal Dynamics - An Introduction for Applied Scientists and Engineers, pp. 307–309. Wiley Interscience, New York (1992)
[17] Pecora, L.M., Carroll, T.L.: Synchronization in chaotic systems. Physical Review Letters 64(8), 821–824 (1990)
[18] Jovic, B., Unsworth, C.P.: Chaos based multi-user time division multiplexing communication system. IET Communications 1(4), 549–555 (2007)
[19] Jordan, D.W., Smith, P.: Mathematical Techniques: An introduction for the engineering, physical, and mathematical sciences, 2nd edn., p. 8. Oxford University Press, Oxford (1997)

[20] Jovic, B., Unsworth, C.P., Berber, S.M.: De-noising 'Initial Condition Modulation' Wideband Chaotic Communication Systems with Linear & Wavelet Filters. In: Proceedings of the First IEEE International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2006), Sydney, Australia, March 13-16, pp. 1–6 (2006)
[21] Grzesiak, M.: Wavelet filtering of chaotic data. Nonlinear processes in geophysics 7, 111–116 (2000)
[22] Broomhead, D., Huke, J., Muldoon, M.: Linear Filters and Nonlinear Systems. Journal of the Royal Statistical Society 54(2), 373–382 (1992)
[23] Roy, M., Kumar, V., Kulkarni, B., Sanderson, J., Rhodes, M., Stappen, M.: Simple denoising algorithm using wavelet transform. AIChE Journal 45(11), 2461–2466 (1999)
[24] Constantine, W., Reinhall, P.: Wavelet-based in-band denoising technique for chaotic sequences. International Journal of Bifurcation and Chaos 11(2), 483–495 (2000)
[25] Boccalleti, S., Guiaquinta, A., Arecchi, F.: Adaptive recognition and filtering of noise using wavelets. Physical Review E 55(5), 5393–5397 (1997)
[26] Lee, C.: Noise reduction methods for chaotic signals with application to secure communications, PhD thesis, Georgia institute of technology (1995)
[27] Carroll, T.L.: Approximating chaotic time series through unstable periodic orbits. Physical Review E 59(2), 1615–1621 (1999)
[28] Nievergelt, Y.: Wavelets made easy, ch. 1, 2 and 3. Birkhauser, Boston (1999)

Chapter 3
Chaotic Synchronization, Conditional Lyapunov Exponents and Lyapunov's Direct Method

In chapter 2, the underlying characteristic of chaos, such as their high sensitivity to parameter and initial condition perturbations, the random like nature and the broadband spectrum, were outlined. Due to these characteristics it was originally thought that chaotic systems could not be synchronized and thus could not be used as part of the coherent communication systems, where synchronization is an integral part of operation. However, this was not the case and in this and the next two chapters, synchronization of chaotic systems is investigated. In this chapter, the basic concepts of chaotic synchronization are outlined. Its characteristics are examined in terms of the conditional Lyapunov exponents and Lyapunov's direct method. Lyapunov's direct method is then used to develop a general approach in the design of synchronous chaotic systems.

The first to study the topic of chaotic synchronization were Yamada and Fujisaka in 1983 [1], and Afraimovich et al. in 1986 [2]. However it was not until 1990 when Pecora and Carroll (PC) introduced their method of chaotic synchronization [3] and suggested application to secure communications that the topic started to arouse major interest. In the PC method one has a master system and a slave system, with a single signal of the master system driving the slave system [3,4-11]. Similar master-slave synchronization schemes have also been investigated in [12,13]. Besides the PC synchronization method, numerous chaos synchronization methods have been developed in the last decade and a half, such as the Ott-Grebogi-York (OGY) based chaos synchronization method [14,15], John and Amritkar (JA) synchronization method [16] and Pyragas' synchronization method [17]. In more general terms the chaotic synchronization phenomena can be divided into identical synchronization (IS) and general synchronization (GS), among other types [18]. IS, as the name suggests, involves two identical systems, whereas generalized synchronization is an extension of IS, involving non-identical systems [18,19]. However, it has been shown that in fact identical systems can also exhibit GS, thus proving that non-identity of the systems is not a necessary condition for GS [18]. This chapter examines a number of systems based on IS.

The motivation for the study of chaotic synchronization lies in its numerous potential applications. The applications of chaotic synchronization range from

B. Jovic: Synchronization Techniques for Chaotic Commun. Syst., SCT 5, pp. 49–78.
springerlink.com

living systems applications [20,19] to the non-living systems applications [19,21]. The examples of applications of chaotic synchronization to living systems include synchronization in neurobiology [19] and chemical reactions among pancreatic cells [20], among other. The examples of applications of chaotic synchronization to non-living systems include synchronization in earth sciences [19], synchronization of chaotic electrochemical oscillators [22,23], synchronization in communications [8,10,16,24-31] etc. The synchronization schemes presented in this chapter are the backbone of many chaotic communication systems in the literature today [26,30,8,10,32-39]. The application of chaotic synchronization to secure communications is investigated in chapter 6.

In Section 3.1 the principles of chaotic synchronization based on the PC scheme are presented. These are analysed in terms of the conditional Lyapunov exponents (CLEs) in Section 3.2 and Lyapunov's direct method in Section 3.3. Furthermore, in Section 3.4, Lyapunov's direct method is then used to demonstrate a general approach in the design of synchronous chaotic systems.

3.1 Pecora-Carroll Chaotic Synchronization Method

The Pecora-Carroll (PC) synchronization scheme has often been described as a "master-slave" system [7,37]. Essentially, a master-slave system consists of two chaotic systems. The two systems are described by the same set of differential equations, with the same parameter values. It was shown in [3] that for synchronization to occur, the output from, at least, one of the coupled differential equations of the first chaotic system must be made available to the second chaotic system, as shown in Figure 3.1. Thus, one chaotic system is said to drive the other chaotic system by the time-series signal generated from one of its differential equations. The driving chaotic system is known as the master system and the driven chaotic system is known as the slave system. As discussed in chapter 1, and as will be demonstrated in chapter 6, the master-slave system can also be viewed as the transmitter-receiver communication system.

The master system is made up of a driving master subsystem ($\mathbf{u}$) with initial conditions $\mathbf{u}(0)$ and a non-driving master subsystem ($\mathbf{v}$) with initial conditions $\mathbf{v}(0)$ which are independent of the master driving subsystem. The slave system is made up of a driven slave subsystem ($\hat{\mathbf{u}}$), which is identical to ($\mathbf{u}$), and a non driven slave subsystem ($\hat{\mathbf{v}}$), which has initial conditions $\hat{\mathbf{v}}(0) \neq \mathbf{v}(0)$. Since the driving master subsystem is fully available to the slave system it is said that the master system drives the slave system with the driving master subsystem. The non-driven slave subsystem ($\hat{\mathbf{v}}$) has initial conditions that are independent of those of the master system.

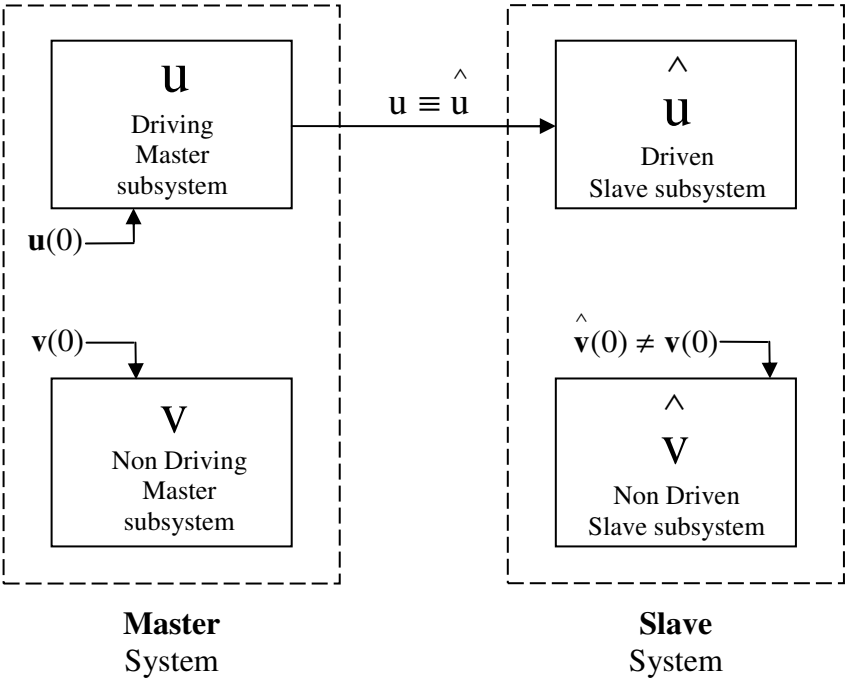


Fig. 3.1 Pecora-Carroll master-slave system divided into subsystems

In general, the master system of Figure 3.1 can be represented by equation 3.1.1:

$$\dot{\mathbf{s}} = \mathbf{f}(t, \mathbf{s}) \tag{3.1.1}$$

where $\mathbf{s} \in \Re^d$, that is, $\mathbf{s}$ is a *d*-dimensional vector. The 'dot' above the variable in equation 3.1.1 denotes the operation *d/dt*. Let the master system $\mathbf{s}$ be decomposed into subsystems as shown in Figure 3.1. The driving and non-driving master subsystems are then given by equations 3.1.2a and 3.1.2b [7]. The corresponding driven and non-driven slave subsystems are given by equations 3.1.3a and 3.1.3b, respectively [7]:

$$\dot{\mathbf{u}} = \mathbf{h}(t, \mathbf{u}, \mathbf{v}) \tag{3.1.2a}$$

$$\dot{\mathbf{v}} = \mathbf{g}(t, \mathbf{u}, \mathbf{v}) \tag{3.1.2b}$$

$$\hat{\mathbf{u}} = \mathbf{u} \tag{3.1.3a}$$

$$\dot{\hat{\mathbf{v}}} = \mathbf{g}(t, \mathbf{u}, \hat{\mathbf{v}}) \tag{3.1.3b}$$

In equations 3.1.2 and 3.1.3 $\mathbf{u} \in \Re^m$ and $\mathbf{v} \in \Re^n$, with the overall dimension of the master system $d = m + n$.

3.2 Conditional Lyapunov Exponents and the Pecora-Carroll Chaotic Synchronization

The necessary and sufficient condition, for master-slave synchronization to occur, is that the non-driven slave subsystem must be asymptotically stable [7]. Asymptotic stability can be theoretically proven via Lyapunov's direct method [7,8,37], or by evaluating the conditional Lyapunov exponents (CLEs) [4,11]. Lyapunov's direct method involves finding the Lyapunov function of the system under consideration and thus demonstrating that asymptotic stability exists. Its use is demonstrated in the next section. Lyapunov's direct method is one of the most powerful tools in the nonlinear system stability analysis. However, it is often too difficult to find the Lyapunov function of the particular system under consideration. The ability to do so often depends on ones intuition and experience [40]. Thus far, there is no systematic general procedure for the construction of the Lyapunov functions [41]. Therefore, it is often desirable, if not necessary, to resort to the CLEs. In order for the master-slave system to synchronize, all the CLEs of the non-driven slave subsystem must be negative [4,11].

The procedure for obtaining the CLEs is now briefly discussed and demonstrated on the simplest piecewise linear master-slave chaotic flow when the master x signal drives [37]. The simplest piecewise linear chaotic flow is given by equation 3.2.1:

$$\begin{aligned} \dot{x} &= y \\ \dot{y} &= z \\ \dot{z} &= -Az - y + |x| - 1 \end{aligned} \tag{3.2.1}$$

It is found that the system of equation 3.2.1 exhibits chaotic behaviour with the parameter value A = 0.6 [42,37]. Its dynamics are shown in Figure 3.2. This system is said to be the master system and is illustrated in Figure 3.3 [37]. The slave system is driven by a single master signal, meaning that this particular

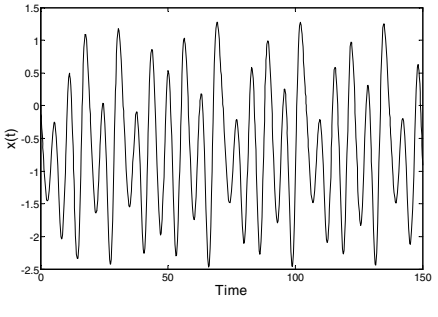


Fig. 3.2a The simplest piecewise linear chaotic time series, $x(t)$

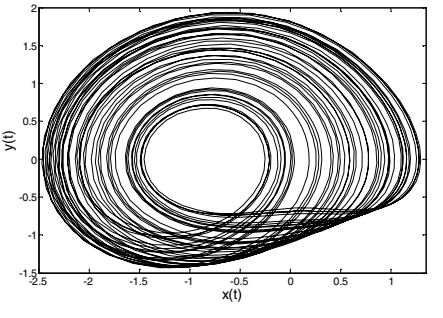


Fig. 3.2b The simplest piecewise linear strange attractor

signals are generated using identical equations to those of the master system except that the initial conditions are different. The '^' (hat) above the variable master signal is fully available to the slave system. The remaining two slave denotes the slave variable. The 'dot' above the variable denotes differentiation with respect to time.

In what follows, the synchronization properties of the system of Figure 3.3 are investigated with no noise in the system. The noise performance of the system such as that of Figure 3.3 is investigated in chapter 6. In chapter 6, a system is first cast into the form of a communication system and its noise performance investigated in terms of BER.

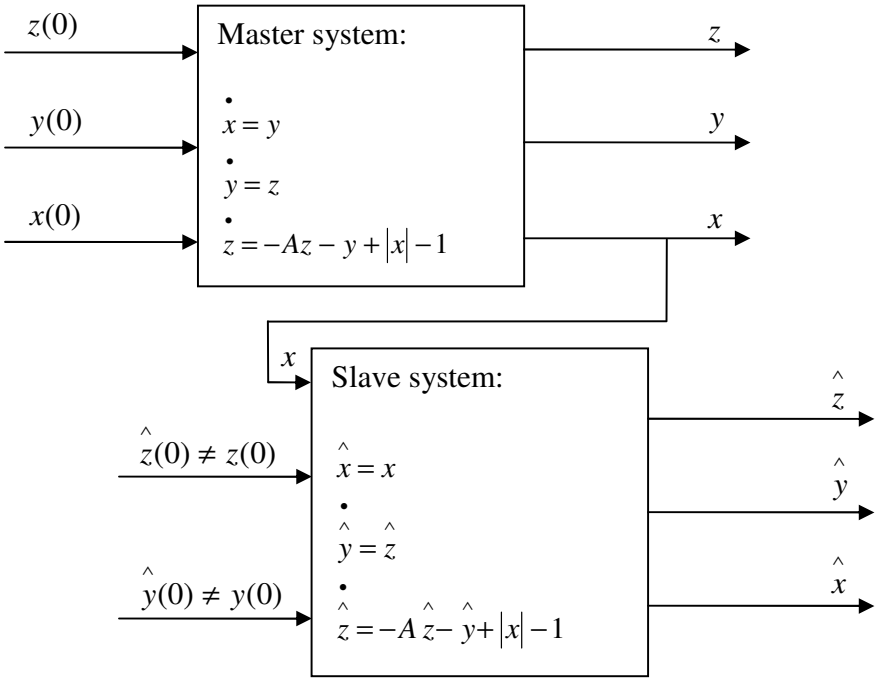


Fig. 3.3 The block diagram of the simplest piecewise linear master-slave chaotic flow, with the x signal driving. The parameter value: $A = 0.6$.

Let the difference among the non-driving master subsystem and the non-driven slave subsystem be denoted by '$*$'. When x drives this difference is given by equation 3.2.2:

$$\boldsymbol{v}^* = \boldsymbol{v} - \hat{\boldsymbol{v}} = \begin{bmatrix} y^* \\ z^* \end{bmatrix} = \begin{bmatrix} y - \hat{y} \\ z - \hat{z} \end{bmatrix} \tag{3.2.2}$$

From Figure 3.3 and equation 3.2.2 one obtains equations 3.2.3 and 3.2.4:

$$\dot{\boldsymbol{v}} = \begin{bmatrix} \dot{y} \\ \dot{z} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & -A \end{bmatrix} \begin{bmatrix} y \\ z \end{bmatrix} \tag{3.2.3}$$

$$\dot{\hat{\boldsymbol{v}}} = \begin{bmatrix} \dot{\hat{y}} \\ \dot{\hat{z}} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & -A \end{bmatrix} \begin{bmatrix} \hat{y} \\ \hat{z} \end{bmatrix} \tag{3.2.4}$$

Differentiating both sides of equation 3.2.2 it should be noted that $\dot{\boldsymbol{v}}^* = \dot{\boldsymbol{v}} - \dot{\hat{\boldsymbol{v}}}$. It is then readily verifiable that by subtracting equation 3.2.4 from equation 3.2.3, equation 3.2.5 is obtained:

$$\dot{\boldsymbol{v}}^* = \begin{bmatrix} \dot{y}^* \\ \dot{z}^* \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & -A \end{bmatrix} \begin{bmatrix} y^* \\ z^* \end{bmatrix} = B \begin{bmatrix} y^* \\ z^* \end{bmatrix} \tag{3.2.5}$$

The conditional Lyapunov exponents are defined as the real parts of the eigenvalues of the matrix *B* of equation 3.2.5. In the general case, provided that the matrix *B* is a constant matrix, that is, the subsystems are linear, the CLEs can be determined analytically. However if the matrix is not constant, that is, the subsystems are non-linear, one must resort to the numerical evaluation of the CLEs [11]. Let the eigenvalues of matrix *B* of equation 3.2.5 be denoted by λ_1 and λ_2. Then the two CLEs are determined by taking the real parts of the eigenvalues of the matrix *B*:

$$CLE_{1,2} = \mathrm{Re}\left\{ \left| \lambda I - B \right| = 0 \right\}$$

$$= \mathrm{Re}\left\{ \left\| \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} - \begin{bmatrix} 0 & 1 \\ -1 & -A \end{bmatrix} \right\| = 0 \right\}, \tag{3.2.6}$$

$$CLE_{1,2} = \mathrm{Re}\{\lambda_1, \lambda_2 = -0.3 \pm j0.954\}, \tag{3.2.7}$$

resulting in:

$$CLE_1 = CLE_2 = \mathrm{Re}\{\lambda_1\} = \mathrm{Re}\{\lambda_2\} - 0.3. \tag{3.2.8}$$

Therefore, as both CLEs are negative, theoretically the master-slave system of Figure 3.3 must synchronize. The numerical simulation, confirming the theoretical result of the equation 3.2.8 is shown in Figures 3.4a and 3.4b. The time series representation of Figure 3.4a demonstrates synchronization of the master-slave *y* and *z* signals by showing that the two master-slave signals merge. In addition, the phase space representation of Figure 3.4b, also demonstrates synchronization by showing that the two trajectories of the master and slave chaotic attractors merge.

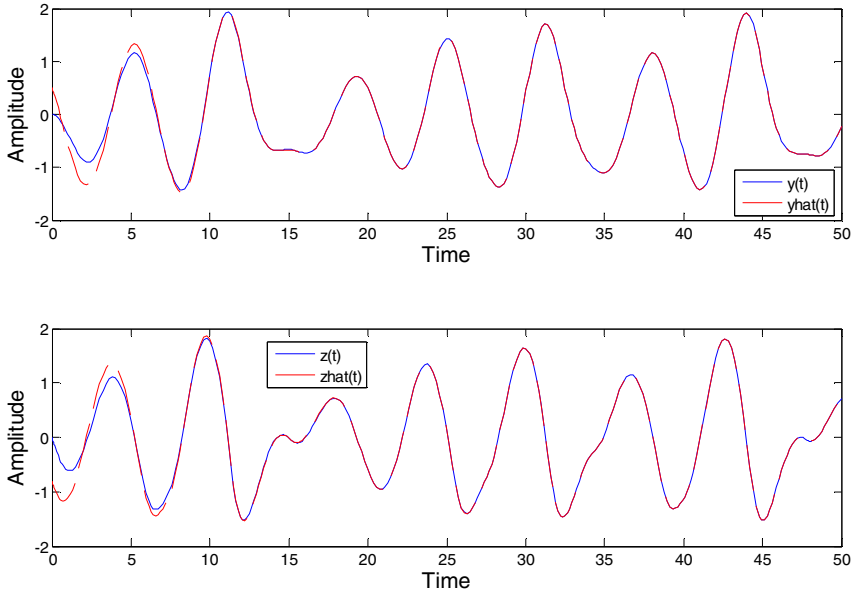


Fig. 3.4a Synchronization of the master-slave simplest piecewise linear chaotic signals, with the *x* signal driving.

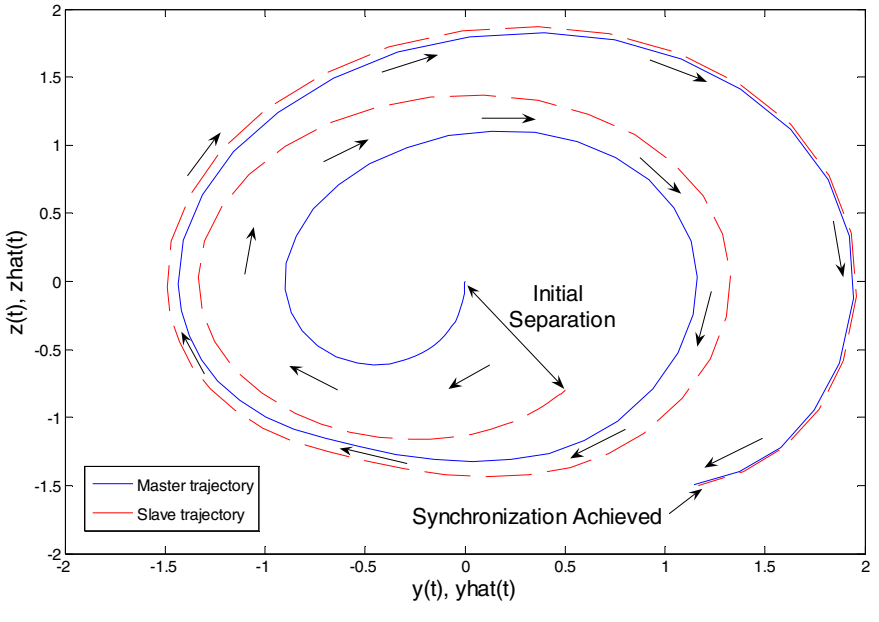


Fig. 3.4b Phase space representation of the synchronization of the master-slave simplest piecewise linear chaotic signals, with the *x* signal driving.

In [37] and chapter 5, Lyapunov's direct method is used to show that the simplest piecewise linear master-slave chaotic flow must synchronize when the master x signal drives.

3.3 Lyapunov's Direct Method and the Pecora-Carroll Chaotic Synchronization

In this subsection, the use of Lyapunov's direct method [40] is demonstrated. Asymptotic stability via Lyapunov's direct method is proven by finding the Lyapunov function and showing that its derivative is negative semi-definite. By definition, a Lyapunov function is a function which is positive definite except at the origin where it equals zero, and its derivative is negative semi-definite [43]. A function $E(t, x)$ is said to be positive semi-definite with respect to x if

$$E(t, 0) = 0 \qquad \text{and} \qquad E(t, x) \geq 0.$$

If $-E(t, x)$ is positive semi-definite with respect to x, then $E(t, x)$ is negative semi-definite with respect to x [40].

Consider the Chua chaotic system, given by equation 3.3.1:

$$\begin{aligned} \dot{x} &= \alpha(-x + y - f(x)) \\ \dot{y} &= x - y + z \\ \dot{z} &= -\beta y \end{aligned} \tag{3.3.1}$$

$$f(x) = bx + 0.5(a-b)(|x+1| - |x-1|)$$

The system described by equation 3.3.1, exhibits chaotic behaviour with the parameter values $\alpha = 10$, $\beta = 18$, $a = -4/3$, $b = -3/4$ [44]. Its dynamics are shown in Figure 3.5. By finding the Lyapunov function it is now shown that the Chua master-slave system of Figure 3.6 must synchronize when x drives.

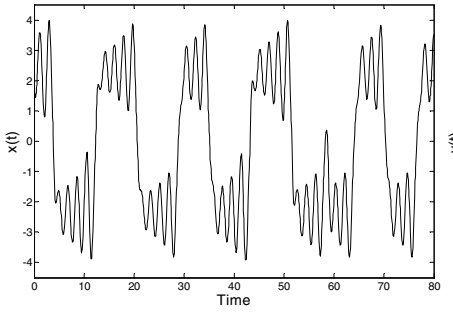


Fig. 3.5a The Chua chaotic time series, $x(t)$

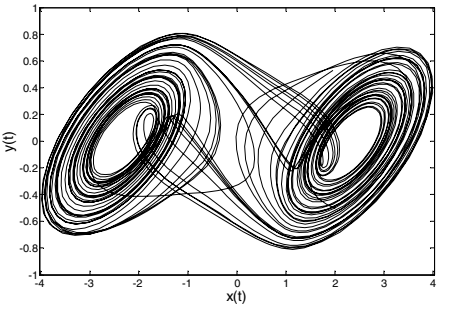


Fig. 3.5b The Chua strange attractor

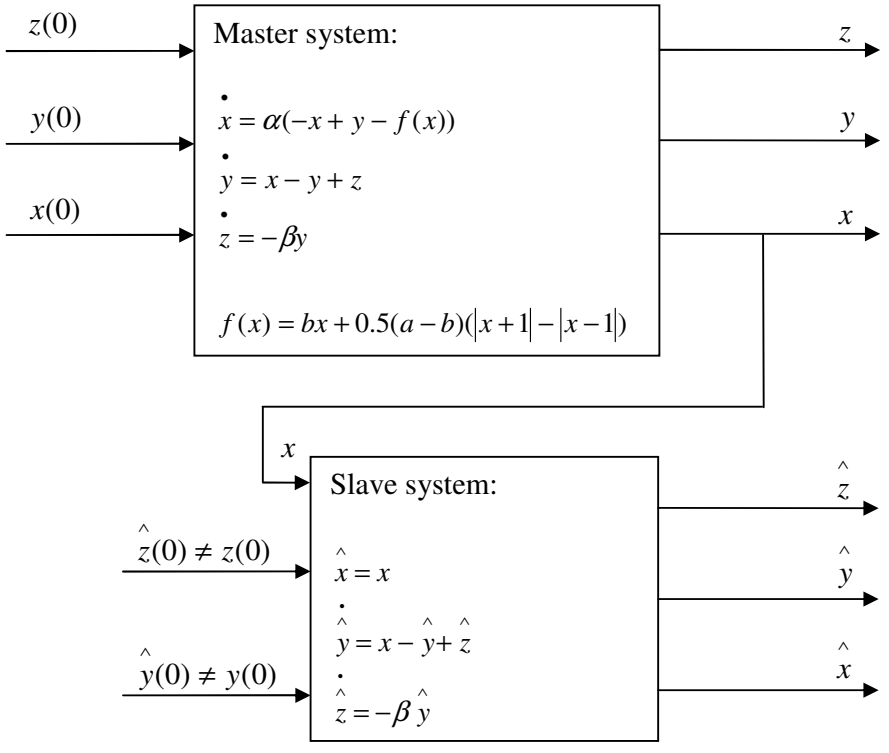


Fig. 3.6 The block diagram of the Chua master-slave chaotic system, with the x signal driving. The parameter values: $\alpha = 10$, $\beta = 18$, $a = -4/3$, $b = -3/4$.

As in the previous section the difference between the non-driving master subsystem and the non-driven slave subsystem is denoted by '*' and when x drives is given by equation 3.3.2:

$$\boldsymbol{v}^* = \boldsymbol{v} - \hat{\boldsymbol{v}} = \begin{bmatrix} y^* \\ z^* \end{bmatrix} = \begin{bmatrix} y - \hat{y} \\ z - \hat{z} \end{bmatrix} \tag{3.3.2}$$

The differential error is then expressed by equation 3.3.3 [37]:

$$\dot{\boldsymbol{v}}^* = \begin{bmatrix} \dot{y}^* \\ \dot{z}^* \end{bmatrix} = \begin{bmatrix} -1 & 1 \\ -\beta & 0 \end{bmatrix} \begin{bmatrix} y^* \\ z^* \end{bmatrix} \tag{3.3.3}$$

Now consider the Lyapunov function given by equation 3.3.4:

$$E = \frac{1}{2}((\beta y^* - z^*)^2 + \beta y^{*2} + (1+\beta) z^{*2}) \tag{3.3.4}$$

Differentiating equation 3.3.4 with respect to time, equation 3.3.5 is obtained:

$$\dot{E} = (\beta y^* - z^*)(\beta \dot{y}^* - \dot{z}^*) + \beta y^* \dot{y}^* + (1+\beta) z^* \dot{z}^* \quad (3.3.5)$$

From equation 3.3.3, equations 3.3.6a and 3.3.6b are derived:

$$\dot{y}^* = (\dot{y} - \dot{\hat{y}}) = -y^* + z^* \quad (3.3.6a)$$

$$\dot{z}^* = (\dot{z} - \dot{\hat{z}}) = -\beta y^* \quad (3.3.6b)$$

Substituting equations 3.3.6a and 3.3.6b into equation 3.3.5, equation 3.3.7 is obtained:

$$\dot{E} = -\beta y^{*2} - \beta z^{*2} = -\beta(y^{*2} + z^{*2}) = -\beta((y - \hat{y})^2 + (z - \hat{z})^2) \le 0 \quad (3.3.7)$$

As the derivative of the Lyapunov function, shown in equation 3.3.7, is always less than zero, the subsystem $\hat{v}$ is asymptotically stable (the equality sign applies only at the origin) i.e. equation 3.3.7 is negative semi-definite. Therefore, as the necessary and sufficient condition for synchronization is satisfied, theoretically the system of Figure 3.6 must synchronize. The numerical simulation, confirming the theoretical result of equation 3.3.7 is shown in Figures 3.7a and 3.7b. The time series representation of Figure 3.7a, and the corresponding phase space representation of Figure 3.7b, demonstrates synchronization by showing that the master-slave trajectories merge.

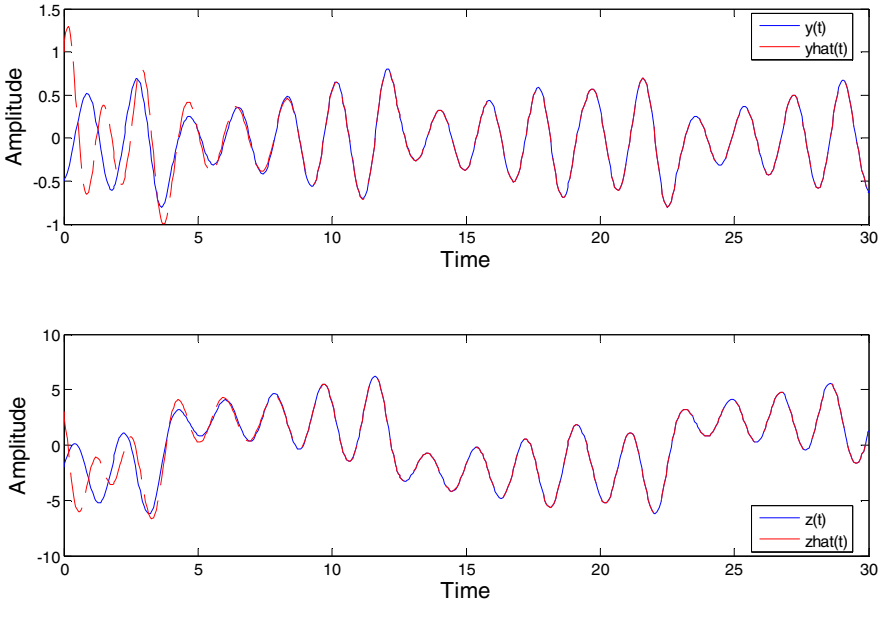


Fig. 3.7a Synchronization of the master-slave Chua chaotic signals, with the x signal driving.

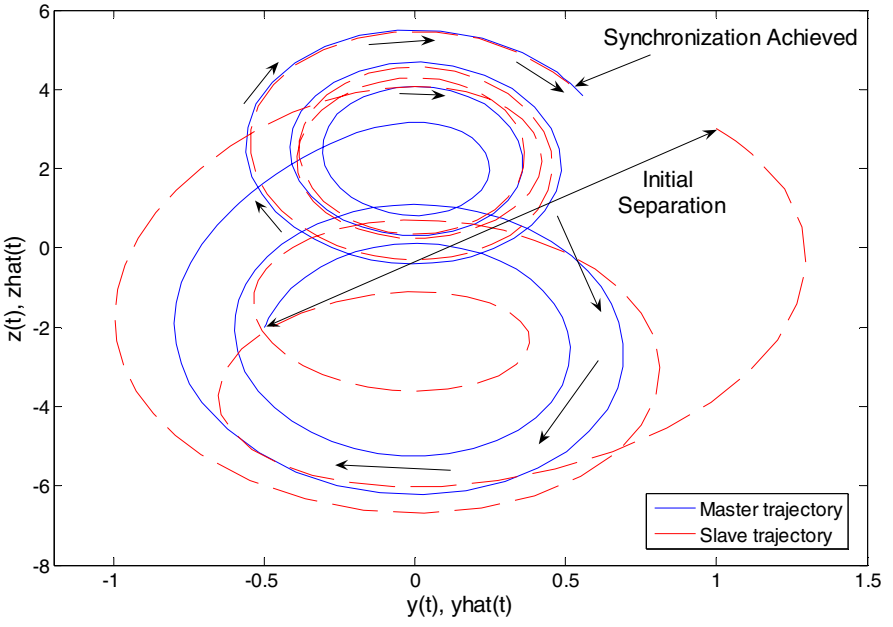


Fig. 3.7b Phase space representation of the synchronization of the master-slave Chua chaotic signals, with the *x* signal driving.

The PC chaotic synchronization properties of the Chua master-slave system have been examined in [11] in terms of the CLEs. The synchronization properties of the Chua chaotic system have been investigated by a number of researchers [11,45,9,26].

3.4 Synchronization of Chaotic Flows via Lyapunov's Direct Method

Sections 3.1-3.3 considered the chaotic synchronization concept when a single signal of the master system was supplied to the slave system. The general result of this is that the master-slave system either synchronizes or does not [3,7,37]. In this section the design of the nonlinear controllers for the chaotic flow master-slave systems is presented [26,46]. In particular the linear feedback rigid body motion (LFRBM), and the Rabinovich-Fabrikant chaotic systems are investigated. In this way, the nonlinear controller design is demonstrated on the system with relatively simple dynamical equations (LFRBM) and the system with more complex dynamical equations (Rabinovich-Fabrikant), thus showing the versatility of this

method. These controllers then ensure the synchronization among the master-slave systems. The design is via the Lyapunov's direct method, that is, Lyapunov's function is used to design the nonlinear control laws [46]. The nonlinear controller design for the chaotic synchronization of maps is studied in the next chapter.

3.4.1 The Linear Feedback Rigid Body Motion (LFRBM) Chaotic System

The LFRBM system [47] is given by equation 3.4.1:

$$\begin{aligned} \dot{x} &= -0.4x + y + 10yz \\ \dot{y} &= -x - 0.4y + 5xz \\ \dot{z} &= \alpha z - 5xy \end{aligned} \tag{3.4.1}$$

With the parameter $\alpha = 0.175$ the system is chaotic. Figures 3.8a and 3.8b show the time series and the chaotic attractor, respectively.

The design procedure of the synchronizing nonlinear control laws, using the LFRBM master-slave chaotic system as an example, is now explained. Let the error be defined by equations 3.4.2a, 3.4.2b and 3.4.2c:

$$e_1(t) = \hat{x}(t) - x(t) \tag{3.4.2a}$$

$$e_2(t) = \hat{y}(t) - y(t) \tag{3.4.2b}$$

$$e_3(t) = \hat{z}(t) - z(t) \tag{3.4.2c}$$

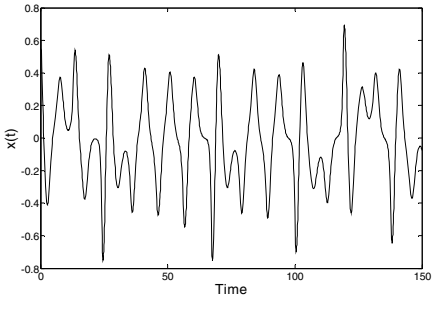


Fig. 3.8a The LFRBM chaotic time series, $x(t)$

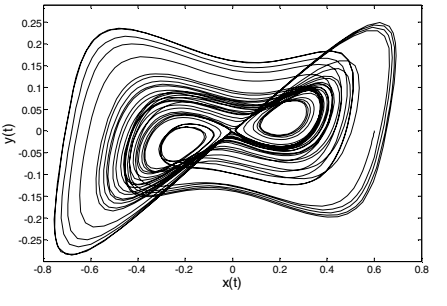


Fig. 3.8b The LFRBM strange attractor plotted in two dimensions

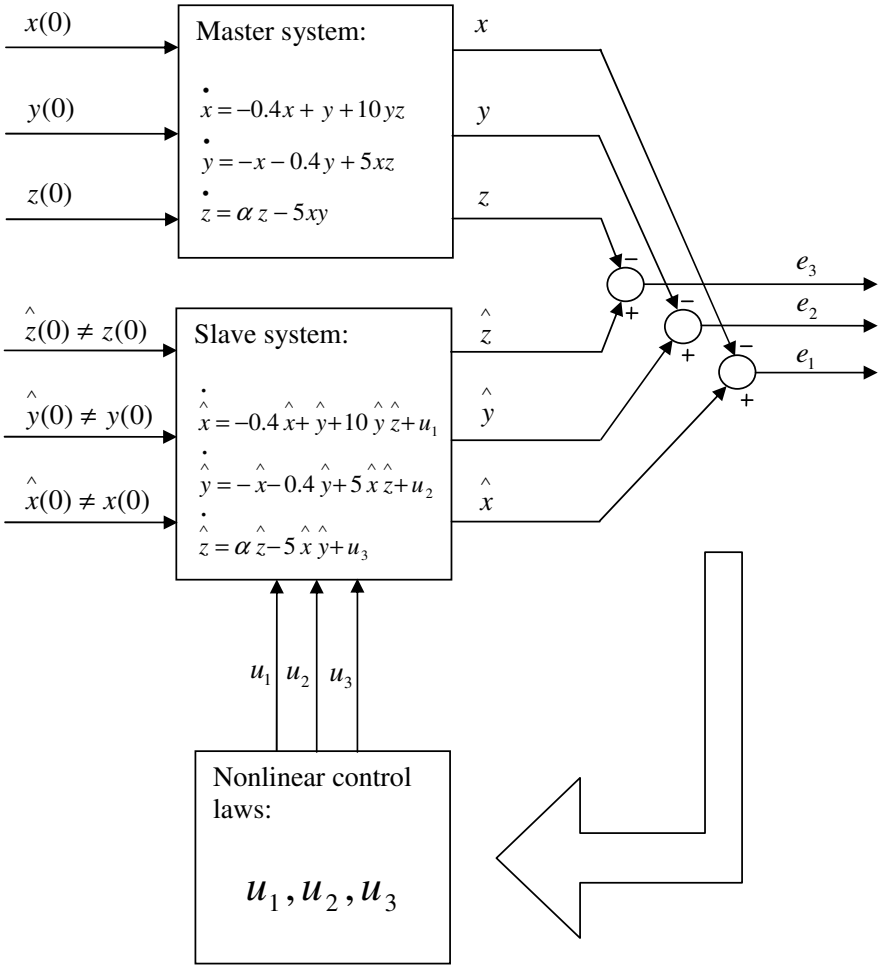


Fig. 3.9 The LFRBM master-slave chaotic system. Note: $\alpha = 0.175$.

In general terms the LFRBM master-slave chaotic system can be represented by Figure 3.9. Keeping in mind equation 3.4.2 the differential error, (the error system), can then be represented by equation 3.4.3:

$$\begin{aligned}
\dot{e}_1 &= \dot{\hat{x}} - \dot{x} = -0.4e_1 + e_2 + 10\hat{y}\hat{z} - 10yz + u_1 \\
\dot{e}_2 &= \dot{\hat{y}} - \dot{y} = -e_1 - 0.4e_2 + 5\hat{x}\hat{z} - 5xz + u_2 \\
\dot{e}_3 &= \dot{\hat{z}} - \dot{z} = \alpha e_3 - 5\hat{x}\hat{y} + 5xy + u_3
\end{aligned} \tag{3.4.3}$$

Equation 3.4.3 can also be represented in terms of error of equation 3.4.2 by equation 3.4.5, keeping in mind the identities of equation 3.4.4:

$$\begin{aligned}
&\hat{y}\hat{z} - yz = ze_2 + \hat{y}e_3 \\
&\hat{x}\hat{z} - xz = ze_1 + \hat{x}e_3 \\
&-\hat{x}\hat{y} + xy = -ye_1 - \hat{x}e_2
\end{aligned} \tag{3.4.4}$$

$$\begin{aligned}
\dot{e}_1 &= \dot{\hat{x}} - \dot{x} = -0.4e_1 + e_2 + 10ze_2 + 10\hat{y}e_3 + u_1 \\
\dot{e}_2 &= \dot{\hat{y}} - \dot{y} = -e_1 - 0.4e_2 + 5ze_1 + 5\hat{x}e_3 + u_2 \\
\dot{e}_3 &= \dot{\hat{z}} - \dot{z} = \alpha\, e_3 - 5ye_1 - 5\hat{x}e_2 + u_3
\end{aligned} \tag{3.4.5}$$

Consider the candidate Lyapunov function given by equation 3.4.6:

$$V = \frac{1}{2}(e_1^2 + e_2^2 + e_3^2) \tag{3.4.6}$$

Differentiating equation 3.4.6 with respect to time, equation 3.4.7 is obtained:

$$\dot{V} = \dot{e}_1 e_1 + \dot{e}_2 e_2 + \dot{e}_3 e_3 \tag{3.4.7}$$

Substituting equation 3.4.5 into equation 3.4.7, and simplifying, equation 3.4.9 is obtained:

$$\begin{aligned}
\dot{V} = &-0.4e_1^2 + e_1e_2 + 10ze_1e_2 + 10\hat{y}e_1e_3 + e_1u_1 \\
&- e_1e_2 - 0.4e_2^2 + 5ze_1e_2 + 5\hat{x}e_2e_3 + e_2u_2 \\
&+ \alpha e_3^2 - 5ye_1e_3 - 5\hat{x}e_2e_3 + e_3u_3
\end{aligned} \tag{3.4.8}$$

$$\begin{aligned}
\dot{V} = &-0.4e_1^2 - 0.4e_2^2 + \alpha e_3^2 + 15ze_1e_2 + 10\hat{y}e_1e_3 - 5ye_1e_3 \\
&+ e_1u_1 + e_2u_2 + e_3u_3
\end{aligned} \tag{3.4.9}$$

For equation 3.4.6 to be a Lyapunov function, equation 3.4.9 must be negative semi-definite. In order for equation 3.4.9 to be negative semi-definite, the terms: αe_3^2, $15ze_1e_2$, $10\hat{y}e_1e_3$ and $-5ye_1e_3$, must be eliminated, and the term $-e_3^2$ must be introduced. The control laws u_1, u_2 and u_3 are designed in such a manner to eliminate the unwanted terms, and introduce the missing necessary terms. The control laws are given by equations 3.4.11, 3.4.13 and 3.4.16.

The design of the first control law u_1:

$$e_1u_1 + 10\hat{y}e_1e_3 - 5ye_1e_3 = 0 \tag{3.4.10}$$

$$u_1 = -5e_3(2\hat{y} - y) = -5e_3(2e_2 + y) \tag{3.4.11}$$

The design of the second control law u_2:

$$e_2u_2 + 15ze_1e_2 = 0 \tag{3.4.12}$$

$$u_2 = -15ze_1 \tag{3.4.13}$$

The design of the third control law u_3:

$$e_3u_3 + \alpha e_3^2 = 0 \tag{3.4.14}$$

$$u_3 = -\alpha e_3 \tag{3.4.15}$$

Besides the requirement for the control law u_3 to eliminate the term αe_3^2, it shall also be used to introduce the term $-e_3^2$, that is, the term $-ke_3^2$ where k is a positive constant acting as the control parameter. Therefore, equation 3.4.16 is obtained:

$$u_3 = -(\alpha + k)e_3 \tag{3.4.16}$$

It should be pointed out that the introduction of the control parameter *k*, within the third control law u_3 of equation 3.4.16, is optional. This control parameter is usually fixed at 1, however, any other number greater than 0 can be used, for synchronization to be achieved. The block diagram of this master-slave synchronization system is given in Figure 3.10.

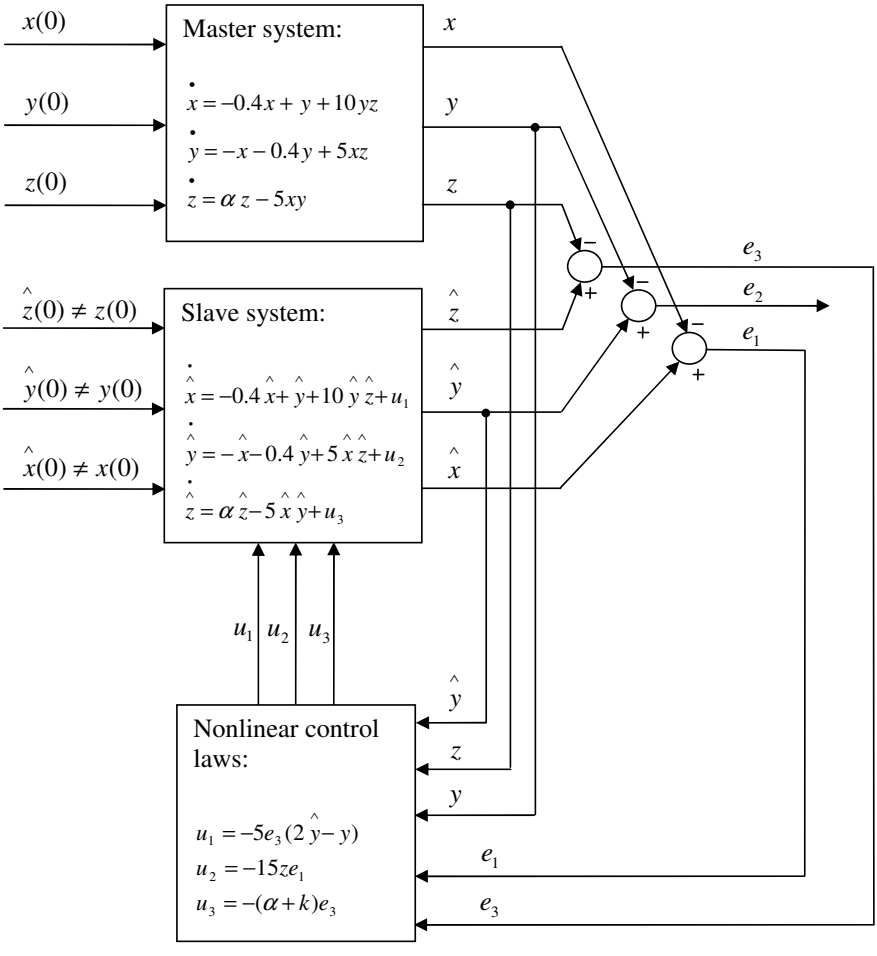


Fig. 3.10 The LFRBM master-slave chaotic system, where: $\alpha = 0.175$.

The functionality of the control laws, given by equations 3.4.11, 3.4.13 and 3.4.16, is demonstrated in Figures 3.11a, 3.11b and 3.11c, when k = 1. From Figure 3.11b it can be seen that the synchronization error for all three master-slave chaotic signals tends to zero. This has also been demonstrated in phase space in Figure 3.11c by showing that the trajectories of the master and slave chaotic attractors merge. Note that when k is negative, for instance k = -0.3, the master-slave system does not synchronize, as Figures 3.12a, 3.12b and 3.12c demonstrate.

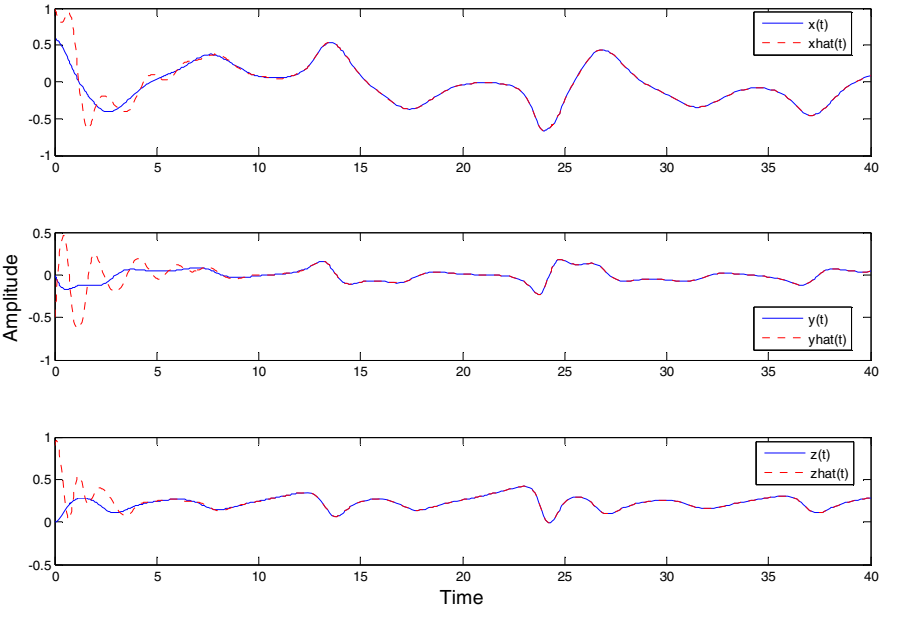


Fig. 3.11a Synchronization of the LFRBM master-slave chaotic signals when $k = 1$

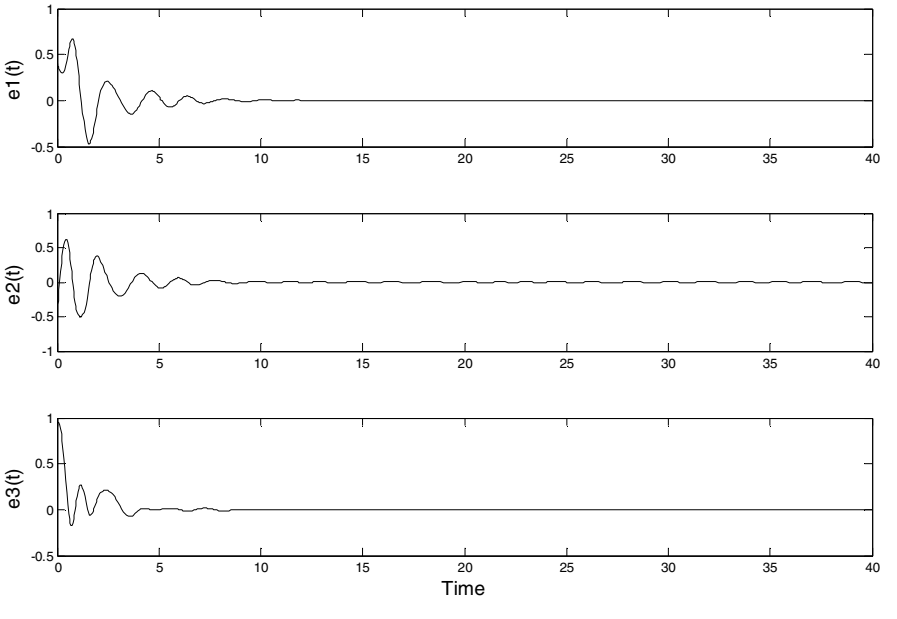


Fig. 3.11b Synchronization error of the LFRBM master-slave chaotic signals when $k = 1$

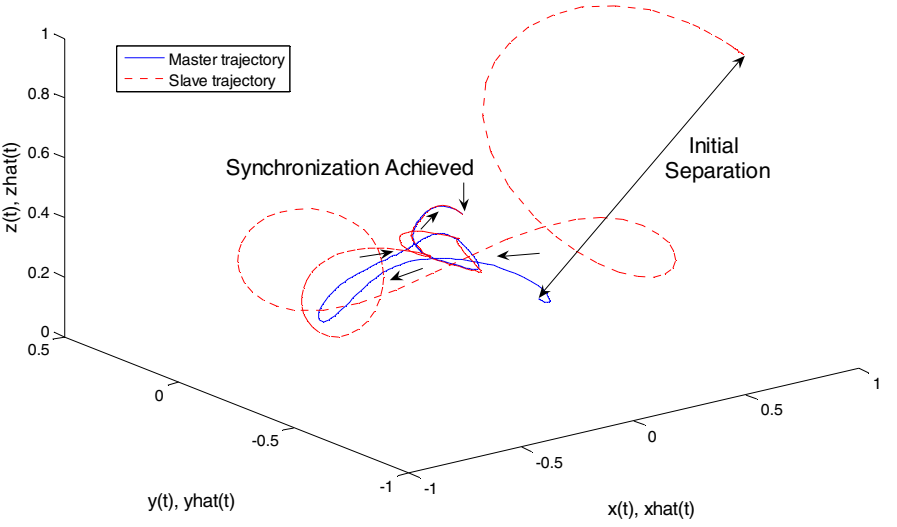


Fig. 3.11c Phase space representation of the synchronization of the master-slave LFRBM chaotic signals when k = 1

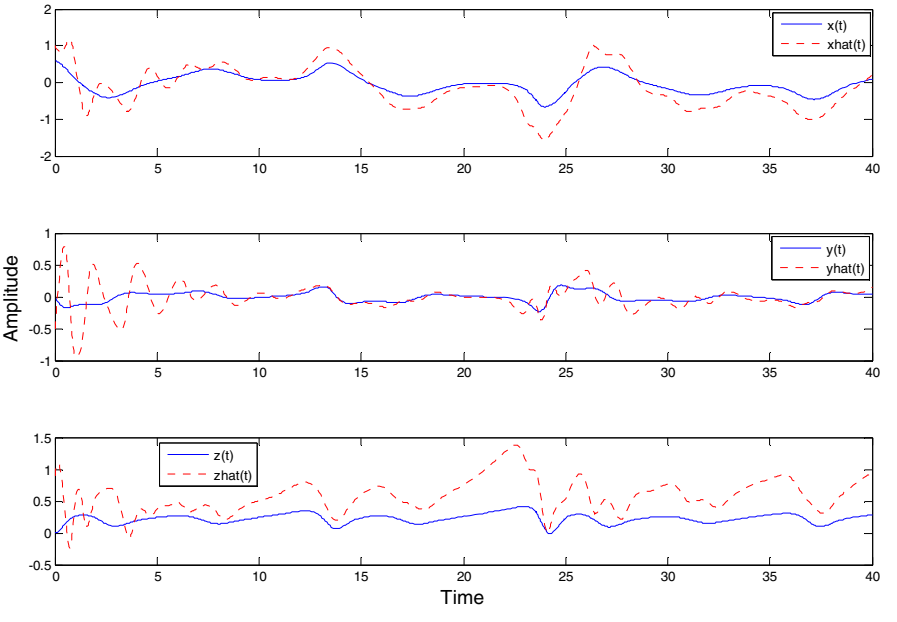


Fig. 3.12a Synchronization of the LFRBM master-slave chaotic signals when k = -0.3

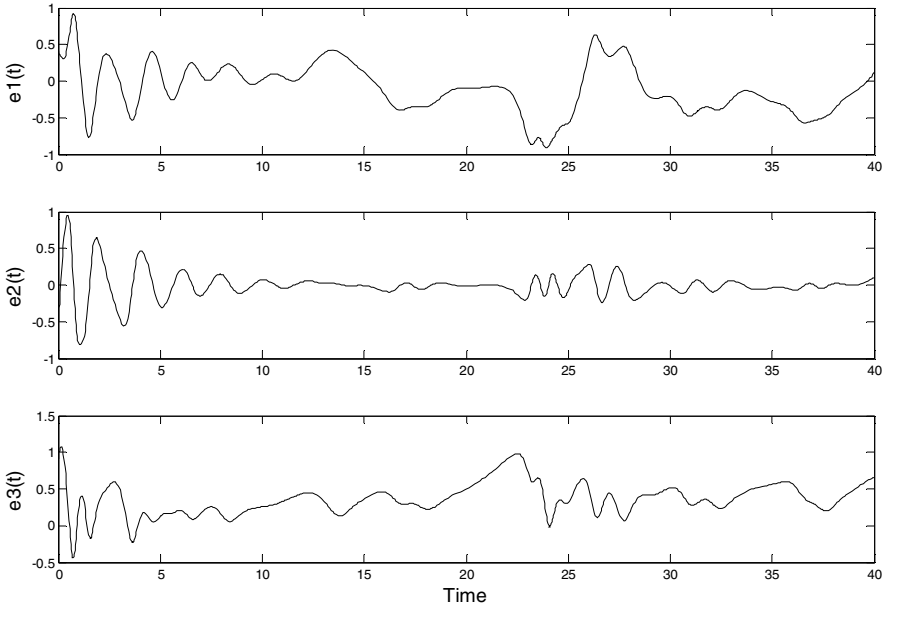


Fig. 3.12b Synchronization error of the LFRBM master-slave chaotic signals when k = -0.3

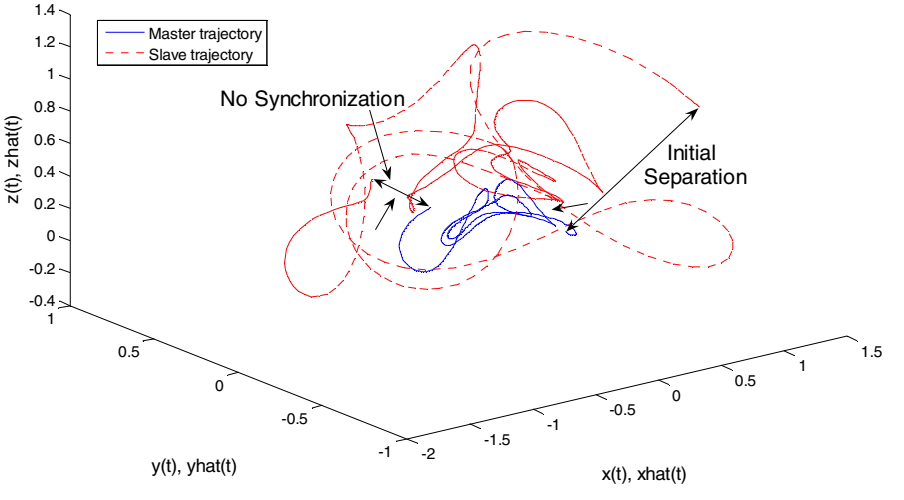


Fig. 3.12c Phase space representation of the synchronization of the master-slave LFRBM chaotic signals when k = -0.3

3.4.2 The Rabinovich-Fabrikant Chaotic System

In this subsection, the nonlinear controller design is demonstrated on the Rabinovich-Fabrikant chaotic system whose dynamical equations are significantly more complex than those of the LFRBM chaotic system. In this way, the versatility of the nonlinear controller design using the Lyapunov's stability theory via Lyapunov's direct method is demonstrated. The Rabinovich-Fabrikant chaotic system is given by equation 3.4.17 [48,42]:

$$\begin{aligned} \dot{x} &= y(z-1+x^2)+\gamma x \\ \dot{y} &= x(3z+1-x^2)+\gamma y \\ \dot{z} &= -2z(\alpha+xy) \end{aligned} \tag{3.4.17}$$

With the parameter $\alpha = 1.1$ and $\gamma = 0.87$ the system is chaotic. Figures 3.13a and 3.13b show the time series and the chaotic attractor, respectively.

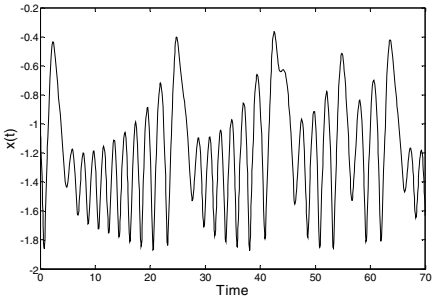


Fig. 3.13a The Rabinovich-Fabrikant chaotic time series, $x(t)$

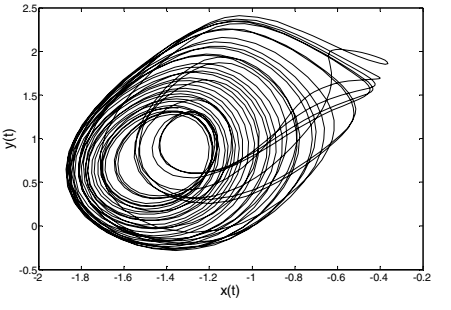


Fig. 3.13b The Rabinovich-Fabrikant strange attractor plotted in two dimensions

Again, let the error of the master-slave system be defined by equations 3.4.18a, 3.4.18b and 3.4.18c:

$$e_1(t) = \hat{x}(t) - x(t) \tag{3.4.18a}$$

$$e_2(t) = \hat{y}(t) - y(t) \tag{3.4.18b}$$

$$e_3(t) = \hat{z}(t) - z(t) \tag{3.4.18c}$$

Expanding equation 3.4.17 and keeping in mind equation 3.4.18, the Rabinovich-Fabrikant master-slave chaotic system can be represented by Figure 3.14. The design procedure of the synchronizing nonlinear control laws, for the Rabinovich-Fabrikant master-slave chaotic system of Figure 3.14, is now explained.

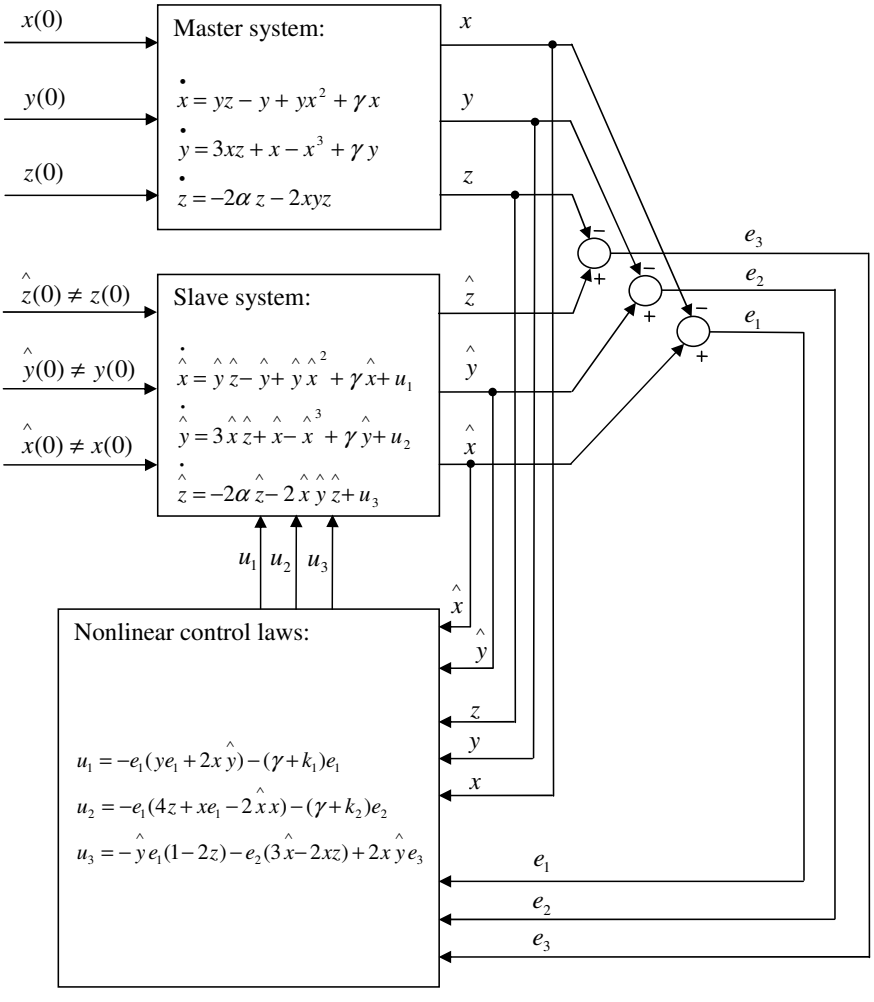


Fig. 3.14 The Rabinovich-Fabrikant master-slave system, where: $\alpha = 1.1$ and $\gamma = 0.87$.

The differential error, the error system, can then be represented by equation 3.4.19:

$$\begin{aligned}
\dot{e}_1 &= \dot{\hat{x}} - \dot{x} = \hat{y}\hat{z} - yz - e_2 + \hat{y}\hat{x}^2 - yx^2 + \gamma e_1 + u_1 \\
\dot{e}_2 &= \dot{\hat{y}} - \dot{y} = 3\hat{x}\hat{z} - 3xz + e_1 - \hat{x}^3 + x^3 + \gamma e_2 + u_2 \\
\dot{e}_3 &= \dot{\hat{z}} - \dot{z} = -2\alpha e_3 - 2\hat{x}\hat{y}\hat{z} + 2xyz + u_3
\end{aligned} \tag{3.4.19}$$

The equation 3.4.19 can also be represented by equation 3.4.21, keeping in mind the identities of equation 3.4.20:

$$\hat{y}\hat{z} - yz = ze_2 + \hat{y}e_3$$

$$\hat{y}\hat{x}^2 - yx^2 = \hat{y}e_1^2 + 2x\hat{y}e_1 + x^2e_2 = \hat{y}e_1(\hat{x} + x) + x^2e_2$$

$$3\hat{x}\hat{z} - 3xz = 3ze_1 + 3\hat{x}e_3$$

$$-\hat{x}^3 + x^3 = -e_1^3 - 3x\hat{x}e_1$$

$$-2\hat{x}\hat{y}\hat{z} + 2xyz = -2ze_1e_2 - 2\hat{y}e_1e_3 - 2xe_2e_3 - 2xye_3 - 2xze_2 - 2yze_1 \tag{3.4.20}$$

$$\dot{e}_1 = \dot{\hat{x}} - \dot{x} = ze_2 + \hat{y}e_3 - e_2 + \hat{y}e_1^2 + 2x\hat{y}e_1 + x^2e_2 + \gamma e_1 + u_1$$

$$\dot{e}_2 = \dot{\hat{y}} - \dot{y} = 3ze_1 + 3\hat{x}e_3 + e_1 - e_1^3 - 3x\hat{x}e_1 + \gamma e_2 + u_2$$

$$\dot{e}_3 = \dot{\hat{z}} - \dot{z} = -2\alpha e_3 - 2ze_1e_2 - 2\hat{y}e_1e_3 - 2xe_2e_3 - 2xye_3 - 2xze_2 - 2yze_1 + u_3 \tag{3.4.21}$$

Consider the candidate Lyapunov function given by equation 3.4.22:

$$V = \frac{1}{2}(e_1^2 + e_2^2 + e_3^2) \tag{3.4.22}$$

Differentiating equation 3.4.22 with respect to time equation 3.4.23 is obtained:

$$\dot{V} = \dot{e}_1 e_1 + \dot{e}_2 e_2 + \dot{e}_3 e_3 \tag{3.4.23}$$

Substituting equation 3.4.21 into equation 3.4.23 and simplifying, equation 3.4.25 is obtained:

$$\begin{aligned}\dot{V} = {} & ze_1e_2 + \hat{y}e_1e_3 - e_1e_2 + \hat{y}e_1^3 + 2x\hat{y}e_1^2 + x^2e_1e_2 + \gamma e_1^2 + e_1u_1 \\ & + 3ze_1e_2 + 3\hat{x}e_2e_3 + e_1e_2 - e_1^3e_2 - 3x\hat{x}e_1e_2 + \gamma e_2^2 + e_2u_2 \\ & - 2\alpha e_3^2 - 2ze_1e_2e_3 - 2\hat{y}e_1e_3^2 - 2xe_2e_3^2 - 2xye_3^2 - 2xze_2e_3 - 2yze_1e_3 + e_3u_3\end{aligned} \tag{3.4.24}$$

$$\begin{aligned}\dot{V} = {} & \hat{y}e_1e_3(1-2z) + e_1e_2(4z + xe_1 - 2\hat{x}x) + ye_1^3 + e_2e_3(3\hat{x} - 2xz) \\ & - 2x\hat{y}e_3^2 + 2x\hat{y}e_1^2 + \gamma e_1^2 + \gamma e_2^2 - 2\alpha e_3^2 + e_1u_1 + e_2u_2 + e_3u_3\end{aligned} \tag{3.4.25}$$

For equation 3.4.22 to be the Lyapunov function, equation 3.4.25 must be negative semi definite. In order for the function of equation 3.4.25 to be negative semi definite all its terms, except the term $-2\alpha e_3^2$, must be eliminated. Also, for it to be negative semi definite, the terms $-e_1^2$ and $-e_2^2$ must be introduced. The control laws u_1, u_2 and u_3 are designed in such a manner to eliminate the unwanted terms, and introduce the missing necessary terms. The control laws are given by equations 3.4.28, 3.4.31 and 3.4.33.

The design of the first control law u_1:

$$e_1 u_1 + y e_1^3 + 2x\hat{y} e_1^2 + \gamma e_1^2 = 0 \tag{3.4.26}$$

$$u_1 = -y e_1^2 - 2x\hat{y} e_1 - \gamma e_1 \tag{3.4.27}$$

Besides the requirement for the control law u_1 to eliminate the terms ye_1^3, $2x\hat{y}e_1^2$ and γe_1^2 it shall also be used to introduce the term $-e_1^2$, that is, the term $-k_1 e_1^2$ where k_1 is a positive constant acting as the control parameter. Therefore, equation 3.4.28 is obtained:

$$u_1 = -e_1(ye_1 + 2x\hat{y}) - (\gamma + k_1)e_1 \tag{3.4.28}$$

The design of the second control law u_2:

$$e_2 u_2 + e_1 e_2(4z + xe_1 - 2\hat{x}x) + \gamma e_2^2 = 0 \tag{3.4.29}$$

$$u_2 = -e_1(4z + xe_1 - 2\hat{x}x) - \gamma e_2 \tag{3.4.30}$$

Besides the requirement for the control law u_2 to eliminate the terms $e_1 e_2(4z + xe_1 - 2\hat{x}x)$ and γe_2^2, it shall also be used to introduce the term $-e_2^2$, that is, the term $-k_2 e_2^2$ where k_2 is a positive constant acting as the control parameter. Therefore equation 3.4.31 is obtained:

$$u_2 = -e_1(4z + xe_1 - 2\hat{x}x) - (\gamma + k_2)e_2 \tag{3.4.31}$$

The design of the third control law u_3:

$$e_3 u_3 + \hat{y} e_1 e_3(1 - 2z) + e_2 e_3(3\hat{x} - 2xz) - 2x\hat{y} e_3^2 = 0 \tag{3.4.32}$$

$$u_3 = -\hat{y} e_1(1 - 2z) - e_2(3\hat{x} - 2xz) + 2x\hat{y} e_3 \tag{3.4.33}$$

The control parameters k_1 and k_2 can be fixed at 1, or any other number greater than 0. They are left to be adjusted as they do not introduce any extra complexity to the control laws u_1 and u_2. The control law u_3, of equation 3.4.33, could also include the control parameter, however in this case it would introduce extra complexity without any need for it. The control laws of equations 3.4.28, 3.4.31 and 3.4.33 are shown within the control unit of the master-slave system of Figure 3.14.

The functionality of the control laws, given by equations 3.4.28, 3.4.31 and 3.4.33, is demonstrated in Figures 3.15a, 3.15b and 3.15c, when $k_1 = 1$ and $k_2 = 1$. From Figure 3.15b it can be seen that the synchronization error for all three master-slave chaotic signals tends to zero. This has also been demonstrated in phase space in Figure 3.15c by showing that the trajectories of the master and slave chaotic attractors merge. When, for instance, the control parameters are negative: $k_1 = k_2 = -0.6$, the master-slave system does not synchronize, as Figures 3.16a, 3.16b and 3.16c demonstrate.

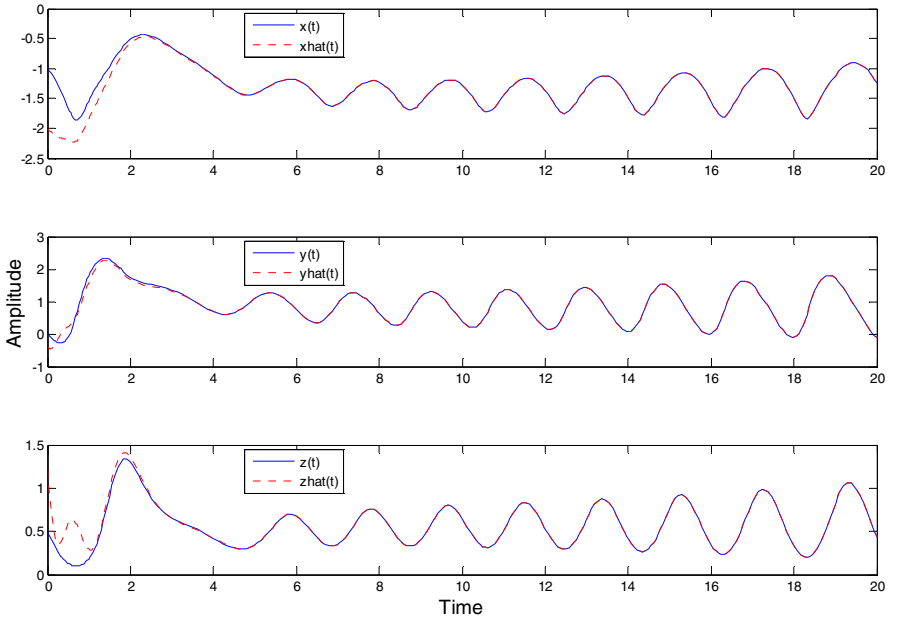


Fig. 3.15a Synchronization of the Rabinovich-Fabrikant master-slave chaotic signals when $k_1 = k_2 = 1$

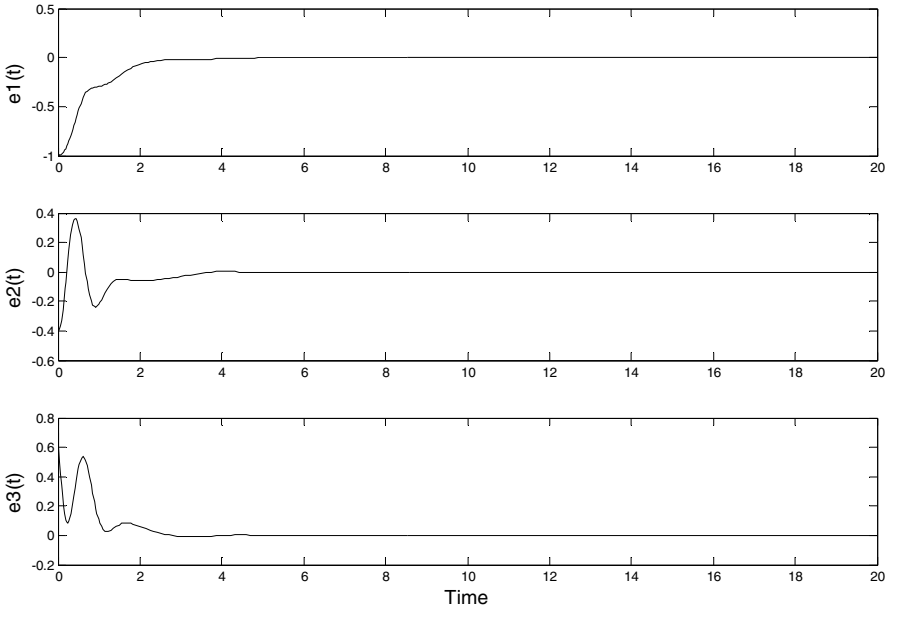


Fig. 3.15b Synchronization error of the Rabinovich-Fabrikant master-slave chaotic signals when $k_1 = k_2 = 1$

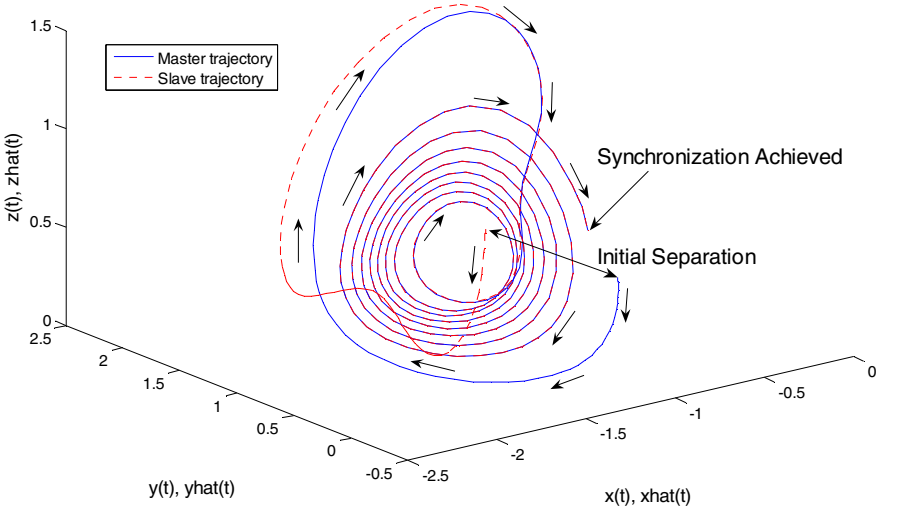


Fig. 3.15c Phase space representation of the synchronization of the master-slave Rabinovich-Fabrikant chaotic signals when $k_1 = k_2 = 1$

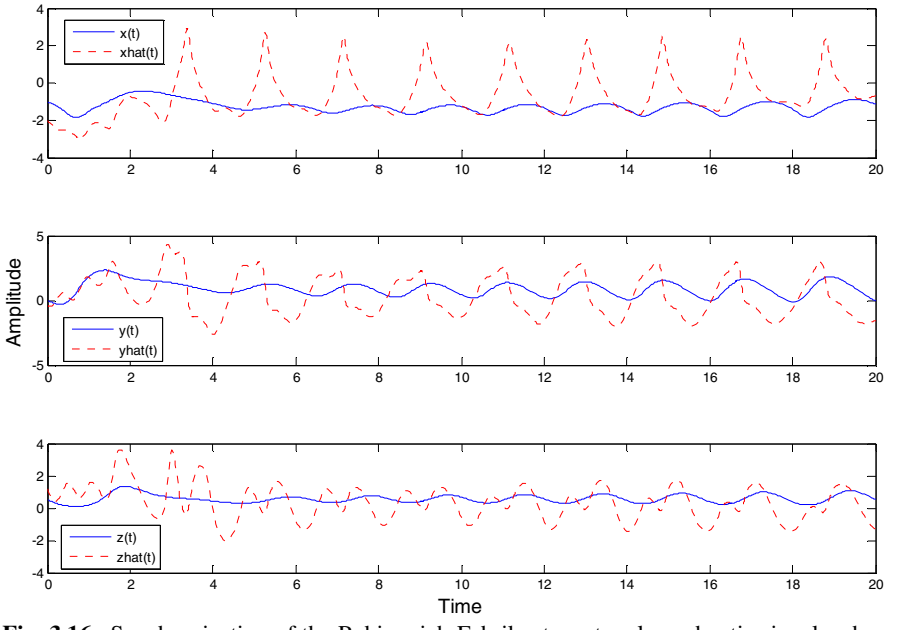


Fig. 3.16a Synchronization of the Rabinovich-Fabrikant master-slave chaotic signals when $k_1 = k_2 = -0.6$

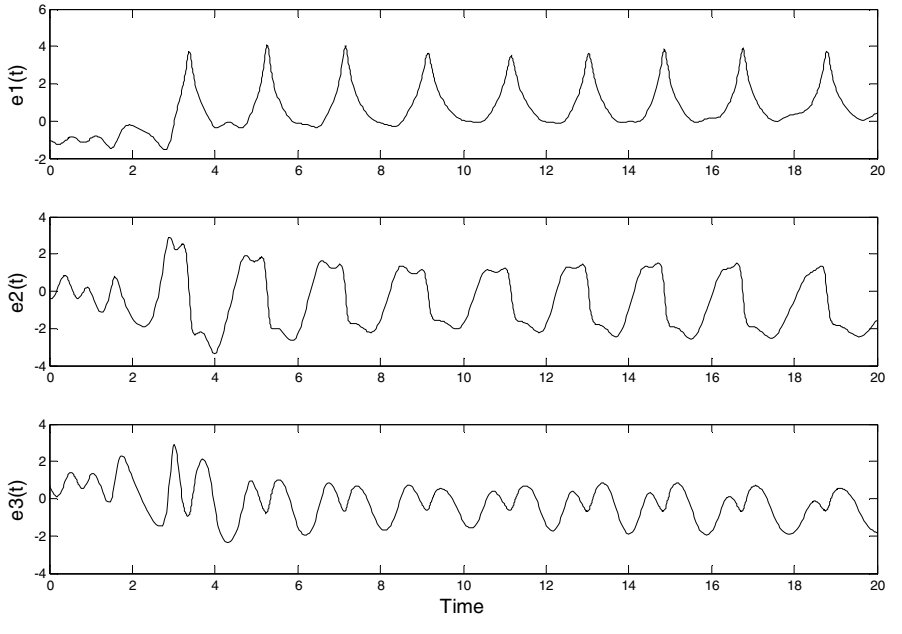


Fig. 3.16b Synchronization error of the Rabinovich-Fabrikant master-slave chaotic signals when $k_1 = k_2 = -0.6$

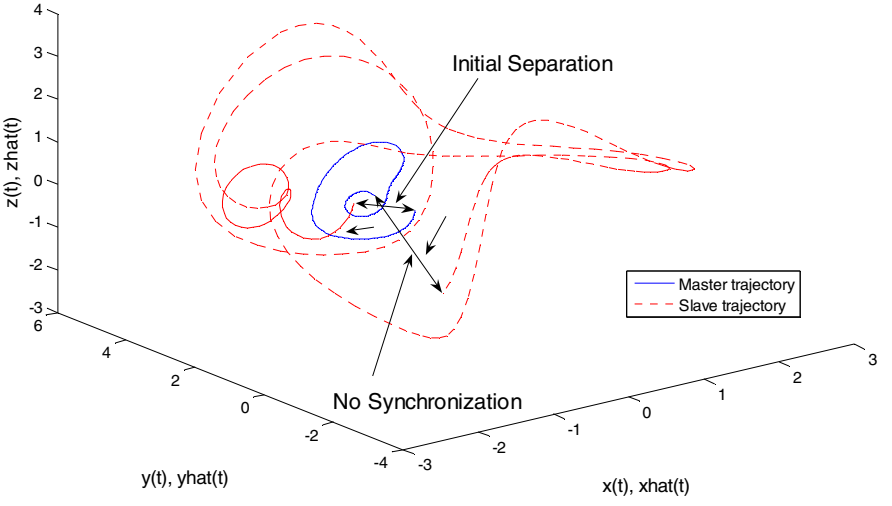


Fig. 3.16c Phase space representation of the synchronization of the master-slave Rabinovich-Fabrikant chaotic signals when $k_1 = k_2 = -0.6$

3.5 Conclusion

The apparent random behaviour, high sensitivity to parameter and initial condition perturbations and the broadband nature of chaotic systems originally led to the belief that they cannot be synchronized. In this chapter, synchronization of chaotic systems has been examined. The concept of the Pecora-Carroll chaotic synchronization has been described and its properties examined in terms of the conditional Lyapunov's exponents and Lyapunov's direct method. These demonstrate two different, yet most common approaches to the analysis of chaotic synchronization. Furthermore, Lyapunov's direct method has then been used to show a general approach to the design of nonlinear controllers for master-slave chaotic systems.

References

[1] Yamada, T., Fujisaka, H.: Stability Theory of Synchronized Motion in Coupled-Oscillator Systems. II. Progress of Theoretical Physics 70(5), 1240–1248 (1983)
[2] Afraimovich, V.S., Verichev, N.N., Rabinovich, M.I.: Stochastic synchronization of oscillations in dissipative systems. Izvestija Vuzov, Radiofizika 29, 795–803 (1986)
[3] Pecora, L.M., Carroll, T.L.: Synchronization in chaotic systems. Physical Review Letters 64(8), 821–824 (1990)
[4] Pecora, L.M., Carroll, T.L.: Driving systems with chaotic signals. Physical Review A 44(4), 2374–2383 (1991)
[5] Carroll, T.L., Pecora, L.M.: Synchronizing chaotic circuits. IEEE Transactions on Circuits and Systems 38(4), 453–456 (1991)

[6] Carroll, T.L., Pecora, L.M.: A circuit for studying the synchronization of chaotic systems. International Journal of Bifurcation and Chaos 2(3), 659–667 (1992)
[7] He, R., Vaidya, P.G.: Analysis and synthesis of synchronous periodic and chaotic systems. Physical Review A 46(12), 7387–7392 (1992)
[8] Murali, K., Lakshmanan, M.: Transmission of signals by synchronization in a chaotic Van der Pol-Duffing oscillator. Physical Review E, Rapid Communications 48(3), R1624–R1626 (1993)
[9] Murali, K., Lakshmanan, M.: Synchronizing chaos in driven Chua's circuit. International Journal of Bifurcation and Chaos 3(4), 1057–1066 (1993)
[10] Wu, C.W., Chua, L.O.: A unified framework for synchronization and control of dynamical systems. International Journal of Bifurcation and Chaos 4(4), 979–998 (1994)
[11] Chua, L.O., Itoh, M., Kocarev, L., Eckert, K.: Chaos synchronization in Chua's circuit. Journal of Circuits, Systems and Computers 3(1), 93–108 (1993)
[12] Suykens, J.A.K., Curran, P.F., Chua, L.O.: Master-slave synchronization using dynamic output feedback. International Journal of Bifurcation and Chaos [in Applied Sciences and Engineering] 7(3), 671–679 (1997)
[13] Suykens, J.A.K., Vandewalle, J.: Master-slave synchronization of Lur'e systems. International Journal of Bifurcation and Chaos [in Applied Sciences and Engineering] 7(3), 665–669 (1997)
[14] Ott, E., Grebogi, C., York, J.A.: Controlling chaos. Physical Review Letters 64(11), 1196–1199 (1990)
[15] Lai, Y.C., Grebogi, C.: Synchronization of chaotic trajectories using control. Physical Review E 47(4), 2357–2360 (1993)
[16] John, J.K., Amritkar, R.E.: Synchronization of unstable orbits using adaptive control. Physical Review E 49(6), 4843–4848 (1994)
[17] Pyragas, K.: Continuous control of chaos by self-controlling feedback. Physics Letters A 170(6), 421–428 (1992)
[18] González-Miranda, J.M.: Generalized synchronization in directionally coupled systems with identical individual dynamics. Physical Review E 65(4), 047202-1–047202-4 (2002)
[19] González-Miranda, J.M.: Synchronization and Control of Chaos, pp. 108–196. Imperial College Press, London (2004)
[20] Mosekilde, E., Maistrenko, Y., Postnov, D.: Chaotic Synchronization Applications to Living Systems, p. 177. World Scientific Publishing Co. Pte. Ltd., New Jersey (2002)
[21] Ott, E.: Chaos in Dynamical Systems Second Edition, pp. 399–401. Cambridge University Press, Cambridge (2002)
[22] Manrubia, S.C., Mikhailov, A.S., Zanette, D.H.: Emergence of Dynamical Order: Synchronization Phenomena in Complex Systems. World Scientific Lecture Notes in Complex Systems, pp. 109–234. World Scientific Publishing Co. Pte. Ltd., Singapore (2004)
[23] Kiss, I.Z., Hudson, J.L.: Chaotic cluster itinerancy and hierarchical cluster trees in electrochemical experiments. Chaos 13(3), 999–1009 (2003)
[24] Stavroulakis, P.: Introduction. In: Stavroulakis, P. (ed.) Chaos Applications in Telecommunications, pp. 1–12. CRC Press LLC, Boca Raton (2006)
[25] Kennedy, M.P., Kolumban, G., Jako, Z.: Chaotic Modulation Schemes. In: Kennedy, M.P., Rovatti, R., Setti, G. (eds.) Chaotic Electronics in Telecommunications, pp. 163–175. CRC Press LLC, Boca Raton (2000)

[26] Chen, G., Dong, X.: From chaos to order: Methodologies, Perspectives and Applications, pp. 598–614. World Scientific Publishing Co. Pte. Ltd., Singapore (1998)
[27] Lau, F.C.M., Tse, C.K.: Chaos-Based Digital Communication Systems, ch. 1, pp. 1–20. Springer, Berlin (2004)
[28] Kolumban, G., Kennedy, M.P.: Correlator-Based Chaotic Communications: Attainable Noise and Multipath Performance. In: Chen, G., Ueta, T. (eds.) Chaos in Circuits and Systems, pp. 443–485. World Scientific Publishing Co. Pte. Ltd., New Jersey (2002)
[29] Kennedy, M.P., Kolumban, G.: Digital Communications Using Chaos. In: Chen, G. (ed.) Controlling Chaos and Bifurcations in Engineering Systems, pp. 477–500. CRC Press LLC, Boca Raton (1999)
[30] Wu, C.W.: Synchronization in coupled chaotic circuits and systems, pp. 13–33. World Scientific Publishing Co. Pte. Ltd., New Jersey (2002)
[31] Setti, G., Rovatti, R., Mazzini, G.: Control of Chaos Statistics for Optimization of DS-CDMA Systems. In: Chen, G., Yu, X. (eds.) Chaos Control Theory and Applications, pp. 295–319. Springer, Berlin (2003)
[32] Oppenheim, A.V., Wornell, G.W., Isabelle, S.H., Cuomo, K.M.: Signal processing in the context of chaotic signals. In: Proceedings IEEE ICASSP, pp. 117–120 (1992)
[33] Kocarev, L., Halle, K.S., Eckert, K., Chua, L.O., Parlitz, U.: Experimental demonstration of secure communications via chaotic synchronization. International Journal of Bifurcation and Chaos 2(3), 709–713 (1992)
[34] Parlitz, U., Chua, L.O., Kocarev, L., Hale, K.S., Shang, A.: Transmission of digital signals by chaotic synchronization. International Journal of Bifurcation and Chaos 2(4), 973–977 (1992)
[35] Cuomo, K.M., Oppenheim, A.V.: Circuit Implementation of Synchronized Chaos with Applications to Communications. Physical Review Letters 71(1), 65–68 (1993)
[36] Cuomo, K.M., Oppenheim, A.V., Strogatz, S.H.: Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications. IEEE Transactions on Circuits and Systems – II. Analog and Digital Signal Processing 40(10), 626–633 (1993)
[37] Jovic, B., Berber, S., Unsworth, C.P.: A novel mathematical analysis for predicting master – slave synchronization for the simplest quadratic chaotic flow and Ueda chaotic system with application to communications. Physica D 213(1), 31–50 (2006)
[38] Wu, C.W., Chua, L.O.: A simple way to synchronize chaotic systems with applications to secure communication systems. International Journal of Bifurcation and Chaos 3(6), 1619–1627 (1993)
[39] Lu, J., Wu, X., Lü, J.: Synchronization of a unified chaotic system and the application in secure communication. Physics Letters A 305(6), 365–370 (2002)
[40] Rouche, N., Habets, P., Laloy, M.: Stability Theory by Liapunov's Direct Method, pp. 30–31. Springer, Heidelberg (1977)
[41] Skowronski, J.M.: Nonlinear Liapunov Dynamics, p. 192. World Scientific, Singapore (1990)
[42] Sprott, J.C.: Chaos and Time-Series Analysis, pp. 230–440. Oxford University Press, Oxford (2003)
[43] Bacciotti, A., Rosier, L.: Liapunov Functions and Stability in Control Theory, pp. 28–29. Springer, London (2001)

[44] Feki, M.: An adaptive chaos synchronization scheme applied to secure communication. Chaos, Solitons and Fractals 18(1), 141–148 (2003)
[45] Kocarev, L., Halle, K.S., Eckert, K., Chua, L.O., Parlitz, U.: "Applications of Chua's Circuit". In: Madan, R.N. (ed.) Chua's Circuit: A Paradigm for Chaos, pp. 371–403. World Scientific Publishing Co. Pte. Ltd., Singapore (1993)
[46] Park, J.H.: Chaos synchronization of a chaotic system via nonlinear control. Chaos, Solitons and Fractals 25(3), 579–584 (2005)
[47] Leipnik, R.B., Newton, T.A.: Double strange attractors in rigid body motion with linear feedback control. Physics Letters 86A(2), 63–67 (1981)
[48] Rabinovich, M.I., Fabrikant, A.L.: Stochastic self-modulation of waves in non equilibrium media. Soviet Physics JETP 50, 311–317 (1979)

Chapter 4
Chaotic Synchronization of Maps

In chapter 3, the concept of chaotic synchronization was introduced on flows, as is most often done in the literature [1]. However, the principles of chaotic synchronization presented in sections 3.1 and 3.2 [1] are also equally applicable to chaotic maps [2]. In contrast to section 3.4 [1], this chapter proposes a method of designing nonlinear control laws for the synchronization of chaotic map master-slave systems. The general approach to the master-slave chaotic map synchronization is demonstrated on the one dimensional, $\Re^1$, cubic map master-slave system, the two dimensional, $\Re^2$, tinkerbell map master-slave system and the Lorenz three dimensional, $\Re^3$, chaotic map master-slave system. It is shown that it is always possible to achieve instant synchronization within a single iteration of the master-slave system for all three systems. The requirement for instant synchronization is that the error system matrix be reduced to zero [3].

Within PC synchronization, the master-slave system either synchronizes or does not, depending on the nature of the system and the driving signal. In contrast to PC synchronization, it has been shown in chapter 3 that is possible to design controllers to enforce synchronization within the master-slave systems [1]. Such design techniques have been investigated for both chaotic flows [1,4,5] and chaotic maps [6-18]. In a number of cases it has been shown that these techniques can be applied to chaotic communications [1,7,9,10,12-14]. In [6] the in-phase and anti-phase synchronization of chaotic maps has been investigated. Furthermore, in [7], chaotic map synchronization method of [6] was used to synchronize a chaotic communication system similar to that of Parlitz and Ergezinger [19]. Here, the authors of [7] investigated the possibility of regenerating the chaotic spreading sequences at the receiver through the process of chaotic synchronization of [6]. In this way the necessity of assuming perfect synchronization among the chaotic spreading sequences of the transmitter and the receiver was avoided. In [8,9] the synchronization of piecewise linear chaotic maps in a master-slave configuration was investigated. In particular, finite time synchronization of a chaotic map master-slave system was considered and the conditions for it discussed. It was shown that by setting the eigenvalues of the error system matrix to zero the finite time synchronization could be achieved. The general significance of the results in relation to the secure chaotic communications was also discussed. The

B. Jovic: Synchronization Techniques for Chaotic Commun. Syst., SCT 5, pp. 79–102.
springerlink.com

synchronization of coupled one dimensional chaotic maps in the noisy environment, as well as the conditions for robust synchronization, have been investigated in [15]. Some of the most recent advances in the synchronization of chaotic maps can be found in [16-18]. In [16], generalized-type synchronization (called Q-S synchronization) of chaotic maps was investigated using discrete Lyapunov functions. It was demonstrated how this approach could be used to synchronize two $\Re^3$ chaotic maps in the master-slave configuration. In [17], a method termed the "slide and match algorithm" was proposed to synchronize a master-slave system of identical chaotic maps using almost any scalar function of the driving master system.

A similar method to that of the master-slave map synchronization of [18] is proposed here [3]. In our method, the general approach to the master-slave synchronization of chaotic maps is presented and the requirements for synchronization outlined. It is shown that the synchronization is achieved by keeping the eigenvalues of the error system matrix within the unit circle in the z domain. Using this method it is demonstrated that it is always possible to achieve instant synchronization, within a single iteration of the master-slave system. This is achieved when the control laws are designed in such a way to reduce the error system matrix to zero. Furthermore, the method of implementing the synchronized master-slave system within a chaotic parameter modulation (CPM) based secure chaotic communication system is demonstrated in chapter 6 with further elaboration in chapter 10.

In Section 4.1, the design of the nonlinear control laws for the synchronization of the chaotic map master-slave systems is proposed. In Sections 4.2, 4.3 and 4.4 this method is demonstrated on the $\Re^1$ cubic map, the $\Re^2$ tinkerbell map and the Lorenz $\Re^3$ chaotic map master-slave systems, respectively.

4.1 A Design Procedure for the Synchronization of Chaotic Maps

In this section, a general approach in the design of the synchronized chaotic maps is proposed. In the subsequent sections, the method is then applied to the $\Re^1$ cubic, $\Re^2$ tinkerbell and Lorenz $\Re^3$ chaotic map, demonstrating the controller design on three dimensionally different chaotic maps of increasing complexity. These controllers then ensure the synchronization among the master-slave systems. The design of the nonlinear control laws is via the following two theorems:

Theorem 1

Suppose: $e_{n+1} = Be_n, \forall\ n \geq 0,\ |eig(B)| < 1.$

Then: $\|e_n\| \to 0,\ as\ n \to \infty, \forall\ e_0 \in R^n.$

The theorem states that the equilibrium **0,** *of the error system* e_{n+1}, *is globally asymptotically stable if and only if all eigenvalues of B have magnitude less than one* [20].
Special cases also exist when matrix *B* is a function of *n*, and the equilibrium **0,** of the error system e_{n+1}, remains globally asymptotically stable.

Special case: If the matrix B is a function of n, then the condition that $\|B_{n+1} - B_n\|$ *remains bounded must also be satisfied.*

Proof for the special case:

Since: $e_{n+1} = B_n e_n$

Then: $e_{n+2} = B_{n+1} e_{n+1}$

$$e_{n+2} = B_{n+1} B_n e_n$$

$$e_{n+i} = B_{n+i} B_{n+(i-1)} \ldots B_n e_n \quad \forall\ i > 1 \qquad (4.1.1)$$

To ensure that the system represented by equation 4.1.1 remains bounded, that is, to ensure global asymptotic stability of the equilibrium **0** of the error system e_{n+1}, it must be ensured that all the matrix components of $B_{n+i} B_{n+(i-1)} \ldots B_n e_n$ remain bounded, that is, the condition that $\|B_{n+1} - B_n\|$ remains bounded, must be satisfied.

Theorem 1 is now manipulated to obtain Theorem 2 [3], which is suitable for the synchronization of chaotic maps.

Theorem 2

Suppose: $e_{n+1} = A_n e_n + U_n e_n, \forall\ n \geq 0,\ |eig(A_n + U_n)| = |eig(B)| < 1.$

Then: $\|e_n\| \to 0$, *as* $n \to \infty, \forall\ e_0 \in R^n$.

The theorem states that the equilibrium **0,** *of the error system* e_{n+1}, *is globally asymptotically stable if and only if all eigenvalues of* $B = A_n + U_n$ *have magnitude less than one.*

Special case: If the matrix B is a function of n, then the condition that $\|B_{n+1} - B_n\|$ *remains bounded must also be satisfied.*

In the above theorems brackets | | denote the magnitude of the eigenvalues of a matrix, and the brackets ‖ ‖ denote the Euclidian norm. In the following sections Theorem 2 is used for the purpose of synchronizing one, two and three dimensional master-slave chaotic maps.

4.2 Synchronization of the $\Re^1$ Cubic Map Master-Slave Systems

In this section, the master-slave synchronization of a one dimensional map, the cubic map, is considered.

The cubic map [21] is given by equation 4.2.1:

$$X_{n+1} = AX_n(1 - X_n^2) \tag{4.2.1}$$

With the parameter $A = 3$ the system is chaotic. Figures 4.1a and 4.1b show the time series and the chaotic map, respectively.

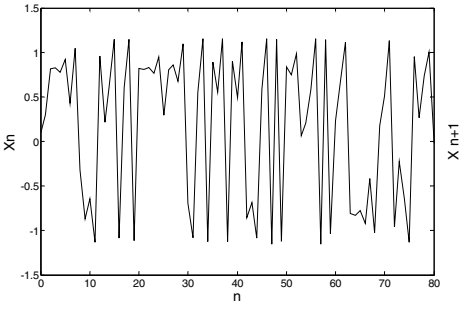


Fig. 4.1a The cubic map chaotic time series, X_n

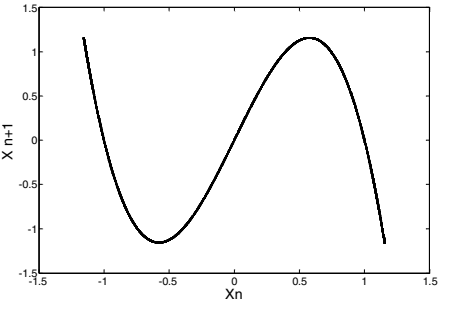


Fig. 4.1b The cubic map

Using the $\Re^1$ cubic map master-slave system as an example, the design procedure of the nonlinear control laws required for synchronization is now explained. In general terms, the cubic map master-slave system can be represented in the form of a block diagram of Figure 4.2. Let the error be defined by equation 4.2.2:

$$e_n = \hat{X}_n - X_n \tag{4.2.2}$$

The difference error, (the error system), can then be represented by equation 4.2.3:

$$e_{n+1} = \hat{X}_{n+1} - X_{n+1} = A\hat{X}_n - AX_n - A\hat{X}_n^3 + AX_n^3 + u_n \tag{4.2.3}$$

Keeping in mind the identity of equation 4.2.4, equation 4.2.3 can also be represented by equation 4.2.5:

$$-\hat{X}_n^3 + X_n^3 = -e_n(e_n^2 + 3\hat{X}_n X_n) \tag{4.2.4}$$

$$e_{n+1} = \hat{X}_{n+1} - X_{n+1} = A(1 - 3\hat{X}_n X_n - e_n^2)e_n + u_n \tag{4.2.5}$$

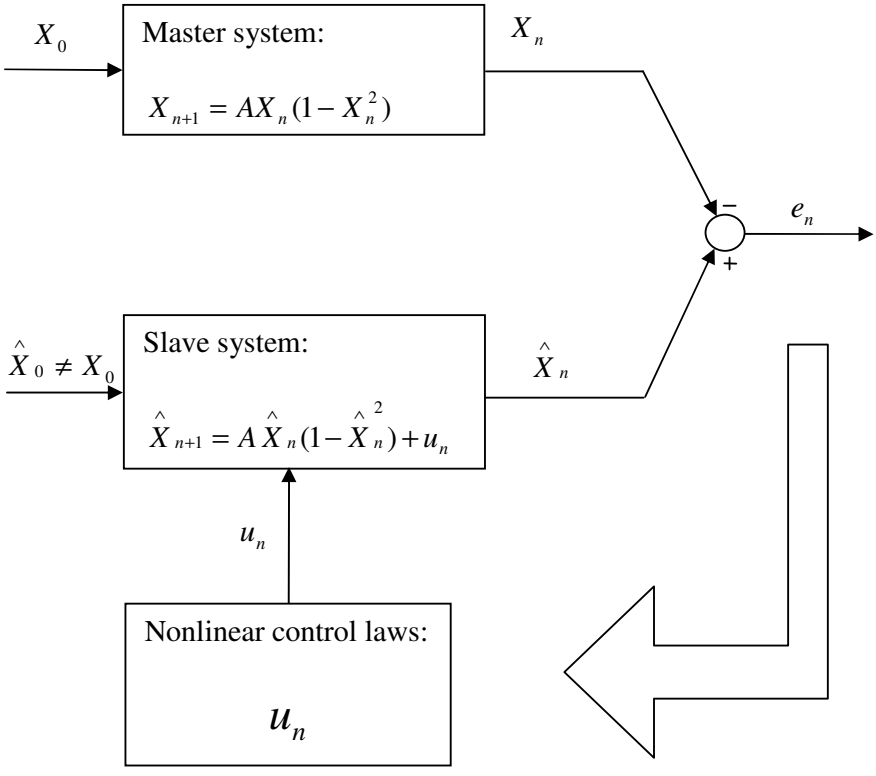


Fig. 4.2 The cubic map master-slave system, where: $A = 3$.

With theorem 2 in mind equation 4.2.6 is now formed:

$$e_{n+1} = A_n e_n + U_n e_n \tag{4.2.6}$$

Modifying equation 4.2.5 to fit the form of equation 4.2.6, equation 4.2.7 is obtained:

$$e_{n+1} = A(1-3\hat{X}_n X_n - e_n^2)e_n + U_n e_n \tag{4.2.7}$$

where: $A_n = A(1-3\hat{X}_n X_n - e_n^2)$ and $u_n = U_n e_n$.

Therefore:

$$B = A_n + U_n = A(1-3\hat{X}_n X_n - e_n^2) + U_n \tag{4.2.8}$$

From theorem 2 it is required that the magnitude of eigenvalues of equation 4.2.8 be less than unity (ie. be within the unit circle in the z domain). As B of equation 4.2.8 is a 1x1 matrix, that is a scalar, it is then required that it be in the

range -1 < B < 1, that is |B| < 1. This condition is now used to formulate the conditions upon U_n. When satisfied, they globally asymptotically stabilise the system of equation 4.2.7, and thus synchronize the master-slave system of Figure 4.2.

It is readily verifiable that equation 4.2.8 is in the range -1 < B < 1 when:

$$U_n = \lambda - A(1 - 3\hat{X}_n X_n - e_n^2) \qquad \text{where: } -1 < \lambda < 1 \tag{4.2.9}$$

From equation 4.2.9, it can be observed that $U_n = -A(1 - 3\hat{X}_n X_n - e_n^2)$ is the optimal solution as it reduces equation 4.2.8 to zero and thus causes the fastest possible synchronization between the master and slave systems of Figure 4.2.

Therefore, the control law u_n is given by equation 4.2.10 and incorporated into Figure 4.2 to produce Figure 4.3.

$$u_n = U_n e_n = -A(1 - 3\hat{X}_n X_n - e_n^2)e_n \tag{4.2.10}$$

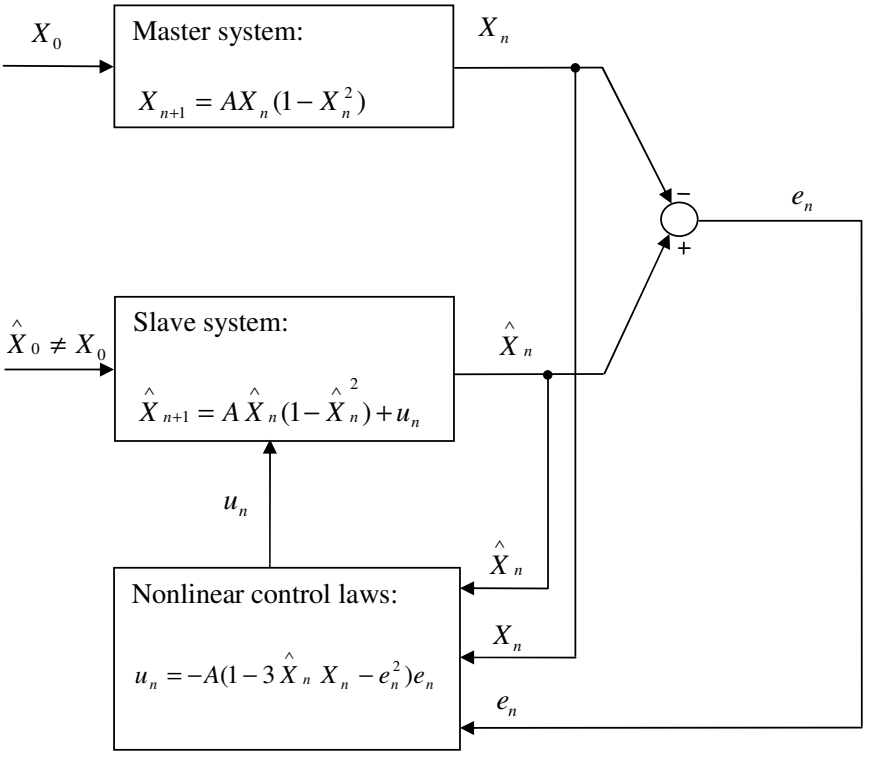


Fig. 4.3 The cubic map master-slave system, where: $A = 3$.

Figure 4.4 demonstrates that the system does not synchronize when $\lambda = 1$, that is, when: $u_n = (1 - A(1 - 3\hat{X}_n X_n - e_n^2))e_n$. It can be observed from Figure 4.4 that in this case the synchronization error among the master-slave signals is constant. When $\lambda = 0.99$, that is when: $u_n = (0.99 - A(1 - 3\hat{X}_n X_n - e_n^2))e_n$, the master-slave system synchronizes, as Figure 4.5 demonstrates. However, in this case, the system is on the border of synchronization and it takes approximately 500 iterations for the system to synchronize. It should be noted that here the slave signal asymptotically approaches the master signal. The instant synchronization, achieved by the control law of equation 4.2.10, is demonstrated in Figure 4.6. It can be observed from Figure 4.6 that the master-slave system synchronizes in a single iteration.

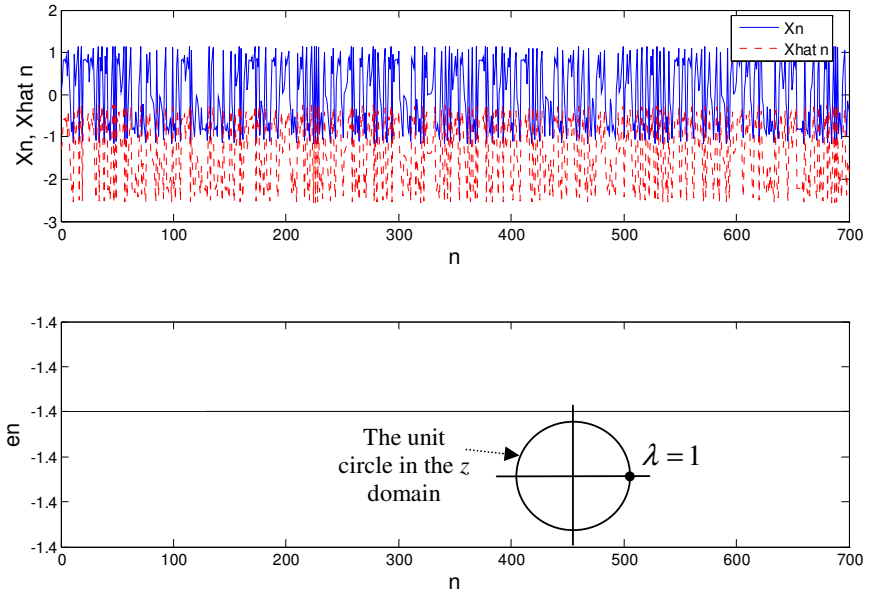


Fig. 4.4 Synchronization of the master-slave cubic chaotic signals, when $\lambda = 1$.

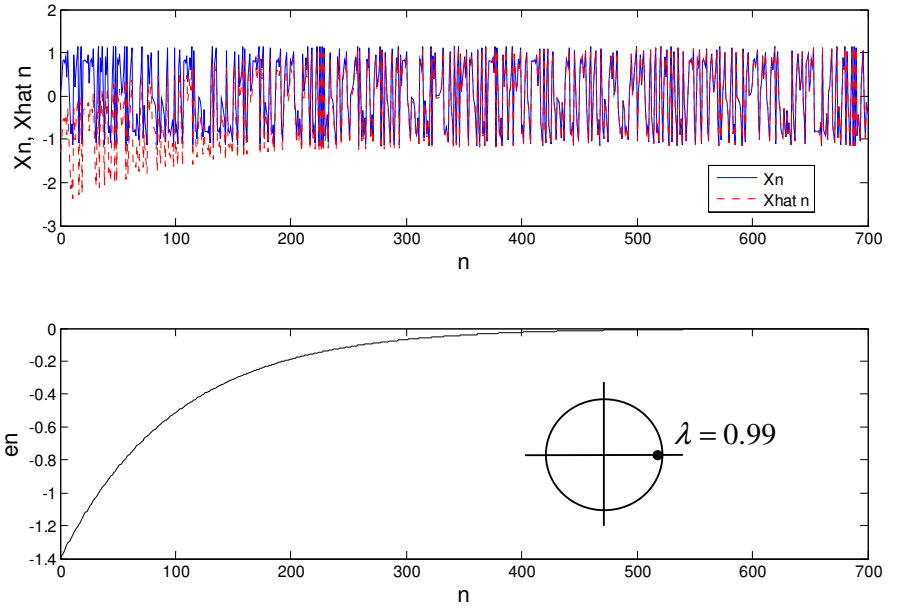


Fig. 4.5 Synchronization of the master-slave cubic chaotic signals, when $\lambda = 0.99$.

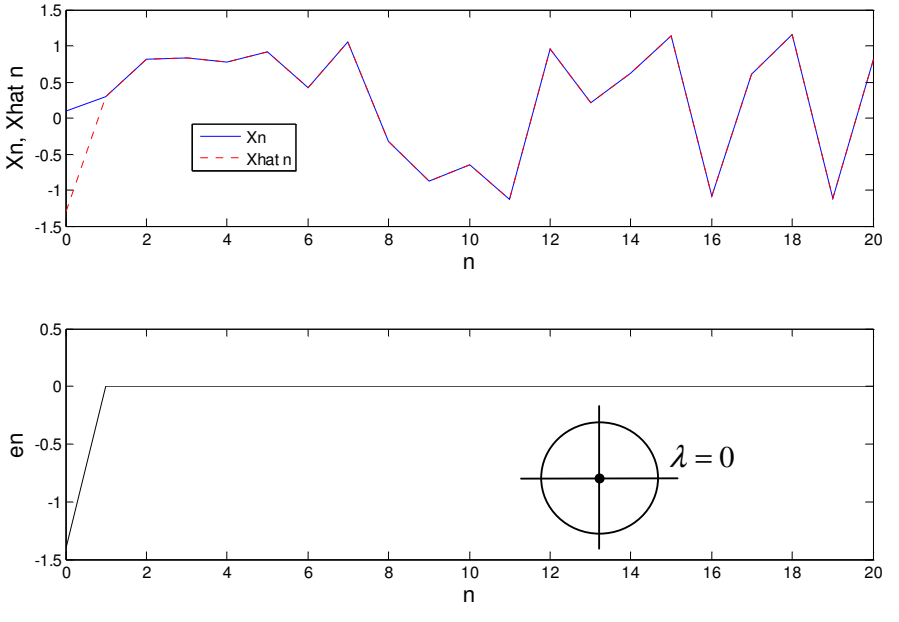


Fig. 4.6 Synchronization of the master-slave cubic chaotic signals, when $\lambda = 0$.

4.3 Synchronization of the $\Re^2$ Tinkerbell Map Master-Slave Systems

In this section, the complexity is increased to $\Re^2$. Here, the master-slave synchronization of a two dimensional map, the tinkerbell map, is considered.

The tinkerbell map [21] is given by equation 4.3.1:

$$\begin{aligned} X_{n+1} &= X_n^2 - Y_n^2 + aX_n + bY_n \\ Y_{n+1} &= 2X_nY_n + cX_n + dY_n \end{aligned} \tag{4.3.1}$$

With the parameter $a = 0.9$, $b = -0.6$, $c = 2$ and $d = 0.5$ the system exhibits chaos. Figures 4.7a and 4.7b show the time series and the chaotic map, respectively.

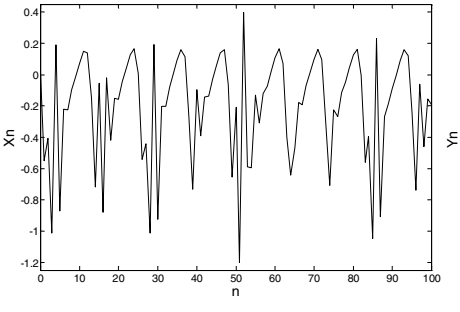


Fig. 4.7a The tinkerbell map chaotic time series, X_n

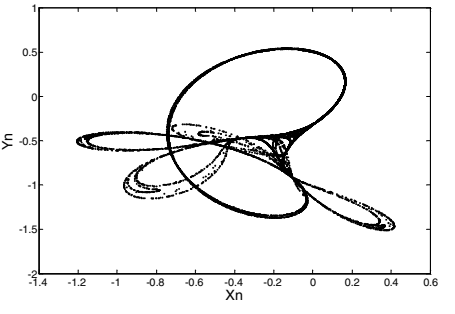


Fig. 4.7b The tinkerbell map

The design procedure of the nonlinear control laws necessary for synchronization of the tinkerbell map master-slave system of Figure 4.8 is now explained. Let the error be defined by equation 4.3.2:

$$e_{1n} = \hat{X}_n - X_n \tag{4.3.2a}$$

$$e_{2n} = \hat{Y}_n - Y_n \tag{4.3.2b}$$

The difference error, (the error system), can then be represented by equation 4.3.3:

$$\begin{aligned} e_{1n+1} &= \hat{X}_{n+1} - X_{n+1} = \hat{X}_n^2 - X_n^2 - \hat{Y}_n^2 + Y_n^2 + a\hat{X}_n - aX_n + b\hat{Y}_n - bY_n + u_{1n} \\ e_{2n+1} &= \hat{Y}_{n+1} - Y_{n+1} = 2\hat{X}_n\hat{Y}_n - 2X_nY_n + c\hat{X}_n - cX_n + d\hat{Y}_n - dY_n + u_{2n} \end{aligned} \tag{4.3.3}$$

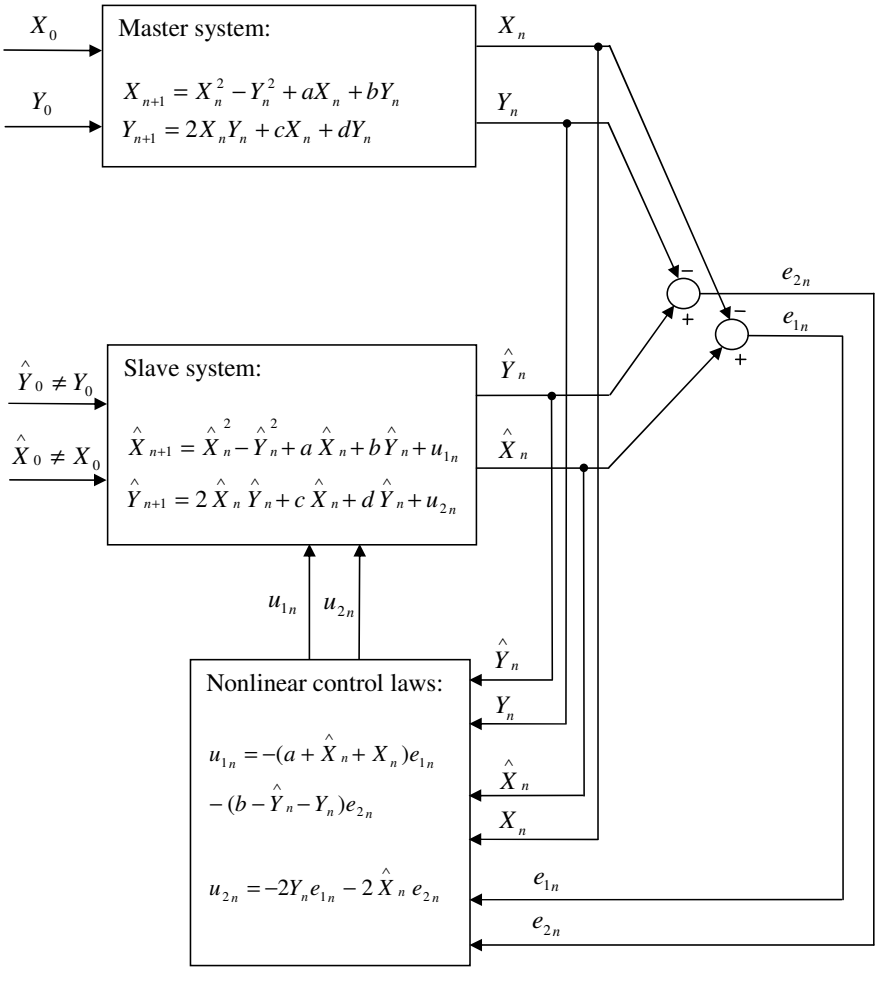


Fig. 4.8 The tinkerbell map master-slave system, where: $a = 0.9$, $b = -0.6$, $c = 2$ and $d = 0.5$.

Keeping in mind the identities of equation 4.3.4, equation 4.3.3 can also be represented by equation 4.3.5:

$$\begin{aligned}
\hat{X}_n^2 - X_n^2 &= \hat{X}_n e_{1n} + X_n e_{1n} \\
-\hat{Y}_n^2 + Y_n^2 &= -\hat{Y}_n e_{2n} - Y_n e_{2n} \\
\hat{X}_n\hat{Y}_n - X_nY_n &= Y_n e_{1n} + \hat{X}_n e_{2n}
\end{aligned} \tag{4.3.4}$$

$$\begin{aligned} e_{1n+1} &= \hat{X}_{n+1} - X_{n+1} = e_{1n}(a + \hat{X}_n + X_n) + e_{2n}(b - \hat{Y}_n - Y_n) + u_{1n} \\ e_{2n+1} &= \hat{Y}_{n+1} - Y_{n+1} = e_{1n}(c + 2Y_n) + e_{2n}(d + 2\hat{X}_n) + u_{2n} \end{aligned} \tag{4.3.5}$$

With theorem 2 in mind matrix equation 4.3.6 is formed:

$$e_{n+1} = A_n e_n + U_n e_n \tag{4.3.6}$$

In matrix notation equation 4.3.6 takes the form of equation 4.3.7:

$$e_{n+1} = \begin{bmatrix} a_{11n} & a_{12n} \\ a_{21n} & a_{22n} \end{bmatrix} e_n + \begin{bmatrix} u_{11n} & u_{12n} \\ u_{21n} & u_{22n} \end{bmatrix} e_n \tag{4.3.7}$$

where: $A = \begin{bmatrix} a_{11n} & a_{12n} \\ a_{21n} & a_{22n} \end{bmatrix}$, $U = \begin{bmatrix} u_{11n} & u_{12n} \\ u_{21n} & u_{22n} \end{bmatrix}$ and $e_n = \begin{bmatrix} e_{1n} \\ e_{2n} \end{bmatrix}$.

Modifying equation 4.3.5 to fit the matrix form of equation 4.3.7, equation 4.3.8 is obtained:

$$e_{n+1} = \begin{bmatrix} a + \hat{X}_n + X_n & b - \hat{Y}_n - Y_n \\ c + 2Y_n & d + 2\hat{X}_n \end{bmatrix} e_n + \begin{bmatrix} u_{\mathrm{i}n} & u_{\mathrm{ii}n} \\ u_{\mathrm{iii}n} & u_{\mathrm{iv}n} \end{bmatrix} e_n \tag{4.3.8}$$

where: $u_{1n} = u_{\mathrm{i}n} e_{1n} + u_{\mathrm{ii}n} e_{2n}$ and $u_{2n} = u_{\mathrm{iii}n} e_{1n} + u_{\mathrm{iv}n} e_{2n}$.

Therefore:

$$\begin{aligned} B = A_n + U_n &= \begin{bmatrix} a + \hat{X}_n + X_n & b - \hat{Y}_n - Y_n \\ c + 2Y_n & d + 2\hat{X}_n \end{bmatrix} + \begin{bmatrix} u_{\mathrm{i}n} & u_{\mathrm{ii}n} \\ u_{\mathrm{iii}n} & u_{\mathrm{iv}n} \end{bmatrix} \\ &= \begin{bmatrix} a + \hat{X}_n + X_n + u_{\mathrm{i}n} & b - \hat{Y}_n - Y_n + u_{\mathrm{ii}n} \\ c + 2Y_n + u_{\mathrm{iii}n} & d + 2\hat{X}_n + u_{\mathrm{iv}n} \end{bmatrix} \end{aligned} \tag{4.3.9}$$

Following theorem 2, the control laws can be chosen in the following manner to obtain a constant matrix *B*:

$$\begin{aligned} u_{\mathrm{i}n} &= -(a + \hat{X}_n + X_n) \\ u_{\mathrm{ii}n} &= -(b - \hat{Y}_n - Y_n) \\ u_{\mathrm{iii}n} &= -2Y_n \\ u_{\mathrm{iv}n} &= -2\hat{X}_n \end{aligned} \tag{4.3.10}$$

With the control laws of equation 4.3.10, equation 4.3.9 takes the form of equation 4.3.11:

$$B = \begin{bmatrix} 0 & 0 \\ c & d \end{bmatrix} \tag{4.3.11}$$

From theorem 1, it is then required that the magnitude of eigenvalues of the matrix B be less than one (ie. be within the unit circle in the z domain). The eigenvalues are given by equation 4.3.13, where I is the 2X2 identity matrix and λ is the scalar denoting the eigenvalues:

$$\det[\lambda I - B] = \det\begin{bmatrix} \lambda & 0 \\ c & \lambda - d \end{bmatrix} = \lambda(\lambda - d) = 0 \tag{4.3.12}$$

$$\lambda = 0 \qquad \text{and} \qquad \lambda = d = 0.5 \tag{4.3.13}$$

As with cubic map, the eigenvalues are within the unit circle in z domain, thus making the system of equation 4.3.8 globally asymptotically stable. Therefore, the control laws u_{1_n} and u_{2_n} are given by equations 4.3.14 and 4.3.15, respectively, and incorporated into Figure 4.8.

$$u_{1_n} = u_{\mathrm{i}_n} e_{1_n} + u_{\mathrm{ii}_n} e_{2_n} = -(a + \hat{X}_n + X_n) e_{1_n} - (b - \hat{Y}_n - Y_n) e_{2_n} \tag{4.3.14}$$

$$u_{2_n} = u_{\mathrm{iii}_n} e_{1_n} + u_{\mathrm{iv}_n} e_{2_n} = -2Y_n e_{1_n} - 2\hat{X}_n e_{2_n} \tag{4.3.15}$$

The control law performance, given by equations 4.3.14 and 4.3.15, is demonstrated in Figure 4.9 from which one can observe that the master-slave system synchronizes. In particular, it should be observed that in the case of the master-slave signals Y, the slave signal $\hat{Y}$ asymptotically approaches the master signal Y.

It should be noted that the control laws of equations 4.3.14 and 4.3.15 are not the only possible control laws which cause the master-slave system of Figure 4.8 to synchronize. For instance, the control laws of equations 4.3.16 and 4.3.17:

$$u_{1_n} = u_{\mathrm{i}_n} e_{1_n} + u_{\mathrm{ii}_n} e_{2_n} = -(a + \hat{X}_n + X_n) e_{1_n} - (b - \hat{Y}_n - Y_n) e_{2_n} \tag{4.3.16}$$

$$u_{2_n} = u_{\mathrm{iii}_n} e_{1_n} + u_{\mathrm{iv}_n} e_{2_n} = -2Y_n e_{1_n} - (d + 2\hat{X}_n) e_{2_n}, \tag{4.3.17}$$

cause both eigenvalues of the matrix B to be equal to zero.

The performance of the control laws of equations 4.3.16 and 4.3.17 is illustrated in Figure 4.10, demonstrating finite time synchronization of the master-slave system. It can be observed from Figure 4.10, that the master-slave X signals synchronize within one time step. However, it requires two time steps to synchronize the master-slave Y signals. In order to achieve the fastest possible (instant) synchronization it would be required to redesign the control laws of equation 4.3.10 to reduce the matrix B of equation 4.3.9 to zero. This would not cause a significant increase in the complexity of the control laws of equations 4.3.14 and 4.3.15 as only constants need to be introduced into the control laws of equation 4.3.10, as demonstrated by equations 4.3.18 and 4.3.19:

$$u_{1_n} = u_{\mathrm{i}_n} e_{1_n} + u_{\mathrm{ii}_n} e_{2_n} = -(a + \hat{X}_n + X_n) e_{1_n} - (b - \hat{Y}_n - Y_n) e_{2_n} \tag{4.3.18}$$

$$u_{2_n} = u_{\mathrm{iii}_n} e_{1_n} + u_{\mathrm{iv}_n} e_{2_n} = -(c + 2Y_n) e_{1_n} - (d + 2\hat{X}_n) e_{2_n} \tag{4.3.19}$$

The performance of the control laws, given by equations 4.3.18 and 4.3.19, is shown in Figure 4.11. Observe the instant synchronization within one time step.

Setting the eigenvalues of the system to zero, results in the synchronization time faster than for any other eigenvalues, within the unit circle in the z domain. However, as can be seen from figure 4.10, setting the eigenvalues to zero does not guarantee instant synchronization within one time step. In order to achieve instant synchronization in one time step, it is required to design the control laws in such a way to reduce the matrix B to zero. The proof of this is trivial and is obtained by substituting the ultimate control laws of equations 4.3.18 and 4.3.19 into the slave equations of Figure 4.8, respectively, and showing that the slave equations reduce to the master equations:

$$\begin{aligned}\hat{X}_{n+1} &= \hat{X}_n^2 - \hat{Y}_n^2 + a\hat{X}_n + b\hat{Y}_n - (a + \hat{X}_n + X_n)e_{1n} - (b - \hat{Y}_n - Y_n)e_{2n} \\ \hat{Y}_{n+1} &= 2\hat{X}_n\hat{Y}_n + c\hat{X}_n + d\hat{Y}_n - (c + 2Y_n)e_{1n} - (d + 2\hat{X}_n)e_{2n}\end{aligned} \tag{4.3.20}$$

$$\begin{aligned}\hat{X}_{n+1} &= X_{n+1} = X_n^2 - Y_n^2 + aX_n + bY_n \\ \hat{Y}_{n+1} &= Y_{n+1} = 2X_nY_n + cX_n + dY_n\end{aligned} \tag{4.3.21}$$

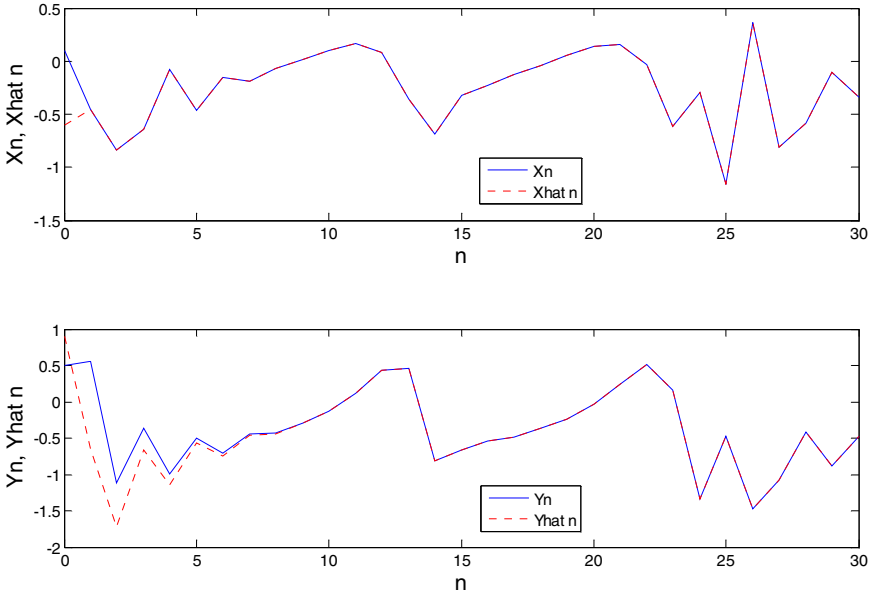


Fig. 4.9 Synchronization of the master-slave tinkerbell chaotic signals with the control laws of equations 4.3.14 and 4.3.15, that is, when one of the eigenvalues is equal to zero while the other is equal to 0.5

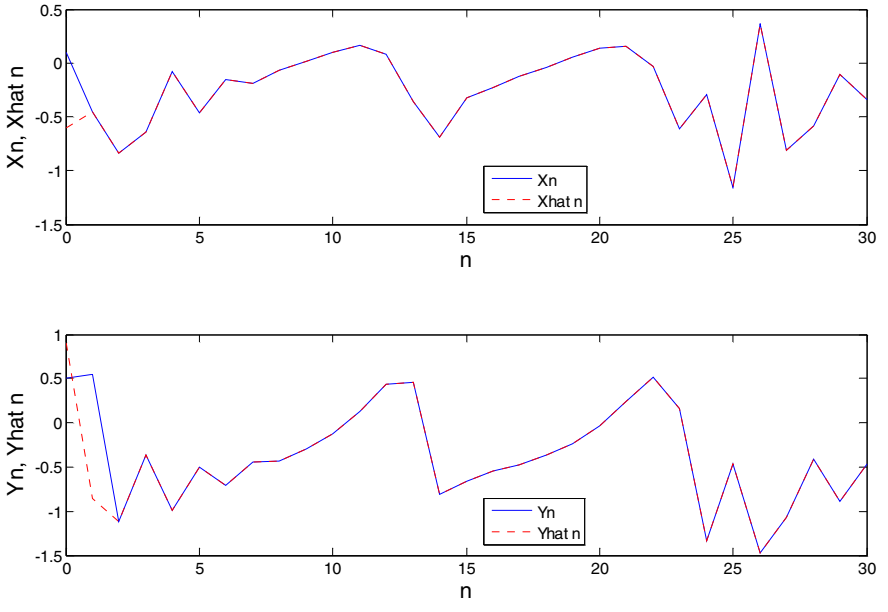


Fig. 4.10 Finite time synchronization of the master-slave tinkerbell chaotic signals with the control laws of equations 4.3.16 and 4.3.17, that is, when both eigenvalues are equal to zero

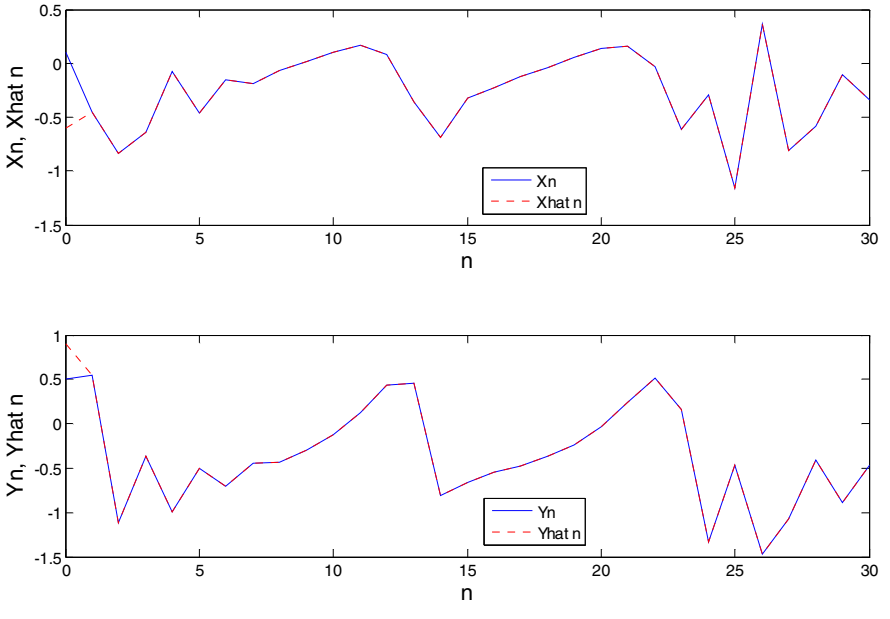


Fig. 4.11 Instant synchronization of the master-slave tinkerbell chaotic signals using the control laws of equations 4.3.18 and 4.3.19, that is, when matrix B is equal to zero

4.4 Synchronization of the Lorenz $\Re^3$ Chaotic Map Master-Slave Systems

In this section the chaotic map complexity is further increased to $\Re^3$. The master-slave synchronization of a three dimensional map, the Lorenz three-dimensional chaotic map, is considered.

The Lorenz three-dimensional chaotic map [21] is given by equation 4.4.1:

$$\begin{aligned} X_{n+1} &= X_n Y_n - Z_n \\ Y_{n+1} &= X_n \\ Z_{n+1} &= Y_n \end{aligned} \tag{4.4.1}$$

Figures 4.12a and 4.12b show the time series and the chaotic map, respectively.

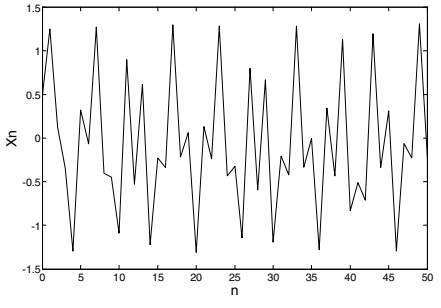


Fig. 4.12a The Lorenz $\Re^3$ chaotic map time series, X_n

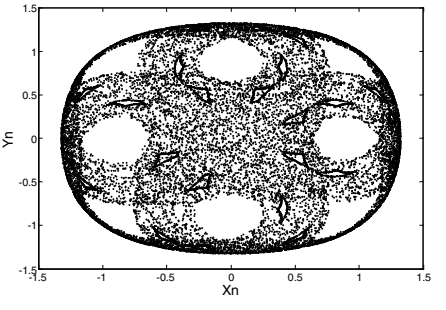


Fig. 4.12b The Lorenz $\Re^3$ chaotic map

The same procedure for designing nonlinear control laws, as that in the $\Re^1$ and $\Re^2$ cases, is now used to demonstrate the design of the nonlinear control laws of the Lorenz $\Re^3$ chaotic map master-slave system of Figure 4.13. Let the error be defined by equation 4.4.2:

$$e_{1n} = \hat{X}_n - X_n \tag{4.4.2a}$$

$$e_{2n} = \hat{Y}_n - Y_n \tag{4.4.2b}$$

$$e_{3n} = \hat{Z}_n - Z_n \tag{4.4.2c}$$

Note the extra error term introduced as the dimension increases, highlighted in equation 4.4.2c and Figure 4.13.

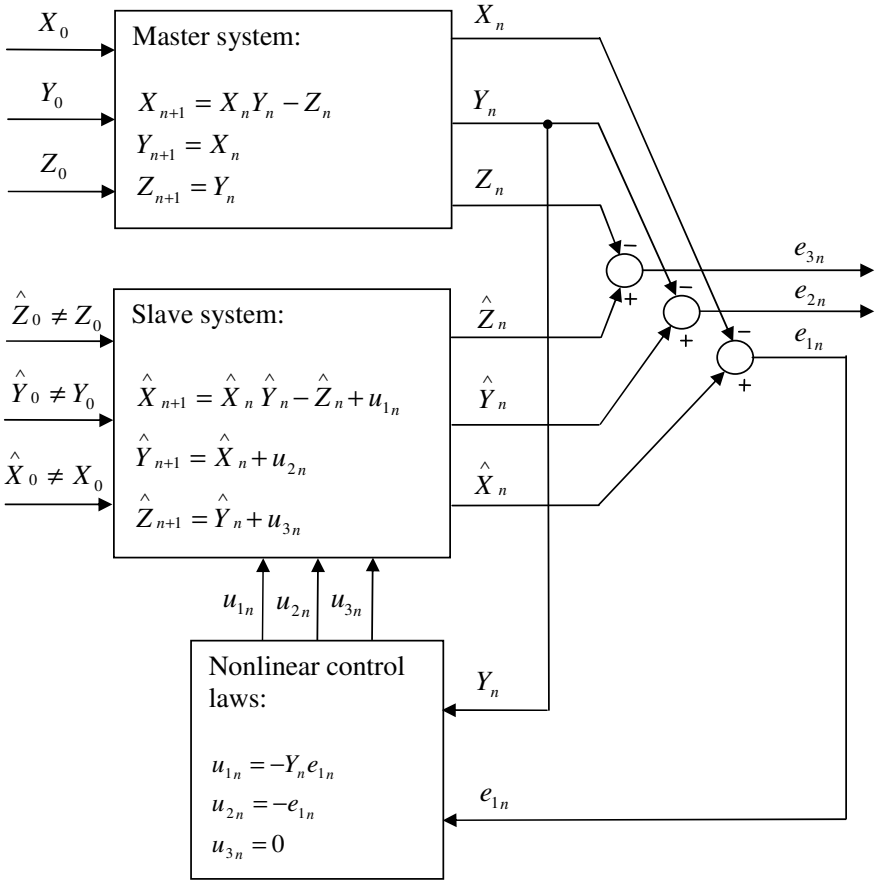


Fig. 4.13 The Lorenz three-dimensional chaotic map master-slave system.

The difference error, (the error system), can then be represented by equation 4.4.3:

$$
\begin{aligned}
e_{1n+1} &= \hat{X}_{n+1} - X_{n+1} = \hat{X}_n \hat{Y}_n - X_n Y_n - \hat{Z}_n + Z_n + u_{1n} \\
e_{2n+1} &= \hat{Y}_{n+1} - Y_{n+1} = \hat{X}_n - X_n + u_{2n} \\
e_{3n+1} &= \hat{Z}_{n+1} - Z_{n+1} = \hat{Y}_n - Y_n + u_{3n}
\end{aligned}
\tag{4.4.3}
$$

Keeping in mind the identities of equation 4.4.4, equation 4.4.3 can also be represented by equation 4.4.5:

$$\hat{X}_n \hat{Y}_n - X_n Y_n = Y_n e_{1_n} + \hat{X}_n e_{2_n} \tag{4.4.4}$$

$$\begin{aligned} e_{1_{n+1}} &= \hat{X}_{n+1} - X_{n+1} = Y_n e_{1_n} + \hat{X}_n e_{2_n} - e_{3_n} + u_{1_n} \\ e_{2_{n+1}} &= \hat{Y}_{n+1} - Y_{n+1} = e_{1_n} + u_{2_n} \\ e_{3_{n+1}} &= \hat{Z}_{n+1} - Z_{n+1} = e_{2_n} + u_{3_n} \end{aligned} \tag{4.4.5}$$

With theorem 2 in mind matrix equation 4.4.7 is formed:

$$e_{n+1} = A_n e_n + U_n e_n \tag{4.4.6}$$

$$e_{n+1} = \begin{bmatrix} a_{11_n} & a_{12_n} & a_{13_n} \\ a_{21_n} & a_{22_n} & a_{23_n} \\ a_{31_n} & a_{32_n} & a_{33_n} \end{bmatrix} e_n + \begin{bmatrix} u_{11_n} & u_{12_n} & u_{13_n} \\ u_{21_n} & u_{22_n} & u_{23_n} \\ u_{31_n} & u_{32_n} & u_{33_n} \end{bmatrix} e_n \tag{4.4.7}$$

where:

$$A_n = \begin{bmatrix} a_{11_n} & a_{12_n} & a_{13_n} \\ a_{21_n} & a_{22_n} & a_{23_n} \\ a_{31_n} & a_{32_n} & a_{33_n} \end{bmatrix}, \quad U_n = \begin{bmatrix} u_{11_n} & u_{12_n} & u_{13_n} \\ u_{21_n} & u_{22_n} & u_{23_n} \\ u_{31_n} & u_{32_n} & u_{33_n} \end{bmatrix} \quad \text{and}$$

$$e_n = \begin{bmatrix} e_{1_n} \\ e_{2_n} \\ e_{3_n} \end{bmatrix}.$$

Modifying equation 4.4.5 to fit the matrix form of equation 4.4.7, equation 4.4.8 is obtained:

$$e_{n+1} = \begin{bmatrix} Y_n & \hat{X}_n & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} e_n + \begin{bmatrix} u_{\mathrm{i}_n} & 0 & 0 \\ u_{\mathrm{ii}_n} & 0 & 0 \\ u_{\mathrm{iii}_n} & 0 & 0 \end{bmatrix} e_n \tag{4.4.8}$$

where: $u_{1_n} = u_{\mathrm{i}_n} e_{1_n}$, $u_{2_n} = u_{\mathrm{ii}_n} e_{1_n}$ and $u_{3_n} = u_{\mathrm{iii}_n} e_{1_n}$.

Therefore:

$$B = A_n + U_n = \begin{bmatrix} Y_n & \hat{X}_n & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} + \begin{bmatrix} u_{\mathrm{i}\,n} & 0 & 0 \\ u_{\mathrm{ii}\,n} & 0 & 0 \\ u_{\mathrm{iii}\,n} & 0 & 0 \end{bmatrix} = \begin{bmatrix} Y_n + u_{\mathrm{i}\,n} & \hat{X}_n & -1 \\ 1 + u_{\mathrm{ii}\,n} & 0 & 0 \\ u_{\mathrm{iii}\,n} & 1 & 0 \end{bmatrix} \tag{4.4.9}$$

Following theorem 2 the control laws can be chosen in the following manner:

$$\begin{aligned} u_{\mathrm{i}\,n} &= -Y_n + k \\ u_{\mathrm{ii}\,n} &= -1 \\ u_{\mathrm{iii}\,n} &= 0 \end{aligned} \tag{4.4.10}$$

where k is the parameter to be determined.

With the control laws of equation 4.4.10, equation 4.4.9 takes the form of equation 4.4.11:

$$B_n = \begin{bmatrix} k & \hat{X}_n & -1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{4.4.11}$$

From theorem 2, it is then required that the magnitude of the eigenvalues of the matrix B_n be less than one (ie. be within the unit circle in the z domain). This condition is now used to formulate the conditions upon k, that is, upon $u_{\mathrm{i}\,n}$. The eigenvalues of the matrix B_n are obtained by evaluating equation 4.4.12, where I is the 3X3 identity matrix and λ is the scalar denoting the eigenvalues:

$$\det[\lambda I - B_n] = \det\begin{bmatrix} \lambda - k & -\hat{X}_n & 1 \\ 0 & \lambda & 0 \\ 0 & -1 & \lambda \end{bmatrix} = (\lambda - k)\begin{vmatrix} \lambda & 0 \\ -1 & \lambda \end{vmatrix} + \hat{X}_n \begin{vmatrix} 0 & 0 \\ 0 & \lambda \end{vmatrix} + 1 \begin{vmatrix} 0 & \lambda \\ 0 & -1 \end{vmatrix} = 0 \tag{4.4.12}$$

$$\lambda^2(\lambda - k) = 0 \tag{4.4.13}$$

From equation 4.4.13 it is observed that two out of three eigenvalues are always at zero, whereas the third eigenvalue is equal to zero provided k is equal to zero. Keeping in mind the condition of theorem 1 (2) that $|\lambda| = |eig(B)| < 1$, it is evident from equation 4.4.13 that k must be kept within the unit circle in z domain: $|k| < 1$. Clearly, in this case, choosing $k = 0$ is the optimal solution as it forces the third eigenvalue of equation 4.4.13 to zero, so that:

$$u_{\mathrm{i}n} = -Y_n \tag{4.4.14}$$

Therefore, the control laws u_{1n}, u_{2n} and u_{3n} are given by equations 4.4.15, 4.4.16 and 4.4.17, respectively, and incorporated into Figure 4.13.

$$u_{1n} = u_{\mathrm{i}n} e_{1n} = -Y_n e_{1n} \tag{4.4.15}$$

$$u_{2n} = u_{\mathrm{ii}n} e_{1n} = -e_{1n} \tag{4.4.16}$$

$$u_{3n} = u_{\mathrm{iii}n} e_{1n} = 0 \tag{4.4.17}$$

With such control laws, the eigenvalues of the matrix B_n of equation 4.4.11 are equal to 0 and the matrix B_n takes the form of equation 4.4.18:

$$B_n = \begin{bmatrix} 0 & \hat{X}_n & -1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{4.4.18}$$

However, theorem 2 requires matrix B to be constant. As the matrix B is a function of n, it must also be ensured that $\|B_{n+1} - B_n\|$ remains bounded to guarantee global asymptotic stability which is the requirement for synchronization. The fact that $\|B_{n+1} - B_n\|$ remains bounded is demonstrated by equation 4.4.19 (4.4.20):

$$B_{n+2}B_{n+1}B_n = \begin{bmatrix} 0 & \hat{X}_{n+2} & -1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & \hat{X}_{n+1} & -1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & \hat{X}_n & -1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{4.4.19}$$

That is:

$$B_{n+i}B_{n+(i-1)}\ldots B_n e_n = \begin{bmatrix} 0 & \hat{X}_{n+i} & -1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & \hat{X}_{n+(i-1)} & -1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}\ldots\begin{bmatrix} 0 & \hat{X}_{n} & -1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = 0 \tag{4.4.20}$$

for $i = 3$.

In Figure 4.14, synchronization of the master-slave system is demonstrated when the control parameter k is a complex number within the unit circle, that is, $k = 0.6 + j0.5$. It can be observed from Figure 4.14 that the master-slave system synchronizes. Furthermore, it should be observed that in the case of the master-slave signals X, the slave signal $\hat{X}$ asymptotically approaches the master signal X. The performance of the control laws when $k = 0$, given by equations 4.4.15-4.4.17, is demonstrated in Figure 4.15. From Figure 4.15, one can observe the finite time synchronization among the master-slave signals.

In order to achieve instant synchronization, the control matrix U_n of equation 4.4.8 must be redefined to obtain the matrix equation 4.4.21:

$$e_{n+1} = A_n e_n + U_n e_n = \begin{bmatrix} Y_n & \hat{X}_n & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} e_n + \begin{bmatrix} u_{\mathrm{i}n} & u_{\mathrm{iv}n} & u_{\mathrm{v}n} \\ u_{\mathrm{ii}n} & 0 & 0 \\ u_{\mathrm{iii}n} & u_{\mathrm{vi}n} & 0 \end{bmatrix} e_n \tag{4.4.21}$$

where: $u_{1n} = u_{\mathrm{i}n}e_{1n} + u_{\mathrm{iv}n}e_{2n} + u_{\mathrm{v}n}e_{3n}$, $u_{2n} = u_{\mathrm{ii}n}e_{1n}$ and $u_{3n} = u_{\mathrm{iii}n}e_{1n} + u_{\mathrm{vi}n}e_{2n}$.

To reduce the matrix B to zero, and thus achieve instant synchronization, the control laws $u_{\mathrm{i}n}$ to $u_{\mathrm{vi}n}$ must be chosen in the following manner:

$$\begin{aligned} u_{\mathrm{i}n} &= -Y_n \\ u_{\mathrm{ii}n} &= -1 \\ u_{\mathrm{iii}n} &= 0 \\ u_{\mathrm{iv}n} &= -\hat{X}_n \\ u_{\mathrm{v}n} &= 1 \\ u_{\mathrm{vi}n} &= -1 \end{aligned} , \tag{4.4.22}$$

Then, the control laws u_{1_n}, u_{2_n} and u_{3_n} take the form of equations 4.4.23, 4.4.24 and 4.4.25, respectively:

$$u_{1_n} = -Y_n e_{1_n} - \hat{X}_n e_{2_n} + e_{3_n} \tag{4.4.23}$$

$$u_{2_n} = -e_{1_n} \tag{4.4.24}$$

$$u_{3_n} = -e_{2_n} \tag{4.4.25}$$

The performance of the control laws of equations 4.4.23-4.4.25 is demonstrated in Figure 4.16, from which instant synchronization of all three master-slave signals can be observed.

It has thus been demonstrated that by following theorem 2 it is possible to achieve synchronization for $\Re^1$, $\Re^2$ and $\Re^3$ master-slave chaotic maps. Furthermore, by reducing the error system matrix *B* to zero, it has been shown that all master slave signals synchronize instantly, that is, within one time step. The important advantage of instant synchronization on the performance of a chaotic communication system is demonstrated in chapter 6.

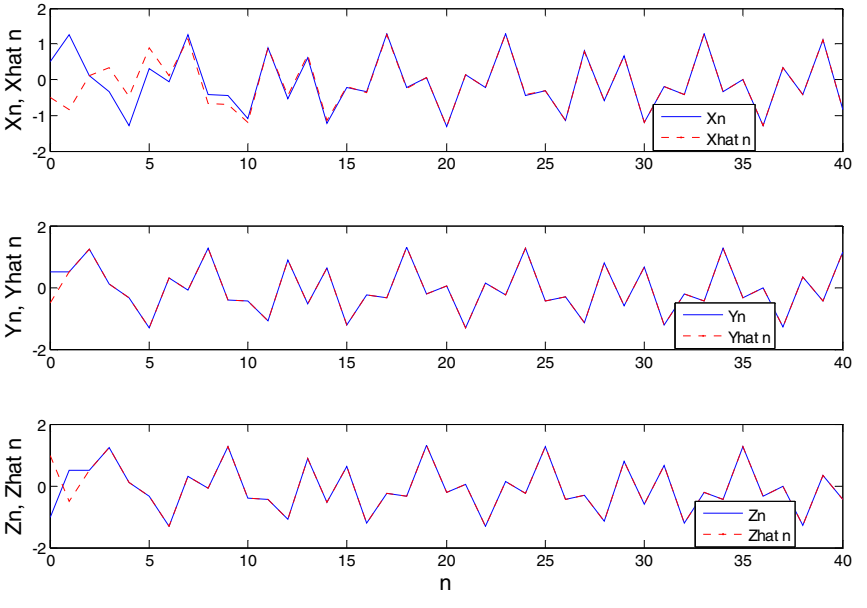


Fig. 4.14 Synchronization of the master-slave Lorenz $\Re^3$ chaotic signals when two of the eigenvalues are equal to zero while the third one is equal to $0.6 + j0.5$, where *j* denotes the complex number

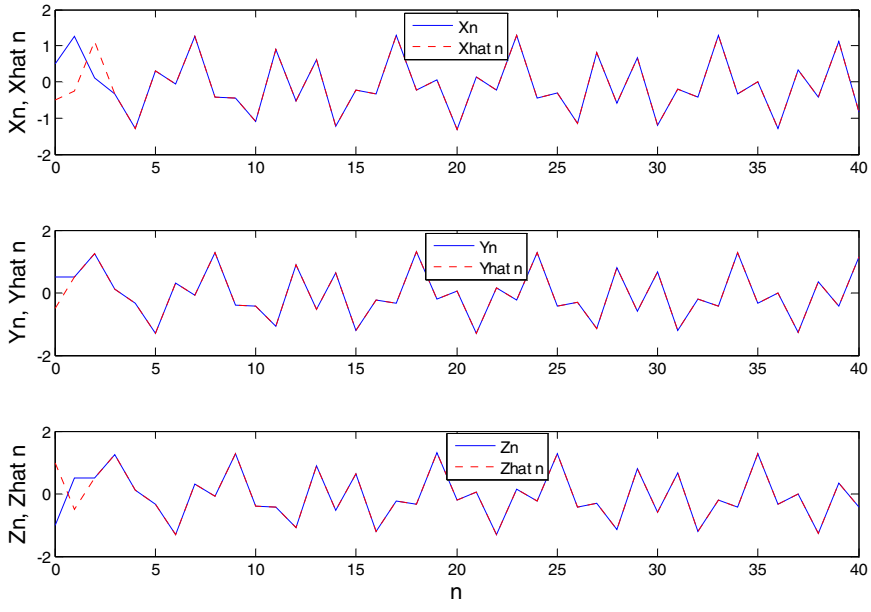


Fig. 4.15 Finite time synchronization of the master-slave Lorenz $\Re^3$ chaotic signals with the control laws of equations 4.4.15-4.4.17, that is, when all eigenvalues are equal to zero

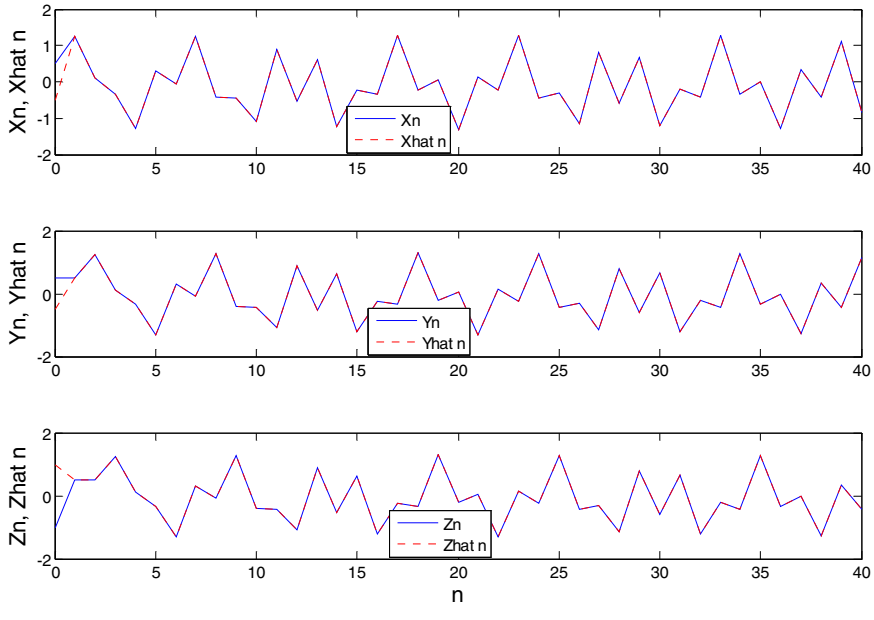


Fig. 4.16 Instant synchronization of the master-slave Lorenz $\Re^3$ chaotic signals using the control laws of equations 4.4.23-4.4.25, that is, when matrix B is equal to zero

4.5 Conclusion

In this chapter a method of designing the nonlinear control laws for the synchronization of the chaotic map master-slave systems has been proposed. The nonlinear control laws are designed in such a way to ensure that the eigenvalues of the error system matrix always fall within the unit circle in the z domain. This ensures the global asymptotic stability of the error system and thus causes the master-slave system of any complexity to synchronize. The general approach to the master-slave chaotic map synchronization has been demonstrated on the $\Re^1$ cubic map master-slave system, the $\Re^2$ tinkerbell map master-slave system and the Lorenz $\Re^3$ chaotic map master-slave system. Furthermore, it has been shown that it is always possible to achieve instant synchronization, within a single iteration of the master-slave system, when the control laws are designed in such a way to reduce the error system matrix to zero.

References

[1] Jovic, B., Unsworth, C.P.: Synchronization of Chaotic Communication Systems. In: Wang, C.W. (ed.) Nonlinear Phenomena Research Perspectives. Nova Publishers, New York (2007)

[2] Pecora, L.M., Carroll, T.L.: Synchronization in chaotic systems. Physical Review Letters 64(8), 821–824 (1990)

[3] Jovic, B., Unsworth, C.P.: Fast synchronisation of chaotic maps for secure chaotic communications. IET Electronics Letters 46(1) (2010)

[4] Park, J.H.: Chaos synchronization of a chaotic system via nonlinear control. Chaos, Solitons and Fractals 25(3), 579–584 (2005)

[5] Chen, G., Dong, X.: From chaos to order: Methodologies, Perspectives and Applications, pp. 598–614. World Scientific Publishing Co. Pte. Ltd., Singapore (1998)

[6] Ushio, T.: Chaotic synchronization and controlling chaos based on contraction mappings. Physics Letters A 198(1), 14–22 (1995)

[7] Zhou, C.-S., Chen, T.-L.: Robust communication via chaotic synchronization based on contraction maps. Physics Letters A 225(1-3), 60–66 (1997)

[8] Millerioux, G., Mira, C.: Finite-Time Global Chaos Synchronization for Piecewise Linear Maps. IEEE Transactions on Circuits and Systems – I: Fundamental Theory and Applications 48(1), 111–116 (2001)

[9] Millerioux, G., Mira, C.: Communicating via Chaos Synchronization Generated by Noninvertible Maps. In: Proceedings of the 1998 International Symposium on Circuits and Systems (ISCAS 1998), Monterey, CA, May 31-June 3, pp. IV-510–IV-513 (1998)

[10] Millerioux, G., Mira, C.: Noninvertible piecewise linear maps applied to chaos synchronization and secure communications. International Journal of Bifurcation and Chaos 7(7), 1617–1634 (1997)

[11] Millerioux, G.: Chaotic synchronization conditions based on control theory for systems described by discrete piecewise linear maps. International Journal of Bifurcation and Chaos 7(7), 1635–1649 (1997)

[12] Millerioux, G., Mira, C.: Coding scheme based on chaos synchronization from non-invertible maps. International Journal of Bifurcation and Chaos 8(10), 2019–2029 (1998)
[13] Nan, M., Wong, C.-n., Tsang, K.-f., Shi, X.: Secure digital communication based on linearly synchronized chaotic maps. Physics Letters A 268(1-2), 61–68 (2000)
[14] Guedes de Oliveira, A., Jones, A.J.: Synchronisation of chaotic maps by feedback control and application to secure communications using chaotic neural networks. International Journal of Bifurcation and Chaos 8(11), 2225–2237 (1998)
[15] Sushchik, M.M., Rulkov, N.F., Abarbanel, H.D.I.: Robustness and Stability of Synchronized Chaos: An Illustrative Model. IEEE Transactions on Circuits and Systems – I: Fundamental Theory and Applications 44(10), 867–873 (1997)
[16] Yan, Z.: Q-S synchronization in 3D Henon-like map and generalized Henon map via a scalar controller. Physics Letters A 342(4), 309–317 (2005)
[17] Dutta, M.: Synchronizing chaotic maps using an arbitrary scalar signal. Physical Review E 72(2), 026217-1–026217-5 (2005)
[18] Masoller, C., Marti, A.C.: Random Delays and the Synchronization of Chaotic Maps. Physical Review Letters 94(13),134102-1–134102-4 (2005)
[19] Parlitz, U., Ergezinger, S.: Robust communication based on chaotic spreading sequences. Physics Letters A 188(2), 146–150 (1994)
[20] Vidyasagar, M.: Nonlinear Systems Analysis, 2nd edn., p. 267. Society for Industrial and Applied Mathematics, Philadelphia (2002)
[21] Sprott, J.C.: Chaos and Time-Series Analysis, pp. 230–440. Oxford University Press, Oxford (2003)

Chapter 5
A Novel Mathematical Analysis for Predicting Master-Slave Chaotic Synchronization

In this chapter, a novel mathematical analysis for predicting master-slave chaotic synchronization is presented. In most situations when examining this type of synchronization one considers the asymptotic stability of the particular system via Lyapunov's direct method, or conditional Lyapunov exponents are considered. Initially, in this chapter, Lyapunov's direct method is used to show the asymptotic stability within the simplest piecewise linear master-slave chaotic flow. However, primarily the master-slave synchronization properties of the simplest quadratic chaotic flow and Ueda chaotic system are examined directly by means of mathematical manipulation of their dynamical equations, where possible, as well as via numerical simulations. In order to achieve this, numerical simulations and theoretical analysis are made use of in conjunction. In this way, it is shown that the synchronization error of the two aforementioned chaotic master-slave systems can indeed be predicted for certain driving signals, without the need for either analytical or numerical evaluation of the conditional Lyapunov exponents or employment of Lyapunov's direct method.

In [1], it has been demonstrated that the necessary condition for PC master-slave synchronization to occur is for the sub-Lyapunov exponents, (later renamed conditional Lyapunov exponents [2]), of the non-driving/non-driven subsystem to be less than zero. In particular, this has been shown for the Lorenz and Rossler chaotic systems [1]. The necessary and sufficient condition for master-slave synchronization to occur is that the part of the slave system not being driven by the master system must be asymptotically stable [3]. As shown in chapter 3, asymptotic stability of a system can be demonstrated via Lyapunov's direct (or second) method [4] by demonstrating the existence of the Lyapunov function. This method was used in [3] to show that the Lorenz master-slave systems must synchronize when the master x signal drives the slave system. Using the methodology from [3] a similar proof was derived for the Van der Pol Duffing oscillator in [5]. In this chapter, initially the existence of the Lyapunov function is briefly demonstrated, following the procedure of section 3.3, for the simplest piecewise linear chaotic flow, when the x signal drives. The simplest piecewise linear chaotic flow is easily realizable in the form of an electronic circuit [6]. However, the main emphasis of this chapter is on the master-slave synchronization via direct mathematical analysis of the dynamics of the simplest quadratic master-slave

B. Jovic: Synchronization Techniques for Chaotic Commun. Syst., SCT 5, pp. 103–133.
springerlink.com

chaotic flow and the Ueda master-slave chaotic system [7]. These systems have been selected for the analysis due to it being possible, as shown in this chapter [7], to analyze their PC synchronization properties without the use of Lyapunov's stability theory or the need to obtain the conditional Lyapunov exponents. Numerical simulations are used to further support the analysis. Unlike the Lyapunov's stability theory which describes the general behaviour of the system, the novel mathematical analysis presented in this chapter [7] describes the system's behaviour using the strict mathematical equations. It therefore gives a deeper insight mathematically into what dynamically occurs. A secure communication system based on the chaotic synchronization phenomena presented here is presented in chapter 6.

In Section 5.1 it is shown that the asymptotic stability, which is a necessary and sufficient condition for synchronization, exists within the simplest piecewise linear master-slave chaotic flow, when the master x signal drives the slave subsystem. This is followed by the numerical simulations and a mathematical analysis of the simplest quadratic master-slave chaotic flow in Section 5.2 and the Ueda master-slave chaotic system in Section 5.3.

5.1 Synchronization and Asymptotic Stability of the Simplest Piecewise Linear Master-Slave Chaotic Flow

The simplest piecewise linear chaotic flow is given by equation 3.2.1, repeated below for convenience as equation 5.1.1:

$$\begin{aligned} \dot{x} &= y \\ \dot{y} &= z \\ \dot{z} &= -Az - y + |x| - 1 \end{aligned} \tag{5.1.1}$$

The system of equation 5.1.1 exhibits chaotic behaviour with the parameter value $A = 0.6$ [6]. As outlined in section 3.1 of chapter 3, this system is said to be the master system [1,3] which drives the slave system by one of its signals. The remaining two slave signals are generated using identical equations to those of the master system except that the initial conditions are different.

5.1.1 Master-Slave System with the Master x Signal Driving

The simplest piecewise linear master-slave chaotic flow when the master x signal drives has been presented in Figure 3.3 of chapter 3. As in chapter 3, the slave variables are denoted by '^' (hat), while the 'dot' above the variable denotes the operation *d/dt*. The parameter values of the master and slave systems are identical. Initial conditions of x, y and z signals are denoted as $x(0)$, $y(0)$ and $z(0)$.

In the top graph of Figure 5.1 the difference between the output signal y of the master and the output signal $\hat{y}$ of the slave system are shown. The difference between the two signals decreases in time, becoming negligible after approximately 10 time units, when the master and slave systems synchronize. This difference between the master and slave signals is defined as the synchronization error. It can be observed from Figure 5.1 that the synchronization error tends to zero for both, the master-slave signals y and the master-slave signals z.

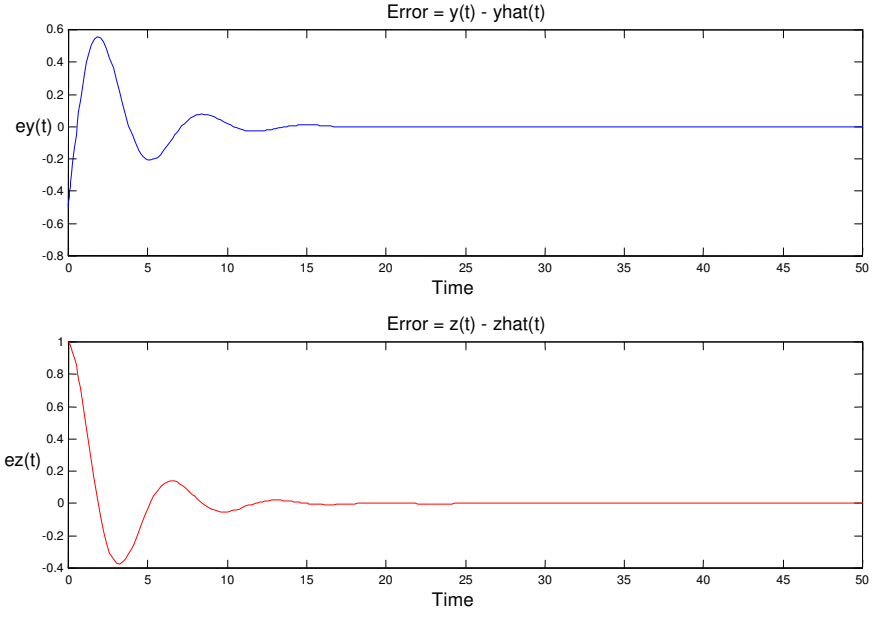


Fig. 5.1 Upper graph: The error of the simplest piecewise linear master-slave y signals. Lower graph: The error of the simplest piecewise linear master-slave z signals.

It is now shown, via the Lyapunov's direct method, that the simplest piecewise linear master-slave chaotic flow must synchronize when x drives. The difference between the non-driving master subsystem and non-driven slave subsystem is denoted by '*', and when x drives it is given by equation 5.1.2:

$$\boldsymbol{v}^* = \boldsymbol{v} - \hat{\boldsymbol{v}} = \begin{bmatrix} y^* \\ z^* \end{bmatrix} = \begin{bmatrix} y - \hat{y} \\ z - \hat{z} \end{bmatrix} \tag{5.1.2}$$

For the master-slave system of Figure 3.3 the differential error is expressed by equation 5.1.3:

$$\dot{\boldsymbol{v}}^* = \begin{bmatrix} \dot{y}^* \\ \dot{z}^* \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & -A \end{bmatrix} \begin{bmatrix} y^* \\ z^* \end{bmatrix} \tag{5.1.3}$$

Now consider the Lyapunov function given by equation 5.1.4:

$$E = y^{*2} + \frac{1}{2} z^{*2} + \frac{1}{2}(Ay^* + z^*)^2 \tag{5.1.4}$$

Differentiating equation 5.1.4 with respect to time, equation 5.1.5 is obtained:

$$\dot{E} = 2y^* \dot{y}^* + z^* \dot{z}^* + (Ay^* + z^*)(A\dot{y}^* + \dot{z}^*) \tag{5.1.5}$$

Substituting the expressions for $\dot{y}^*$ and $\dot{z}^*$ of equation 5.1.3 into equation 5.1.5, equation 5.1.6 is obtained:

$$\dot{E} = -Ay^{*2} - Az^{*2} = -A(y^{*2} + z^{*2}) = -A((y - \hat{y})^2 + (z - \hat{z})^2) \leq 0 \tag{5.1.6}$$

As the derivative of the Lyapunov function, shown in equation 5.1.6, is always less than zero, the subsystem $\hat{v}$ is asymptotically stable (the equality sign applies only at the origin), i.e. equation 5.1.6 is negative semi-definite. Therefore, as the necessary and sufficient condition for synchronization is satisfied, theoretically the system of Figure 3.3 must synchronize.

5.1.2 Master-Slave System with the Master y Signal Driving

With the master *y* signal driving, the master-slave *z* signals do not synchronize, while the synchronization error of the master-slave *x* signals is governed by equation 5.1.7:

$$x - \hat{x} = x(0) - \hat{x}(0) = J \tag{5.1.7}$$

The numerical simulation confirming the result of equation 5.1.7 is shown in the upper graph of Figure 5.2. It can be observed from the upper graph of Figure 5.2 that the synchronization error is indeed constant and equal to the difference among the master slave *x* initial conditions. The lower graph of Figure 5.2 shows

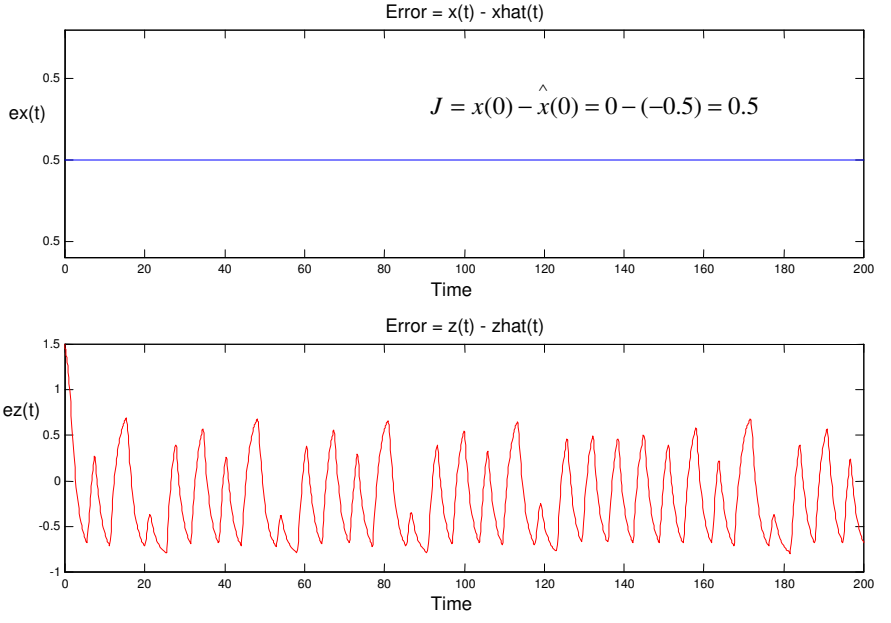


Fig. 5.2 Upper graph: The error of the simplest piecewise linear master-slave x signals. Lower graph: The error of the simplest piecewise linear master-slave z signals.

that the master-slave z signals do not synchronize as the synchronization error is non-zero for all time.

5.1.3 Master-Slave System with the Master z Signal Driving

With the master z signal driving, the synchronization error of the master-slave y signals is governed by equation 5.1.8, while the synchronization error of the master-slave x signals is governed by equation 5.1.9:

$$y - \hat{y} = y(0) - \hat{y}(0) = K \tag{5.1.8}$$

$$x - \hat{x} = (x(0) - \hat{x}(0)) + (y(0) - \hat{y}(0))t = L + Kt \tag{5.1.9}$$

The results of equations 5.1.8 and 5.1.9 are confirmed by the numerical simulations presented in Figure 5.3. In the next section, the mathematical procedure of obtaining equations analogous to equations 5.1.7-5.1.9 will be presented.

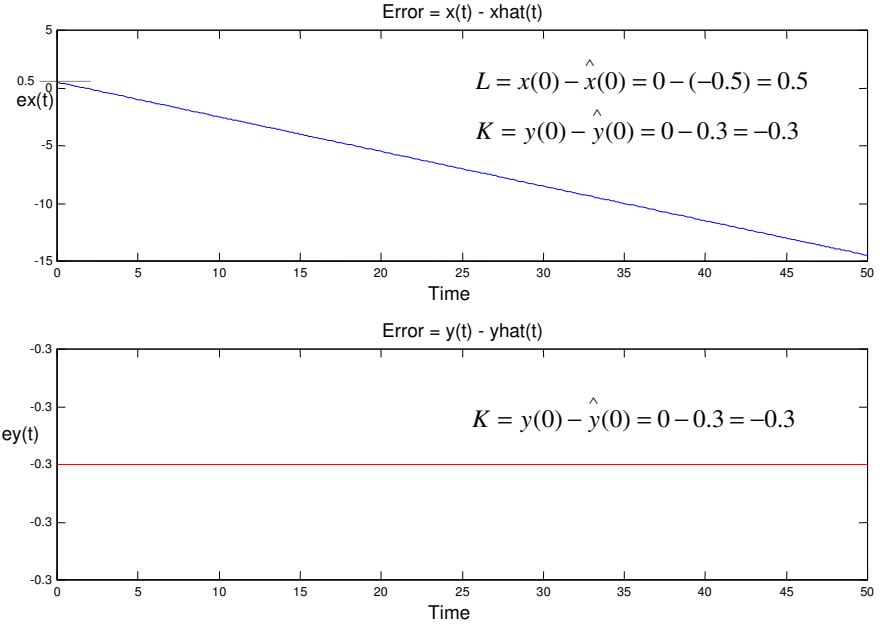


Fig. 5.3 Upper graph: The error of the simplest piecewise linear master-slave x signals. Lower graph: The error of the simplest piecewise linear master-slave y signals.

5.1.4 Summary of the Synchronization Properties

Overall, for the simplest piecewise linear master-slave chaotic flow it has been shown that when ***x* drives**, the master-slave system synchronizes. When ***y* drives**, the synchronization error of the master-slave x signals is constant while the master-slave z signals do not synchronize. Finally, when ***z* drives**, the synchronization error of the master-slave y signals is constant while the error of the master-slave x signals increases linearly.

5.2 The Simplest Quadratic Master-Slave Chaotic Flow

The simplest quadratic chaotic flow is given by equation 5.2.1:

$$\begin{aligned} \dot{x} &= y \\ \dot{y} &= z \\ \dot{z} &= -Az + y^2 - x \end{aligned} \tag{5.2.1}$$

The system of equation 5.2.1, exhibits chaotic behaviour with the parameter value $A = 2.017$ [6].

5.2.1 Master-Slave System with the Master z Signal Driving

Figure 5.4, shows the simplest quadratic master-slave chaotic flow when the master z signal drives.

In Figure 5.5a, the synchronization of the master-slave signals when z drives is shown. From Figure 5.5b, one can see that the error is constant for y signals, and that the error is linearly increasing (in the negative sense) for x signals. The initial conditions of the master system are chosen to be $x(0) = -0.01$, $y(0) = -0.001$, $z(0) = 0.01$. The initial conditions of the slave system are chosen to be $\hat{x}(0) = -0.5$, $\hat{y}(0) = 0.9$.

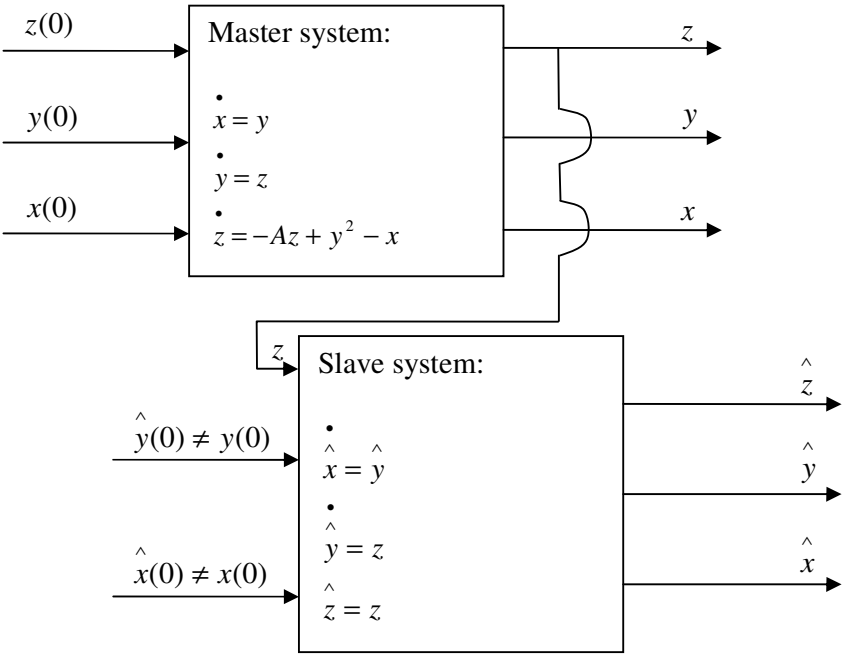


Fig. 5.4 The block diagram of the simplest quadratic master-slave chaotic flow, with the z signal driving. The parameter value is $A = 2.017$.

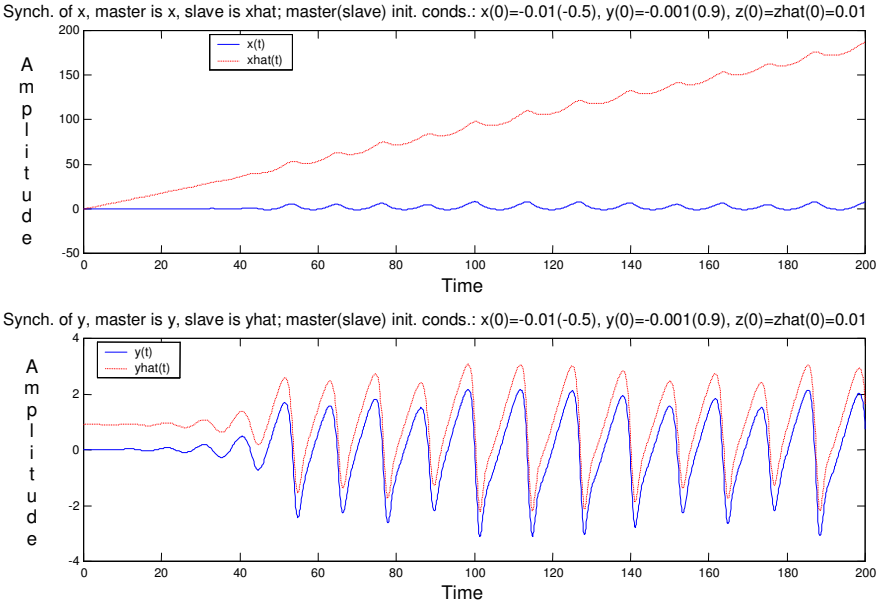


Fig. 5.5a Synchronization of the master-slave simplest quadratic chaotic signals, with the z signal driving.

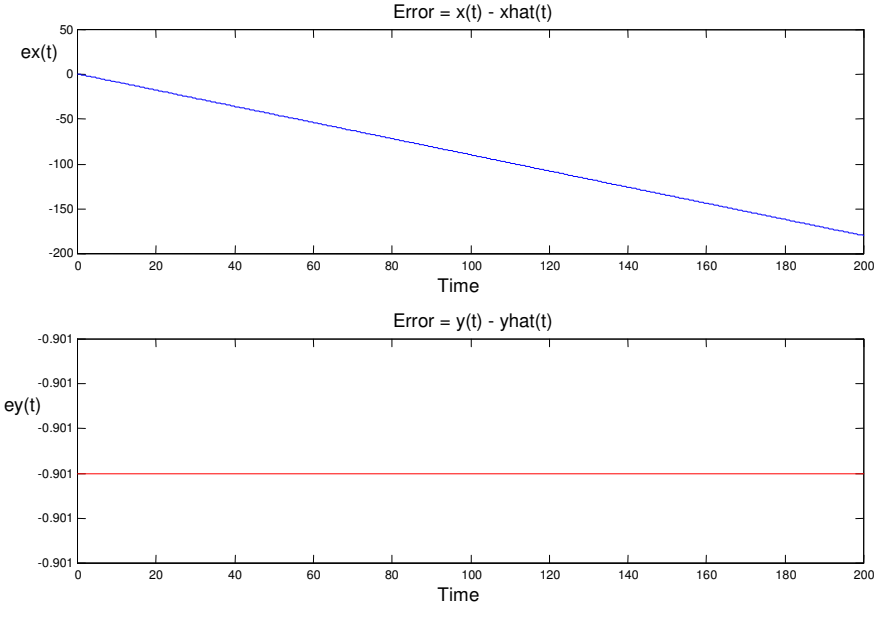


Fig. 5.5b Upper graph: The error of the simplest quadratic master-slave x signals. Lower graph: The error of the simplest quadratic master-slave y signals.

The constant error of the master-slave y signals, observed in Figure 5.5b, lower graph, can be determined in the following manner. Keeping in mind that $\dot{y} = z$ and $\dot{\hat{y}} = z$, equation 5.2.2 is obtained:

$$\dot{\hat{y}} = \dot{y} \tag{5.2.2}$$

Integrating both sides of equation 5.2.2, and assuming unequal initial conditions,

$$\int \dot{\hat{y}}\, dt = \int \dot{y}\, dt$$

equation 5.2.3 is obtained:

$$\hat{y} + D = y + C \qquad \text{or} \qquad \hat{y} - D = y - C$$

$$\hat{y} - y = A \qquad \text{or} \qquad y - \hat{y} = A \tag{5.2.3}$$

where $A = C - D = y(0) - \hat{y}(0) = -0.001 - 0.9 = -0.901$. The second version of equation 5.2.3 ($y - \hat{y} = A$) suits the situation more, as in this case it precisely describes the lower graph of Figure 5.5b – it does not just indicate the constant difference between the master-slave y signals. In [8] the constant error among master-slave signals was predicted by demonstrating that one or more of the conditional Lyapunov exponents (CLEs) are zero and none are positive. In contrast, it has been shown here that this constant error can be determined by direct mathematical manipulation of the master-slave equations. This technique will also be further used in this chapter.

With z as the driving signal, and keeping in mind that $y - \hat{y} = A$, equations 5.2.4 and 5.2.5 are obtained:

$$\dot{x} = y \tag{5.2.4}$$

$$\dot{\hat{x}} = \hat{y} = y - A \qquad \text{(from } y - \hat{y} = A \text{, equation 5.2.3)} \tag{5.2.5}$$

$$\dot{\hat{x}} = \dot{\hat{y}} = \dot{x} - A \qquad \text{(from equation 5.2.4 and 5.2.5)} \qquad (5.2.6)$$

$$\dot{x} = \dot{\hat{x}} + A \qquad \text{(from equation 5.2.6)} \qquad (5.2.7)$$

Integrating both sides of equation 5.2.7, and assuming unequal initial conditions,

$$\int \dot{x}\, dt = \int \dot{\hat{x}}\, dt + \int A dt$$

equation 5.2.8 is obtained:

$$x + E = \hat{x} + F + At \quad \text{or} \quad x - E = \hat{x} - F + At$$

$$\hat{x} - x = B - At \quad \text{or} \quad x - \hat{x} = B + At \qquad (5.2.8)$$

where $B = E - F = x(0) - \hat{x}(0) = 0.49$ (recall $A = C - D = y(0) - \hat{y}(0) = -0.901$).

The second version of equation 5.2.8 ($x - \hat{x} = B + At$) suits the situation more, as in this case it precisely describes the upper graph of Figure 5.5b – it does not just indicate the general behaviour of master-slave x signals.

5.2.2 Master-Slave System with the Master y Signal Driving

When the y signal drives, the simplest quadratic master-slave chaotic flow is represented by Figure 5.6.

In Figures 5.7a and 5.7b, the situation when the y signal drives is investigated. The initial conditions of the master system are chosen to be $x(0)$ = -0.01, $y(0)$ = -0.001, $z(0)$ = 0.01. The initial conditions of the slave system are chosen to be $\hat{x}(0) = -0.5$, $\hat{z}(0) = -2$.

From Figure 5.7a, one can see that as time tends to infinity the master and slave systems do not synchronize. Figure 5.7b shows that the error is always constant, with a value of 0.49, for master-slave x signals. For master-slave z signals, the error settles to a constant value of -0.2429 as time tends to infinity.

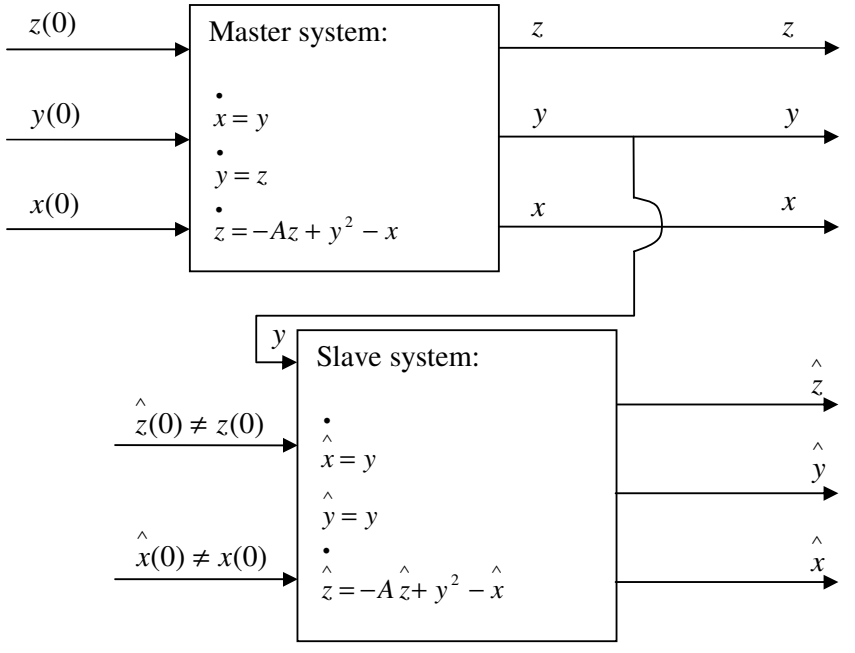


Fig. 5.6 The block diagram of the simplest quadratic master-slave chaotic flow, with the y signal driving. The parameter value is $A = 2.017$.

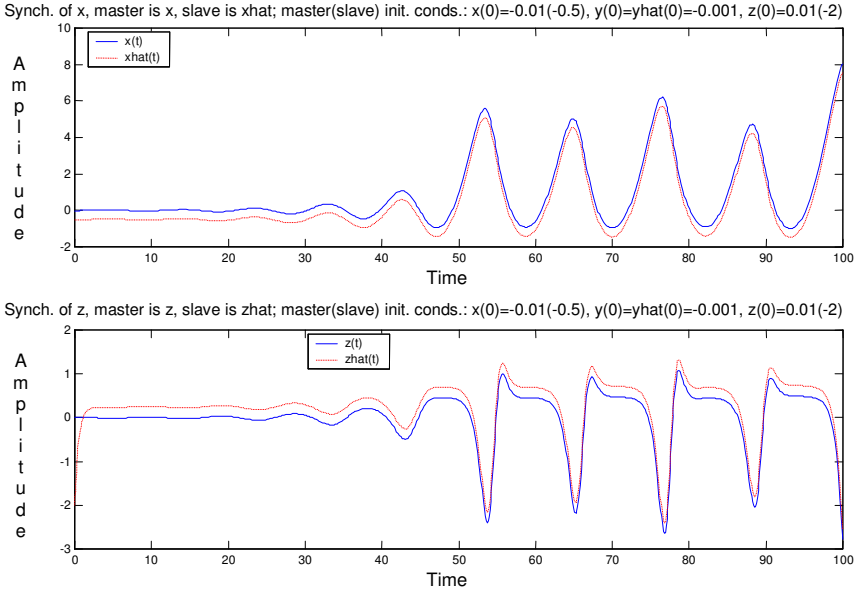


Fig. 5.7a Synchronization of the simplest quadratic master-slave chaotic signals, with the y signal driving.

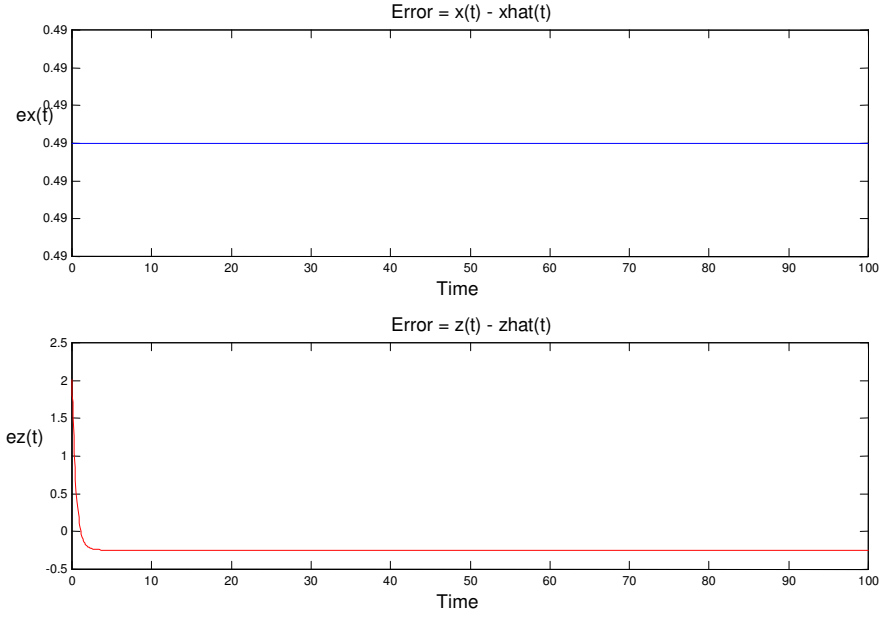


Fig. 5.7b Upper graph: The error of the simplest quadratic master-slave x signals. Lower graph: The error of the simplest quadratic master-slave z signals.

The constant error observed in Figure 5.7b, upper graph, is determined in the same manner as in the previous case and is given by equation 5.2.9:

$$x - \hat{x} = \alpha \tag{5.2.9}$$

where: $\alpha = x(0) - \hat{x}(0) = 0.49$.

The behaviour of the synchronization error of the master-slave z signals (Figure 5.7b, lower graph) is now considered. With the y signal driving, equations 5.2.10a and 5.2.10b are obtained by making y^2 the subject of the formulae (see Figure 5.6):

$$y^2 = \dot{z} + Az + x \tag{5.2.10a}$$

$$y^2 = \dot{\hat{z}} + A\hat{z} + \hat{x} \tag{5.2.10b}$$

Equating equations 5.2.10a and 5.2.10b and rearranging terms, equation 5.2.11 is obtained, which expresses the differential error of the master-slave z signals:

$$\dot{z} - \dot{\hat{z}} = -A(z - \hat{z}) - (x - \hat{x}) \tag{5.2.11}$$

Substituting equation 5.2.9 into equation 5.2.11, equation 5.2.12 is obtained:

$$\dot{z} - \dot{\hat{z}} = -A(z - \hat{z}) - \alpha \tag{5.2.12}$$

Integrating both sides of equation 5.2.12, one obtains equation 5.2.13:

$$\int (\dot{z} - \dot{\hat{z}})dt = -A\int (z - \hat{z})dt - \int \alpha \cdot dt$$

$$z - \hat{z} = \delta - A\int_0^t (z - \hat{z})dl - \alpha \cdot t \tag{5.2.13}$$

where δ is the constant of integration.

At a particular time $t = t_o$ equation 5.2.13 can be rewritten in the form of equation 5.2.14:

$$z(t_o) - \hat{z}(t_o) = \delta - A\int_0^{t=t_o} (z(t) - \hat{z}(t))dt - \alpha \cdot t_o \tag{5.2.14}$$

From the lower graph of Figure 5.7b, it is observed that the synchronization error of the master-slave z signals tends to a constant as time tends to infinity, which is expressed by equation 5.2.15:

$$\lim_{t\to\infty}(z(t) - \hat{z}(t)) = \text{constant} \tag{5.2.15}$$

Therefore equation 5.2.14, which represents this error, must tend to a constant as time t_o tends to infinity. Since the only isolated constant in equation 5.2.14 is δ, it must be the case that equation 5.2.14 tends to δ as time tends to infinity. Therefore, as time tends to infinity equation 5.2.14 takes the form of equation 5.2.16, and equation 5.2.15 can be rewritten as equation 5.2.17:

$$\lim_{t_o\to\infty}(z(t_o) - \hat{z}(t_o)) = \lim_{t_o\to\infty}(\delta - A\int_0^{t=t_o} (z(t) - \hat{z}(t))dt - \alpha \cdot t_o) = \delta \tag{5.2.16}$$

$$\lim_{t\to\infty}(z(t) - \hat{z}(t)) = \delta \tag{5.2.17}$$

Keeping in mind that the behaviour of $z - \hat{z}$ after the transients have died down is required, equation 5.2.17 is substituted into equation 5.2.16 to obtain equation 5.2.18:

$$\lim_{t_o\to\infty}(z(t_o) - \hat{z}(t_o)) = \lim_{t_o\to\infty}(\delta - A\int_0^{t=t_o} \delta \cdot dt - \alpha \cdot t_o) = \delta \tag{5.2.18}$$

Evaluating the definite integral of equation 5.2.18 one obtains equation 5.2.19:

$$\lim_{t_o \to \infty}(z(t_o) - \hat{z}(t_o)) = \lim_{t_o \to \infty}(\delta - A\delta \cdot t_o - \alpha \cdot t_o) = \delta \tag{5.2.19}$$

Equation 5.2.19 can also be rewritten as equation 5.2.20:

$$\lim_{t_o \to \infty}(z(t_o) - \hat{z}(t_o)) = \lim_{t_o \to \infty}(\delta - (A\delta + \alpha) \cdot t_o) = \delta \tag{5.2.20}$$

In order for equation 5.2.20 to be true, equation 5.2.21 must be true:

$$(A\delta + \alpha) \cdot t_o = 0 \tag{5.2.21}$$

Rearranging equation 5.2.21 one obtains equation 5.2.22:

$$\delta = -\frac{\alpha}{A} \tag{5.2.22}$$

Therefore, δ is equal to the negative difference in initial conditions of the master-slave x signals, divided by the A parameter of the chaotic system. Equation 5.2.22 therefore represents the constant value to which the synchronization error of the master-slave z signals tends as time tends to infinity.

It is known that in the case of the systems used to obtain Figure 5.7b, lower graph, the constants A and α are as given below:

$$A = 2.017 \qquad \text{and} \qquad \alpha = x(0) - \hat{x}(0) = -0.01 - -0.5 = 0.49$$

Substituting the above values for A and α into equation 5.2.22 one sees that, in fact, the constant synchronization error is equal to $\delta = -\alpha/A = -0.49/2.017 = -0.2429$. This value is indeed returned by the computer simulation used to form Figure 5.7b, lower graph. This confirms the validity of equation 5.2.22.

5.2.3 Master-Slave System with the Master x Signal Driving

In Figures 5.8a and 5.8b, the synchronization when the x signal drives is investigated. The initial conditions of the master system are chosen to be $x(0)$ = -0.01, $y(0)$ = -0.001, $z(0)$ = 0.01. The initial conditions of the slave system are chosen to be $\hat{y}(0) = 0.8$, $\hat{z}(0) = -3$.

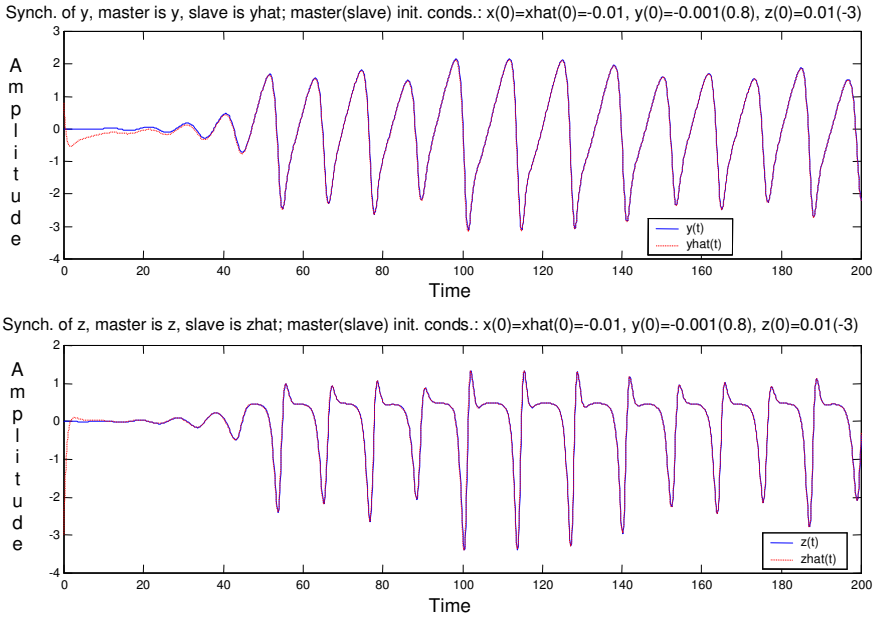


Fig. 5.8a Synchronization of the simplest quadratic master-slave chaotic signals, with the x signal driving.

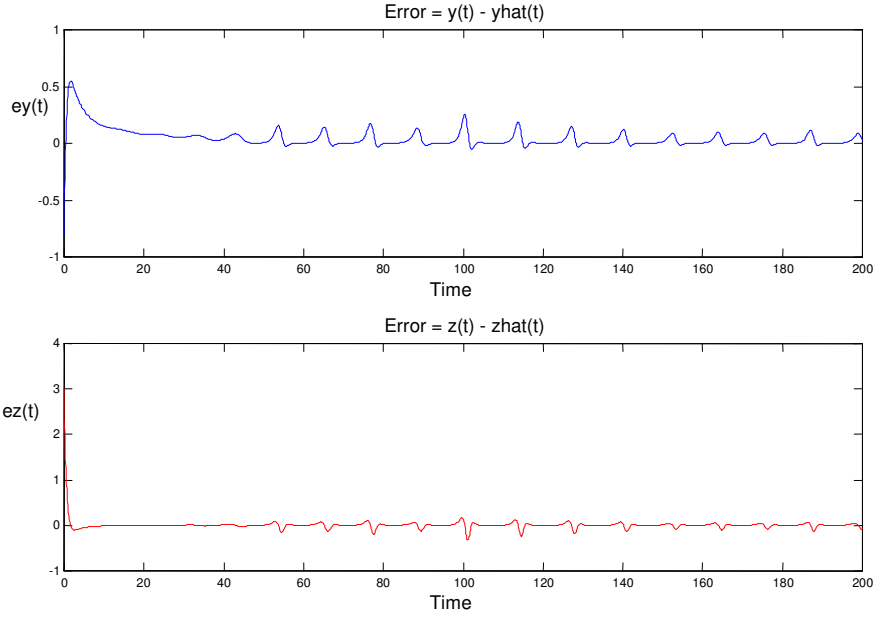


Fig. 5.8b Upper graph: The error of the simplest quadratic master-slave y signals. Lower graph: The error of the simplest quadratic master-slave z signals.

From Figure 5.8a, one can see that as time tends to infinity the master and slave systems appear to synchronize. However, Figure 5.8b reveals that the synchronization is not exact, as the minimal, periodic-like, error always remains and is always in the very close vicinity of zero.

5.2.4 Summary of the Synchronization Properties

Overall, for the simplest quadratic master-slave chaotic flow it has been observed that when ***x* drives**, the master-slave system synchronizes. When ***y* drives**, the synchronization error of the master-slave x signals is a constant while the error of the master-slave z signals settles to a constant value. Finally when ***z* drives**, the synchronization error of the master-slave y signals is constant while the error of the master-slave x signals increases linearly.

5.3 The Ueda Master-Slave Chaotic System

Consider the Ueda chaotic system, given by equation 5.3.1 [9]:

$$\begin{aligned} \dot{x} &= y \\ \dot{y} &= -x^3 - ky + B\cos(z) \\ \dot{z} &= 1 \end{aligned} \tag{5.3.1}$$

The system described by equation 5.3.1 exhibits chaotic behaviour with the parameter values $k = 0.05$, $B = 7.5$ [6].

5.3.1 Master-Slave System with the Master x Signal Driving

Figure 5.9 shows the Ueda master-slave system when the master x signal drives.

In Figures 5.10a and 5.10b, synchronization when the x signal drives is investigated. The initial conditions of the master system are chosen to be $x(0) = 1$, $y(0) = 0$, $z(0) = 0$. The initial conditions of the slave system are chosen to be $\hat{y}(0) = 2$, $\hat{z}(0) = 1$. From Figure 5.10a, one can see that the master-slave signals do not synchronize; however, Figure 5.10b reveals that the error of the master-slave y signals seems to settle to a periodic behaviour as time tends to infinity, and that the error of the master-slave z signals is constant.

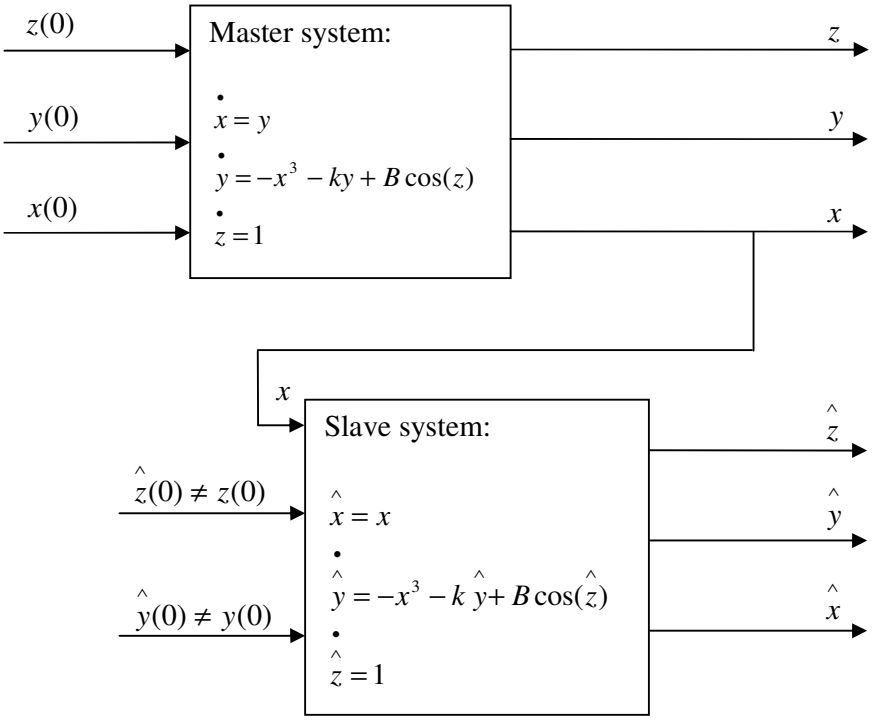


Fig. 5.9 The block diagram of the Ueda master-slave chaotic system, with the *x* signal driving. The parameter values are $k = 0.05$, $B = 7.5$.

The fact that the error of the master-slave *z* signals is constant can be explained in the same fashion as in the previous cases above, and it is given by equation 5.3.2:

$$z - \hat{z} = C - D = \alpha \tag{5.3.2}$$

where: $\alpha = C - D = z(0) - \hat{z}(0) = -1$.

The fact that the error of the master-slave *y* signals seems to settle to a periodic behaviour is now explained. By manipulating equation 5.3.2 and introducing the term $-2\hat{z}$ to allow for the expression for $z + \hat{z}$, equation 5.3.4 is obtained:

$$z + \hat{z} - 2\hat{z} = C - D \tag{5.3.3}$$

$$z + \hat{z} = C - D + 2\hat{z} \tag{5.3.4}$$

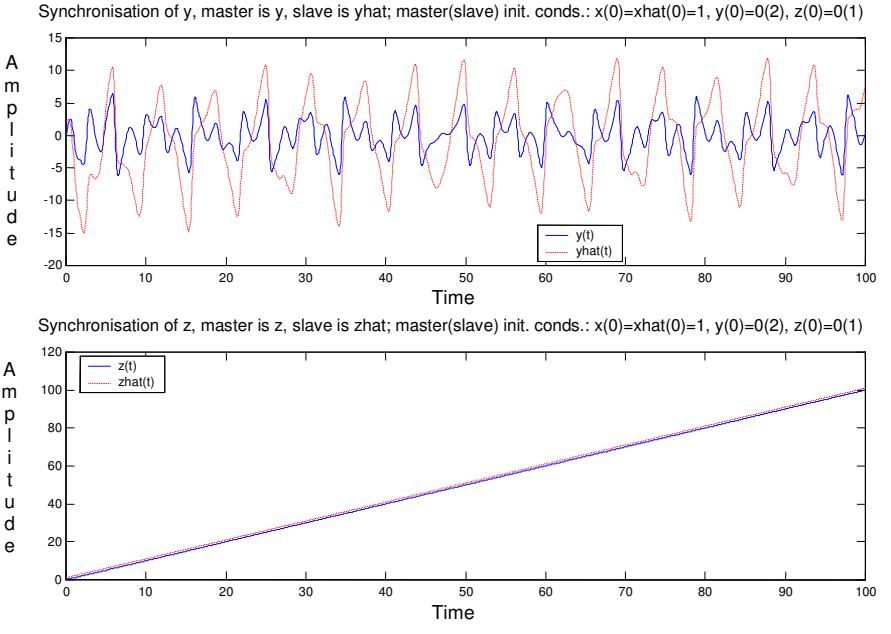


Fig. 5.10a Synchronization of the master-slave Ueda chaotic signals, with the *x* signal driving.

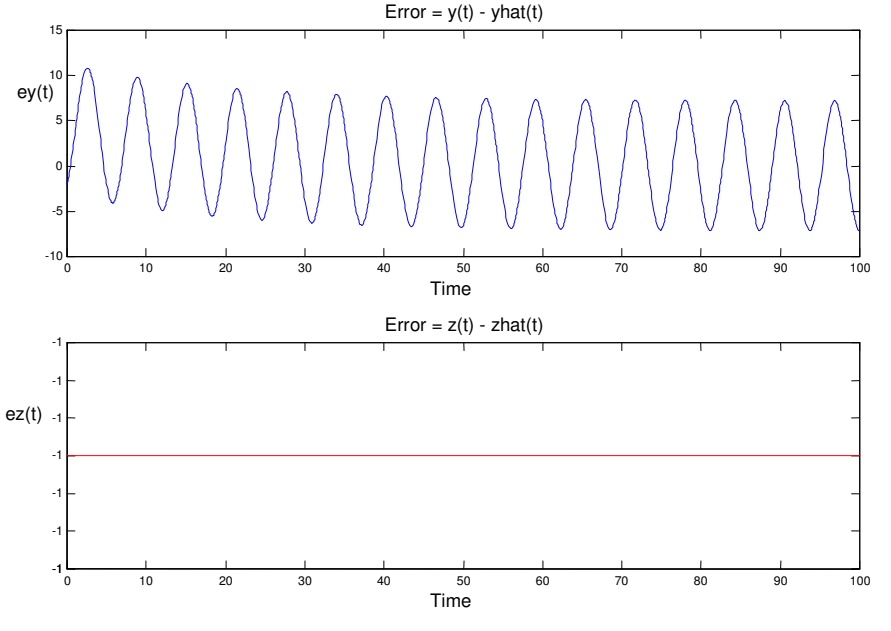


Fig. 5.10b Upper graph: The error of the Ueda master-slave *y* signals. Lower graph: The error of the Ueda master-slave *z* signals.

From Figure 5.9 it is also observed that equations 5.3.5a and 5.3.5b hold:

$$\dot{z} = 1 \qquad \text{(5.3.5a)} \qquad\qquad \dot{\hat{z}} = 1 \qquad \text{(5.3.5b)}$$

Integrating equation 5.3.5a, equation 5.3.6a is obtained; integrating equation 5.3.5b, equation 5.3.6b is obtained:

$$z = t + C \qquad \text{(5.3.6a)} \qquad\qquad \hat{z} = t + D \qquad \text{(5.3.6b)}$$

Substituting equation 5.3.6b into equation 5.3.4, equation 5.3.7 is obtained:

$$z + \hat{z} = C - D + 2(t + D)$$
$$z + \hat{z} = C + D + 2t \qquad \text{(5.3.7)}$$

Plotting, in Figure 5.11, $z + \hat{z}$, it can be seen that equation 5.3.7 holds. Note that $C + D = (0 + 1) = 1$, so that $z + \hat{z} = 1 + 2t$, as is shown in Figure 5.11.

From master and slave systems of Figure 5.9 equations 5.3.8 and 5.3.9 are obtained:

$$-x^3 = \dot{y} + ky - B\cos(z) \qquad \text{(5.3.8)}$$

$$-x^3 = \dot{\hat{y}} + k\hat{y} - B\cos(\hat{z}) \qquad \text{(5.3.9)}$$

Equating equations 5.3.8 and 5.3.9 and rearranging terms, equation 5.3.10 is obtained. Manipulating and solving equation 5.3.10 for the error of the master-slave y signals, one proceeds to eventually obtain equation 5.3.19 by following the steps given below:

$$\dot{y} - \dot{\hat{y}} = -k(y - \hat{y}) + B(\cos(z) - \cos(\hat{z})) \qquad \text{(5.3.10)}$$

Note that $\cos(z)$ and $\cos(\hat{z})$ represent two cosines of the same frequency, but starting at different initial conditions, (C and D), as shown by equations 5.3.6a and 5.3.6b, respectively.

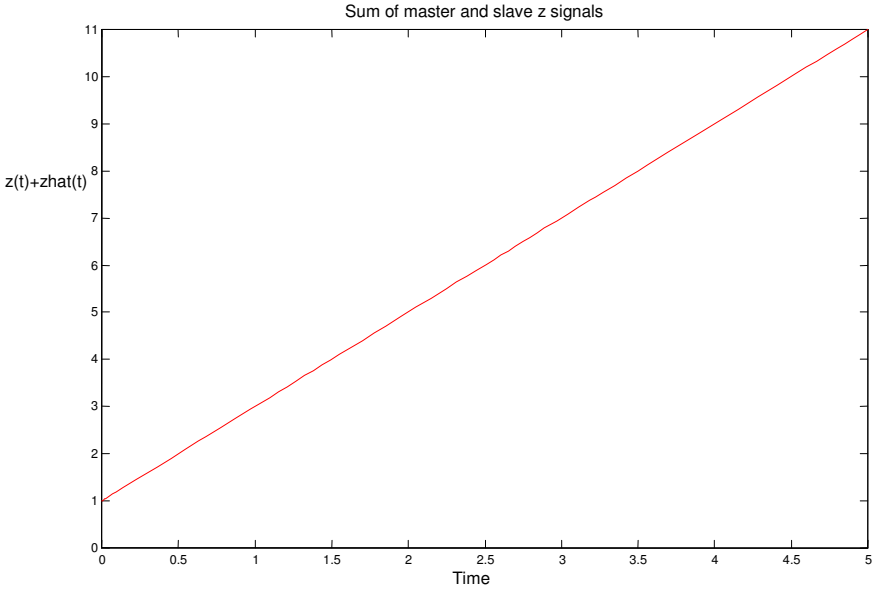


Fig. 5.11 Sum of the master and slave z signals, represented as: $z+\hat{z}=1+2t$.

Integrating both sides of equation 5.3.10, and using standard trigonometric identities, equation 5.3.11 is obtained:

$$\int(\dot{y}-\dot{\hat{y}})dt=-k\int(y-\hat{y})dt+B\int(\cos(z)-\cos(\hat{z}))dt$$

$$=-k\int(y-\hat{y})dt-2B\int\left(\sin\left(\frac{z+\hat{z}}{2}\right)\sin\left(\frac{z-\hat{z}}{2}\right)\right)dt \qquad (5.3.11)$$

But from equation 5.3.2 it is known that $z-\hat{z}$ is a constant ($z-\hat{z}=C-D=\alpha$).

Now define a new constant ϕ:

$$\phi=\frac{z-\hat{z}}{2}=\frac{C-D}{2}=\frac{\alpha}{2} \qquad (5.3.12)$$

Substituting equation 5.3.7, i.e. ($z+\hat{z}=C+D+2t$), as well as equation 5.3.12, into equation 5.3.11, equation 5.3.13 is obtained:

$$\int (\dot{y} - \dot{\hat{y}})dt = -k\int (y - \hat{y})dt - 2B\sin(\phi)\int \sin\left(\frac{C+D}{2} + t\right)dt \qquad (5.3.13)$$

Now define a constant θ:

$$\theta = \frac{C+D}{2} = \frac{\alpha + 2D}{2} = \phi + D \qquad (5.3.14)$$

Substituting equation 5.3.14, into equation 5.3.13, equation 5.3.15 is obtained:

$$\int (\dot{y} - \dot{\hat{y}})dt = -k\int (y - \hat{y})dt - 2B\sin(\phi)\int \sin(\theta + t)dt \qquad (5.3.15)$$

Again using the trigonometric identities, it can be seen that equation 5.3.15 can be written in the form of equation 5.3.16:

$$\int (\dot{y} - \dot{\hat{y}})dt = -k\int (y - \hat{y})dt - 2B\sin(\phi)\int (\sin(\theta)\cos(t) + \cos(\theta)\sin(t))dt \qquad (5.3.16)$$

Simplifying equation 5.3.16 and evaluating the integrals, equation 5.3.17 is obtained. It must be noted that in equation 5.3.17 the first term of equation 5.3.16 becomes a definite integral. Equation 5.3.17 represents a general case at some time *to*:

$$y(t_o) - \hat{y}(t_o) = A - k\int_{t=0}^{t=t_o} (y(t) - \hat{y}(t))dt + 2B\sin(\phi)(-\sin(\theta)\sin(t_o) + \cos(\theta)\cos(t_o)) \qquad (5.3.17)$$

where *A* is the constant of integration.

The trigonometric identity given by equation 5.3.18 will be used in what follows:

$$a\sin(t) + b\cos(t) = R\sin(t + \Omega) \qquad (5.3.18)$$

where $R = \sqrt{a^2 + b^2}$ and $\sin\Omega = \frac{b}{R}$, $\cos\Omega = \frac{a}{R}$.

Relating part of the third term of equation 5.3.17 $(-\sin(\theta)\sin(t_o) + \cos(\theta)\cos(t_o))$ to equation 5.3.18, it is seen that it can be put into the form of equation 5.3.18 in the following manner:

$$a = -\sin\theta$$
$$b = \cos\theta \qquad \sin\Omega = \frac{\cos\theta}{1} \qquad \text{and} \qquad \cos\Omega = \frac{-\sin\theta}{1}$$
$$R = \sqrt{\sin^2\theta + \cos^2\theta} = 1$$

Therefore, to find Ω one must satisfy both $\sin\Omega = \cos\theta$ and $\cos\Omega = -\sin\theta$. Clearly, this condition is satisfied for $\Omega = \theta + \pi/2$, as then $\sin\Omega = \sin(\theta + \pi/2) = \cos\theta$ and $\cos\Omega = \cos(\theta + \pi/2) = -\sin\theta$.

Therefore, equation 5.3.17 can be rewritten in the form of equation 5.3.19:

$$y(t_o) - \hat{y}(t_o) = A - k\int_{t=0}^{t=t_o} (y(t) - \hat{y}(t))dt + 2B\sin(\phi)\sin(t_o + \Omega) \qquad (5.3.19)$$

where: $\Omega = \theta + \pi/2$.

Therefore, it can be seen that the error $y - \hat{y}$ depends on three terms, namely the offset *A*, the definite integral and the sinusoidal component. From the upper graph of Figure 5.10b it is observed that soon after the start the third term of equation 5.3.19 seems to dominate and fully control the system. Using numerical simulations this has been observed for very small values of *k*, that is, for the values of *k* near zero. The results of equation 5.3.19, and equation 5.2.22 of previous section, are both important findings as they describe the synchronization error using the strict mathematical equations.

The theoretical finding expressed by equation 5.3.19 is now verified by comparing the theoretical results to the results obtained by numerical simulation. Note that in the case of Figures 5.10a and 5.10b:

$$\phi = \frac{z - \hat{z}}{2} = \frac{C - D}{2} = \frac{0 - 1}{2} = -0.5 \qquad \text{and} \qquad \theta = \frac{C + D}{2} = 0.5 \ \textit{radians}$$

Therefore, in the case of Figures 5.10a and 5.10b, the amplitude and phase of the dominating third term of equation 5.3.19 are given by

$$Amplitude = |2B\sin(\phi)| = |2 \cdot 7.5 \cdot \sin(-0.5)| = |-2 \cdot 7.5 \cdot \sin(0.5)| = |-7.19| = 7.19$$

.

From (5.3.19), $\Omega = \theta + \pi/2 = 0.5 + \pi/2 = 2.0708$. Therefore,

$$Phase = 2.0708 - \pi = -1.0708 \ \textit{radians} \quad \text{or} \quad Phase = -61.35°.$$

Finally, the constant *A* is now determined for the case of Figures 5.10a and 5.10b, that is, for those particular initial conditions. From Figure 5.10b, top graph, enlarged in Figure 5.12, one can see that the function of the error of the master-slave *y* signals starts from -2 at *t* = 0. This is as expected since the difference in

the initial conditions between the master-slave y signals is $y(0) - \hat{y}(0) = -2$. Also, at $t = 0$ the second and third terms of equation 5.3.19 are equal to 0 and -6.3110 as shown by equations 5.3.20 and 5.3.21, respectively:

$$-k\int_{t=0}^{t=t_o=0} (y(t) - \hat{y}(t))dt = 0 \tag{5.3.20}$$

$$2B\sin(\phi)\sin(t_o + \Omega) = 2 \cdot 7.5 \cdot \sin(-0.5) \cdot \sin(0 + 2.0708) = -6.3110 \tag{5.3.21}$$

Therefore, constant A can now be found by substituting equations 5.3.20 and 5.3.21 into equation 5.3.19:

$$y(0) - \hat{y}(0) = A + 0 - 6.3110 \quad \Rightarrow \quad -2 = A + 0 - 6.311 \quad \Rightarrow \quad A = 4.3110$$

Therefore, equation 5.3.19, in terms of initial conditions from Figures 5.10a and 5.10b, can now be rewritten as equation 5.3.22:

$$y(t_o) - \hat{y}(t_o) = 4.31 - 0.05 \cdot \int_{t=0}^{t=t_o} (y(t) - \hat{y}(t))dt + 7.19 \cdot \sin(t_o - 61.35°) \tag{5.3.22}$$

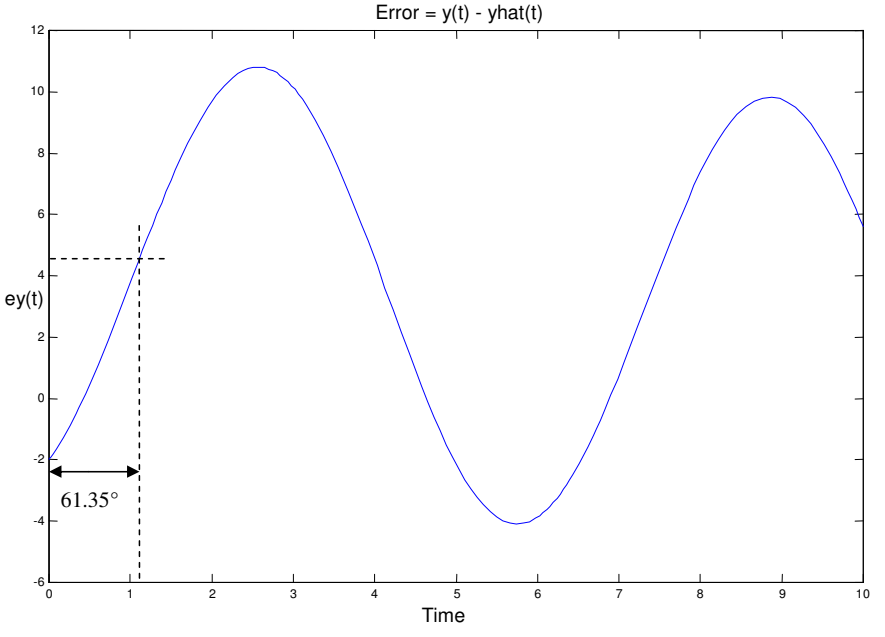


Fig. 5.12 Enlargement of Figure 5.10b. Note that time and angle scales are equal, as $\omega = 1$ radians/second, where ω would be the angular frequency of the cosine term of equation 5.3.1.

Equation 5.3.22 tells us that the sinusoid of the function is in fact a sinusoid lagging by $61.35°$. This fact is indeed confirmed by observing Figure 5.12. Note that at $t = 0$ the function is not a perfect sinusoid and thus the indication of the phase lag is approximate.

The error between the master-slave y signals is now investigated further. One can see that equation 5.3.19 goes to zero if its third term is made to go to zero. To make the third term go to zero, the initial conditions of the master-slave z signals must be chosen such that:

$$\sin(\phi) = \sin\left(\frac{z - \hat{z}}{2}\right) = \sin\left(\frac{C - D}{2}\right) = 0 \tag{5.3.23}$$

To make equation 5.3.23 true, equation 5.3.24 must be satisfied:

$$\phi = \pm n\pi \qquad \text{(where } n \text{ is any integer)} \tag{5.3.24}$$

To make equation 5.3.24 true, equation 5.3.25 must be satisfied:

$$2\phi = \pm 2n\pi = C - D \tag{5.3.25}$$

where n is any integer and C and D are initial conditions of the master and slave z signals, respectively.

Therefore, according to equation 5.3.19, one must have a difference between the master-slave z initial conditions of $\pm 2n\pi$ for the synchronization of the master-slave y signals to occur. This fact is confirmed by numerical simulations, presented in Figures 5.13a and 5.13b, when the x signal drives. The initial conditions of the master system are chosen to be $x(0) = 1$, $y(0) = -3$, $z(0) = \pi$. The initial conditions of the slave system are chosen to be $\hat{y}(0) = 2$, $\hat{z}(0) = -\pi$.

From Figure 5.13a, one can see that as time tends to infinity the master-slave y signals synchronize. Figure 5.13b shows that the error of the master-slave y signals tends to zero.

Also it is important to mention that the error between the master-slave y signals is at its maximum when equation 5.3.26 is satisfied (see equation 5.3.19):

$$\sin(\phi) = \sin\left(\frac{z - \hat{z}}{2}\right) = \sin\left(\frac{C - D}{2}\right) = \pm 1 \tag{5.3.26}$$

To make equation 5.3.26 true, equation 5.3.27 must be satisfied:

$$\phi = \pm \frac{n}{2}\pi \qquad \text{(where } n \text{ is any odd integer)} \tag{5.3.27}$$

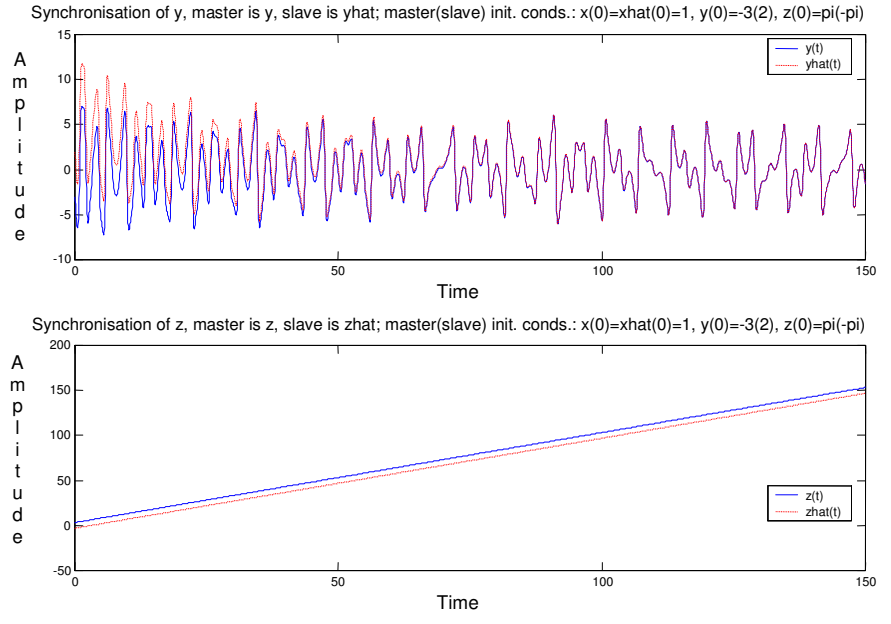


Fig. 5.13a Synchronization of the Ueda master-slave chaotic signals, with the *x* signal driving and $\phi = \pi$.

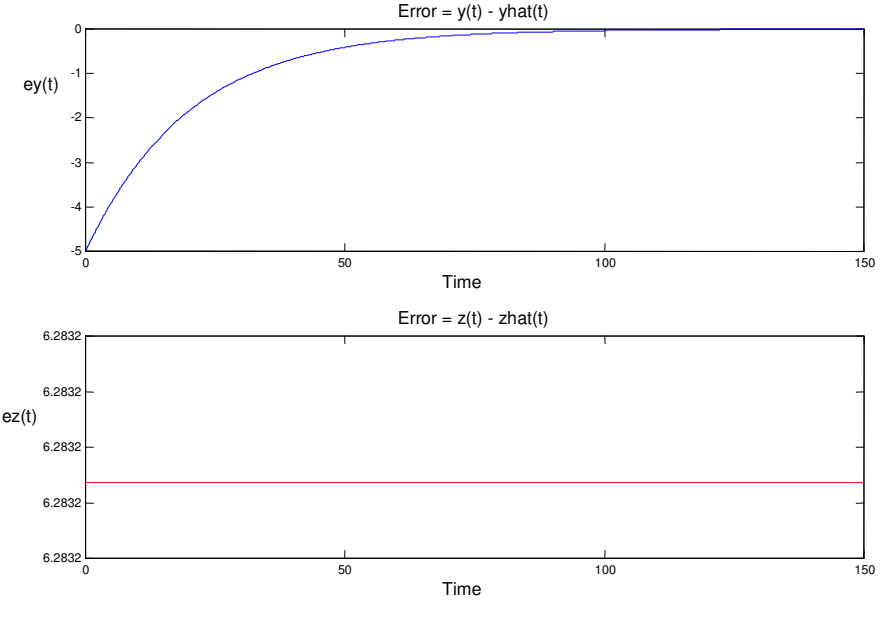


Fig. 5.13b The error tends to zero as time tends to infinity for the master-slave *y* signals. Signal *x* drives and $\phi = \pi$.

To make equation 5.3.27 true, equation 5.3.28 must be satisfied:

$$2\phi = \pm n\pi = C - D \tag{5.3.28}$$

where n is any odd integer and C and D are initial conditions of the master and slave z signals, respectively. Therefore, according to equation 5.3.19, one must have a difference between the master-slave z initial conditions of $\pm n\pi$, where n is odd, for the maximum error of the master-slave y signals to occur. This fact is confirmed by numerical simulations, presented in Figures 5.14a and 5.14b, when the x signal drives. The initial conditions of the master system are chosen to be $x(0) = 1$, $y(0) = -2.5$, $z(0) = 2\pi$. The initial conditions of the slave system are chosen to be $\hat{y}(0) = 2.4$, $\hat{z}(0) = \pi$.

Therefore, in the case of Figures 5.14a and 5.14b, the amplitude and phase of the dominating third term of equation 5.3.19 are given by

$$Amplitude = \left|2B\sin(\phi)\right| = \left|2 \cdot 7.5 \cdot \sin(\frac{\pi}{2})\right| = \left|15 \cdot 1\right| = 15$$

$$Phase = \Omega = \theta + \frac{\pi}{2} = \frac{2\pi + \pi}{2} + \frac{\pi}{2} = 2\pi \ \ radians$$

or: $$Phase = \Omega = (2\pi) \cdot \frac{180}{\pi} = 360° \Rightarrow 0°$$

The enlargement of Figure 5.14b is presented in Figure 5.14c showing the zero phase. Also, in the case of Figures 5.14a and 5.14b the constant A of equation 5.3.19 is found to be equal to -4.9 so that equation 5.3.19 takes the form of equation 5.3.29:

$$y(t_o) - \hat{y}(t_o) = -4.9 - 0.05 \cdot \int_{t=0}^{t=t_o} (y(t) - \hat{y}(t))dt + 15 \cdot \sin(t_o) \tag{5.3.29}$$

From Figure 5.14a, one can see that as time tends to infinity the master-slave y signals do not synchronize. Figure 5.14b shows that the amplitude of the synchronization error of the master-slave y signals indeed tends to 15.

Note that it has also been observed that making the difference between the initial conditions of the master-slave y signals near to $-\left|2B\sin(\phi)\right|$ makes the synchronization error settle into periodic behaviour more quickly.

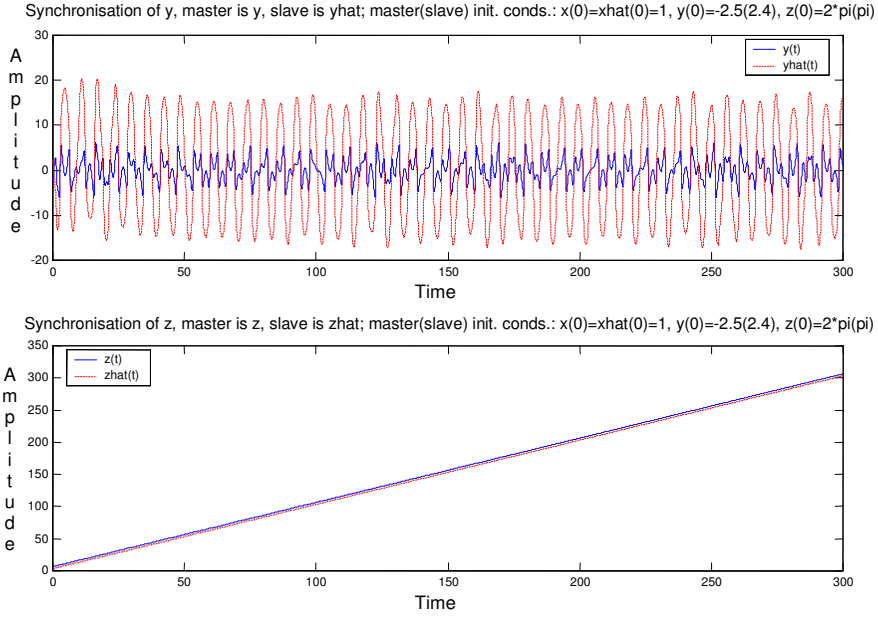


Fig. 5.14a Synchronization of the Ueda master-slave chaotic signals, with the x signal driving and $\phi = \pi/2$.

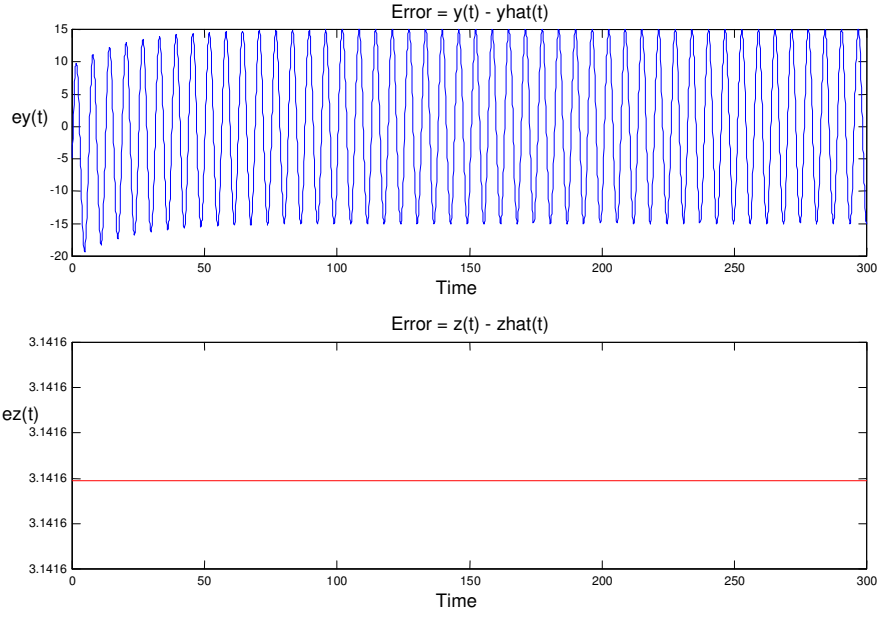


Fig. 5.14b The error exhibits maximum oscillations as time tends to infinity for the master-slave y signals. Signal x drives and $\phi = \pi/2$.

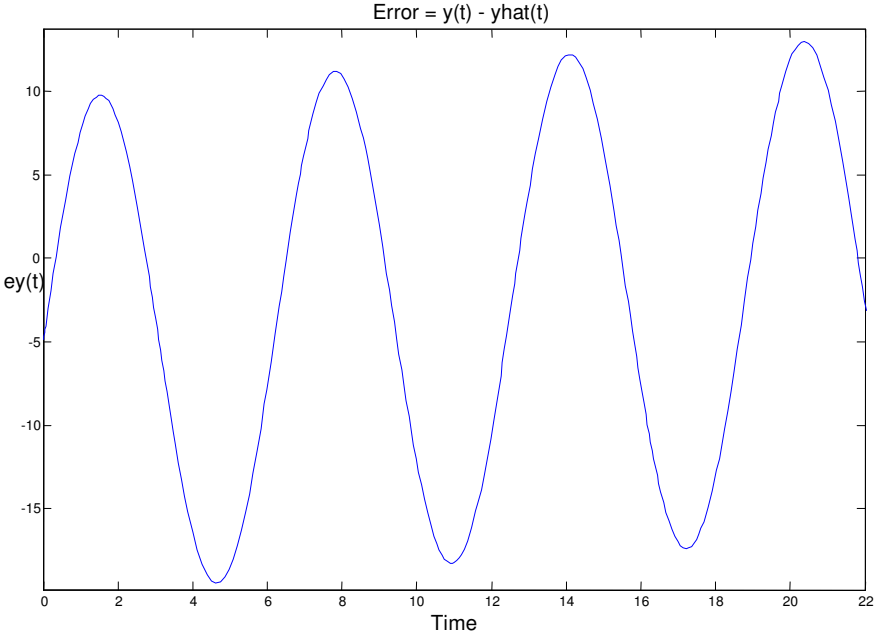


Fig. 5.14c Enlargement of Figure 5.14b showing the zero phase of equation 5.3.29.

5.3.2 Master-Slave System with the Master y Signal Driving

When the y signal drives, the synchronization error is constant for both master-slave x and master-slave z signals, and it is governed by equations 5.3.30 and 5.3.31, respectively. This is easily shown in the same fashion as for the previous cases presented above.

$$x - \hat{x} = x(0) - \hat{x}(0) = A \tag{5.3.30}$$

$$z - \hat{z} = z(0) - \hat{z}(0) = B \tag{5.3.31}$$

5.3.3 Master-Slave System with the Master z Signal Driving

Finally, when the z signal drives, the master-slave system does not synchronize, as Figure 5.15 demonstrates.

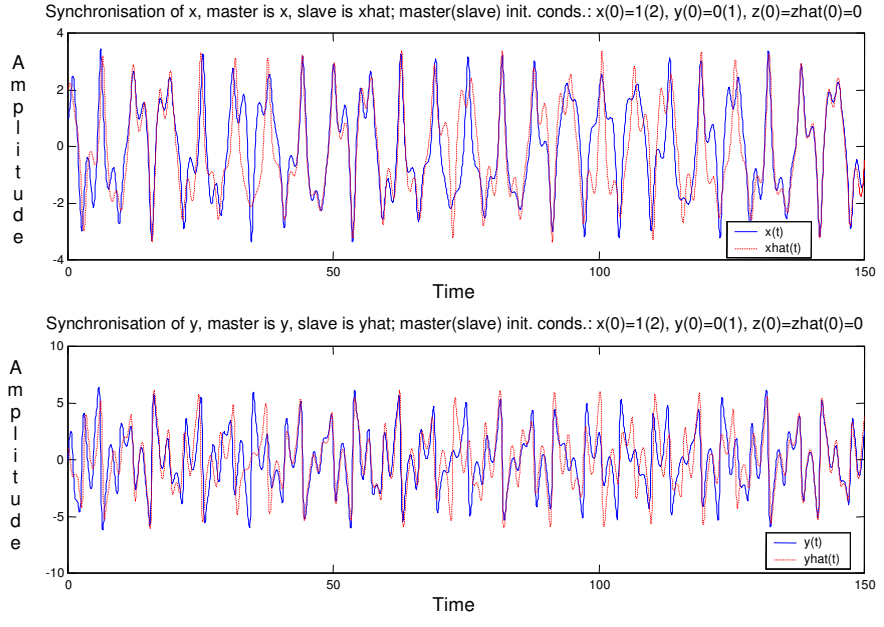


Fig. 5.15 Synchronization of the Ueda master-slave chaotic signals, with the z signal driving.

5.3.4 Summary of the Synchronization Properties

Overall, for the Ueda master-slave chaotic system it has been shown that when ***x* drives**, the synchronization error of the master-slave y signals is sinusoidal while the error of the master-slave z signals is constant. The master-slave y signals synchronize only when the difference between the master-slave z signals' initial conditions is $\pm 2n\pi$, where n is any integer. When ***y* drives**, the synchronization error is constant for both master-slave x and master-slave z signals. Finally, when ***z* drives**, the master-slave system does not synchronize.

5.4 Conclusion

In this chapter it has been demonstrated, via Lyapunov's direct method, that the simplest piecewise linear master-slave chaotic flow synchronizes when the master x signal drives. However, when the system does not synchronize and Lyapunov's direct method cannot be used, it has been shown that the novel mathematical analysis presented here can often be used to predict the system's synchronization error.

In this chapter, primarily the master-slave synchronization properties of the simplest quadratic chaotic flow and Ueda chaotic system have been investigated

by direct mathematical analysis. It has been shown that when the z signal drives, the synchronization error of the simplest quadratic master-slave y signals is constant whereas the synchronization error of the master-slave x signals increases linearly. Using numerical simulations, in conjunction with mathematical analysis, it has been demonstrated that the simplest quadratic master-slave chaotic flow does not synchronize when the y signal drives; however, the synchronization error of the master-slave z signals tends to a constant value which is predictable and can be expressed as a combination of the master-slave x signals' initial conditions and the system's parameter value. It has also been found that the simplest quadratic master-slave chaotic flow synchronizes when the x signal drives.

The analysis has then been performed on the Ueda master-slave chaotic system. It has been shown that the Ueda master-slave system does not synchronize when the master y or master z signal drives. However, it has been shown here that the master-slave y signals do synchronize under certain conditions when the master x signal drives. When the signal x drives, mathematical manipulation of the system's dynamics allows one to determine a useful mathematical expression for the error of the master-slave y signals. This expression, along with the numerical simulations, allows one to predict that if the difference between the master-slave z signals' initial conditions equals $\pm 2n\pi$, the master-slave y signals will always synchronize. When the y signal drives, the synchronization error is constant and has been mathematically expressed. In this way it has been demonstrated that the novel mathematical analysis presented describes the system's behaviour using the strict mathematical equations what is in contrast to Lyapunov's stability theory which describes the general behaviour of the system. The novel analysis therefore gives a deeper insight mathematically into what dynamically occurs.

In general, it can be concluded that the synchronization properties of chaotic systems, in particular Pecora - Carroll synchronization properties, do not necessarily have to be investigated by Lyapunov's stability theory, or by evaluation of conditional Lyapunov exponents. Instead, an alternative direct mathematical analysis can be used in certain cases, as has been demonstrated in this chapter for the simplest quadratic chaotic flow and Ueda chaotic system. The work of this chapter has been published in [7].

References

[1] Pecora, L.M., Carroll, T.L.: Synchronization in chaotic systems. Physical Review Letters 64(8), 821–824 (1990)

[2] Pecora, L.M., Carroll, T.L.: Driving systems with chaotic signals. Physical Review A 44(4), 2374–2383 (1991)

[3] He, R., Vaidya, P.G.: Analysis and synthesis of synchronous periodic and chaotic systems. Physical Review A 46(12), 7387–7392 (1992)

[4] Rouche, N., Habets, P., Laloy, M.: Stability Theory by Liapunov's Direct Method, pp. 30–31. Springer, Heidelberg (1977)

[5] Murali, K., Lakshmanan, M.: Transmission of signals by synchronization in a chaotic Van der Pol-Duffing oscillator. Physical Review E, Rapid Communications 48(3), R1624–R1626 (1993)

[6] Sprott, J.C.: Chaos and Time-Series Analysis, pp. 230–440. Oxford University Press, Oxford (2003)
[7] Jovic, B., Berber, S., Unsworth, C.P.: A novel mathematical analysis for predicting master – slave synchronization for the simplest quadratic chaotic flow and Ueda chaotic system with application to communications. Physica D 213(1), 31–50 (2006)
[8] Chua, L.O., Itoh, M., Kocarev, L., Eckert, K.: Chaos synchronization in Chua's circuit. Journal of Circuits, Systems and Computers 3(1), 93–108 (1993)
[9] Moon, F.C.: Chaotic Vibrations - An Introduction for Applied Scientists and Engineers, pp. 24–36. Wiley Interscience, New York (1987)

Chapter 6
Application of Chaotic Synchronization to Secure Communications

In chapters 3, 4 and 5 the phenomenon of chaotic synchronization has been studied. In this chapter, a popular application of chaotic synchronization in the area of secure communications is presented. Several chaotic communication systems with the receiver based on the chaotic synchronization concept are described. It is shown how a general approach to synchronization of chaotic flows via Lyapunov's direct method and chaotic maps via the theorems of chapter 4 can be used for the development of chaotic communication systems. The communication schemes examined include those of chaotic masking, chaotic modulation and the newly developed chaotic communication scheme of initial condition modulation. Finally, the noise performance of the chaotic parameter modulation and the initial condition modulation are compared in terms of the bit error rate. It is shown that the newly developed initial condition modulation scheme outperforms the chaotic parameter modulation scheme.

Since the onset of chaotic synchronization research, a number of demodulation techniques based on chaotic synchronization have been proposed for potential communication systems [1-13]. Of those, the following are based on the Pecora-Carroll synchronization method [1,2,4-6,8-11,13].

Pecora and Carroll's (PC) original paper on chaotic synchronization [14], suggested the application of chaotic synchronization in communications, and shortly after Oppenheim et al. presented a communication system based on the PC synchronization method [4]. The method of [4], termed "chaotic masking", was experimentally demonstrated in [5] using Chua's circuit. In this method, the information signal is added onto the chaotic carrier directly, and transmitted. The requirement of this method is that the power of the information signal has to be significantly lower than the power of the chaotic carrier [4]. In contrast to chaotic masking, a technique of "chaotic modulation" incorporates the message into the dynamical equations producing the chaotic carrier. Chaotic parameter modulation is an example of the chaotic modulation technique where a binary message modulates one or more of the system's parameters [8,9]. Other forms of chaotic modulation involve techniques where one or more of the state variables is modulated by the message [2,11,13]. As opposed to chaotic modulation, the technique of "initial condition modulation" introduces the binary message into the system through its initial conditions [10,15,16].

B. Jovic: Synchronization Techniques for Chaotic Commun. Syst., SCT 5, pp. 135–169.
springerlink.com

Communication methods based on chaotic synchronization other than PC synchronization have also been proposed. For instance in [7] chaotic masking and Pyragas' synchronization method have been used to transmit and receive information, whereas in [3] chaotic modulation and John and Amritkar (JA) synchronization method have been used.

Section 6.1 presents the communication technique of chaotic masking. The communication techniques based on chaotic modulation are presented in section 6.2. In addition, it is shown how a general approach to chaotic synchronization of flows via Lyapunov's direct method and chaotic synchronization of maps via the theorems of chapter 4 can be used in the design of chaotic communication systems. In section 6.3, a recently developed technique of initial condition modulation is presented. Finally, section 6.4 evaluates and compares the noise performance of the presented systems in terms of the bit error rate. It is shown that the initial condition modulation technique exhibits better noise performance than the chaotic parameter modulation technique.

6.1 Chaotic Masking

Chaotic masking (CM) was one of the earliest chaotic communication techniques proposed [4,5,8]. It is based on the principles of PC synchronization. It primarily involves the transmission of analog signals [4].

6.1.1 Principles of Chaotic Masking

Chaotic masking involves the addition of a message signal m to a chaotic carrier signal x, before the transmission of the sum of the two signals takes place [4]. The block diagram illustrating the principles of chaotic masking is shown in Figure 6.1 [16].

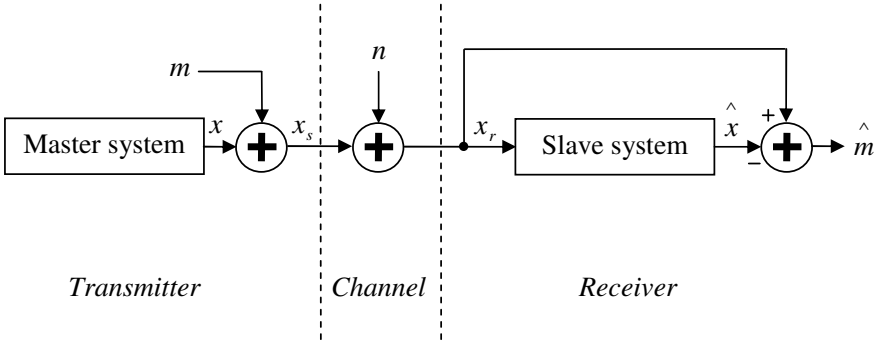


Fig. 6.1 General block diagram of the chaotic communication system based on the chaotic masking concept

In Figure 6.1 n denotes the additive white Gaussian noise (AWGN) component introduced by the channel and x_r denotes the received signal affected by AWGN. The slave system of the receiver generates a signal $\hat{x}$ which is expected to be synchronized with the corresponding master signal x of the transmitter. Assuming that the AWGN component is near zero, and that sufficient amount of time has passed for x and $\hat{x}$ to synchronize, the transmitted message m can be recovered in the form of $\hat{m}$:

$$\hat{m} = x_r - \hat{x} = (m + x) - \hat{x} \approx m \tag{6.1.1}$$

The requirement of a chaotic masking scheme is for the power of the information signal to be significantly lower than the power of the chaotic carrier.

6.1.2 Chaotic Masking within the Lorenz Master-Slave System

Chaotic masking within the Lorenz master-slave system has been demonstrated in [4,8, 9]. The system has been designed using the Lorenz x signal as the driving signal. Lyapunov's direct method has been used in [8] to show that using the x signal as the driving signal the master-slave system synchronizes. It has then also been shown that by adding a small amplitude speech signal onto the chaotic carrier one is able to recover the speech signal at the receiver. The communication system based on chaotic masking, while implementing the Lorenz master-slave system, is shown in Figure 6.2. An ability to recover the transmitted information is demonstrated under noiseless conditions in Figure 6.3 by processing the word "Oak" through the system. By comparing the top and the bottom graphs of Figure 6.3 one can see that the transmitted original message has been recovered with

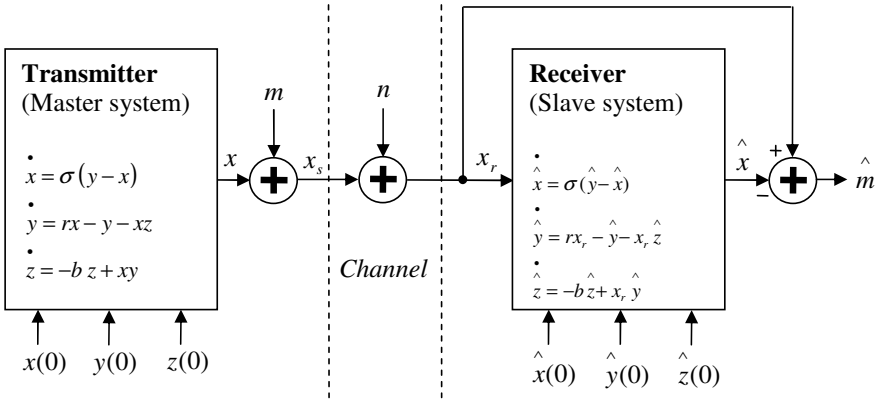


Fig. 6.2 The Lorenz based communication system implementing chaotic masking

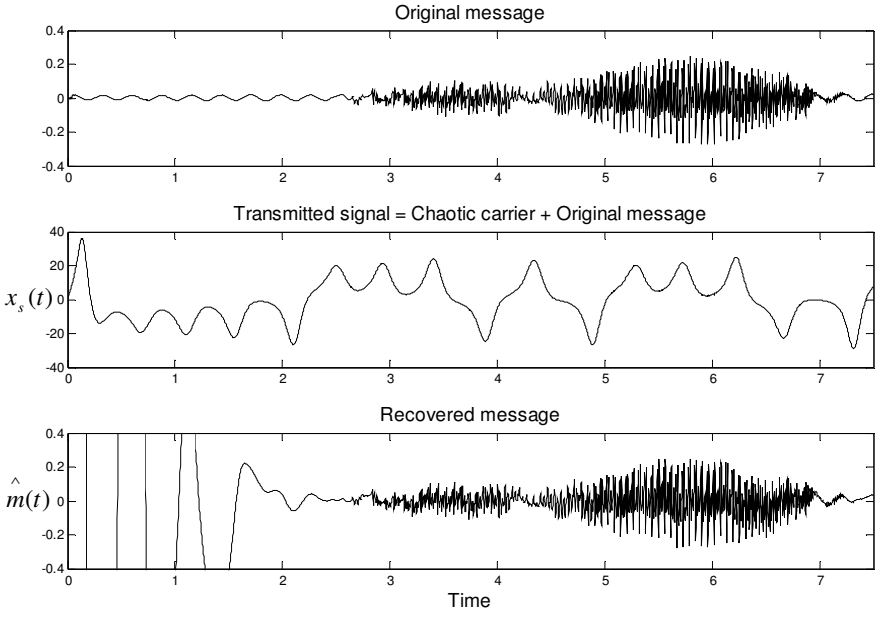


Fig. 6.3 The signals of the Lorenz based communication system implementing chaotic masking

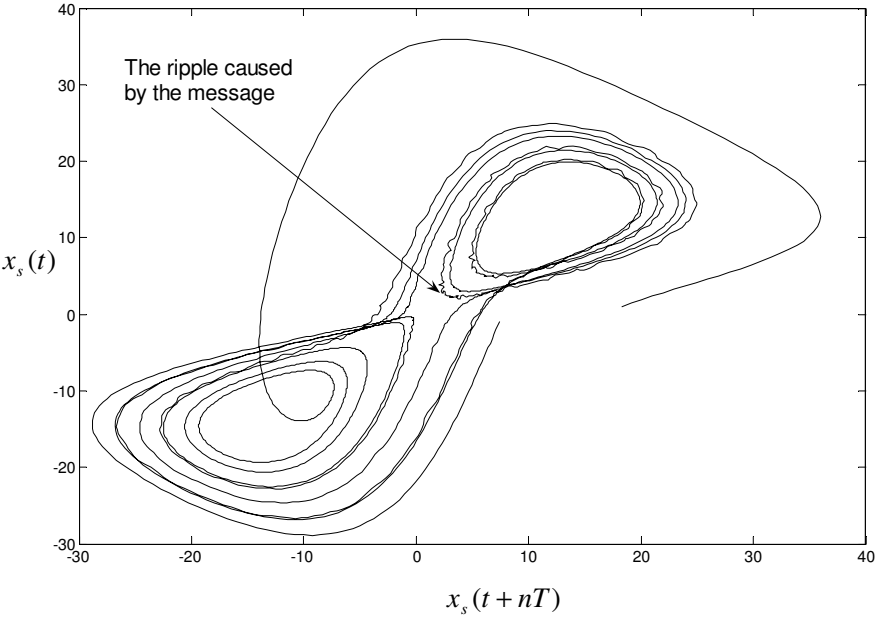


Fig. 6.4 The transmitted signal $x_s(t)$ plotted in phase space

reasonable accuracy. In the case of Figure 6.3 the chaotic parameter values of the system of Figure 6.2 have been set to: $\sigma = 16$, $r = 45.6$ and $b = 4$. An evident difference in power between the chaotic carrier and the speech signal can be observed in Figure 6.3. The transmitted signal of Figure 6.3 has been plotted in phase space in Figure 6.4. The small ripple, observed on the strange attractor of Figure 6.4, is caused by the message *m* embedded within it.

6.2 Chaotic Modulation

In the chaotic masking scheme, described above, information is added directly onto the chaotic carrier without the influence of the message on the dynamical equations producing the carrier. In contrast to chaotic masking, chaotic modulation incorporates the message into the dynamical equations producing the chaotic carrier.

6.2.1 Chaotic Parameter Modulation

As opposed to chaotic masking which is primarily used for analog transmission, chaotic parameter modulation (CPM) is used for transmission of binary information.

6.2.1.1 Principles of Chaotic Parameter Modulation

A block diagram of a chaotic communication system based on the CPM concept is shown in Figure 6.5 [16]. As for the CM scheme, a requirement for the CPM scheme is for the master-slave system to synchronize for a given driving signal, as outlined in sections 3.1-3.3.

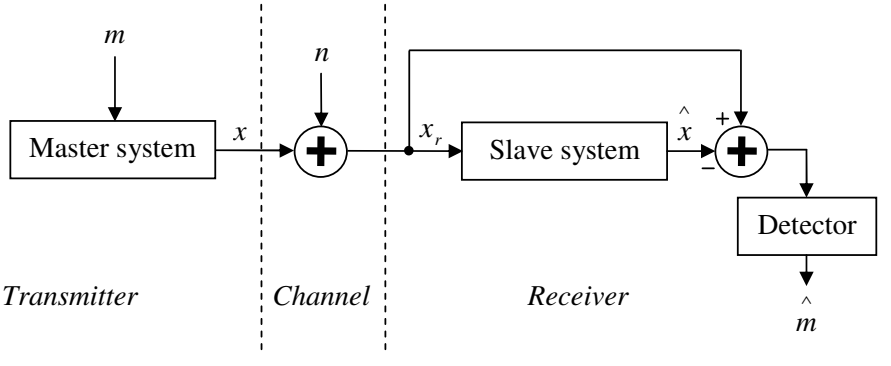


Fig. 6.5 A block diagram of the chaotic communication system based on the parameter modulation concept

In Figure 6.5, the message m varies between the two particular values, depending on whether a binary 0 or a binary 1 is to be transmitted. The message is incorporated into a certain modulating parameter of the master system causing it to change its value with the change in the message. The parameters of the slave system are fixed at all time. When the master-slave parameters are identical synchronization occurs. This forces the synchronization error to zero, indicating that bit 0 has been transmitted. Alternatively, with the master-slave parameter mismatch the system does not synchronize, indicating that bit 1 has been transmitted. Therefore, this is a form of on-off keying. This concept is illustrated in Figure 6.6. The choice of the modulating parameter of the master chaotic system must be chosen with care to ensure the chaotic properties of the system at all time. This ensures the increased security within the communication system.

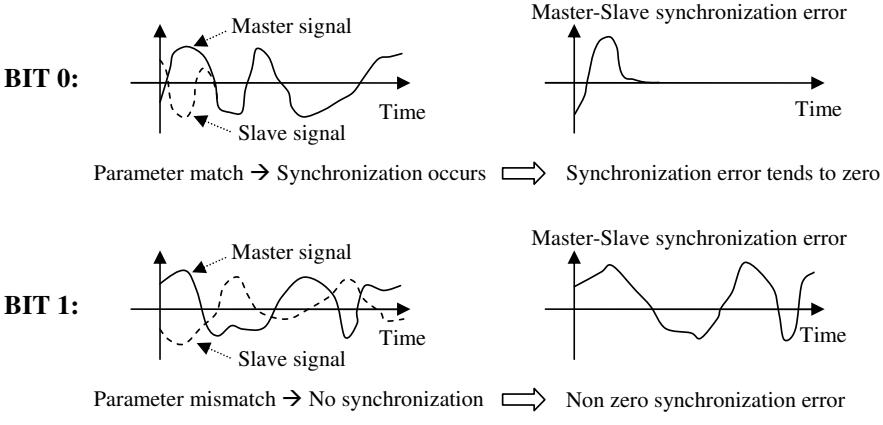


Fig. 6.6 The chaotic parameter modulation concept

6.2.1.2 Chaotic Parameter Modulation within the Lorenz Master-Slave System

The concept of parameter modulation is now demonstrated on the Lorenz master-slave chaotic system [8,9]. In [8] the binary message is used to alter the parameter b of the master (transmitter) Lorenz chaotic system between 4 and 4.4 depending on whether a bit 0 or bit 1 is to be transmitted. However, at the slave (receiver) side the parameter b is fixed at 4 for all time. Thus, the synchronization either occurs or does not, depending on the state of the parameter b at the transmitter (master) side. The parameters σ and r are fixed at 16 and 45.6, respectively. For these parameter values the system is chaotic. In order to implement the CPM scheme the authors of [8] have scaled the Lorenz chaotic system to allow for the limited dynamic range of the operational amplifiers. This system, based on the PC synchronization concept, is presented in Figure 6.7.

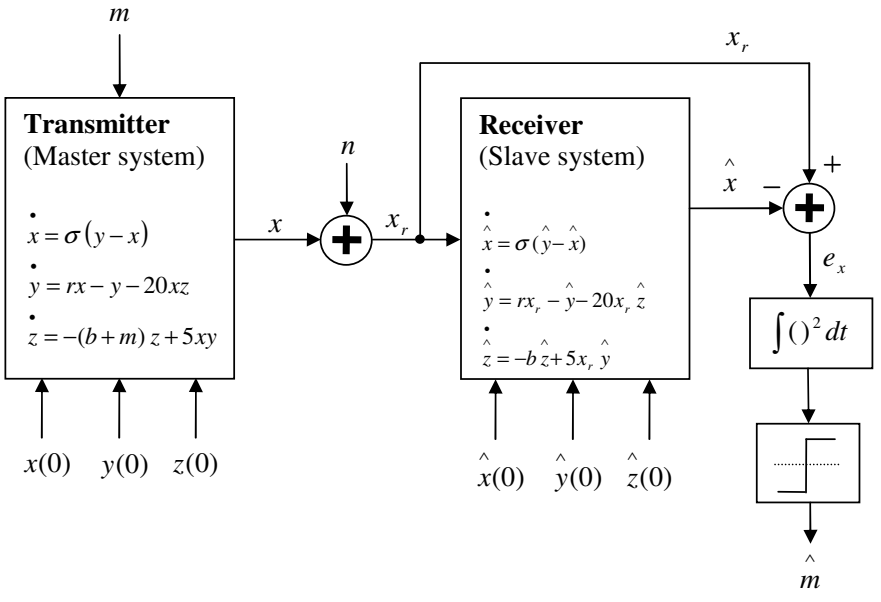


Fig. 6.7 The Lorenz based communication system implementing chaotic parameter modulation. The parameter values: $\sigma = 16$, $r = 45.6$ and $b = 4$.

The transmitted signal x, of Figure 6.7, is shown in Figure 6.8 when the series of 10 bits is transmitted, that is, when m = [0, 0, 0.4, 0, 0.4, 0.4, 0, 0.4, 0, 0.4], or in binary terms: *message* = [0 0 1 0 1 1 0 1 0 1]. Figure 6.8 also shows the corresponding squared synchronization error, e_x^2, under noiseless conditions. The received bits are detected by squaring and integrating the error e_x. The output of the integrator is then compared to the predetermined threshold and the decision is made whether a bit 0 or a bit 1 was sent. The behaviour of the system, corresponding to the master-slave parameter match (bit 0) and mismatch (bit 1), can also be illustrated in phase space. In Figure 6.9 the strange attractors corresponding to the third, fourth, fifth and sixth transmitted bit have been plotted. It can be observed from Figure 6.9 that in the case of the third, fifth and sixth bit the master-slave trajectories do not synchronize, but follow their own separate paths [16]. This is as expected due to the master-slave parameter mismatch. However, in the case of the fourth bit, the master-slave parameters match, causing the trajectories to synchronize. Note that the spreading factor of 400 has been used to represent one bit. By definition the spreading factor denotes the number of discrete sample points (chips) contained within one information bit. It is the ratio of a bit period to a chip period [17]. A spreading factor that is too small may be insufficient for synchronization to take place and thus make it more difficult to decode the transmitted information. Alternatively, a spreading factor that is too large may be impractical from the bandwidth point of view. A transient period of 1000 chips has been

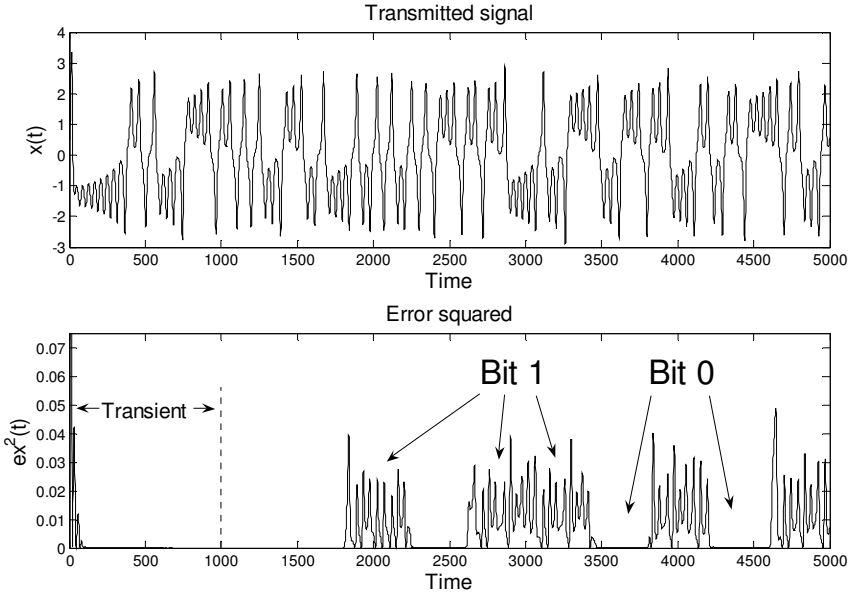


Fig. 6.8 The transmitted signal x and the squared synchronization error e_x^2

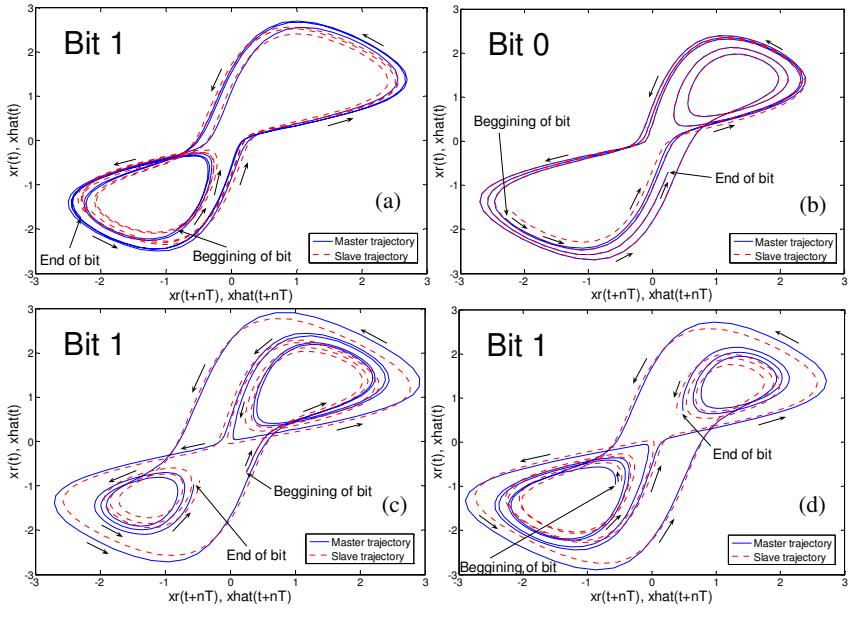


Fig. 6.9 Phase space representation of the received signal x_r and the corresponding slave signal $\hat{x}$ for: (a) the 3rd bit of the transmitted message sequence: [0 0 1 0 1 1 0 1 0 1], (b) the 4th bit, (c) the 5th bit, and (d) the 6th bit.

allowed for the case of Figure 6.8. During the transient period there is no data transmission taking place.

6.2.2 General Approach to Chaotic Parameter Modulation

In this subsection, a general approach to chaotic parameter modulation is developed. It involves the design of the nonlinear controller via Lyapunov's direct method, as outlined in section 3.3. In contrast to the CPM scheme presented in subsection 6.2.1, the scheme presented here does not rely on the inherent synchronization properties of the master-slave system for a given drive signal. It instead enforces synchronization upon the master-slave system by designing the control laws which ensure asymptotic stability within the system.

6.2.2.1 Principles of the General Approach to Chaotic Parameter Modulation

Consider a general block diagram, given in Figure 6.10 [16], of the chaotic communication system based on the parameter modulation concept.

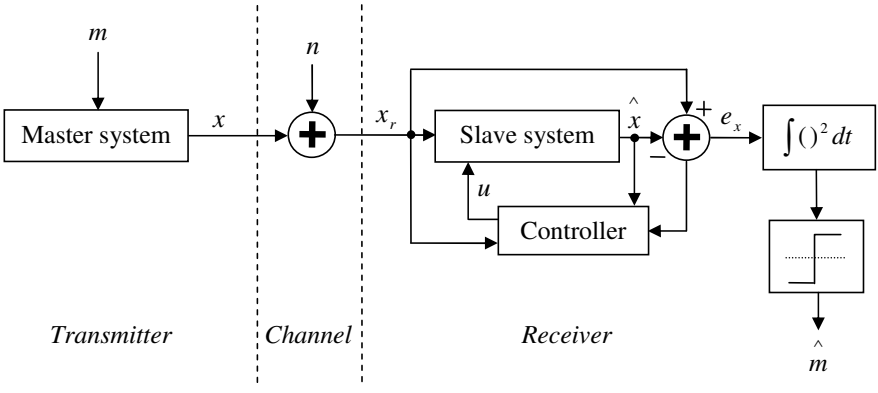


Fig. 6.10 General block diagram of the chaotic communication system based on the parameter modulation concept

In Figure 6.10, the binary message m is introduced into the system by varying one or more of the parameters of the master system. As in subsection 6.2.1, the parameters of the slave system are fixed at all time. Therefore, synchronization occurs or not, depending on the state of the parameters at the transmitter side. The controller of Figure 6.10 is designed via Lyapunov's direct method, as outlined in section 3.3. The controller output, u, then ensures the synchronization of the master-slave system when the master-slave parameters match. Note that, in general, the signal x may be an interleaved version of more than one signal of the master system [10], such as in a TDM system, as discussed in chapters 8 and 9.

6.2.2.2 Chaotic Parameter Modulation within the Ueda Master-Slave System

Here the control law for the Ueda master-slave chaotic system, with the master signal x driving, is designed. The system is then applied to a CPM based communication system. In order to justify a design of a controller for the Ueda master-slave chaotic system its inherent synchronization properties without the controller must first be investigated. Figure 6.11, shows the Ueda master-slave chaotic system with the master signal x driving. The dynamics of the Ueda master chaotic system are shown in Figure 6.12. In Figure 6.11, the initial conditions of the master-slave z signals have been set to an equal value. As will be shown, with the initial conditions so chosen the controller design is significantly simplified. In Figure 6.13, the synchronization errors for the x, y and z master-slave chaotic signals are shown. These errors demonstrate that the master-slave x signals of the system of Figure 6.11 do not synchronize and thus the system warrants a controller design. Note that the master-slave system synchronization error has been defined by equation 6.2.1:

$$e_1(t) = x(t) - \hat{x}(t), \qquad e_2(t) = y(t) - \hat{y}(t), \qquad e_3(t) = z(t) - \hat{z}(t). \tag{6.2.1}$$

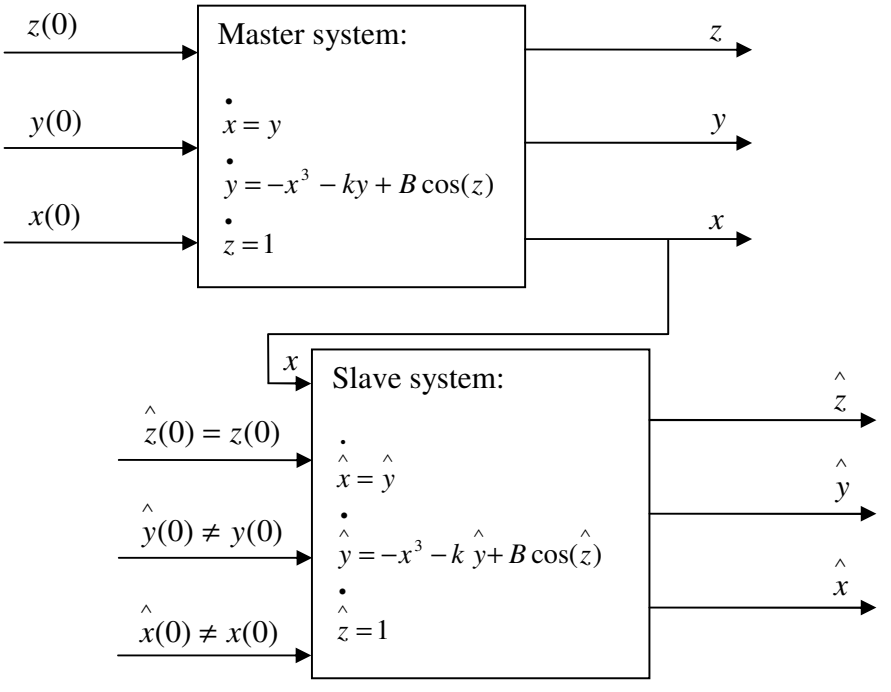


Fig. 6.11 The block diagram of the Ueda master-slave chaotic system, with the x signal driving. The parameter values are $k = 0.05$, $B = 7.5$. Note that this system differs from that of Figure 5.9 of chapter 5 in that $\hat{x} \neq x$.

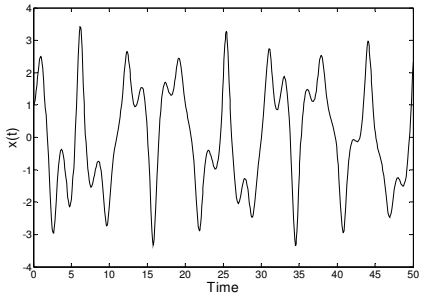


Fig. 6.12a The Ueda chaotic time series, $x(t)$

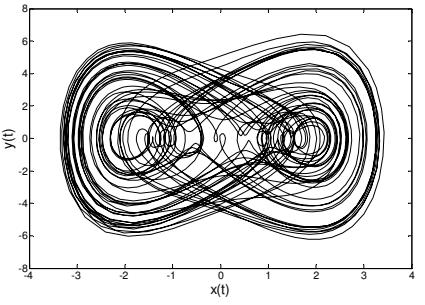


Fig. 6.12b The Ueda strange attractor

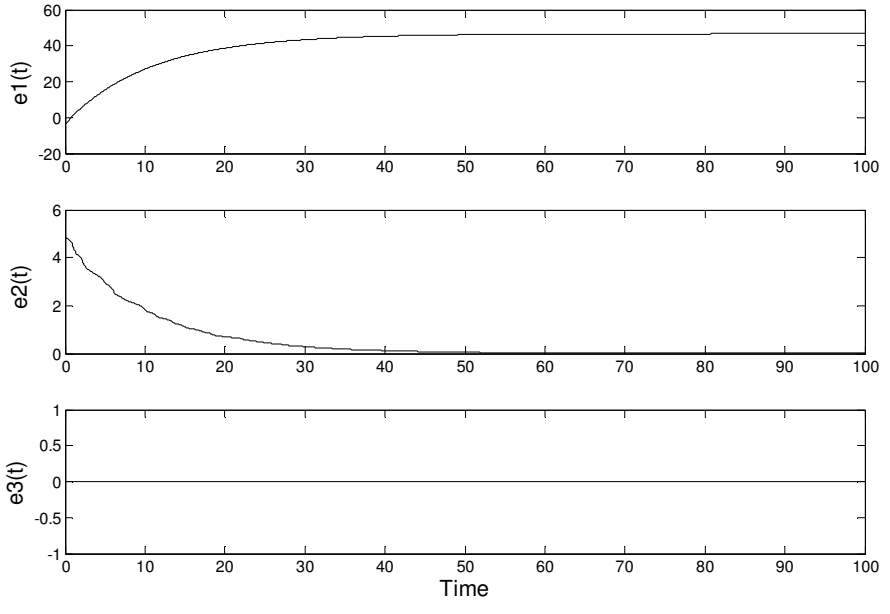


Fig. 6.13 Inherent synchronization error of the Ueda master-slave chaotic signals without the controller

Consider the CPM Ueda communication system of Figure 6.14. The constants f and g of the master system can be of any value and are chosen so that the parameters k and B take on the appropriate values for a given m.

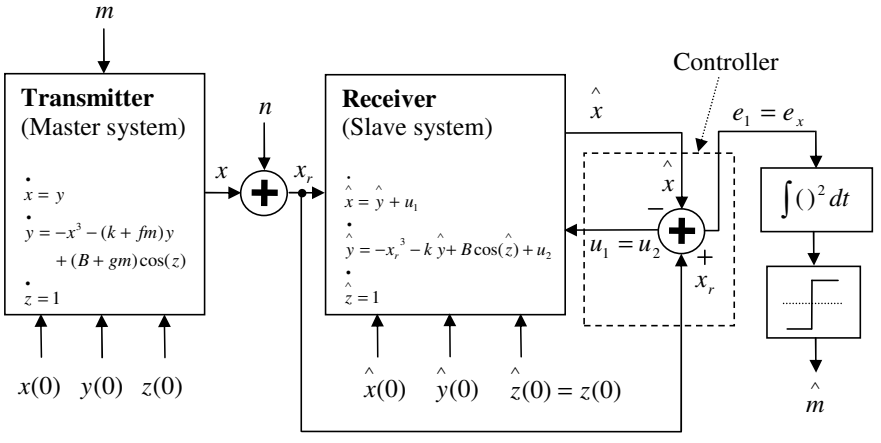


Fig. 6.14 The Ueda chaotic communication system based on the parameter modulation concept

In order to demonstrate the design of the controller of Figure 6.14 assume no noise in the system. It follows then that: $x_r = x$, so that the slave system, including the control laws, takes the form given by equation 6.2.2:

$$\begin{aligned} \dot{\hat{x}} &= \hat{y} + u_1 \\ \dot{\hat{y}} &= -x^3 - k\hat{y} + B\cos(\hat{z}) + u_2 \\ \dot{\hat{z}} &= 1 \end{aligned} \tag{6.2.2}$$

The differential synchronization error of the master-slave system of Figure 6.14 is then given by equation 6.2.3:

$$\begin{aligned} \dot{e}_1 &= \dot{x} - \dot{\hat{x}} = y - \hat{y} - u_1 \\ \dot{e}_2 &= \dot{y} - \dot{\hat{y}} = -ky + k\hat{y} + B\cos(z) - B\cos(\hat{z}) - u_2 \\ \dot{e}_3 &= \dot{z} - \dot{\hat{z}} = 0 \end{aligned} \tag{6.2.3}$$

The difference between the master-slave z signals is governed by equation 6.2.6 [10]:

$$\dot{z} = \dot{\hat{z}} \tag{6.2.4}$$

$$\int \dot{z}\, dt = \int \dot{\hat{z}}\, dt \tag{6.2.5}$$

$$z - \hat{z} = z(0) - \hat{z}(0) \tag{6.2.6}$$

Given that the master-slave z initial conditions are equal to each other, or that their difference is equal to $\pm 2n\pi$, where n is any integer, equation 6.2.6 can be reduced to equation 6.2.7 [10]:

$$z - \hat{z} = \pm 2n\pi \tag{6.2.7}$$

Using the standard trigonometric identities, equation 6.2.3 can be rewritten in the form of equation 6.2.8:

$$\begin{aligned}
\dot{e}_1 &= \dot{x} - \dot{\hat{x}} = y - \hat{y} - u_1 \\
\dot{e}_2 &= \dot{y} - \dot{\hat{y}} = -ky + k\hat{y} + 2B \sin\left(\frac{z + \hat{z}}{2}\right) \sin\left(\frac{z - \hat{z}}{2}\right) - u_2 \\
\dot{e}_3 &= \dot{z} - \dot{\hat{z}} = 0
\end{aligned} \tag{6.2.8}$$

Substituting equation 6.2.7 into equation 6.2.8, equation 6.2.9 is obtained:

$$\begin{aligned}
\dot{e}_1 &= \dot{x} - \dot{\hat{x}} = y - \hat{y} - u_1 \\
\dot{e}_2 &= \dot{y} - \dot{\hat{y}} = -ky + k\hat{y} + 2B \sin\left(\frac{z + \hat{z}}{2}\right) \sin(\pm n\pi) - u_2 \\
\dot{e}_3 &= \dot{z} - \dot{\hat{z}} = 0
\end{aligned} \tag{6.2.9}$$

Finally simplifying equation 6.2.9, equation 6.2.10 is obtained:

$$\begin{aligned} \dot{e}_1 &= e_2 - u_1 \\ \dot{e}_2 &= -ke_2 - u_2 \\ \dot{e}_3 &= 0 \end{aligned} \tag{6.2.10}$$

In order to design the controller for this particular master-slave system, consider the candidate Lyapunov function given by equation 6.2.11:

$$V = \frac{1}{2}(e_1^2 + e_2^2) \tag{6.2.11}$$

Differentiating equation 6.2.11 with respect to time equation 6.2.12 is obtained:

$$\dot{V} = \dot{e}_1 e_1 + \dot{e}_2 e_2 \tag{6.2.12}$$

Substituting equation 6.2.10 into equation 6.2.12 and simplifying, equation 6.2.13 is obtained:

$$\dot{V} = e_1 e_2 - e_1 u_1 - ke_2^2 - e_2 u_2 \tag{6.2.13}$$

For equation 6.2.11 to be the Lyapunov function, equation 6.2.13 must be negative semi-definite. In order for equation 6.2.13 to become negative semi-definite the term $e_1 e_2$ must be eliminated, while the term $-e_1^2$ must be introduced. It is readily verifiable that this is achieved with the control laws of equations 6.2.15 and 6.2.17:

$$-e_1 u_1 = -e_1^2 \tag{6.2.14}$$

$$u_1 = e_1 \tag{6.2.15}$$

$$-e_2 u_2 + e_1 e_2 = 0 \tag{6.2.16}$$

$$u_2 = e_1 \tag{6.2.17}$$

From equations 6.2.15 and 6.2.17 it can be seen that the control laws are identical, as shown in Figure 6.14. The functionality of the control laws of equations 6.2.15 and 6.2.17 is demonstrated in Figure 6.15 from which it can be observed that all of the master-slave signals synchronize.

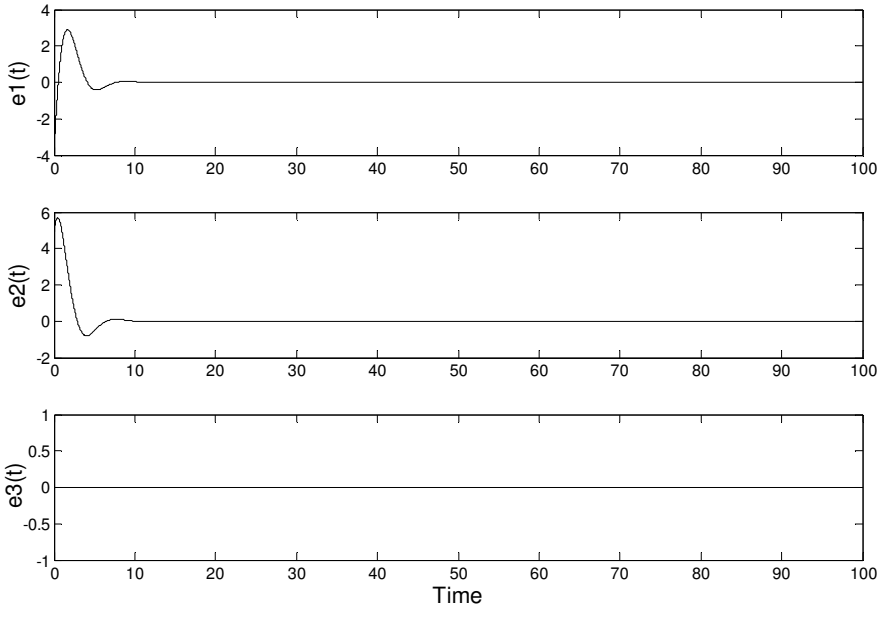


Fig. 6.15 Synchronization error of the Ueda master-slave chaotic signals with the controller

In Figure 6.14 the master system parameter set of $k = 0.05$ and $B = 7.5$ has been chosen to represent a bit 0. The master system parameter set of $k = 0.1$ and $B = 10$ has been chosen to represent a bit 1. Thus, the constants f and g of the master system of Figure 6.14 are set at 0.05 and 2.5, respectively. This allows for the adjustment of parameters k and B when bit 1 is to be transmitted. The slave system parameters are set for all time at $k = 0.05$ and $B = 7.5$, so that synchronization at the receiver side signals a bit 0 and de-synchronization signals a bit 1. Both parameter sets, $k = 0.05$, $B = 7.5$ and $k = 0.1$, $B = 10$ generate chaotic behaviour within the system [18].

The transmitted signal x is shown in Figure 6.16 when the series of 10 bits is transmitted, that is, when m = [0 0 1 0 1 1 0 1 0 1]. Figure 6.16 also shows the corresponding squared synchronization error, e_x^2, under noiseless conditions. As for the Lorenz based CPM scheme, the spreading factor of 400 has been used.

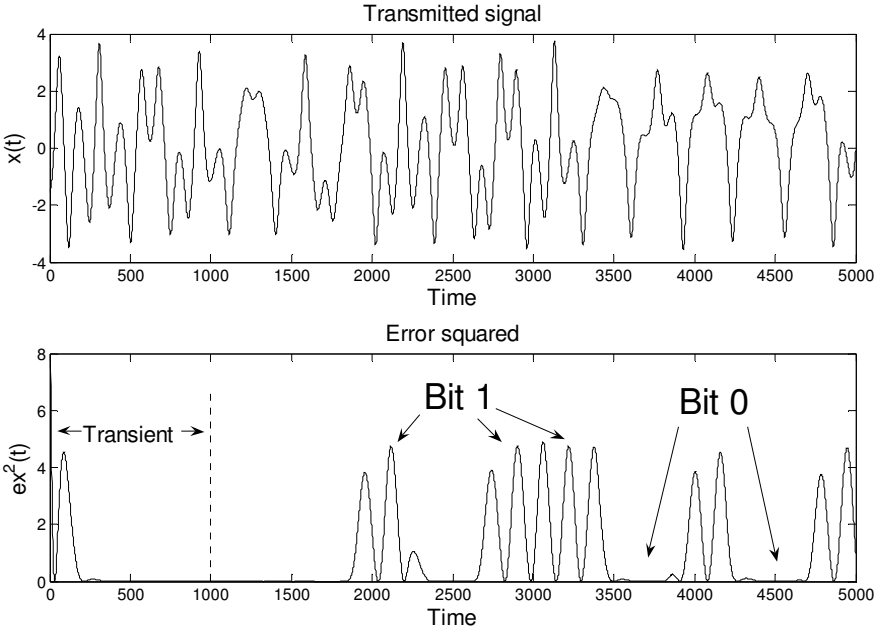


Fig. 6.16 The transmitted signal x and the squared synchronization error e_x^2

6.2.2.3 Chaotic Parameter Modulation within the Cubic Map Master-Slave System

The method of implementing the synchronized chaotic map master-slave system of chapter 4 within a CPM based communication system is now demonstrated on the $\Re^1$ cubic map. It is thus shown that one can apply either a flow or a map to a CPM based communication system when the nonlinear control laws are designed in such a way to cause synchronization among the master and slave systems. Furthermore, it is shown that the instant synchronization, as defined in chapter 4, within CPM based communication systems is of particular importance. In chapter 10, the CPM based communication system is demonstrated on the $\Re^2$ Burgers' chaotic map and its security evaluated and compared to the other chaotic communication systems.

The CPM based chaotic communication system implementing the cubic map master-slave system and the nonlinear controller of Figure 4.3, section 4.2, is shown in Figure 6.17.

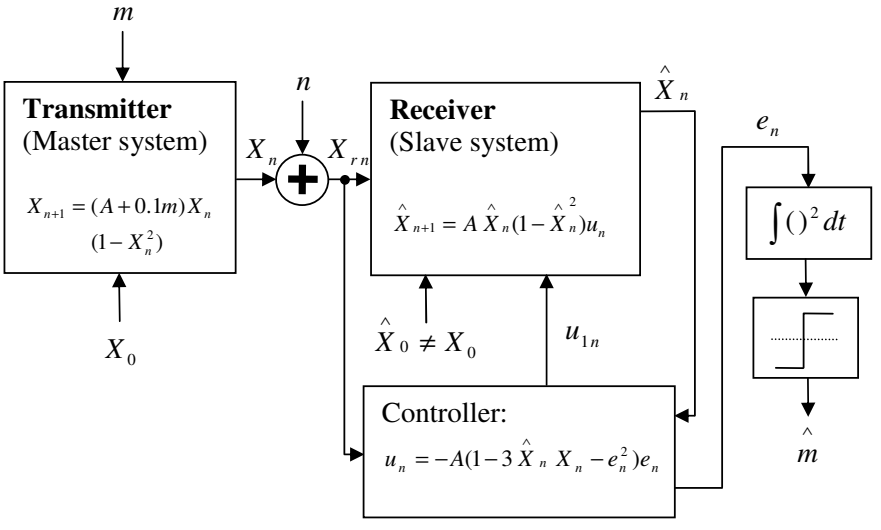


Fig. 6.17 The cubic map chaotic communication system based on the parameter modulation concept

In Figure 6.17, the master system parameter $A = 2.9$ has been chosen to represent a bit 0. The master system parameter $A = 3$ has been chosen to represent a bit 1. The message *m* of Figure 6.17 takes on the values of 0 and 1 depending on the polarity of a bit transmitted. The slave system parameter *A* is set for all time at $A = 2.9$, so that synchronization at the receiver side signals a bit 0 and desynchronization signals a bit 1. Both parameter values, $A = 2.9$ and $A = 3$, generate chaotic behaviour within the system.

The transmitted signal X_n is shown in Figure 6.18 when the series of 10 bits is transmitted, that is, when *m* = [0 0 1 0 1 1 0 1 0 1]. Figure 6.18, also shows the corresponding squared synchronization error, e_n^2, under noiseless conditions, that is, when *n* = 0. The squared synchronization error, e_n^2, is shown for the three different cases, that is, when the eigenvalues are equal to 1, 0.99 and 0. As for the Lorenz and Ueda CPM based schemes, the spreading factor of 400 has been used. A transient period of 10 chips has been allowed for the case of Figure 6.18.

It can be observed from Figure 6.18c that the system exhibits the worst performance when the eigenvalue of the system is equal to 1. This is to be expected as when the eigenvalue is outside the unit circle in the *z* domain the system does not synchronize even when the master-slave parameters match. Thus, in this case, the receiver cannot discriminate among bits 0 and 1. In contrast to this, it can be observed from Figure 6.18d that when the eigenvalue is just within the unit circle, that is, at 0.99, the system synchronizes for bits 0 and does not for bits 1. However, as can be seen from Figure 6.18d, the time it takes to synchronize is long and thus affects the performance of the system by impeding with the time period of the

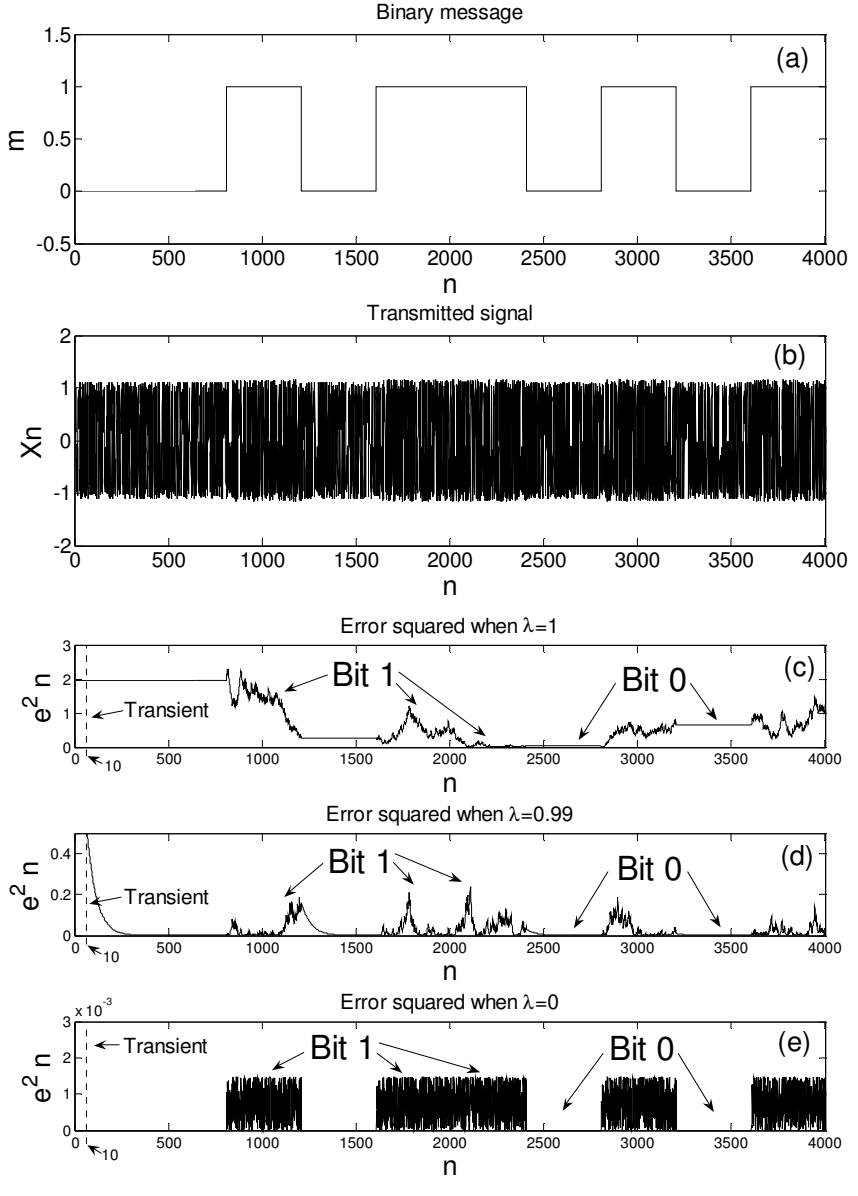


Fig. 6.18 (a) The binary message *m*, (b) The transmitted signal X_n, and: The squared synchronization error e_n^2 when: (c) $\lambda = 1$, that is, when the control law: $u_n = (1 - A(1 - 3\hat{X}_n X_n - e_n^2))e_n$, (d) $\lambda = 0.99$, that is, when the control law: $u_n = (0.99 - A(1 - 3\hat{X}_n X_n - e_n^2))e_n$, (e) $\lambda = 0$, that is, with the control law of Figure 6.17.

next bit. Finally, with the eigenvalue at 0, that is, with the error system at 0, in this $\Re_1$ case, synchronization with the matched parameters is instant. As can be seen by comparing Figures 6.18c, d and e, this allows for the most efficient discrimination among bits 0 and 1.

6.2.3 Other Forms of Chaotic Modulation

In the case of chaotic parameter modulation, the binary message is introduced into the dynamical equations of the system through one or more of the system's parameters. Alternatively, it is also possible to introduce the message into the dynamical equations of the system by incorporating it into one or more of the system's state variables. For instance, in [11,2] a binary message has been incorporated into the dynamics of the Chua master-slave system. Also, in [11], a chaotic communication system with a sinusoidal message incorporated into the dynamics of the Lorenz master-slave chaotic system has been presented. Furthermore, Lyapunov's direct method has been used to prove that the master-slave system must synchronize in the presence of the message. Using a similar approach to the one of [11,19], the authors of [13] introduce the message into the system through the x state variable. However, in this case, the message is recovered through an extra, purpose designed, state variable of the system.

The principles of operation of the Lorenz based chaotic communication system of [11], are now briefly demonstrated. The system is shown in Figure 6.19. Note that the Lorenz chaotic system has been modified here by introducing the parameter μ. The asymptotic stability within the master-slave system of Figure 6.19 has been demonstrated in [11], by showing the existence of the Lyapunov function:

$$V = \frac{1}{2}\left(\frac{1}{\sigma}e_1^2 + e_2^2 + e_3^2\right) \tag{6.2.18}$$

where: $e_1(t) = \hat{x}(t) - x(t)$, $e_2(t) = \hat{y}(t) - y(t)$, $e_3(t) = \hat{z}(t) - z(t)$.

Therefore, under noiseless conditions, the master-slave x signals must synchronize for a given drive signal $x_r = x + m$. Assuming that the sufficient amount of time has passed for x and $\hat{x}$ to synchronize, the transmitted message m can then be exactly recovered in the form of $\hat{m}$:

$$\hat{m} = x_r - \hat{x} = (x + m) - \hat{x} = m \tag{6.2.19}$$

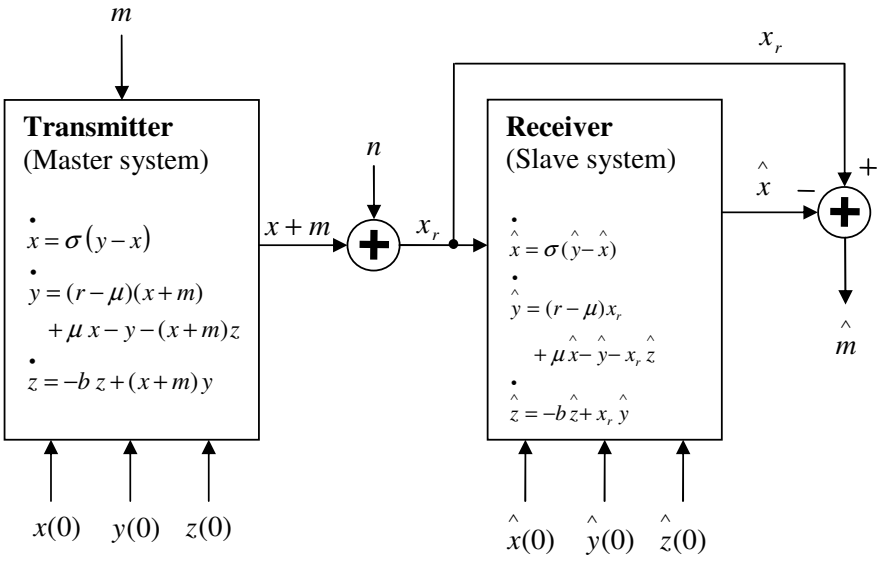


Fig. 6.19 The Lorenz based chaotic communication system of [11]. The parameter values: $\sigma = 16$, $r = 45.6$, $b = 4$ and $\mu = 0.98$.

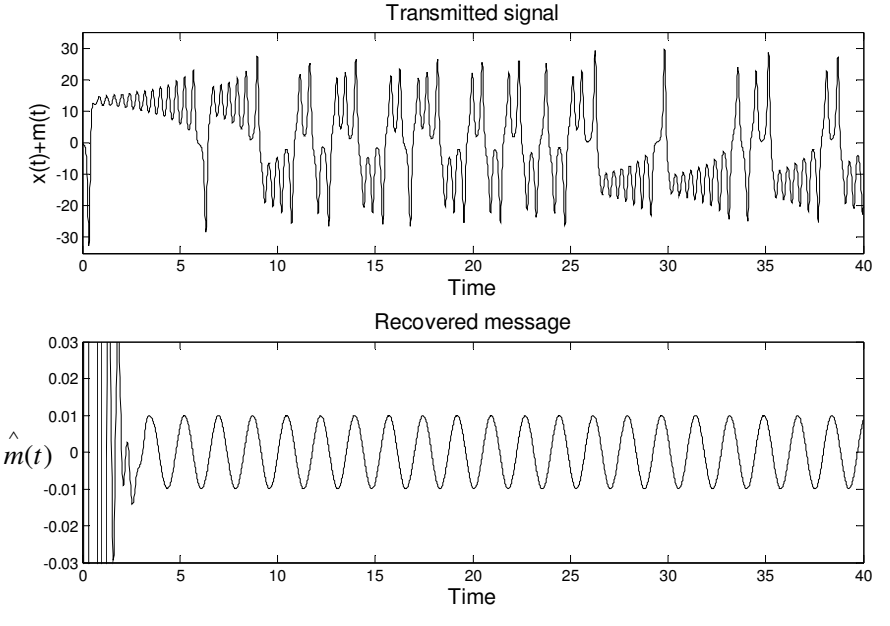


Fig. 6.20 The transmitted signal $x + m$ and the recovered message $\hat{m}$

Figure 6.20 demonstrates the operation of the system in a noiseless environment when: $m = A_m \sin(2\pi f_m)$, and: $A_m = 0.01$, $f_m = 1.8/\pi$ [11]. The upper graph of Figure 6.20 shows the transmitted signal $x + m$. From the lower graph of Figure 6.20 it can be observed that as the transients die out the sinusoidal message remains.

6.3 Initial Condition Modulation

This section presents a recently developed chaotic communication technique based on the initial condition modulation (ICM) of the chaotic carrier by the binary message, published in [10,16]. The chaotic modulation techniques of section 6.2 introduce the message into the system by incorporating it into the dynamical equations of the system. In contrast to those, the ICM technique introduces the message into the system through the system's initial conditions. The ICM technique is based on the principles of the novel mathematical analysis for predicting master-slave synchronization presented in chapter 5 [10].

6.3.1 Principles of Initial Condition Modulation

A general block diagram of a chaotic communication system based on the initial condition modulation concept is shown in Figure 6.21. The binary message *m* is introduced into the system through an initial condition (*IC*) of one of the master signals. The choice of the initial condition depends on the synchronization properties of the particular master-slave system under consideration. Using the mathematical analysis of chapter 5 [10], it is often possible to show that the mathematical expression for the synchronization error of the master-slave signals can be expressed in terms of the initial conditions of the system. The communication system is then designed by choosing two different sets of initial conditions to represent binary symbols 0 and 1. To represent a bit 0 the master-slave initial conditions are so chosen to cause the system to synchronize, that is, to cause the synchronization error to go to zero. Alternatively, to represent bit 1, the master-slave initial conditions are so chosen to inhibit synchronization. Therefore the operation of the ICM scheme resembles that of the CPM scheme in that they both rely on the state of the synchronization error at the receiver. However, the ICM scheme operates in accordance with the mathematical expression for the synchronization error. In general, the signal *x* may be an interleaved version of more than one signal of the master system [10].

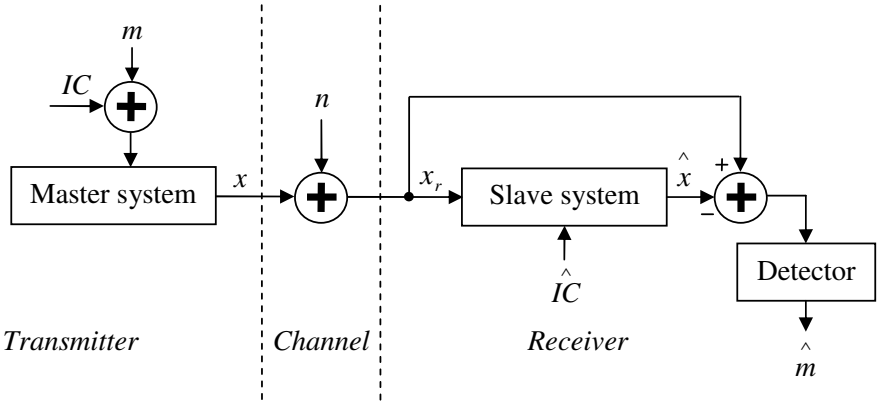


Fig. 6.21 A block diagram of the chaotic communication system based on the initial condition modulation concept

6.3.2 *Initial Condition Modulation within the Ueda Master-Slave Chaotic System*

Consider the Ueda master-slave chaotic system of Figure 5.9, section 5.3, when the master signal x drives. It has been shown in section 5.3 that in this configuration equation 5.3.19, repeated below as equation 6.3.1, governs the synchronization error of the master-slave y signals [10]:

$$y(t_o) - \hat{y}(t_o) = A - k\int_{t=0}^{t=t_o} (y(t) - \hat{y}(t))dt + 2B\sin(\phi)\sin(t_o + \Omega) \qquad (6.3.1)$$

where: $$\phi = \frac{z - \hat{z}}{2} = \frac{z(0) - \hat{z}(0)}{2}, \qquad \Omega = \phi + \hat{z}(0) + \frac{\pi}{2}.$$

In addition, it has also been shown in section 5.3 [10] that as time tends to infinity equation 6.3.1 settles to the steady state behaviour governed by its third term. Furthermore, note that the third term of equation 6.3.1 is governed by the initial conditions of the master-slave z signals. By observing equation 6.3.1 it is then readily verifiable that the error of the master-slave y signals tends to zero when the difference among the master-slave z initial conditions is equal to $\pm 2n\pi$ (where n is any integer). Alternatively, when the difference is equal to $\pm n\pi$, (where n is any odd integer), the error of the master-slave y signals reaches its maximum possible value. These two chaotic synchronization properties of the Ueda master-slave chaotic system have been utilized to construct the communication system of Figure 6.22. The master initial condition of the z signal is varied according to the value of the bit to be transmitted, bit 0 being represented by $m = 2\pi$ and bit 1 by $m = \pi$. In this way, the overall difference among the

master-slave z initial conditions entering the transmitter and the receiver is equal to either π or 2π. Therefore, under noiseless conditions, the system either synchronizes or does not [10].

As explained in chapter 1, for optimal performance of the system in the AWGN channel, it is essential that the symbols (bits) are as far apart as possible in their symbol space [20]. For the communication system of Figure 6.22 the separation of symbols 0 and 1 in their symbol space is largest when the difference among the master-slave z initial conditions is equal to $\pm 2n\pi$ (where n is any integer) and $\pm n\pi$, (where n is any odd integer), respectively. These two properties of the Ueda master-slave chaotic system are expressed by equations 5.3.25 and 5.3.28 and illustrated by Figures 5.13b and 5.14b of section 5.3.

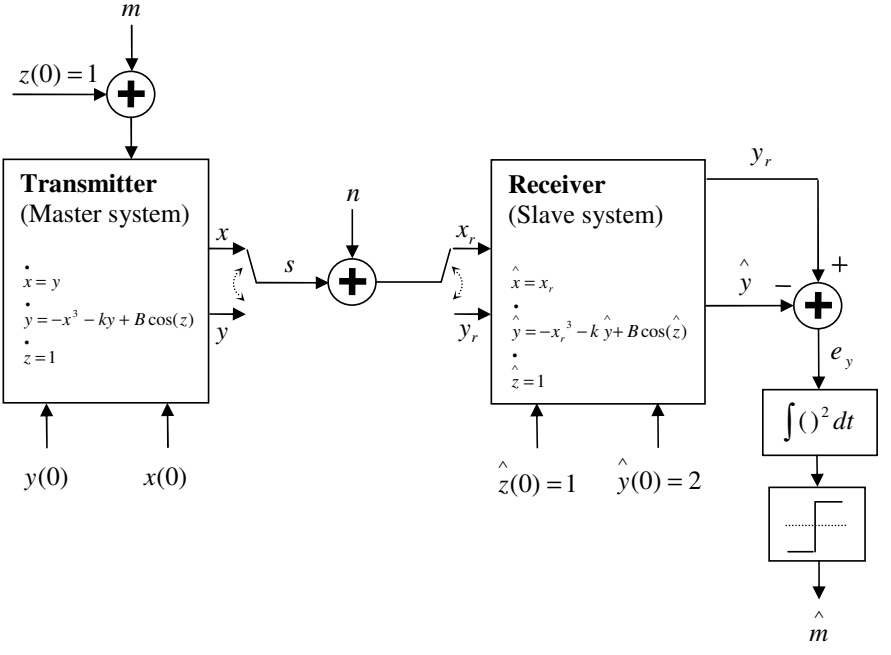


Fig. 6.22 The Ueda chaotic communication system based on the initial condition modulation

In order to evaluate e_y at the receiver, both master signals x and y, must be transmitted. Therefore, in Figure 6.22, the transmitted signal s is a signal composed of x and y master signals interleaved in the fashion described by Eqs. 6.3.2 and 6.3.3, respectively [10]:

$$x(t) = \sum_{i=1}^{N} x_t \delta(t - 2n + 1) \qquad (6.3.2) \qquad\qquad y(t) = \sum_{i=1}^{N} y_t \delta(t - 2n) \qquad (6.3.3)$$

In equations 6.3.2 and 6.3.3 $\delta(t)$ is the impulse function and N is the spreading factor, that is, the number of x (y) chaotic points representing a single bit.

The x_r and y_r signals, at the receiver side of Figure 6.22, represent the noisy x and y signals of the transmitted signal, where n denotes AWGN, composed of the two components represented in time domain by equations 6.3.4 and 6.3.5:

$$n_x(t) = \sum_{i=1}^{N} n_{x\,t}\, \delta(t - 2i + 1) \tag{6.3.4}$$

$$n_y(t) = \sum_{i=1}^{N} n_{y\,t}\, \delta(t - 2i) \tag{6.3.5}$$

The x_r and y_r signals are represented by equations 6.3.6 and 6.3.7, respectively:

$$x_r(t) = x(t) + n_x(t) = \sum_{i=1}^{N} (x_t + n_{x\,t})\, \delta(t - 2i + 1) \tag{6.3.6}$$

$$y_r(t) = y(t) + n_y(t) = \sum_{i=1}^{N} (y_t + n_{y\,t})\, \delta(t - 2i) \tag{6.3.7}$$

In order to avoid periodicity of chaotic sequences representing bit 0 (or bit 1), it is essential to alter $x(0)$ and $y(0)$ with every new bit sent. Also, in order to ensure the continuity of the smooth nature of the signals at the transition of the transmitted bits, the initial conditions of x and y for every new bit transmitted are chosen as the final values of the chaotic carrier of the preceding bit. The interleaved transmitted signal s is shown in Figure 6.23 when the series of 10 bits is transmitted, that is, when m = [2π, 2π, π, 2π, π, π, 2π, π, 2π, π], or in binary terms: *message* = [0 0 1 0 1 1 0 1 0 1]. Figure 6.23 also shows the corresponding squared synchronization error, e_y^2, under noiseless conditions. The spreading factor of 400 has been used.

In order to demonstrate the performance of the Ueda ICM based communication system of Figure 6.22, an empirical BER curve has been produced and compared to the BER curve of the BPSK communication system [20,21]. In addition, an empirical BER curve of the Lorenz based CPM scheme presented above [8] has also been produced [21]. The results of the BER analysis are displayed in Figure 6.24. From Figure 6.24 it is observed that it requires 13-14 dB less energy per bit to achieve the same probability of error using the Ueda ICM based system of Figure 6.22 as compared to the Lorenz CPM based system of [8]. The empirical BER curves have been obtained in the following manner. The bit energy was obtained by first determining the average power of the chaotic carrier and

multiplying it by the bit period [10,20]. Then for specified bit energy to noise power spectral density ratio (E_b / N_o), the required power (variance) of noise was calculated and thus white Gaussian noise of that power generated. Finally for each E_b / N_o the probability of error, that is the bit error rate, was determined.

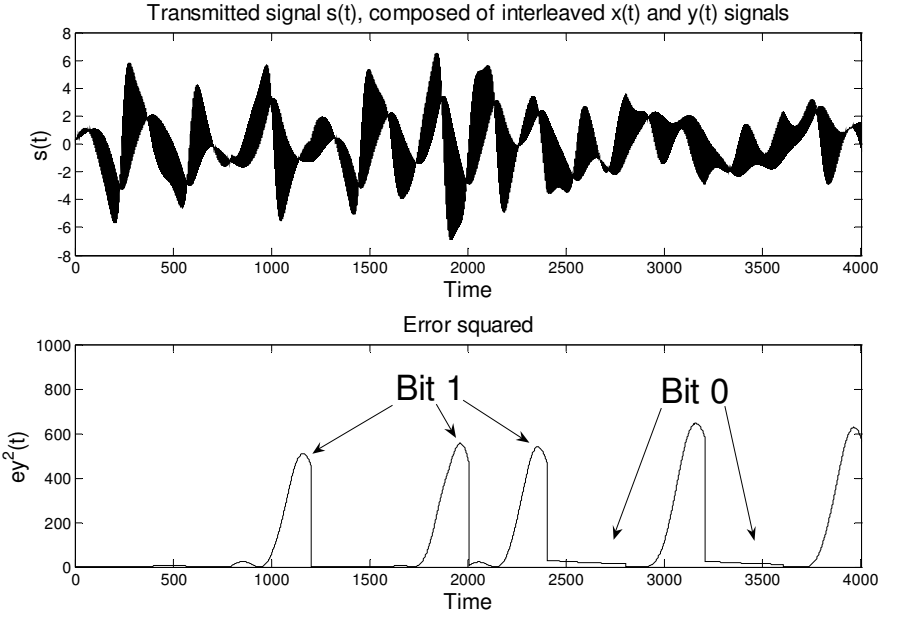


Fig. 6.23 The interleaved transmitted signal *s*, and the squared synchronization error e_y^2

It should be pointed out that the scheme of Figure 6.22 is not the only possible configuration of implementing the system presented. For instance, in order to avoid transmission of both *x* and *y* master signals across the channel, it is possible to introduce a differentiator at the receiver side and pass the received *x* signal through it to obtain an estimate of the master *y* signal, as from equation 5.3.1, section 5.3, it is observed that in fact $\dot{x} = y$. Such a configuration has the advantage from the aspect of the reduced bandwidth requirement by transmitting a single signal instead of two interleaved signals. However, in this case, the robustness to noise of the system is significantly reduced as is demonstrated by the open squares BER curve of Figure 6.24.

Yet another, more robust scheme which shows how to implement the Ueda ICM scheme by transmitting only the master signal *x* is proposed. This scheme is outlined in the appendix [15]. In this particular configuration it is shown that the

transmitted bits can be recovered by only observing the slave signal $\hat{y}$ thus eliminating the requirement of transmitting the master signal y as well.

Similar ICM based communication systems can also be constructed as is demonstrated in the next two subsections on the simplest quadratic and the simplest piecewise linear master-slave chaotic flows.

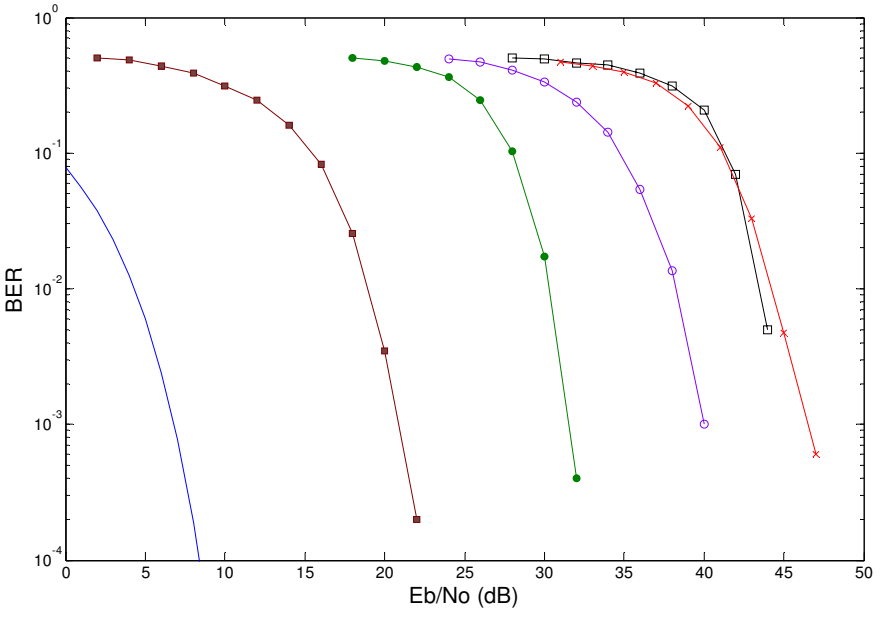


Fig. 6.24 The BER curves: (a) the solid line is for the theoretical BPSK, (b) the solid circles are for the Ueda ICM based system of Figure 6.22, (c) the crosses are for the Lorenz CPM based system of Figure 6.7 [8], (d) the open squares are for the Ueda ICM based system of Figure 6.22 but with the differentiator and only x transmitted, (e) the solid squares are for the simplest quadratic ICM based system of Figure 6.25, (f) the open circles are for the simplest piecewise linear ICM based system of Figure 6.27.

6.3.3 The Communication System Implementing the Simplest Quadratic Master-Slave Chaotic Flow

In Figure 6.25 the communication system implementing the simplest quadratic master-slave chaotic flow is outlined.

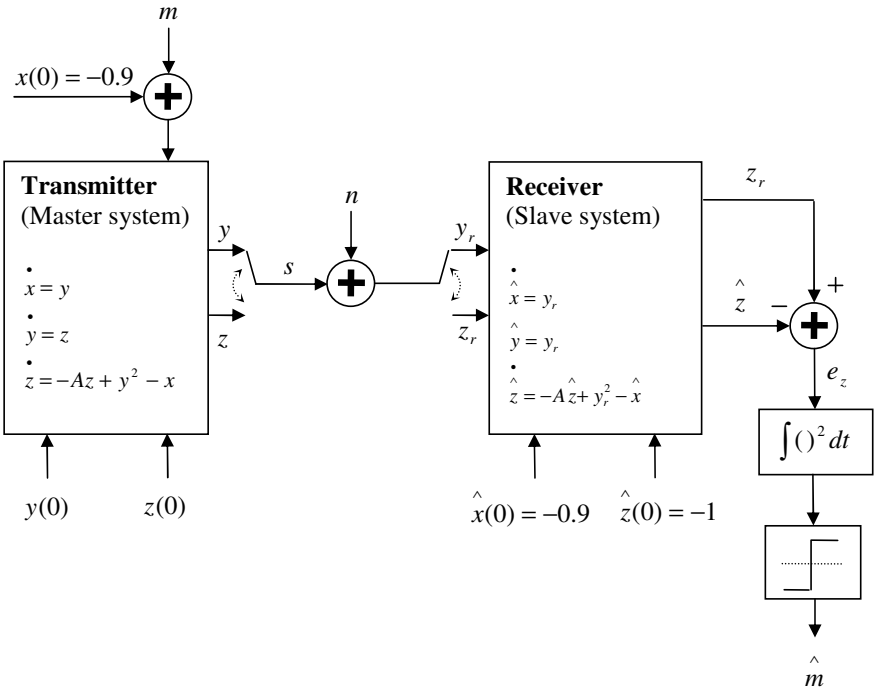


Fig. 6.25 The simplest quadratic chaotic communication system based on the initial condition modulation

The transmitted signal s is a signal composed of y and z master signals, interleaved in the same fashion as signals x and y of the previous section. The signals y_r and z_r, are described by equations 6.3.8 and 6.3.9, respectively:

$$y_r(t) = y(t) + n_y(t) = \sum_{i=1}^{N} (y_t + n_{y\,t})\,\delta(t - 2i + 1) \tag{6.3.8}$$

$$z_r(t) = z(t) + n_z(t) = \sum_{i=1}^{N} (z_t + n_{z\,t})\,\delta(t - 2i) \tag{6.3.9}$$

The operation of the communication system of Figure 6.25 is based on the synchronization error of the master-slave z signals. It has been shown in section 5.2 [10] that after the transients die down, the synchronization error of the master-slave z signals is governed by equation 5.2.22, repeated below as equation 6.3.10 for convenience:

$$\delta = -\frac{\alpha}{A} \tag{6.3.10}$$

Recall that in equation 6.3.10, $\alpha = x(0) - \hat{x}(0) = x - \hat{x}$, and A is the system parameter.

The master initial condition of the x signal is varied according to the value of the bit to be transmitted, bit 1 being represented by $m = 8.9$ and bit 0 by $m = 0$. Such choice of m ensures that the distance of symbols (bits) in their symbol space is large, while still maintaining the chaotic properties of the system. The symbol space of this system is limited by the basin of attraction of the initial conditions of the simplest quadratic chaotic flow and therefore care must be taken in the choice of the initial conditions [22] to avoid the system going off to infinity.

To avoid periodicity of chaotic sequences representing bit 0 (or bit 1), it is essential to alter $y(0)$ and $z(0)$ with every new bit sent. However, in this case, the initial conditions of y and z for every new bit transmitted have not been chosen as the final values of the chaotic carrier of the preceding bit, due to the limited basin of attraction of the initial conditions. Instead, they have been randomly assigned within the basin of attraction for every new bit transmitted. This ensures the chaotic properties of the system; however, it may jeopardize the security of the system as compared to the system of Figure 6.22, due to the non-smooth bit transitions and the more restricted choice of initial conditions. The interleaved transmitted signal s is shown in Figure 6.26 when the series of 10 bits is transmitted, that is, when $m = [2\pi, 2\pi, \pi, 2\pi, \pi, \pi, 2\pi, \pi, 2\pi, \pi]$, or in binary terms: *message* = [0 0 1 0 1 1 0 1 0 1]. Figure 6.26 also shows the corresponding squared synchronization

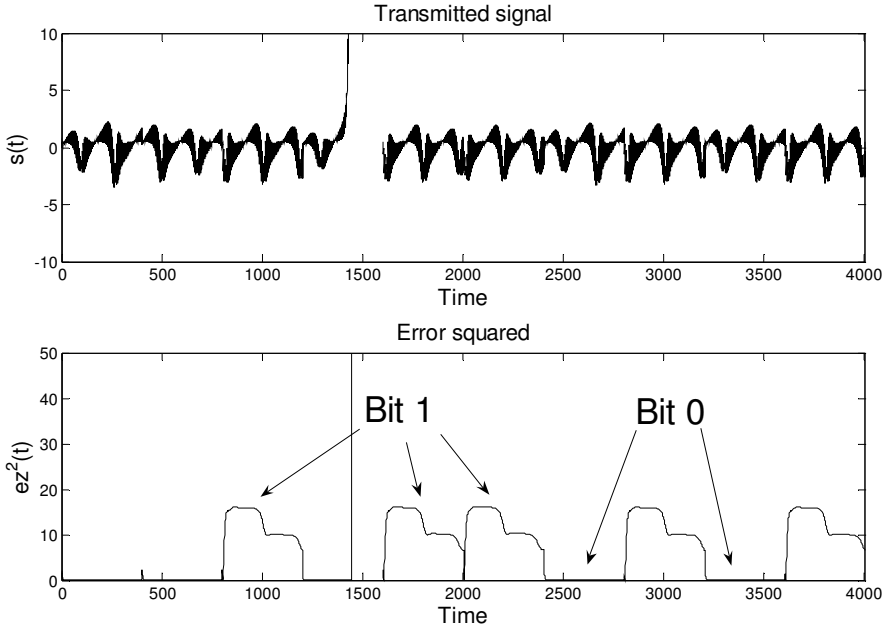


Fig. 6.26 The interleaved transmitted signal s, and the squared synchronization error e_z^2

error, e_y^2, under noiseless conditions. The spreading factor of 400 has been used. From Figure 6.26 one can observe that the transmitted signal diverges to infinity if the chosen initial conditions of a particular bit are not within the basin of attraction.

The result of the BER analysis for the simplest quadratic ICM based system of Figure 6.25 is displayed in Figure 6.24 by the curve marked by solid squares. From Figure 6.24 it is observed that it requires 11-12 dB less energy per bit to achieve the same probability of error using the simplest quadratic ICM based system of Figure 6.25 as compared to the Ueda ICM based system of Figure 6.22.

6.3.4 *The Communication System Implementing the Simplest Piecewise Linear Master-Slave Chaotic Flow*

In Figure 6.27 the communication system implementing the simplest piecewise linear master-slave chaotic flow, where the transmitted signal *s* is composed of the interleaved signals *y* and *x*, is outlined.

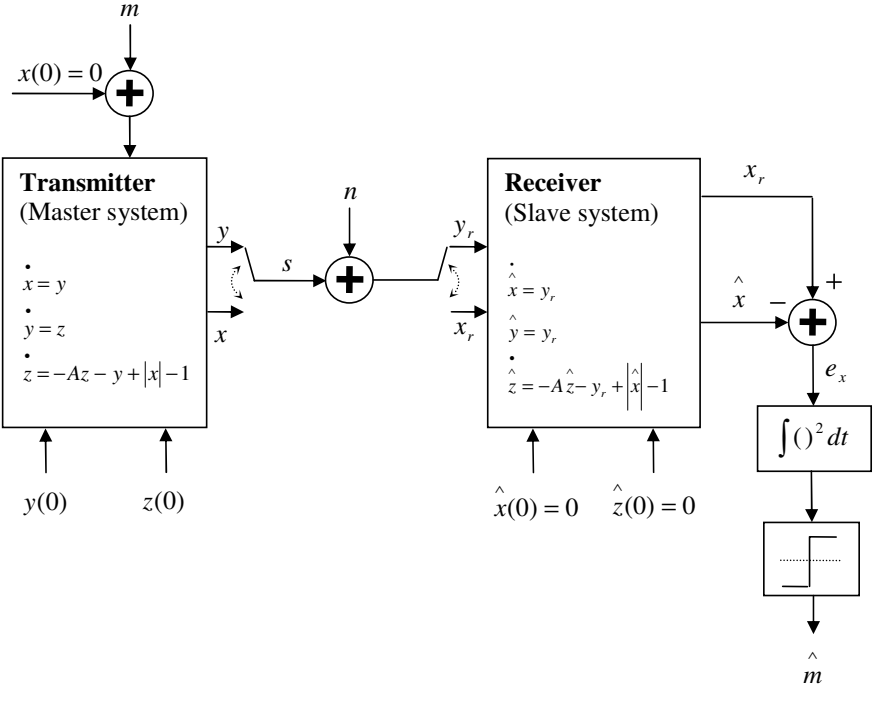


Fig. 6.27 The simplest piecewise linear chaotic communication system based on the initial condition modulation

The signals y_r and x_r, are described by equations 6.3.11 and 6.3.12, respectively:

$$y_r(t) = y(t) + n_y(t) = \sum_{i=1}^{N} (y_t + n_{yt})\,\delta(t - 2i + 1) \tag{6.3.11}$$

$$x_r(t) = x(t) + n_x(t) = \sum_{i=1}^{N} (x_t + n_{xt})\,\delta(t - 2i) \tag{6.3.12}$$

The operation of the communication system of Figure 6.27 is based on the synchronization error of the master-slave x signals, represented by equation 5.1.7, and repeated below as equation 6.3.13 for convenience:

$$x - \hat{x} = x(0) - \hat{x}(0) = J \tag{6.3.13}$$

The initial condition of the master signal x is varied according to the value of the bit to be transmitted, bit 1 being represented by $m = 1$ and bit 0 by $m = 0$. Such a choice of m ensures that the separation of symbols (bits) in their symbol space is relatively large, while still maintaining the chaotic properties of the system, that is, preventing the system from going off to infinity. In order to preserve smoothness of the transmitted chaotic sequence y, as well as to avoid periodicity, the initial condition of y for every new bit transmitted is chosen as the final value of the chaotic carrier of the preceding bit. The disadvantage of this system is that the initial conditions of the master signal x modulate the message to be transmitted while at the same time transmitting the master signal x, thus jeopardizing the security of the information transmitted as compared to the systems of Figure 6.22 and Figure 6.25. The interleaved transmitted signal s is shown in Figure 6.28 when the series of 10 bits is transmitted, that is, when m = [2π, 2π, π, 2π, π, π, 2π, π, 2π, π], or in binary terms: *message* = [0 0 1 0 1 1 0 1 0 1]. Figure 6.28 also shows the corresponding squared synchronization error, e_y^2, under noiseless conditions. The spreading factor of 400 has been used. From Figure 6.28 one can observe that the transmitted signal does not diverge to infinity at any time if the chosen initial conditions of a particular bit are within the basin of attraction.

The result of the BER analysis for the simplest piecewise linear ICM based system of Figure 6.27 is displayed in Figure 6.24 by the curve marked by open circles. From Figure 6.24 it is observed that it requires 6-9 dB more energy per bit to achieve the same probability of error using the simplest piecewise linear ICM based system of Figure 6.27 as compared to the Ueda ICM based system of Figure 6.22.

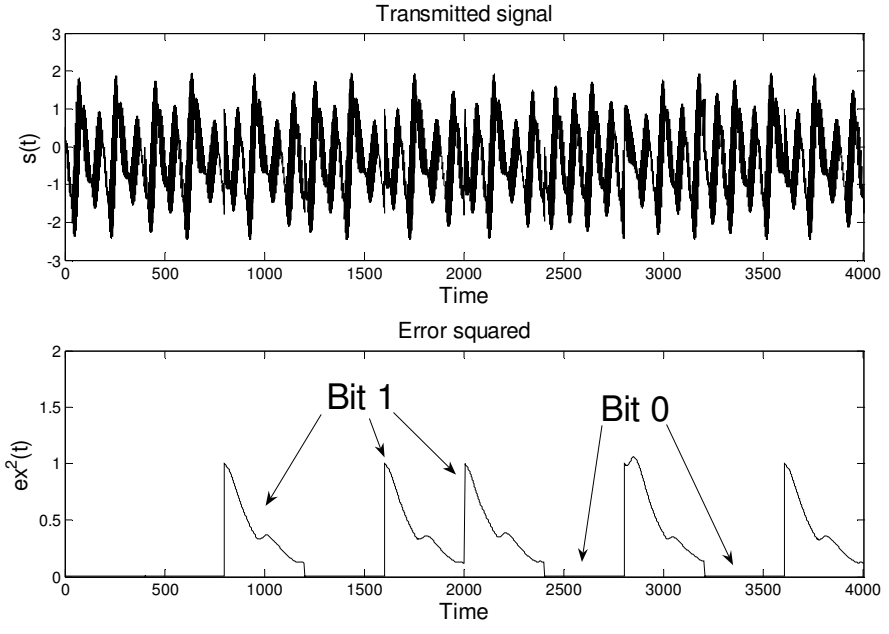


Fig. 6.28 The interleaved transmitted signal *s*, and the squared synchronization error e_x^2

6.3.5 Discussion

In this section the three chaotic communication systems, based on the initial condition modulation of the message to be transmitted, have been presented. They are now discussed in terms of their performance.

The communication system based on the simplest quadratic master-slave chaotic flow exhibits the best performance in terms of the bit error rate, as compared to the other two systems, due to the largest relative separation of the bits transmitted in their symbol space at the receiver. Due to having the smallest relative separation of the bits transmitted in their symbol space, the communication system based on the simplest piecewise linear master-slave chaotic flow exhibits the worst bit error rate performance.

From the security point of view, the communication system based on the Ueda master-slave chaotic system may offer the most security out of the three systems presented, as this system is not limited by the basin of attraction. This allows for the widest range of initial conditions for the message modulation, that is, it enables for the smooth nature of the transmitted signal at the bit transitions. The communication system based on the simplest piecewise linear master-slave chaotic flow uses the error of the master-slave *x* signals to demodulate the message while at the same time the initial conditions of the transmitted master signal *x* modulate the message. This can be seen from equation 6.3.13 and Figure 6.27. Therefore the security of this system is jeopardized as compared to the other two

systems whose demodulation, that is, steady state synchronization error, equations are independent of their own initial conditions, but depend on the modulating initial conditions of the signal not transmitted. This can be seen from equations 6.3.1 and 6.3.10, and Figures 6.22 and 6.25, respectively.

6.4 Performance Evaluation in the Presence of Noise

In this section, the noise performance of the binary modulation techniques of sections 6.2 and 6.3 is examined and compared in terms of the bit error rate.

In Figure 6.29 the BER performance of the Lorenz, Ueda and cubic CPM systems is compared to that of the ICM systems of section 6.3. Furthermore, the BER curve of the filtered and plain Ueda ICM system with only x transmitted [15], (outlined in the appendix), is also presented.

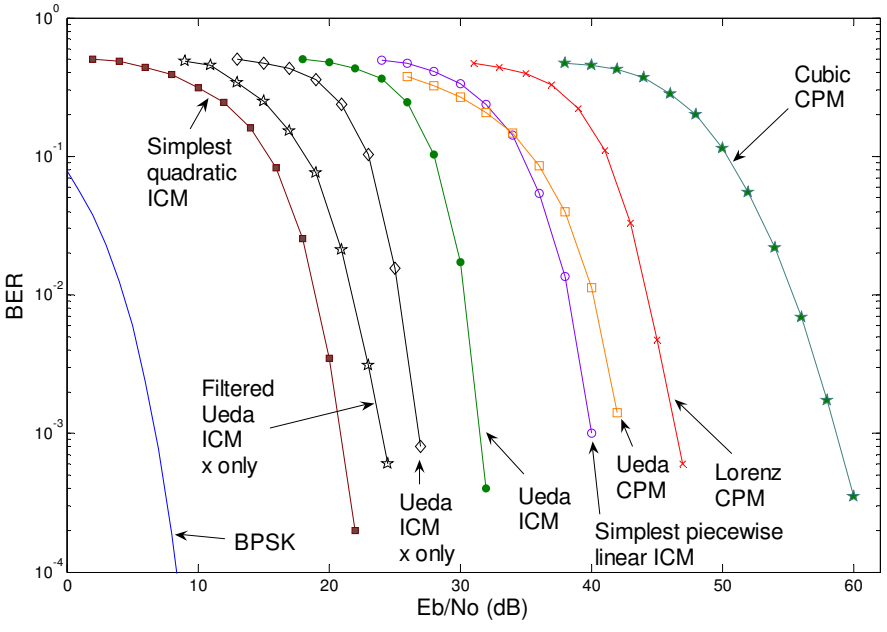


Fig. 6.29 The BER curves: (a) the solid line is for the theoretical BPSK, (b) the solid squares are for the simplest quadratic ICM system of Figure 6.25 [10], (c) the open pentagram stars are for the Filtered Ueda ICM system of the appendix [15], (d) the open diamonds are for the Ueda ICM system of the appendix [15], (e) the solid circles are for the Ueda ICM system of Figure 6.22 [10], (f) the open circles are for the simplest piecewise linear ICM system of Figure 6.27 [10], (g) the open squares are for the Ueda CPM system of Figure 6.14 [16], (h) the crosses are for the Lorenz CPM system of Figure 6.7 [8], (i) the open pentagram stars are for the cubic CPM system of Figure 6.17.

While evaluating the BER curves of Figure 6.29 it has been assumed that the clock synchronization among the clock at the transmitter and the clock at the receiver has already been achieved. As discussed in chapter 1, this assumption is used in most cases when evaluating the performance of binary modulation techniques [20,10].

From Figure 6.29 it is observed that it requires 7-10 dB less energy per bit to achieve the same probability of error using the Ueda ICM system as compared to the Ueda CPM system. Furthermore, it requires 4-6 dB less energy per bit to achieve the same probability of error using the Ueda CPM system as compared to the Lorenz CPM system. Therefore, the Ueda ICM system exhibits better noise performance than the Ueda CPM system which in turn exhibits better noise performance than the Lorenz CPM system. However, most importantly, it should be observed that all of the ICM based systems developed here outperform the CPM based systems. In particular, the best performance is exhibited by the simplest quadratic ICM based system and the worst by the cubic CPM based system. Although the simplest quadratic ICM based chaotic communication system exhibits the best performance in terms of BER it has been argued in section 6.3 that it may not be the most secure system. Similarly, it was argued that Ueda ICM based system exhibits the best overall performance in terms of security and BER. Therefore, the further 4-5 dB BER improvement exhibited by the Ueda ICM based system with only the master signal x transmitted over the Ueda ICM based system with both master x and y signals transmitted (Figure 6.22) is of particular importance. Furthermore, it has been shown in the appendix [15] that by applying filters to the received signal x further improves the performance of the system by 3-4 dB. However, it can be observed from Figure 6.29 that even the simplest quadratic ICM based system which exhibits the best BER performance, out of all of the chaotic synchronization based systems examined, is still outperformed by the BPSK system by approximately 14 dB. In the next chapter, a robust synchronization unit for the chaos based DS-CDMA systems is proposed. It is shown that in terms of BER it outperforms the communication systems based on the principle of chaotic synchronization presented and examined in this chapter.

It should be noted that all of the communication systems presented in this chapter are inherently single user systems. It will be shown in chapter 9, how principles of TDM can be used to allow these systems to become multi-user systems. Their performance will be examined in both AWGN and Rayleigh fading channels. Furthermore, it will be shown that by using different receiver architectures BER performance can be improved in certain cases.

6.5 Conclusion

In this chapter, several chaotic communication systems with the receiver based on chaotic synchronization have been described. These include the chaotic communication schemes of chaotic masking, chaotic modulation and the new chaotic communication scheme of initial condition modulation.

It has been shown how Lyapunov's direct method presented in chapter 3 can be used in the design of CPM based communication systems. In particular, this has been shown on the Ueda master-slave chaotic system.

Furthermore, a method of implementing the synchronized chaotic map master-slave system of chapter 4 within a CPM based secure communication system, was demonstrated on the $\Re^1$ cubic map. It was shown that instant synchronization within the chaotic map CPM based communication system allows for the highest level of discrimination among bits 0 and 1.

On the basis of findings of chapter 5, a secure communication system based on the initial condition modulation of the chaotic carrier by the binary message was then presented. In particular, this system utilizes a novel approach to the master-slave synchronization properties of the three chaotic flows investigated. The empirical BER curves for the presented communication systems have then been produced and compared to the empirical BER curve of the Lorenz CPM based communication system of [8], demonstrating a significant improvement. It has been shown that the communication system based on the simplest quadratic master-slave chaotic flow exhibits the best performance in terms of BER, as compared to the other two presented systems based on the Ueda and the simplest piecewise linear master-slave chaotic flows. From the security point of view it has been observed that the communication system based on the Ueda master-slave chaotic system may be the most secure of the three systems presented.

Finally, the overall performance of the chaotic parameter and initial condition modulation techniques has been examined and compared in the presence of AWGN. It has been shown in terms of BER that the ICM based chaotic communication systems exhibit better noise performance than the CPM based ones. Therefore, most importantly, it can be concluded that all of the chaotic synchronization ICM based systems presented here outperform the presented CPM based systems. Furthermore, it has been shown on the Ueda ICM based chaotic communication system that the denoising techniques can be used to further improve the BER performance. The details of the denoising techniques developed have been described in the appendix. The work of this chapter has been published in [10,16,15].

References

[1] Murali, K., Lakshmanan, M.: Transmission of signals by synchronization in a chaotic Van der Pol-Duffing oscillator. Physical Review E, Rapid Communications 48(3), R1624–R1626 (1993)

[2] Wu, C.W., Chua, L.O.: A unified framework for synchronization and control of dynamical systems. International Journal of Bifurcation and Chaos 4(4), 979–998 (1994)

[3] John, J.K., Amritkar, R.E.: Synchronization of unstable orbits using adaptive control. Physical Review E 49(6), 4843–4848 (1994)

[4] Oppenheim, A.V., Wornell, G.W., Isabelle, S.H., Cuomo, K.M.: Signal processing in the context of chaotic signals. In: Proceedings IEEE ICASSP, pp. 117–120 (1992)

[5] Kocarev, L., Halle, K.S., Eckert, K., Chua, L.O., Parlitz, U.: Experimental demonstration of secure communications via chaotic synchronization. International Journal of Bifurcation and Chaos 2(3), 709–713 (1992)
[6] Parlitz, U., Chua, L.O., Kocarev, L., Hale, K.S., Shang, A.: Transmission of digital signals by chaotic synchronization. International Journal of Bifurcation and Chaos 2(4), 973–977 (1992)
[7] Kapitaniak, T., Sekieta, M., Ogorzalek, M.: Monotone synchronization of chaos. International Journal of Bifurcation and Chaos 6(1), 211–217 (1996)
[8] Cuomo, K.M., Oppenheim, A.V.: Circuit Implementation of Synchronized Chaos with Applications to Communications. Physical Review Letters 71(1), 65–68 (1993)
[9] Cuomo, K.M., Oppenheim, A.V., Strogatz, S.H.: Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications. IEEE Transactions on Circuits and Systems – II. Analog and Digital Signal Processing 40(10), 626–633 (1993)
[10] Jovic, B., Berber, S., Unsworth, C.P.: A novel mathematical analysis for predicting master – slave synchronization for the simplest quadratic chaotic flow and Ueda chaotic system with application to communications. Physica D 213(1), 31–50 (2006)
[11] Wu, C.W., Chua, L.O.: A simple way to synchronize chaotic systems with applications to secure communication systems. International Journal of Bifurcation and Chaos 3(6), 1619–1627 (1993)
[12] Halle, K.S., Wu, C.W., Itoh, M., Chua, L.O.: Spread spectrum communication through modulation of chaos. International Journal of Bifurcation and Chaos 3(2), 469–477 (1993)
[13] Lu, J., Wu, X., Lü, J.: Synchronization of a unified chaotic system and the application in secure communication. Physics Letters A 305(6), 365–370 (2002)
[14] Pecora, L.M., Carroll, T.L.: Synchronization in chaotic systems. Physical Review Letters 64(8), 821–824 (1990)
[15] Jovic, B., Unsworth, C.P., Berber, S.M.: De-noising 'Initial Condition Modulation' Wideband Chaotic Communication Systems with Linear & Wavelet Filters. In: Proceedings of the First IEEE International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2006), Sydney, Australia, March 13-16, pp. 1–6 (2006)
[16] Jovic, B., Unsworth, C.P.: Synchronization of Chaotic Communication Systems. In: Wang, C.W. (ed.) Nonlinear Phenomena Research Perspectives, Nova Publishers, New York (2007)
[17] Lau, F.C.M., Tse, C.K.: Chaos-Based Digital Communication Systems, ch. 1, pp. 1–20. Springer, Berlin (2004)
[18] Ueda, Y.: Survey of Regular and Chaotic Phenomena in the Forced Duffing Oscillator. Chaos, Solitons and Fractals 1(3), 199–231 (1991)
[19] Kennedy, M.P., Kolumban, G.: Digital Communications Using Chaos. In: Chen, G. (ed.) Controlling Chaos and Bifurcations in Engineering Systems, pp. 477–500. CRC Press LLC, Boca Raton (1999)
[20] Carroll, T.L., Pecora, L.M.: Using multiple attractor chaotic systems for communication. Chaos 9(2), 445–451 (1999)
[21] Reddell, N.F., Welch, T.B., Bollt, E.M.: A covert communication system using an optimized wideband chaotic carrier. In: MILCOM Proceedings, vol. 2, pp. 1330–1334 (2002)
[22] Sprott, J.C.: Chaos and Time-Series Analysis, pp. 230–440. Oxford University Press, Oxford (2003)

Chapter 7
A Robust Sequence Synchronization Unit for Multi-user Chaos Based DS-CDMA Communication Systems

This chapter demonstrates two ways of achieving and maintaining sequence synchronization in multi-user chaos based direct sequence code division multiple access (CBDS-CDMA) communication systems. In both cases, synchronization is achieved and maintained through code acquisition and code tracking phases, respectively. The performance of the proposed systems is evaluated in the presence of additive white Gaussian noise and interuser interferences as well as in a Rayleigh fading channel. A pseudo random binary sequence (PRBS) and a logistic chaotic map are used as the synchronizing periodic, and non-periodic, pilot signals within the multi-user chaotic communication system. In addition, the Bernoulli chaotic map is also used as the pilot signal in the investigation of the code acquisition performance. The code acquisition circuit is evaluated in terms of the probability of detection and probability of false alarm. The corresponding results demonstrate an ability to achieve initial synchronization. Furthermore, it is shown that in terms of code acquisition the PRBS outperforms the logistic and Bernoulli chaotic maps when used as pilot signals. The mathematical models of the code tracking loops are then developed and their validity demonstrated by means of a simulation for both PRBS and chaotic pilot based CBDS-CDMA systems. From the models, the control laws for the generation of time offset estimates are derived. The robustness of the synchronization units is then demonstrated in terms of the bit error rate. It has been shown that for the PRBS based system, in an AWGN channel, for the case of 1, 2, 3, 4, and 5 users the bit error rate goes below the maximum acceptable limit of 10^{-3} at the bit energy to noise power spectral density ratio of approximately 8, 9, 9.5, 11 and 12 dB, respectively. The chaotic pilot based CBDS-CDMA systems exhibit marginally better performance for a single user plus a chaotic pilot signal than the corresponding PRBS pilot based CBDS-CDMA system at the BER level of 10^{-4} and below. In particular, at the BER level of 10^{-6}, this improvement in performance is approximately equal to 0.175 dB. Their BER performances match for more than one user in the system. It has also been shown that the periodic and non-periodic chaotic pilot based CBDS-CDMA systems' BER performances match for any number of users in the system. Furthermore a gradual degradation in performance, above the maximum acceptable

B. Jovic: Synchronization Techniques for Chaotic Commun. Syst., SCT 5, pp. 171–227.
springerlink.com

bit error rate limit, is demonstrated for the increasing number of users for all systems. Finally, it is shown that although the systems are robust to the influence of AWGN and interuser interferences, they all fail to satisfy the maximum allowable bit error rate limit of 10^{-3} in the Rayleigh fading channel. By introducing a chaotic pilot signal in place of a PRBS signal, the CBDS-CDMA system is made fully chaotic. In this way, the CBDS-CDMA systems' security is significantly improved by eliminating an inherently different PRBS pilot signal.

As mentioned in chapter 3, the synchronization of chaotic systems was first studied by Yamada and Fujisaka in 1983 [1], and Afraimovich et al. in 1986 [2]. However it was not until 1990 when Pecora and Carroll (PC) introduced their method of chaotic synchronization (CS) [3] and suggested application to secure communications that the topic started to arouse major interest. The chaotic synchronization of [3] is most often established by employing Lyapunov's direct method [4-6] or by considering the conditional Lyapunov exponents [7-9], leading to the design of the chaotic communication systems. Alternatively, the synchronization techniques of traditional spread spectrum communication systems [10-15] achieve synchronization between the transmitter and receiver in two distinct phases. These are called the code acquisition and the code tracking phase [10-21]. The code acquisition [11,10,13,14,15,18,20,21], or the initial synchronization phase, involves determining the time offset amidst the incoming signal and the basis function copy at the receiver to within a specified range known as the pull-in region of the tracking loop [11,12,10,15-17,19]. Upon the successful completion of the acquisition phase, the code tracking phase starts with the fine alignment followed by the process of maintaining synchronization of the two signals. Due to the mutually orthogonal properties of some chaotic signals [22-25] the synchronization techniques of the traditional code division multiple access (CDMA) spread spectrum communication systems have a potential to be applied to the chaotic communication systems [24,26-36]. In most cases, when evaluating the sequence synchronization of the chaos based DS-CDMA systems the code acquisition is analysed only [24,26,27,29-35]. In [26,27] Setti et. al. investigate the acquisition procedure of a chaos based DS-CDMA system and briefly discuss the possible general model for the tracking operation. The tracking model of [26,27] is essentially based on a continuance of the acquisition procedure and it does not deal with the synchronization within the chip level which is required for the fine alignment between the received and the despreading sequences. It has been suggested in [26,27] that the Bernoulli and the Tailed Shift chaotic maps may in fact yield somewhat better performance during the code acquisition phase than the classical spread spectrum sequences such as *m* (PRBS) and Gold sequences. Furthermore, in [29], the authors use the Gaussian approximation for the self-interference term to show its effect on the acquisition performance. In [30] the moments approach is used to obtain a more accurate characterization of the self-interference term. Throughout [26,27,29,30] the noise has not been included in the system in order to study the effects of the interuser interferences on the acquisition performance. However in any real communication system noise is an inevitable part of operation and is thus included here in the study of the system performance. In [32,34] the authors look at the acquisition performance of Markov chaotic sequences

when used as the spreading codes within a DS-CDMA system. It is shown in [34] that the bit error rate and code acquisition performance of the Markov based DS-CDMA systems are superior to that of the independent and identically distributed (i.i.d.) based DS-CDMA systems. In [33], the distribution of self-interferences of an incompletely synchronized, (to within a fraction of a chip), Markov based DS-CDMA system is considered. It is shown that Markov codes show promise in this regard; however, no tracking circuit is proposed to completely synchronize the system. In addition, in [36], the author investigates the generation of spread spectrum chaotic sequences via Markov chains whose autocorrelation values always take real numbers. Due to the reduction in the number of unknown parameters, it is argued that the synchronization of such sequences is simpler than the synchronization of Markov chain sequences whose autocorrelation values take complex values. A more recent advance in the synchronization of chaotic CDMA systems combines the interior penalty method of optimization theory and chaotic synchronization theory to achieve detection at the receiver [37].

Studies into the optimal spreading sequences for DS-CDMA systems have been conducted in [24-27,32-35,38-45], and it has been found that in many instances chaotic time series are the optimal spreading sequences [24,26,27,34,35,38-45]. For instance, in [24,43], it has been shown that quantized chaotic spreading codes can be generated for any number of users and exhibit generally better performance than the classical, *m* and Gold, sequences. Alternatively, in [38] an estimation technique for the minimum achievable interference in DS-CDMA systems is proposed and used in [42] to find the autocorrelation function resulting in the minimum possible interference-to-signal ratio. Furthermore, it has been shown in [39-41], that in terms of capacity, where capacity is defined as the maximum rate at which information can be transmitted without error, the suitably chosen chaotic spreading sequences outperform the classical spreading sequences. Quantization of chaotic time series is recognised as one of the possible practical problems in the generation of the spreading sequences as it may affect the security and the system performance [23,44]. In [44] a practical implementation of the optimal real-valued Chebyshev chaotic spreading sequence is investigated in terms of the finite precision representation. It is shown that the bit error rate performance of a 31 bit precision machine matches that of a double precision machine. Therefore, a 31 bit precision machine is sufficient for the practical implementation of some chaotic sequences within DS-CDMA systems. The digital signal processors (DSPs) are the devices commonly used to investigate the implementation of chaotic communication systems [46-51]. Under the assumption of perfect synchronization the chaos based DS-CDMA system of [22] has been investigated in [51] on a 32 bit precision TigerSHARC DSP chip by Analog Devices. It has been shown that the quantization of the logistic map at this precision does not affect the bit error rate performance of the system.

Broadly speaking, chaotic communication systems can be classified into those that require sequence synchronization at the receiver, the coherent systems, and those that do not, the non-coherent systems. However, in many cases when studying coherent chaotic communication systems perfect synchronization between the spreading code at the transmitter and its replica, or copy, at the receiver is

assumed [52,22,23,51,53,54-56]. Such analyses only provide the benchmark performance of the system [53]. In [57] it was reported that the PC chaotic synchronization method of [3] is insufficiently robust for the implementation within the practical chaotic communication systems. In order for the CDMA multi-user chaotic communication systems to become of practical and not just academic interest robust synchronization techniques must be developed [57,53,54,58-61,62]. The motivation for the work of this chapter was to develop a robust and secure synchronization technique for the multi-user DS-CDMA chaotic communication system of [22] using the traditional techniques of sequence synchronization within the CDMA systems.

In this chapter, the code acquisition and tracking phase of the sequence synchronization system are implemented within the multi-user DS-CDMA chaotic communication scheme of Parlitz and Ergezinger [22]. The proposed systems are evaluated in the presence of additive white Gaussian noise (AWGN) and the interuser interferences as well as in the Rayleigh fading channel. The synchronization systems utilize a pseudo random binary sequence (PRBS) pilot signal and a periodic and non-periodic logistic map chaotic pilot signals within the multi-user chaotic communication system to achieve and maintain synchronization. Under the assumption of perfect synchronization the benchmark performance of the system of [22] has already been investigated in the presence of noise and interuser interferences in [22,55] as well as in the Rayleigh fading channel of [56], demonstrating the potentially robust nature of this system. Also under the assumption of perfect synchronization the security of the system of [22] has been evaluated in [62], demonstrating some weaknesses of the system to the return map and correlation function attacks.

Section 7.1, presents the entire system, consisting of the system in [22] and the sequence synchronization system proposed. The interconnections of the two systems are explained. In section 7.2, the code acquisition circuit is presented and analysed in terms of the probability of false alarm and the probability of detection. The ability to achieve initial synchronization in the presence of noise and interuser interferences is demonstrated. The mathematical model of the code tracking loop for a PRBS pilot based CBDS-CDMA system is presented in section 7.3. The control law used for the generation of the time offset estimates is then derived. This is followed by the investigation into the overall noise performance of the system in terms of the bit error rate for different numbers of chaotic users in an AWGN channel. Furthermore, the performance of the system proposed is compared to the initial condition modulation (ICM) scheme of chapter 6 [63] based on the principles of PC synchronization. Finally, the performance of the system is evaluated in the Rayleigh fading channel with AWGN and interuser interferences present. In section 7.4, the periodic and non-periodic chaotic pilot based CBDS-CDMA systems are proposed and evaluated in AWGN and Rayleigh fading channel. The mathematical model of the code tracking loop is presented for both chaotic pilot based CBDS-CDMA systems. The control laws used for the generation of the time offset estimates are derived. This is followed by the investigation into the overall noise and fading performance of the systems in terms of the bit error rate for different numbers of chaotic users and comparison of the results to those of PRBS pilot based CBDS-CDMA system.

7.1 The Chaotic Communication System with the Synchronization Unit

Figure 7.1 shows the 'DS-CDMA communication scheme based on the chaotic dynamics' introduced in [22], with the synchronization unit proposed here. Thus, the system of Figure 7.1 does not assume perfect sequence synchronization. The mathematical model of the chaos based DS-CDMA communication system of Figure 7.1 with perfect sequence synchronization assumed has been presented in chapter 2 [52].

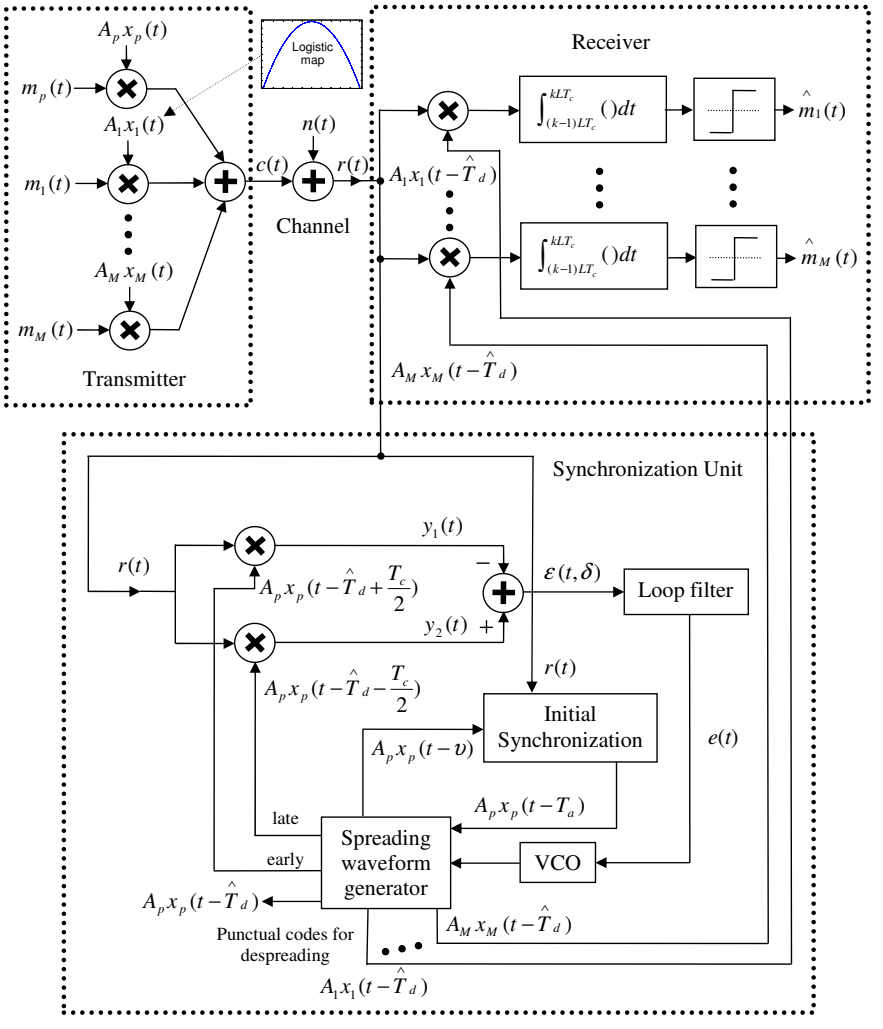


Fig. 7.1 DS-CDMA chaotic communication system with the synchronization unit

In Figure 7.1, $x(t)$ denotes the chaotic spreading signals which are multiplied by the binary message signals $m(t)$. The products are then summed up to produce the signal $c(t)$ which is transmitted through the channel. $x_p(t)$ denotes the pseudo random binary sequence (PRBS) which acts as the periodic pilot signal used for synchronization purposes. Provided that the power of the noise in the system is comparatively low to the power of the signal, the synchronization unit uses the received signal $r(t)$ to generate the despreading codes which are punctually synchronized to the spreading codes at the transmitter. In order for the spreading waveform generator at the receiver to produce punctual despreading codes the initial conditions of the spreading codes of each of the M users at the transmitter must be available to it. The received signal $r(t)$ is then correlated with the punctual despreading codes. For sufficiently low noise levels in the system the correlation value produced at the output of each correlator is positive if the bit 1 is transmitted and negative if the bit 0 is transmitted [22]. Note that the correlator receiver of Figure 7.1 has been represented by integrals, rather than sums as in [22], in order to conform to the continuous time domain which is used in this chapter.

The synchronization unit of Figure 7.1 is composed of two interconnected units, namely the acquisition or the initial synchronization unit and the tracking unit which includes everything but the initial synchronization unit. For the communication between the transmitter and the receiver to take place the synchronization between the chaotic spreading codes $x(t)$ at the transmitter and their replicas at the receiver must be established and maintained. The synchronization is established through the acquisition or the initial synchronization unit [11,10,13,14] by acquiring the time offset of the received signal $r(t)$ to within a certain fraction of the chip period T_c. Once the synchronization has been established it is continuously maintained by the tracking unit [11,12,10] by ensuring that the incoming time offset is matched by the estimated time offset $\hat{T}_d$, as explained in section 7.3. Synchronization using the PRBS signal as the pilot signal within the chaotic communication system is possible due to the fact that the PRBS signal and the chaotic signal used, the logistic map [22] shown in phase-space [62] in Figure 7.1, are highly orthogonal as is demonstrated in Figure 7.2a by the cross-correlation function with no dominant peaks. The autocorrelation function of the logistic map time series is presented in Figure 2.13b, repeated below as Figure 7.2b, showing the dominant peak. The logistic map time series has been generated using the equation 2.1.5, repeated below for convenience as equation 7.1.1 [22]:

$$X_{n+1} = 1 - 2X_n^2 \tag{7.1.1}$$

The length of the logistic map time series used to produce Figures 7.2a and 7.2b is equal to 511 points (chips). The dynamic range of the logistic map time series is confined to ±1 [22]. In Figures 7.2a and 7.2b t denotes the time delay. Also, note that the correlation functions have been normalized to the peak of the autocorrelation function.

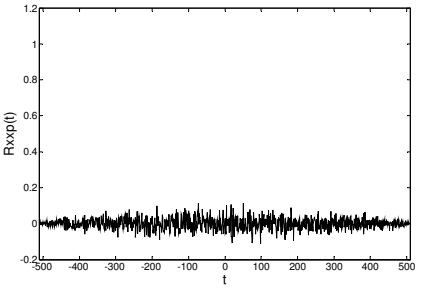


Fig. 7.2a Cross-correlation of logistic map and PRBS time series

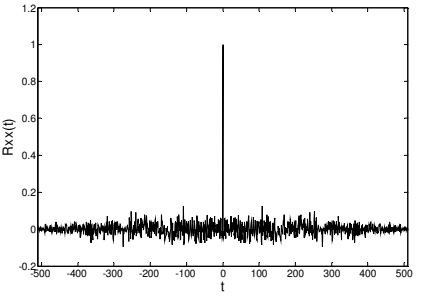


Fig. 7.2b Autocorrelation of logistic map time series

7.2 The Code Acquisition

In this section, the first phase of the sequence synchronization process known as the code acquisition or the initial synchronization phase is presented [15,64].

7.2.1 Theoretical Model of the System

In Figure 7.3, the circuit diagram of the code acquisition circuit is shown [15]. The following mathematical analysis of the acquisition circuit is performed at band-pass, as is the common practice when dealing with this kind of circuitry [65,10,11].

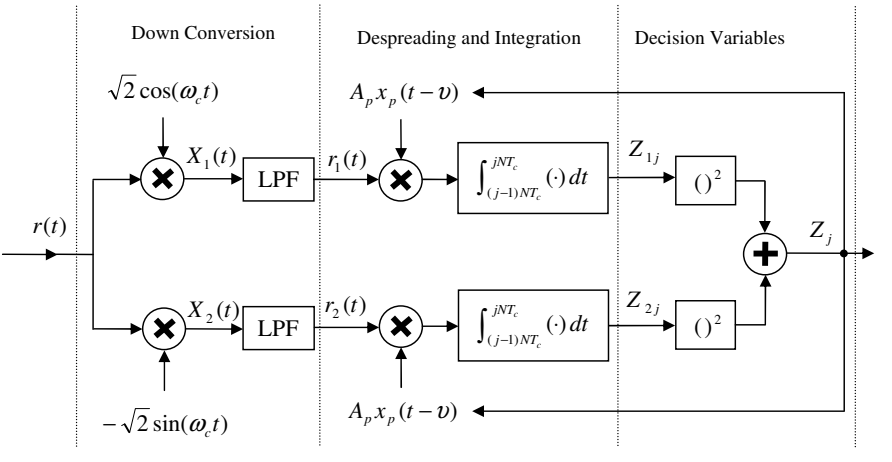


Fig. 7.3 Code acquisition circuit

The physical description of the circuit is as follows. The input signal $r(t)$, is composed of the M user signals combined together and up converted, as well as the noise component introduced by the channel. Among the user signals is the pilot signal which is used for the sequence synchronization purposes of the communication system. The $r_1(t)$, $r_2(t)$ pair are the baseband signals produced by down converting the signal $r(t)$. The $x_p(t-\upsilon)$ is the copy of the pilot signal with some arbitrary time offset υ. The time offset υ can be represented as $\upsilon = j\Delta T_c$, where j is an integer and Δ any value between zero and one depending on the search strategy employed [66]. The $x_p(t-\upsilon)$ copy of the pilot signal is used to despread the $r_1(t)$, $r_2(t)$ pair. The despread signals are then integrated over the period of the pilot signal $x_p(t)$ equal to NT_c units of time. The decision variables Z_{1j} and Z_{2j} are squared and summed to produce the decision variable Z_j, which is used to decide whether the time offset has or has not been acquired by comparing it to the predetermined threshold. If the time offset has not been acquired the despreading pilot signal is shifted by further ΔT_c and the new decision variable produced. The procedure is repeated until the approximate time offset, (to within $\pm \Delta T_c$), is determined. The reason of having two branches is to eliminate the influence of the carrier component from the decision making [15]. It is assumed that the clock and carrier synchronization between the transmitter and the receiver has already been achieved and is maintained throughout the acquisition procedure, so that the system has the knowledge of where the chips start and end. As discussed in chapter 1, this assumption is used in most cases when evaluating the performance of binary modulation techniques [67,63]. In the bandpass case the received signal of Figure 7.1, $r(t)$, is assumed to be of the up converted form given by equation 7.2.1:

$$\begin{aligned} r(t) &= \sum_{i=p}^{M} A_i\, x_i(t-\eta)\, m_i(t-\eta)\sqrt{2}\cos(\omega_c t+\varphi) + n(t) \\ &= \sum_{i=p}^{M} A_i\, x_i(t-\eta)\, m_i(t-\eta)\sqrt{2}\big(\cos(\omega_c t)\cos(\varphi) - \sin(\omega_c t)\sin(\varphi)\big) \\ &\quad + \sqrt{2}n_I(t)\cos(\omega_c t) - \sqrt{2}n_Q(t)\sin(\omega_c t) \end{aligned} \tag{7.2.1}$$

where: $n(t) = \sqrt{2}n_I(t)\cos(\omega_c t) - \sqrt{2}n_Q(t)\sin(\omega_c t)$

In equation 7.2.1, A_i represents the amplitude of the transmitted signals, x_i the spreading waveforms and m_i the information signals, with η denoting some arbitrary time offset of the received signal. The limit of the sum M denotes the M

users of the system, with p corresponding to an extra user ($p = 0$), that is, the pilot signal, as illustrated in Figure 7.3. The terms $n_I(t)$ and $n_Q(t)$ denote the in phase and quadrature components of the noise signal $n(t)$. The angular frequency of the carrier is denoted by ω_c and its phase by φ. The signal X_1 of Figure 7.3 is expressed by equation 7.2.2:

$$\begin{aligned} X_1(t) &= r(t)\cdot\sqrt{2}\cos(\omega_c t) \\ &= \sum_{i=p}^{M} A_i\, x_i(t-\eta)\, m_i(t-\eta) 2\left(\cos^2(\omega_c t)\cos(\varphi) - \sin(\omega_c t)\cos(\omega_c t)\sin(\varphi)\right) \\ &+ 2n_I(t)\cos^2(\omega_c t) - 2n_Q(t)\sin(\omega_c t)\cos(\omega_c t) \end{aligned} \tag{7.2.2}$$

Rearranging equation 7.2.2, equation 7.2.3 is obtained:

$$\begin{aligned} X_1(t) = \sum_{i=p}^{M} A_i\, x_i(t-\eta)\, m_i(t-\eta)\left(\cos(\varphi) + \cos(2\omega_c t)\cos(\varphi) - \sin(2\omega_c t)\sin(\varphi)\right) \\ + n_I(t) + n_I(t)\cos(2\omega_c t) - n_Q(t)\sin(2\omega_c t) \end{aligned} \tag{7.2.3}$$

Upon low pass filtering signal X_1, signal $r_1(t)$ is obtained:

$$r_1(t) = \left[X_1(t)\right]_{LPF} = \sum_{i=p}^{M} A_i\, x_i(t-\eta)\, m_i(t-\eta)\cos(\varphi) + n_I(t) \tag{7.2.4}$$

$$r_1(t) = A_p\, x_p(t-\eta)\, m_p(t-\eta)\cos(\varphi) + \sum_{\substack{i=1 \\ i\neq p}}^{M} A_i\, x_i(t-\eta)\, m_i(t-\eta)\cos(\varphi) + n_I(t) \tag{7.2.5}$$

In equation 7.2.5, the first term is the wanted signal, the second terms are the interferences of other users and the third term is the noise component. Keeping in mind that it is so chosen that $m_p(t) = 1$ for all time [10,15], equation 7.2.5 is rewritten as equation 7.2.6:

$$r_1(t) = A_p x_p(t-\eta)\cos(\varphi) + n_1(t) \tag{7.2.6}$$

where: $n_1(t) = \sum_{\substack{i=1 \\ i\neq p}}^{M} A_i\, x_i(t-\eta)\, m_i(t-\eta)\cos(\varphi) + n_I(t)$

In a similar manner, equation 7.2.7 is obtained:

$$r_2(t) = A_p x_p(t-\eta)\sin(\varphi) + n_2(t) \tag{7.2.7}$$

where: $n_2(t) = \sum_{\substack{i=1 \\ i\neq p}}^{M} A_i\, x_i(t-\eta)\, m_i(t-\eta)\sin(\varphi) + n_Q(t)$

The decision variable Z_{1j} is expressed by equation 7.2.8:

$$\begin{aligned} Z_{1j} &= \int_{(j-1)NT_c}^{jNT_c} r_1(t)\, x_p(t-\upsilon)\, dt \\ &= \int_{(j-1)NT_c}^{jNT_c} \left[A_p x_p(t-\eta)\cos(\varphi) + n_1(t)\right] x_p(t-\upsilon)\, dt \\ &= A_p \cos(\varphi) \int_{(j-1)NT_c}^{jNT_c} x_p(t-\eta)\; x_p(t-\upsilon)\, dt + \int_{(j-1)NT_c}^{jNT_c} n_1(t)\, x_p(t-\upsilon) dt \end{aligned} \tag{7.2.8}$$

Keeping in mind that η and υ are some arbitrary time offsets with respect to each other, let τ represent the overall time offset between the received signal and the despreading replicas at the receiver. In this case equation 7.2.8 can be rewritten as equation 7.2.9:

$$Z_{1j} = A_p \cos(\varphi) \int_{(j-1)NT_c}^{jNT_c} x_p(t)\; x_p(t-\tau)\, dt + \int_{(j-1)NT_c}^{jNT_c} n_1(t)\, x_p(t-\upsilon) dt \tag{7.2.9}$$

Note that for periodic waveforms the general expression for the autocorrelation function $R(\tau)$ is defined by equation 7.2.10 [10], where the pilot signal period $T = NT_c$:

$$R(\tau) = \frac{1}{T}\int_0^T x(t)\, y(t \pm \tau)\, dt \tag{7.2.10}$$

The decision variable Z_{1j} can then be expressed by equation 7.2.11:

$$Z_{1j} = A_p \cos(\varphi) T R_j(\tau) + N_{1j} \tag{7.2.11}$$

In equation 7.2.11 N_{1j} is expressed by equation 7.2.12:

$$N_{1j} = \int_{(j-1)NT_c}^{jNT_c} n_1(t)\, x_p(t-\upsilon) dt \tag{7.2.12}$$

In a similar manner, equation 7.2.13 is obtained:

$$Z_{2j} = A_p \sin(\varphi) TR_j(\tau) + N_{2j} \tag{7.2.13}$$

In equation 7.2.13 N_{2j} is expressed by equation 7.2.14:

$$N_{2j} = \int_{(j-1)NT_c}^{jNT_c} n_2(t)\, x_p(t-\upsilon)dt \tag{7.2.14}$$

7.2.2 Theoretical Upper Bound on the Probability of Detection

In this subsection, the theoretical expression for the upper bound probability of correctly acquiring the time offset between the received signal and the despreading replicas at the receiver is given. The statistical properties of N_1 are now briefly analysed. Expanding equation 7.2.12 and noting that the phase of the noise term $n_I(t)$ relative to the pilot signal is arbitrary, equation 7.2.15 is obtained:

$$\begin{aligned} N_{1j} &= \gamma_j + I_j \\ &= \int_{(j-1)NT_c}^{jNT_c} n_I(t)\, x_p(t-\tau)dt + \int_{(j-1)NT_c}^{jNT_c} \{\sum_{\substack{i=1 \\ i\neq p}}^{M} A_i\, x_i(t)\, m_i(t)\} \cos(\varphi)\, x_p(t-\tau)dt \end{aligned} \tag{7.2.15}$$

In general, N_1 is composed of the white Gaussian noise term (γ) and the interferences term (I). The mean value of the white Gaussian noise term γ is equal to zero, and its variance can be expressed by equation 7.2.16 [11,10]:

$$\begin{aligned} Var[\gamma] &= \int_0^{NT_c}\int_0^{NT_c} \left[\frac{1}{NT_c}\int_0^{NT_c} n_I(t)\, n_I(u)\, dt\right] x_p(t-\tau)\, x_p(u-\tau)\, dt\, du \\ &= \int_0^{NT_c}\int_0^{NT_c} \overline{n_I(t)\, n_I(u)}\; x_p(t-\tau)\, x_p(u-\tau)\, dt\, du \\ &= \int_0^{NT_c}\int_0^{NT_c} \frac{1}{2} N_o B\, \delta(t-u)\, x_p(t-\tau)\, x_p(u-\tau)\, dt\, du \\ &= \frac{1}{2} N_o B \int_0^{NT_c} x_p^2(t-\tau)\, dt = \frac{1}{2} N_o B N T_c \end{aligned} \tag{7.2.16}$$

In equation 7.2.16 B denotes the bandwidth of the intermediate frequency (IF) filter (not explicitly shown), so that the noise component is the baseband white Gaussian noise process with two-sided power spectral densities $N_o/2$ over the frequency range $|f| < B/2$ [11]. Therefore γ is a Gaussian random variable of zero mean and $N_o BNT_c/2$ variance, and can be represented by equation 7.2.17:

$$\gamma = G(0, \frac{1}{2} N_o BNT_c) \tag{7.2.17}$$

The interference term, I, is expected to always be close to zero due to the orthogonal relationship among the chaotic interferences and the PRBS pilot signal, as demonstrated in Figure 7.2a, with certain variance not equal to zero. With this in mind, equation 7.2.18 is assumed to hold [10]:

$$I = \int_{(j-1)NT_c}^{jNT_c} \{\sum_{\substack{i=1 \\ i \neq p}}^{M} A_i \, x_i(t) \, m_i(t)\} \cos(\varphi) \, x_p(t-\tau) dt \cong 0 \tag{7.2.18}$$

Therefore, N_1 is the Gaussian random variable of zero mean and variance $N_o' BNT_c/2$, where N_o' denotes the effective noise power spectral density that is due to both the receiver noise and the interferences [10,15]. Variance $N_o' BNT_c/2$ thus includes both the variance of γ and I terms. Overall equation 7.2.19 holds:

$$N_1 = G(0, \frac{1}{2} N_o' BNT_c) \tag{7.2.19}$$

Now the general expressions for the decision variables Z_{1j} and Z_{2j} can be re-expressed in the form of equations 7.2.20 and 7.2.21:

$$\begin{aligned} Z_1 &= A_p \cos(\varphi) TR(\tau) + G(0, \frac{1}{2} N_o' BNT_c) \\ &= G(A_p \cos(\varphi) TR(\tau), \frac{1}{2} N_o' BNT_c) \\ &= \sqrt{\frac{1}{2} N_o' BNT_c} \cdot G\left(\frac{A_p}{\sqrt{\frac{1}{2} N_o' BNT_c}} \cos(\varphi) TR(\tau), 1 \right) \end{aligned} \tag{7.2.20}$$

$$\begin{aligned} Z_2 &= A_p \sin(\varphi) TR(\tau) + G(0, \frac{1}{2} N_o' BNT_c) \\ &= G(A_p \sin(\varphi) TR(\tau), \frac{1}{2} N_o' BNT_c) \\ &= \sqrt{\frac{1}{2} N_o' BNT_c} \cdot G\left(\frac{A_p}{\sqrt{\frac{1}{2} N_o' BNT_c}} \sin(\varphi) TR(\tau), 1 \right) \end{aligned} \tag{7.2.21}$$

Keeping in mind that at bandpass $A_p = \sqrt{2E_c / T_c}$, where E_c denotes the energy of a single PRBS chip, equations 7.2.20 and 7.2.21 are rewritten as equations 7.2.22 and 7.2.23, respectively:

$$Z_1 = \sqrt{\frac{1}{2} N_o' BNT_c} \cdot G\left(2\sqrt{\frac{NE_c}{N_o' B}} \cos(\varphi) R(\tau), 1 \right) \tag{7.2.22}$$

$$Z_2 = \sqrt{\frac{1}{2} N_o' BNT_c} \cdot G\left(2\sqrt{\frac{NE_c}{N_o' B}} \sin(\varphi) R(\tau), 1 \right) \tag{7.2.23}$$

Therefore, the decision variable $Z_j = Z_{1j}^2 + Z_{2j}^2$ is $\frac{1}{2} N_o' BNT_c$ times a non-central chi-squared random variable with two degrees of freedom, and the non-centrality parameter is given by equation 7.2.24 [10]:

$$\begin{aligned} \lambda &= \left[2\sqrt{\frac{NE_c}{N_o' B}} \cos(\varphi) R(\tau) \right]^2 + \left[2\sqrt{\frac{NE_c}{N_o' B}} \sin(\varphi) R(\tau) \right]^2 \\ &= \left[2\sqrt{\frac{NE_c}{N_o' B}} R(\tau) \right]^2 = 4NR^2(\tau) \frac{E_c}{N_o' B} \end{aligned} \tag{7.2.24}$$

The probability density function (PDF) for Z_j is given by equation 7.2.25 [10,11], where $\sigma^2 = \frac{1}{2} N_o' BNT_c$:

$$p_{z_j}(z) = \begin{cases} \frac{1}{2\sigma^2} e^{-\frac{1}{2}\left(\lambda + \frac{z}{\sigma^2}\right)} I_o\left(\sqrt{\frac{\lambda z}{\sigma^2}}\right) & z \geq 0 \\ 0 & otherwise \end{cases} \tag{7.2.25}$$

where I_o is the modified Bessel function of the first kind of order zero.

The initial synchronization test can be viewed as a hypothesis test. Let H_1 be the hypothesis that the incoming and local signals are aligned to within one chip length, (by choosing the search strategy with $\Delta = 1$), and let H_0 be the hypothesis that they are not. These hypotheses are represented by equations 7.2.26 and 7.2.27 [10]:

$$H_1: \quad |\tau| \leq T_c \quad \rightarrow \quad R(\tau) > 0,\ N_o^{'} \approx N_o \tag{7.2.26}$$

$$H_0: \quad |\tau| > T_c \quad \rightarrow \quad R(\tau) \approx 0,\ N_o^{'} > N_o \tag{7.2.27}$$

The PDF, conditioned on the hypotheses above, takes the form of equations 7.2.28 and 7.2.29:

$$p_{z_j}(z \mid H_0) = \frac{1}{N_o^{'} BNT_c} e^{-\frac{z}{N_o^{'} BNT_c}} \tag{7.2.28}$$

$$p_{z_j}(z \mid H_1) = \frac{1}{N_o BNT_c} e^{-\frac{1}{2}\left(\lambda + \frac{z}{\frac{1}{2} N_o BNT_c}\right)} I_o\left(\sqrt{\frac{\lambda z}{\frac{1}{2} N_o BNT_c}}\right) \tag{7.2.29}$$

From equations 7.2.28 and 7.2.29, the single run probability of detection and false alarm are now evaluated by integrating the PDF. The false alarm threshold is denoted by β_T. Provided that this threshold is equalled or exceeded by the decision variable Z_j, the system assumes that the time offset has been acquired and switches to the tracking circuit which maintains the acquired time offset. If the noise in the system is too high, or the sequence period over which the integration is performed is too short, the threshold maybe exceeded by the decision variable, when in fact it should not be so. In such a case the time offset is falsely acquired and the false alarm occurs. The threshold β_T, for a particular noise level and sequence length, can be determined from the false alarm probability. The false alarm probability is given by equation 7.2.30:

$$
\begin{aligned}
P_F(j=1) &= P_r(Z_j > \beta_T \mid H_0) \\
&= \int_{\beta_T}^{\infty} p_{z_j}(z \mid H_0)\, dz \\
&= \int_{\beta_T}^{\infty} \frac{1}{N_o' BNT_c} e^{-\frac{z}{N_o' BNT_c}}\, dz \\
&= \left[-e^{-\frac{z}{N_o' BNT_c}} \right]_{\beta_T}^{\infty} = e^{-\frac{\beta_T}{N_o' BNT_c}}
\end{aligned}
\tag{7.2.30}
$$

From equation 7.2.30 expression for the threshold β_T, for a certain probability of false alarm, can be expressed as shown by equation 7.2.31:

$$
\beta_T = -N_o' BNT_c \ln(P_F(j=1)) \tag{7.2.31}
$$

The probability of detection is given by equation 7.2.32:

$$
\begin{aligned}
P_D(j=1) &= P_r(Z_j > \beta_T \mid H_1) \\
&= \int_{\beta_T}^{\infty} p_{z_j}(z \mid H_1)\, dz \\
&= \int_{\beta_T}^{\infty} \frac{1}{N_o BNT_c} e^{-\frac{1}{2}\left(\lambda + \frac{z}{\frac{1}{2} N_o BNT_c}\right)} I_o\left(\sqrt{\frac{\lambda z}{\frac{1}{2} N_o BNT_c}}\right) dz
\end{aligned}
\tag{7.2.32}
$$

Consider the Marcum's Q-function given by the integral of equation 7.2.33:

$$
Q(a,\beta) = \Pr\{r > \beta\} = \int_{\beta}^{\infty} z\, e^{-(a^2+z^2)/2} I_o(az)\, dz \tag{7.2.33}
$$

Equation 7.2.32 is now transformed into the form of the Marcum's Q-function of equation 7.2.33. Let $z = \frac{1}{2} N_o BNT_c x^2$, so that $dz = N_o BNT_c x\, dx$. Substituting z and dz into equation 7.2.32, equation 7.2.34 is obtained:

$$
P_D(j=1) = \int_{\sqrt{2\beta_T/(N_o BNT_c)}}^{\infty} x\, e^{-\frac{1}{2}\left(\lambda + x^2\right)} I_o\left(\sqrt{\lambda}\, x\right) dx \tag{7.2.34}
$$

Equation 7.2.34 is in the form of equation 7.2.33 and is now compactly expressed as shown in equation 7.2.35:

$$P_D(j=1) = Q\left(\sqrt{\lambda},\ \sqrt{2\beta_T / (N_o BNT_c)}\right) \tag{7.2.35}$$

Substituting equations 7.2.24 and 7.2.31 into equation 7.2.35, equation 7.2.36 is obtained:

$$P_D(j=1) = Q\left(2\sqrt{\frac{NE_c}{N_o' B}}R(\tau),\ \sqrt{-2\frac{N_o'}{N_o}\ln(P_F(j=1))}\right) \tag{7.2.36}$$

where $R(\tau) \le R(0) = 1$.

The expression for the upper bound on detection probability is then obtained by assuming that $N_o' \approx N_o$ and $R(\tau) \approx R(0) = 1$ [10], and is expressed by equation 7.2.37:

$$P_D(j=1) \le Q\left(2\sqrt{\frac{NE_c}{N_o B}},\ \sqrt{-2\ln(P_F(j=1))}\right) \tag{7.2.37}$$

In summary, in equation 7.2.37 P_F stands for the probability of false alarm given by $P_F(j=1) = e^{-\frac{\beta_T}{N_o' BNT_c}}$, where β_T denotes the false alarm threshold level.

Using the Gaussian Q-function [10] to approximate Marcum's Q-function, equation 7.2.37 can be accurately estimated by equation 7.2.38:

$$P_D(j=1) \le Q_\gamma\left(\sqrt{-2\ln(P_F(j=1))} - 2\sqrt{\frac{NE_c}{N_o B}}\right) \tag{7.2.38}$$

where Q_γ denotes the Gaussian Q-function.

7.2.3 Empirical Evaluation of the Probability of False Alarm and the Probability of Detection

A way of obtaining the empirical expressions for the probability of false alarm and the probability of detection is now briefly presented [15]. Assume that at a certain level of noise in the system the output of the acquisition circuit is as given in Figure 7.4.

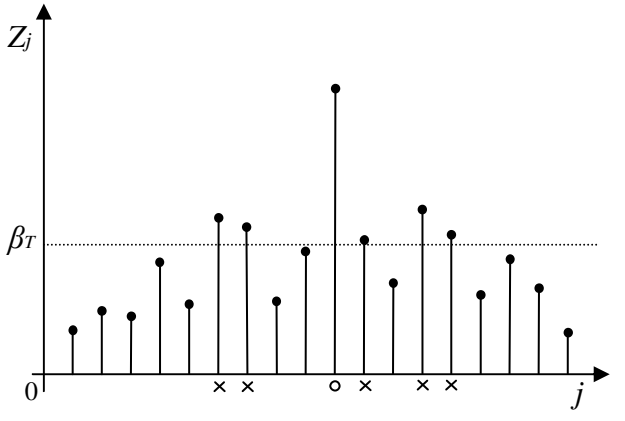


Fig. 7.4 Output Z_j of the code acquisition circuit of Figure 7.3

Then at this certain level of noise the decision variable Z_j will exceed the threshold value six times and in any of those times synchronization will be declared. However, in only one of those six times (denoted by a circle in Figure 7.4) the incoming signal $r(t)$ and the basis function $x_p(t-\upsilon)$ will actually be synchronized, while in the other five times (denoted by the crosses) the two will not be synchronized. Therefore, the circle in Figure 7.4 corresponds to the case when the two are indeed synchronized while crosses correspond to the cases when they are not synchronized but the threshold is exceeded. The probability of one event occurring while another has in fact occurred is termed conditional probability and is represented by equation 7.2.39:

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)} \tag{7.2.39}$$

Equation 7.2.39 states that the probability of event *A* given that event *B* has occurred is equal to the probability of both *A* and *B* occurring divided by the probability of event *B*. The equation 7.2.30 which represents the probability of false alarm can therefore also be written as equation 7.2.40:

$$P_F(j=1) = P(A/B) = P_r(Z_j > \beta_T \mid H_0) = \frac{P_r(Z_j > \beta_T \cap H_0)}{P_r(H_0)} \tag{7.2.40}$$

The expression for the numerator term $P_r(Z_j > \beta_T \cap H_0)$ of equation 7.2.40 is given by equation 7.2.41:

$$P_r(Z_j > \beta_T \cap H_0) = \lim_{S\to\infty}\left(\frac{k}{S}\right) \tag{7.2.41}$$

In equation 7.2.41 k represents the number of crosses in Figure 7.4, that is, the number of decision variables Z_j exceeding the threshold value β_T when in fact they should not. S represents the total number of decision variables Z_j.

The expression for the denominator term $P_r(H_0)$ of equation 7.2.40 is given by equation 7.2.42:

$$P_r(H_0) = \lim_{S\to\infty}\left(\frac{S-1}{S}\right) \tag{7.2.42}$$

Substituting equations 7.2.41 and 7.2.42 into equation 7.2.40, equation 7.2.43 is obtained:

$$P_F(j=1) = \lim_{S\to\infty}\left(\frac{k}{S-1}\right) \tag{7.2.43}$$

Saying that S is unlimited implies that the synchronization time is unlimited. In order to obtain an accurate result, when S is limited, the experiment must be run a number of times, that is, a large number of synchronization bits (periods) must be processed. Processing a large number, m, of bits, while keeping S limited permits an accurate estimation of the probabilities, for a limited size of the synchronization bit. Running the experiment m number of times leads to the expression for the probability of false alarm given by equation 7.2.44:

$$P_F(j=1) = \lim_{m\to\infty}\sum_{n=1}^{m}\left(\frac{k_n}{m(S_n-1)}\right) \tag{7.2.44}$$

Also equation 7.2.32 which represents the probability of detection can be written as equation 7.2.45:

$$P_D(j=1) = P_r(Z_j > \beta_T \mid H_1) = \frac{P_r(Z_j > \beta_T \cap H_1)}{P_r(H_1)} \tag{7.2.45}$$

The expression for the numerator term $P_r(Z_j > \beta_T \cap H_1)$ of equation 7.2.45 has only two outcomes, depending on whether the threshold β_T has been exceeded or not. These two outcomes are given by equation 7.2.46:

$$\begin{aligned} P_r(Z_j > \beta_T \cap H_1) &= \lim_{S\to\infty}\left(\frac{1}{S}\right) = \frac{1}{S} \quad Z_j > \beta_T \\ P_r(Z_j > \beta_T \cap H_1) &= \lim_{S\to\infty}\left(\frac{0}{S}\right) = 0 \quad \textit{otherwise} \end{aligned} \tag{7.2.46}$$

The expression for the denominator term $P_r(H_1)$ of equation 7.2.45 is given by equation 7.2.47:

$$P_r(H_1) = \lim_{S\to\infty}\left(\frac{1}{S}\right) \tag{7.2.47}$$

Substituting equations 7.2.46 and 7.2.47 into equation 7.2.45, equation 7.2.48 is obtained:

$$P_D(j=1) = \frac{P_r(Z_j > \beta_T \cap H_1)}{P_r(H_1)} = \frac{\lim_{S\to\infty}\left(\frac{1}{S}\right)}{\lim_{S\to\infty}\left(\frac{1}{S}\right)} = 1 \quad Z_j > \beta_T$$

$$P_D(j=1) = \frac{P_r(Z_j > \beta_T \cap H_1)}{P_r(H_1)} = \frac{0}{\lim_{S\to\infty}\left(\frac{1}{S}\right)} = 0 \quad otherwise \tag{7.2.48}$$

From equation 7.2.48 it is clear that to obtain the expression for the probability of detection one must run the experiment over more than a single synchronization bit, regardless of the length of the synchronization bit, that is, the synchronization bit period. Running the experiment *m* number of times leads to the expression for the probability of detection given by equation 7.2.49:

$$P_D(j=1) = \lim_{m\to\infty}\sum_{n=1}^{m}\left(\frac{P_D(j=1)_n}{m}\right) \tag{7.2.49}$$

where $P_D(j=1)_n \in \{0,1\}$.

7.2.4 Theoretical and Numerical Simulation Results

The theoretical and empirical performance of the code acquisition circuit of Figure 7.3 is now examined in terms of the probability of detection and the probability of false alarm. In particular, the system performance is examined when the ratio of the chip energy to the noise power spectral density, E_c / N_o, is equal to -15 dB [10], and the chaotic interferences and the period of the synchronizing pilot signal vary. It has been found that the theoretical upper bound on the probability of detection (equation 7.2.37) matches the empirical upper bound on the probability of

detection when $B = 12/7$. Note that the empirical upper bound on the probability of detection is obtained by simply eliminating chaotic users from the system and processing only the pilot signal. Figure 7.5a, shows the theoretical upper bound on the probability of detection, (equation 7.2.37), when $E_c / N_o = -15\,\mathrm{dB}$, $N = 255$ and $B = 12/7$, followed by the corresponding no interference empirical curve. The subsequent empirical curves associated with the increasing number of users in the system, demonstrate the expected degradation in the system performance with the increasing level of interference. For instance, one can see from Figure 7.5a that an integration time equivalent to 255 chips is required to achieve a detection probability of approximately 94 % while maintaining a false alarm probability of 5 % when $E_c / N_o = -15\,\mathrm{dB}$ and the total interference is equivalent to an interference encountered within a 5 user system. On the other hand for a 20 user system, when $E_c / N_o = -15\,\mathrm{dB}$ and $N = 255$, one is only able to achieve a detection probability of approximately 75.5 % while maintaining the same false alarm probability of 5 %.

By increasing the length of the pilot signal from $N = 255$ to $N = 383$ chips and $N = 511$ chips, while keeping E_c / N_o, B and the interferences unaltered, the results shown by Figures 7.5b and 7.5c are obtained, respectively. From Figures 7.5b and 7.5c one can see that by increasing the integration time of the integrators of Figure 7.3 the effect of the noise and the interferences is reduced resulting in a higher probability of detection. However, increasing the integration time inevitably increases the overall initial synchronization time [15]. Therefore, there is a trade off between the time it takes to search the possible pilot time offsets and the reliability of acquiring the correct time offset. Thus, the choice of the particular integration time will depend on the nature of the application. Note that although the cross correlation between the chaotic signal generated by the logistic map and the PRBS pilot signal is very low (Figure 7.2a), the variance caused by the interuser interferences (equation 7.2.18) cannot be ignored in the analytical model, especially for the case when the number of users is large.

The acquisition performance of the chaotic maps, in particular the Bernoulli shift map [68], has been investigated in a noiseless environment in [26,27]. In order to evaluate and compare the acquisition performance of the PRBS pilot signal in a chaotic DS-CDMA system, Figures 7.5d and 7.5e show the results obtained when the logistic and Bernoulli chaotic map sequences are used as the pilot signal, respectively. It can be seen from Figure 7.5d that for $E_c / N_o = -15\,\mathrm{dB}$ and $N = 255$ the logistic map pilot signal exhibits virtually the same performance as the PRBS pilot signal for the first five users. However, when the number of users increases to 10, 15 and 20 the performance of the system with the PRBS pilot signal is better. Furthermore, it can be seen from Figure 7.5e that when the Bernoulli chaotic sequence is used as the pilot signal, in a logistic map based DS-CDMA system, the acquisition performance deteriorates by a non-negligible margin for any number of users in the system. Therefore, the acquisition performance of the logistic map based DS-CDMA system in a noisy environment is better when the

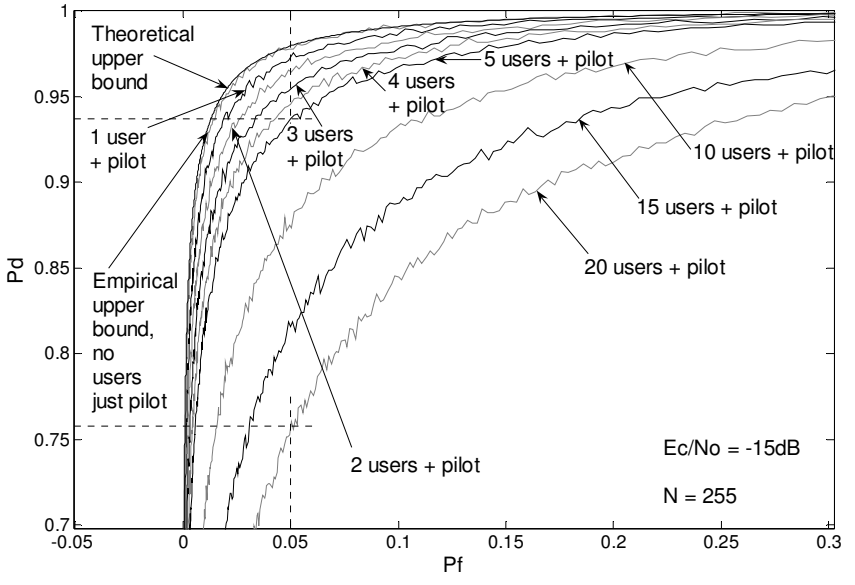


Fig. 7.5a The probability of detection vs. the probability of false alarm for $E_c / N_o = -15\,\text{dB}$, $N = 255$ and varying levels of interference when the PRBS is used as the pilot signal.

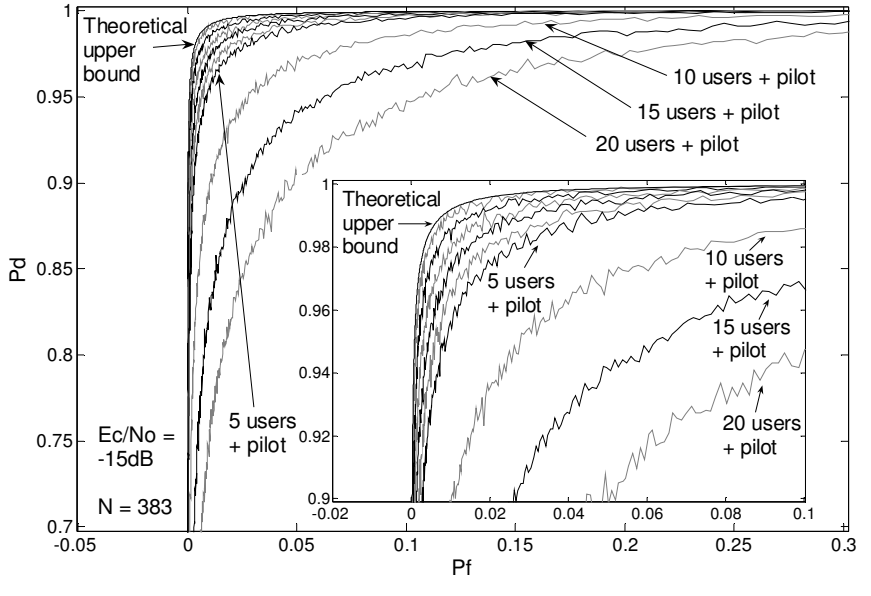


Fig. 7.5b The probability of detection vs. the probability of false alarm for $E_c / N_o = -15\,\text{dB}$, $N = 383$ and varying levels of interference when the PRBS is used as the pilot signal. The close up is shown in the lower right-hand corner.

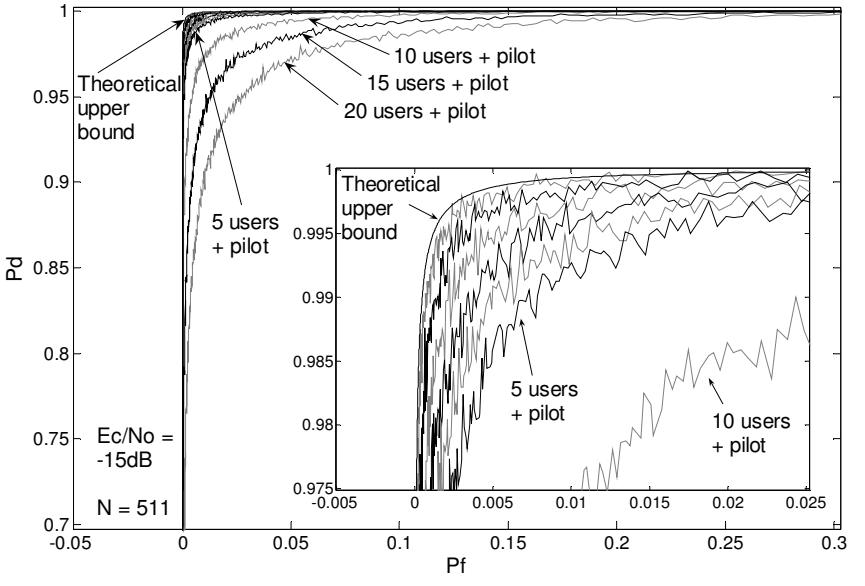


Fig. 7.5c The probability of detection vs. the probability of false alarm for $E_c / N_o = -15\,\mathrm{dB}$, $N = 511$ and varying levels of interference when the PRBS is used as the pilot signal. The close up is shown in the lower right-hand corner.

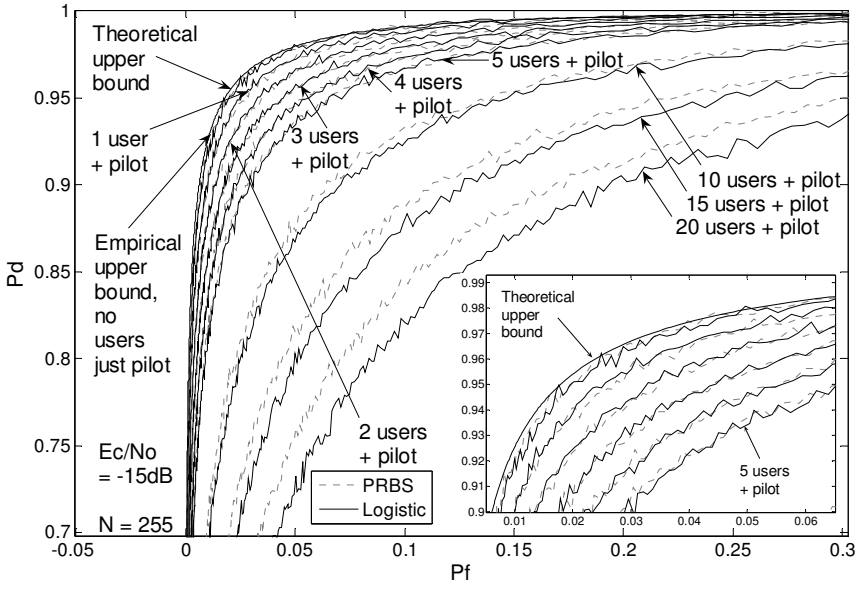


Fig. 7.5d The probability of detection vs. the probability of false alarm for $E_c / N_o = -15\,\mathrm{dB}$, $N = 255$ and varying levels of interference when the logistic map is used as the pilot signal. The close up is shown in the lower right-hand corner.

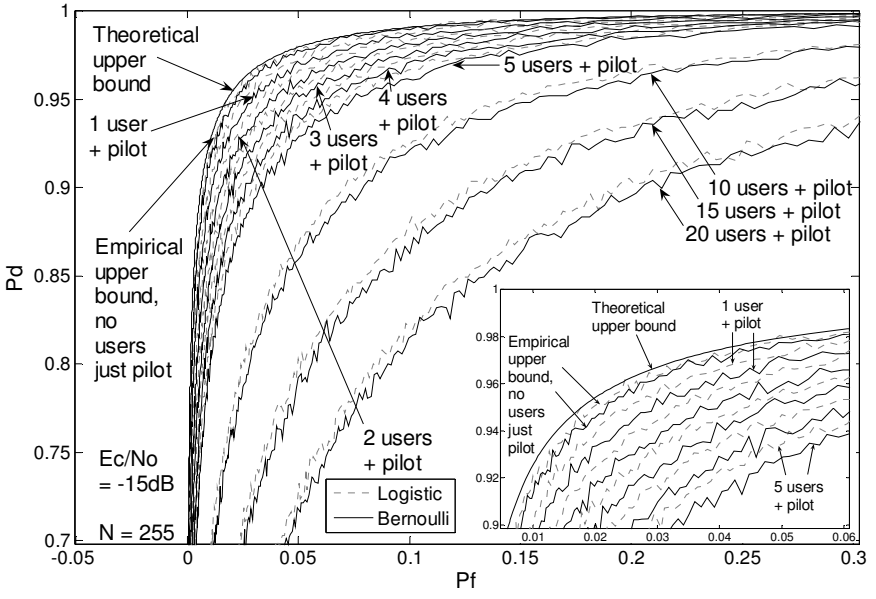


Fig. 7.5e The probability of detection vs. the probability of false alarm for $E_c / N_o = -15\,\text{dB}$, $N = 255$ and varying levels of interference when the Bernoulli map is used as the pilot signal. The close up is shown in the lower right-hand corner.

PRBS is used as the pilot signal than the logistic and Bernoulli chaotic maps. This could be due to better correlation properties.

7.3 Code Tracking with a PRBS Pilot Signal

In this section the second phase of the sequence synchronization process known as the code tracking phase is presented. Once the initial synchronization circuit of Figure 7.1, has established the correct time offset to within the pull-in region of the tracking circuit, the tracking circuit is able to take over the synchronization process. Note that the pull-in region of the tracking circuit is defined as the range of the time offset error that can be successfully corrected by it [66]. The function of the tracking circuit is to fine align the approximate time offset acquired between the received and despreading sequences and to maintain the synchronization from this point onward [11,12,10,66]. In this section, the code tracking loop with a pull-in region of half a chip length is considered. Therefore, to this end it is assumed that the search parameter Δ of the initial synchronization circuit of Figure 7.3 is equal to a ½. This ensures that the acquired time offset of Figure 7.1, T_a, is accurate to within half a chip length of the exact time offset enabling the tracking circuit to correct the inaccuracy and maintain the correct time offset. Thus, we

redefine the incoming time offset η, of section 7.2 as T_d, indicating that the acquisition phase has been finished and that the synchronization unit now has the approximate knowledge of the correct time offset to within half a chip length:

$$-Tc/2 \le (T_a - T_d) \le Tc/2 \tag{7.3.1}$$

7.3.1 Theoretical Model of the System

The tracking circuit examined here is known as the delay lock loop (DLL) [11,12,10,17] and it includes the entire synchronization unit of Figure 7.1 except for the initial synchronization unit. The early work on DLL circuits can be found in [17]. The ultimate function of the synchronization unit of Figure 7.1 is to produce the punctual codes for despreading the received signal $r(t)$. This is achieved by correlating the early and late replicas of the pilot signal by the received signal $r(t)$, subtracting their difference, and ensuring that the resulting error signal $e(t)$ is constantly forced to zero. In Figure 7.1, VCO stands for the "Voltage controlled oscillator" whose function is to increase or decrease the clock frequency depending on the current value of $e(t)$ [11]. The term δ of Figure 7.1 is defined as the normalized difference among the incoming time offset T_d of $r(t)$ signal and the tracking circuit time offset estimate $\hat{T}_d$, that is, $\delta = (T_d - \hat{T}_d)/T_c$. The loop filter of Figure 7.1 is essentially an averaging integrator, integrating over the PRBS pilot signal period:

$$e(t) = \frac{1}{NT_c} \int_{-NT_c/2}^{NT_c/2} \varepsilon(t, \delta) dt \tag{7.3.2}$$

Provided that one is already synchronized to within half a chip period, after successful acquisition, it is now shown how a punctual time offset $\hat{T}_d$, which matches the received signal time offset T_d, is obtained at discrete time instances. With a correct estimate of T_d, the receiver is able to accurately despread the received signal. The following mathematical analysis is performed at baseband and is based on the circuit of Figure 7.1. Therefore, the received baseband signal $r(t)$ can now be represented by equation 7.3.3:

$$r(t) = c(t) + n(t) = \sum_{i=p}^{M} A_i \, x_i(t - T_d) \, m_i(t - T_d) + n(t) \tag{7.3.3}$$

The received signal $r(t)$ is composed of the transmitted signal $c(t)$ and the additive white Gaussian noise component $n(t)$. The transmitted signal $c(t)$ is in turn composed of the mixture of signals of different users as well as the pilot signal.

The signal $y_1(t)$ of Figure 7.1 is then expressed by equation 7.3.4:

$$\begin{aligned} y_1(t) &= r(t)\, A_p x_p(t - \hat{T}_d + \frac{T_c}{2}) \\ &= \sum_{i=p}^{M} A_i\, x_i(t - T_d)\, m_i(t - T_d)\, A_p x_p(t - \hat{T}_d + \frac{T_c}{2}) + n(t)\, A_p x_p(t - \hat{T}_d + \frac{T_c}{2}) \end{aligned} \tag{7.3.4}$$

Equation 7.3.4 can be rewritten as equation 7.3.5:

$$y_1(t) = \sum_{i=p}^{M} A_i\, x_i(t - T_d)\, m_i(t - T_d) A_p\, x_p(t - \hat{T}_d + \frac{T_c}{2}) + n_1(t) \tag{7.3.5}$$

where: $n_1(t) = n(t)\, A_p x_p(t - \hat{T}_d + \frac{T_c}{2})$

Evaluating equation 7.3.5, equation 7.3.6 is obtained:

$$\begin{aligned} y_1(t) &= A_p^2\, x_p(t - T_d)\, x_p(t - \hat{T}_d + \frac{T_c}{2}) \\ &\quad + \sum_{\substack{i=1 \\ i \neq p}}^{M} A_i\, x_i(t - T_d) m_i(t - T_d) A_p\, x_p(t - \hat{T}_d + \frac{T_c}{2}) + n_1(t) \end{aligned} \tag{7.3.6}$$

Recall that the term $m_p(t - T_d)$ disappears, since it is so chosen that $m_p(t) = 1$ for all time [15]. The second and the third term of equation 7.3.6 are the interference and noise terms, respectively, and can be written in a joint form so that equation 7.3.6 takes the form of equation 7.3.7:

$$y_1(t) = A_p^2\, x_p(t - T_d)\, x_p(t - \hat{T}_d + \frac{T_c}{2}) + n_{e_1}(t) \tag{7.3.7}$$

where: $n_{e_1}(t) = \sum_{\substack{i=1 \\ i \neq p}}^{M} A_i\, x_i(t - T_d) m_i(t - T_d) A_p\, x_p(t - \hat{T}_d + \frac{T_c}{2}) + n_1(t)$

In the similar fashion equation 7.3.8, representing $y_2(t)$, is obtained:

$$y_2(t) = A_p^2\, x_p(t-T_d)\, x_p(t-\hat{T}_d-\frac{T_c}{2}) + n_{e_2}(t) \tag{7.3.8}$$

where: $n_{e_2}(t) = \sum_{\substack{i=1 \\ i\neq p}}^{M} A_i\, x_i(t-T_d) m_i(t-T_d) A_p\, x_p(t-\hat{T}_d-\frac{T_c}{2}) + n_2(t)$,

and: $n_2(t) = n(t)\, A_p x_p(t-\hat{T}_d-\frac{T_c}{2})$.

Subtracting equation 7.3.7 from equation 7.3.8, equation 7.3.9 is obtained:

$$\varepsilon(t,\delta) = y_2(t) - y_1(t) = A_p^2\, x_p(t-T_d)\left(x_p(t-\hat{T}_d-\frac{T_c}{2}) - x_p(t-\hat{T}_d+\frac{T_c}{2}) \right) + n_e(t) \tag{7.3.9}$$

where:

$$n_e(t) = n_{e_2}(t) - n_{e_1}(t)$$

$$= \sum_{\substack{i=1 \\ i\neq p}}^{M} A_i\, x_i(t-T_d) m_i(t-T_d) A_p\, x_p(t-\hat{T}_d-\frac{T_c}{2}) + n(t) A_p\, x_p(t-\hat{T}_d-\frac{T_c}{2})$$

$$- \sum_{\substack{i=1 \\ i\neq p}}^{M} A_i\, x_i(t-T_d) m_i(t-T_d) A_p\, x_p(t-\hat{T}_d+\frac{T_c}{2}) - n(t) A_p\, x_p(t-\hat{T}_d+\frac{T_c}{2})$$

$$= \sum_{\substack{i=1 \\ i\neq p}}^{M} A_p A_i\, x_i(t-T_d) m_i(t-T_d) \left(x_p(t-\hat{T}_d-\frac{T_c}{2}) - x_p(t-\hat{T}_d+\frac{T_c}{2}) \right)$$

$$+ A_p n(t) \left(x_p(t-\hat{T}_d-\frac{T_c}{2}) - x_p(t-\hat{T}_d+\frac{T_c}{2}) \right)$$

It is important to note that the term $A_p n(t) \left(x_p(t-\hat{T}_d-\frac{T_c}{2}) - x_p(t-\hat{T}_d+\frac{T_c}{2}) \right)$ is white but not Gaussian [11]. It possesses a two sided power spectral density given by equation 7.3.10:

$$S_{n'}(f) = N_o(1+\frac{1}{N}) \tag{7.3.10}$$

where N is the number of chips in one PRBS period.

Equation 7.3.9 is now integrated over the PRBS period $T = NT_c$ to obtain equation 7.3.11:

$$\begin{aligned} e(t) = {} & \frac{A_p^2}{NT_c}\int_{-NT_c/2}^{NT_c/2} x_p(t-T_d)\, x_p(t-\hat{T}_d-\frac{T_c}{2})\,dt \\ & -\frac{A_p^2}{NT_c}\int_{-NT_c/2}^{NT_c/2} x_p(t-T_d)\; x_p(t-\hat{T}_d+\frac{T_c}{2})\,dt \\ & +\frac{1}{NT_c}\int_{-NT_c/2}^{NT_c/2} n_e(t)\,dt \end{aligned} \tag{7.3.11}$$

Equation 7.3.11 can be rewritten in the form of equation 7.3.12:

$$\begin{aligned} e(t) = {} & \frac{A_p^2}{NT_c}\int_{-NT_c/2}^{NT_c/2} x_p(t)\, x_p(t+T_d-\hat{T}_d-\frac{T_c}{2})\,dt \\ & -\frac{A_p^2}{NT_c}\int_{-NT_c/2}^{NT_c/2} x_p(t)\; x_p(t+T_d-\hat{T}_d+\frac{T_c}{2})\,dt \\ & +\frac{1}{NT_c}\int_{-NT_c/2}^{NT_c/2} n_e(t)\,dt \end{aligned} \tag{7.3.12}$$

Using the general form of equation 7.2.10, let the autocorrelation now be defined by equation 7.3.13 [11]:

$$R_{x_p}(\tau) = \frac{1}{T}C_{x_p}(\tau) = \frac{1}{T}\int_0^T x_p(t)\, x_p(t+\tau)\,dt \tag{7.3.13}$$

In terms of $C_{x_p}(\tau)$, equation 7.3.12 can also be expressed by equation 7.3.14:

$$e(t) = \frac{A_p^2}{NT_c}\left[C_{x_p}\left((\delta-\frac{1}{2})T_c\right) - C_{x_p}\left((\delta+\frac{1}{2})T_c\right)\right] + \frac{1}{NT_c}\int_{-NT_c/2}^{NT_c/2} n_e(t)\,dt \tag{7.3.14}$$

Figure 7.6 shows the plots of $C_{x_p}\left((\delta-\frac{1}{2})T_c\right)$ and $C_{x_p}\left((\delta+\frac{1}{2})T_c\right)$ functions, and their difference, as well as the plot of $C_{x_p}(\delta T_c)$. Note that the peak of the autocorrelation function is given by equation 7.3.16, and its minimum by equation 7.3.17:

$$C_{x_p}(\delta T_c = 0) = \int_0^{NT_c} A_p x_p(t)\, A_p x_p(t)\, dt = NA_p^2 T_c \tag{7.3.16}$$

$$C_{x_p}(\delta T_c = \pm T_c) = \int_0^{NT_c} A_p x_p(t)\, A_p x_p(t \pm T_c)\, dt = -A_p^2 T_c \tag{7.3.17}$$

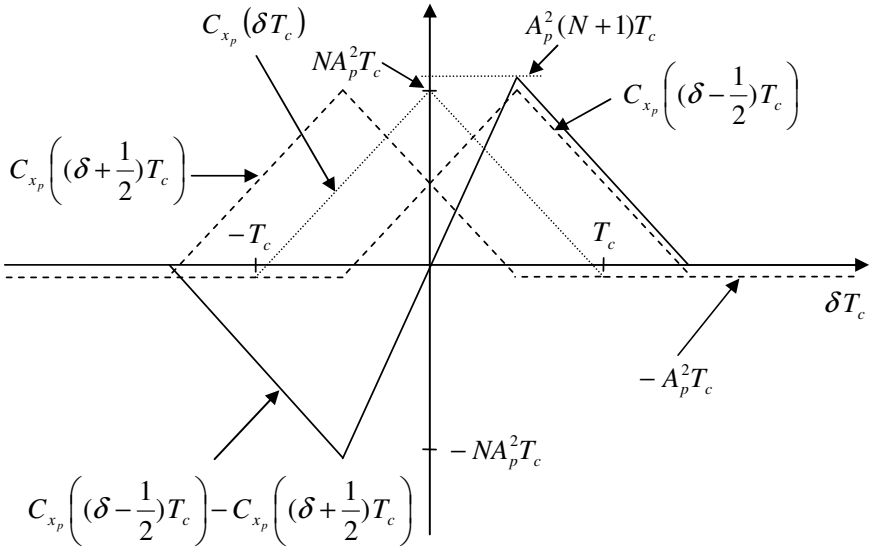


Fig. 7.6 Plot of the early, late, and on time PRBS correlation functions

Assuming that the PRBS pilot signal is tracked over its entire period the gradient in the linear region is then expressed by equation 7.3.18:

$$m = \frac{A_p^2(N+1)T_c}{T_c/2} = 2A_p^2(N+1) \tag{7.3.18}$$

Therefore, in the linear region the operation of the delay lock tracking loop is governed by equation 7.3.19:

$$C_{x_p}\left((\delta-\frac{1}{2})T_c\right)-C_{x_p}\left((\delta+\frac{1}{2})T_c\right)=m\,\delta T_c=2A_p^2(N+1)(T_d-\hat{T}_d) \quad (7.3.19)$$

Rearranging equation 7.3.19 to make $\hat{T}_d$ the subject of the formula, equation 7.3.20 is obtained:

$$\hat{T}_d=T_d-\frac{C_{x_p}\left((\delta-\frac{1}{2})T_c\right)-C_{x_p}\left((\delta+\frac{1}{2})T_c\right)}{2A_p^2(N+1)} \quad (7.3.20)$$

The numerator of the second term of equation 7.3.20 is determined by the DLL, and according to that error, $\hat{T}_d$, which is the estimate of the time offset T_d, is determined. Although T_d and $\hat{T}_d$ are not shown explicitly to be time varying they are [11]. In order to implement equation 7.3.20 digitally T_d and $\hat{T}_d$ must be represented as time variables. Assuming that the DLL executes a cycle, that is, calculates new values of $C_{x_p}\left((\delta-\frac{1}{2})T_c\right)$ and $C_{x_p}\left((\delta+\frac{1}{2})T_c\right)$ every T_c seconds, equation 7.3.20 can be re-represented by equation 7.3.21:

$$\hat{T}_d(nT_c)=T_d(nT_c)-\frac{C_2(nT_c)-C_1(nT_c)}{2A_p^2(N+1)} \quad (7.3.21)$$

where: $C_1=C_{x_p}\left((\delta+\frac{1}{2})T_c\right)$ and $C_2=C_{x_p}\left((\delta-\frac{1}{2})T_c\right)$

Equation 7.3.21 cannot be implemented in practice since it requires the knowledge of the time offset T_d in order to calculate the estimate $\hat{T}_d$ of that time offset in the same time instant. Under the assumption that the time offset has been acquired successfully to within half a chip period, as denoted by equation 7.3.1, every new subsequent value of the time offset estimate can then be calculated based on its previous estimate in the following manner. Assuming that at the moment of the tracking phase start-up $T_a=T_d$, and substituting it into equation 7.3.21, yields equation 7.3.22:

$$\hat{T}_d(T_c)-T_a=-\frac{C_2-C_1}{2A_p^2(N+1)} \quad (7.3.22)$$

Provided that indeed at the tracking phase start-up $T_a = T_d$, $\hat{T}_d(T_c)$ takes the value of T_a since the numerator of the right hand side of equation 7.3.22 goes to zero (refer to Figure 7.6). If, however, $T_a \neq T_d$, when it was assumed that $T_a = T_d$, then $\hat{T}_d(T_c)$ takes on the actual value of T_d at the start-up of the tracking phase, as the right hand side of equation 7.3.22 generates the difference among the acquired and the actual time offset: $T_a - T_d$, so that equation 7.3.22 takes the form of $\hat{T}_d(T_c) - T_a = -(T_a - T_d)$, resulting in $\hat{T}_d(T_c) = T_d$.

With this thought in mind equation 7.3.22 can be rewritten as equation 7.3.23:

$$\hat{T}_d(nT_c + T_c) = \hat{T}_d(nT_c) - \frac{C_2(nT_c) - C_1(nT_c)}{2A_p^2(N+1)} \tag{7.3.23}$$

where the initial condition is set as: $\hat{T}_d(0) = T_a$.

Figures 7.7a and 7.7b demonstrate the operation of the tracking loop model developed at no noise and no interferences present. The tracking loop was set to execute 50 cycles, with the incoming time offset T_d varied for the first 35 cycles and set to a constant value, equal to the one of the previous cycle, thereafter. The figures demonstrate the optimal performance of the tracking loop governed by the control law of equation 7.3.23. In this particular case the pilot period has been set equal to $511 \cdot T_c$ seconds with T_c represented by 8 time units. Choosing the simulation parameters in this way allows one to observe the ability of the tracking loop to actively track the changes in the incoming time offset for the first 35 cycles. Furthermore, when the time offset stabilises for the following 15 cycles, the tracking loop also stabilises its estimate at this particular value, as demonstrated in Figures 7.7a and 7.7b.

In order for the tracking loop to remain operational and thus ensure the transfer of data between the transmitter and the receiver of Figure 7.1, the range of equation 7.3.24 must be satisfied at all times:

$$-T_c/2 \leq \left(\hat{T}_d(nT_c) - T_d(nT_c) \right) \leq T_c/2 \tag{7.3.24}$$

Equivalently, in terms of equation 7.3.23, the range of equation 7.3.25 must be satisfied at all times:

$$-T_c/2 \leq \left(\hat{T}_d(nT_c + T_c) - \hat{T}_d(nT_c) \right) \leq T_c/2 \tag{7.3.25}$$

With the range of equation 7.3.24 (7.3.25) not satisfied the tracking circuit of Figure 7.1 will no longer be able to track the incoming time offset and the connection among the transmitter and the receiver will inevitably be lost. In this case the time offset will need to be re-acquired by the initial synchronization unit, as outlined in section 7.2, before the successful data transfer can take place again.

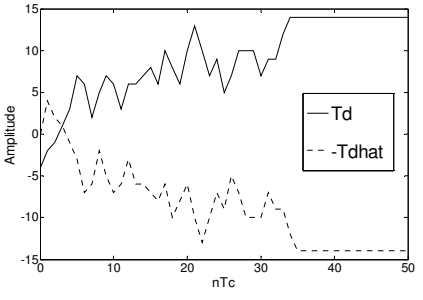


Fig. 7.7a Plot of $T_d(nT_c)$ and $-\hat{T}_d(nT_c)$ vs. nT_c

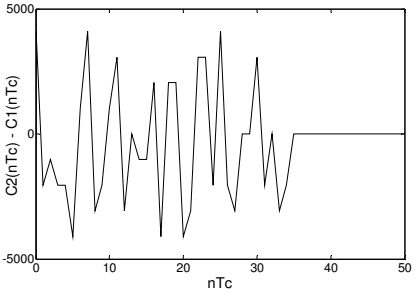


Fig. 7.7b Plot of $C_2(nT_c) - C_1(nT_c)$ vs. nT_c

7.3.2 Performance Evaluation of the System with AWGN and Interuser Interferences

In this subsection, the performance of the system, highlighted in Figure 7.1, is examined under the influence of AWGN and interuser interferences during its tracking mode of operation. The performance is evaluated for different numbers of chaotic users with bit error rate curves [66] for the specified range of the bit energy to noise power spectral density ratio (E_b / N_o). The spreading factor of 73 chips has been used to represent a single information bit transmitted. Tracking is conducted over the synchronization period of the pilot signal which has been chosen to be 511 chips long, that is, seven times the duration of the information bit. The general transmission structure of the signals is plotted in Figure 7.8. The code acquisition is required only at the beginning of the transmission, and when the system is no longer able to track.

The empirical BER curves for the system of Figure 7.1 are presented in Figure 7.9 for 1-5, 10, 15 and 20 chaotic users on top of the system's PRBS pilot signal. The incoming time offset T_d has been uniformly varied within the boundaries of equation 7.3.24.

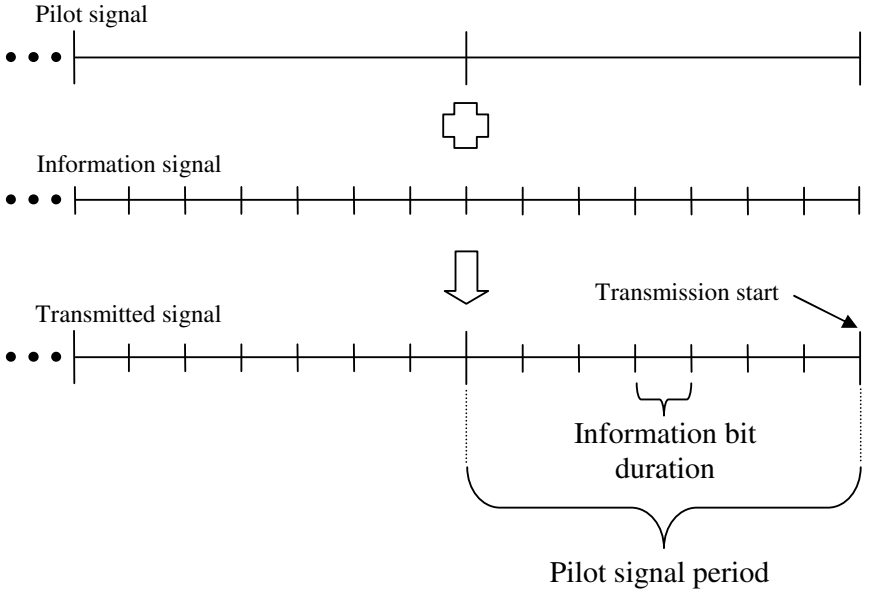


Fig. 7.8 General transmission structure of the signals

Note that with the perfect synchronization assumed, the theoretical bit error rate curves of the system of [22] have been shown to be governed by equation 7.3.26 [55]:

$$BER = \frac{1}{2} erfc\left(\left[\frac{2\Omega}{L} + \frac{2(M-1)}{L} + \left(\frac{E_b}{N_o} \right)^{-1} \right]^{-\frac{1}{2}} \right) \tag{7.3.26}$$

where, *erfc* denotes the complementary error function [55], and Ω is defined as the variance of the chaotic signal squared divided by the square of the average power of the same chaotic signal, and is expressed by equation 7.3.27:

$$\Omega = \frac{\mathrm{var}\left[x_1^2\right]}{P_s^2} = \frac{\mathrm{var}\left[x_2^2\right]}{P_s^2} = \cdots = \frac{\mathrm{var}\left[x_M^2\right]}{P_s^2} \tag{7.3.27}$$

In addition to the empirical BER curves of the system of Figure 7.1, Figure 7.9 also presents the perfect synchronization theoretical BER curves obtained by evaluating equation 7.3.26 for 1-5, 10, 15 and 20 chaotic users without the system's pilot signal. Note that these theoretical BER curves should be used as a guide only since equation 7.3.26 is somewhat inaccurate [55], especially at the low values of BER.

From Figure 7.9 it can be observed that without assuming perfect synchronization the noise performance of the system introduced by Parlitz and Ergezinger [22] degrades by approximately 1-2 dB for the single user case. For a given E_b / N_o the single user plus the pilot signal exhibit the best performance due to the lowest interference at the receiver which subsequently causes the tracking unit of Figure 7.1 to generate least error in the time offset estimates. As the number of users increases the interuser interference inevitably increases, causing further degradation in the performance of the tracking unit, what in turn further degrades the bit error rate. With the decreasing levels of noise, that is with increasing E_b / N_o, the interuser interference dominates, causing the constant bit error rate characterised by the flattening of the BER curves of Figure 7.9.

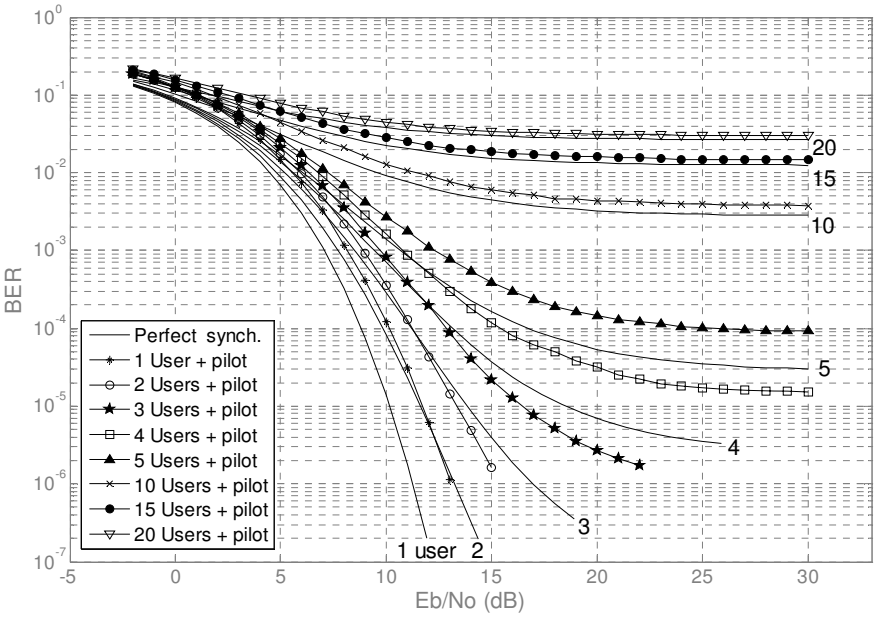


Fig. 7.9 The empirical BER curves of the system of Figure 7.1 (marked curves), with T_d varied within the boundaries of equation 7.3.24. The corresponding theoretical curves with perfect synchronization assumed are shown by unmarked curves.

By assuming that the highest acceptable level of BER equals 10^{-3} [69,70], it can be observed from Figure 7.9 that the E_b / N_o ratio for which the system performance is satisfactory for the case of 1, 2, 3, 4, and 5 users is equal to approximately 8, 9, 9.5, 11 and 12 dB, respectively. In the case of 10, 15 and 20 users the BER curves flatten before reaching the BER level of 10^{-3}. This is unacceptable in practice. However, as seen from Figure 7.9, in the case of 10, 15 and 20 users,

even the perfect synchronization BER curves exceed the BER of 10^{-3}. A possible method to improve the performance in this case would be to use the filters specially designed for the chaotic time series [71]. The clock synchronization between the transmitter and the receiver is assumed, as is in most cases when evaluating the performance of binary modulation techniques [67,12,63].

In Figure 7.10, the BER curves for T_d varied within and beyond the boundaries of equation 7.3.24 are plotted. With the boundaries of equation 7.3.24 violated the tracking loop operates outside the linear region of Figure 7.6 and can no longer estimate the incoming time offset T_d. As seen from Figure 7.10 this results in the significant increase in the bit error rate for a given E_b / N_o. In the case of Figure 7.10 it has been assumed that the time offset is immediately reacquired so that the tracking loop can accurately execute the subsequent cycles, provided that equation 7.3.24 is now satisfied.

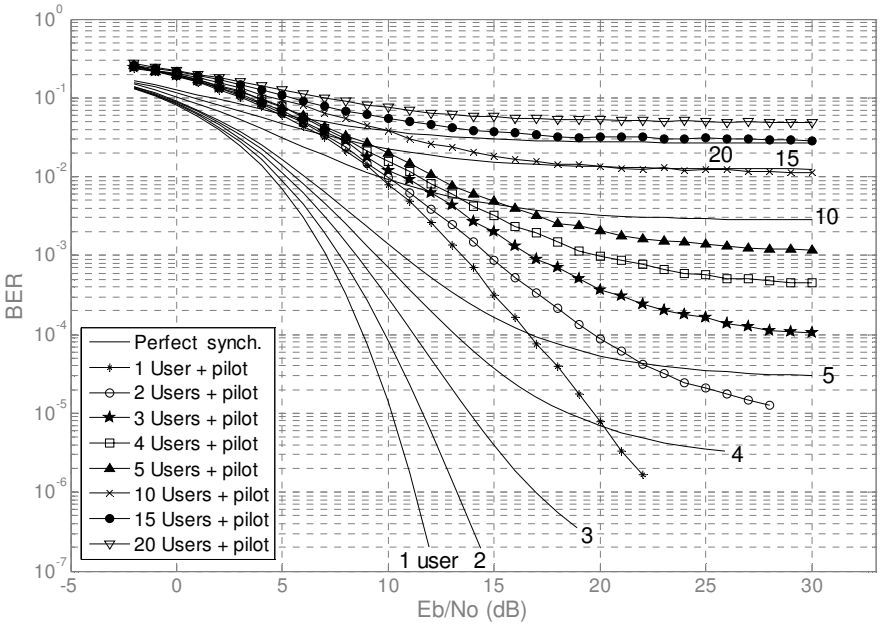


Fig. 7.10 The empirical BER curves of the system of Figure 7.1 (marked curves), with T_d varied within and beyond the boundaries of equation 7.3.24. The corresponding theoretical curves with perfect synchronization assumed are shown by unmarked curves.

7.3.3 Comparison and Discussion in AWGN Channel

In order to evaluate and compare the performance of the system of Figure 7.1 the BER curves for the binary phase shift keying (BPSK) and the CS based

communications technique of initial condition modulation (ICM) of chapter 6 [63,72,71], have been produced in Figure 7.11 alongside the single user curves of Figures 7.9 and 7.10. In this work, the ICM scheme [63] is of interest as it is based on a different form of synchronization strategy [3] used within chaotic communication systems.

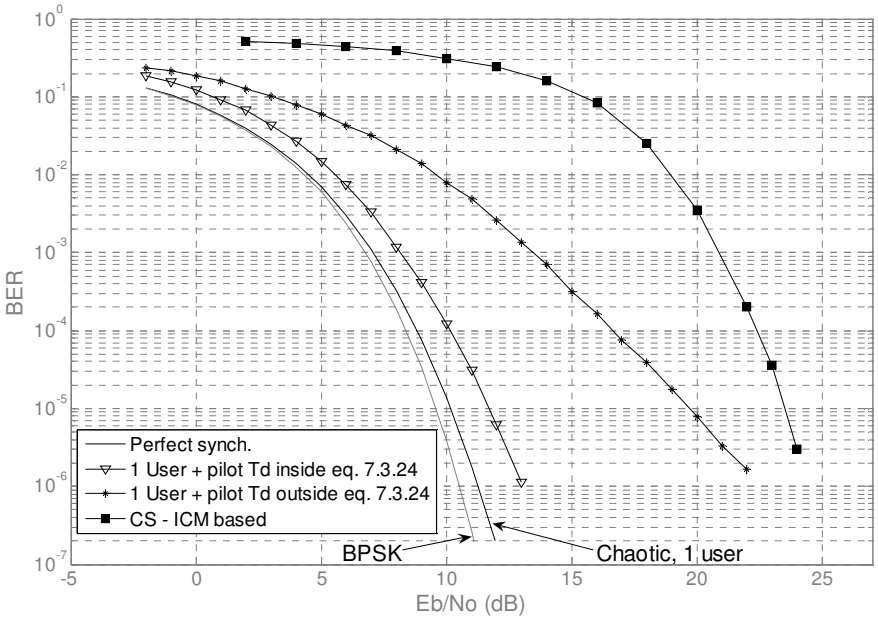


Fig. 7.11 The BER curves: (a) the solid lines are for the theoretical BPSK and chaotic DS-CDMA system of [22] with the perfect synchronization assumed; (b) the inverted triangles are for the system of Figure 7.1 with T_d varied within the boundaries of equation 7.3.24; (c) the asterisks are for the system of Figure 7.1 with T_d varied within and beyond the boundaries of equation 7.3.24; (d) the solid squares are for the CS ICM based system of [63].

From Figure 7.11, it can be observed that the single user chaotic DS-CDMA system of Figure 7.1 outperforms the ICM single user communications scheme based on the principles of CS [63]. Therefore, the synchronization scheme proposed and investigated here has been shown to be more robust to noise than the Pecora – Carroll (PC) CS based ICM communication scheme, which in turn has been shown in chapter 6 [63,72,71] to be one of the more robust PC CS communication schemes [63,72,71].

7.3.4 Performance Evaluation of the System in a Rayleigh Fading Channel with AWGN and Interuser Interferences

In this subsection, the performance of the system of Figure 7.1 is evaluated in a Rayleigh fading channel with AWGN and interuser interferences present [19]. This system, with Rayleigh fading incorporated into Figure 7.1, is shown in Figure 7.12.

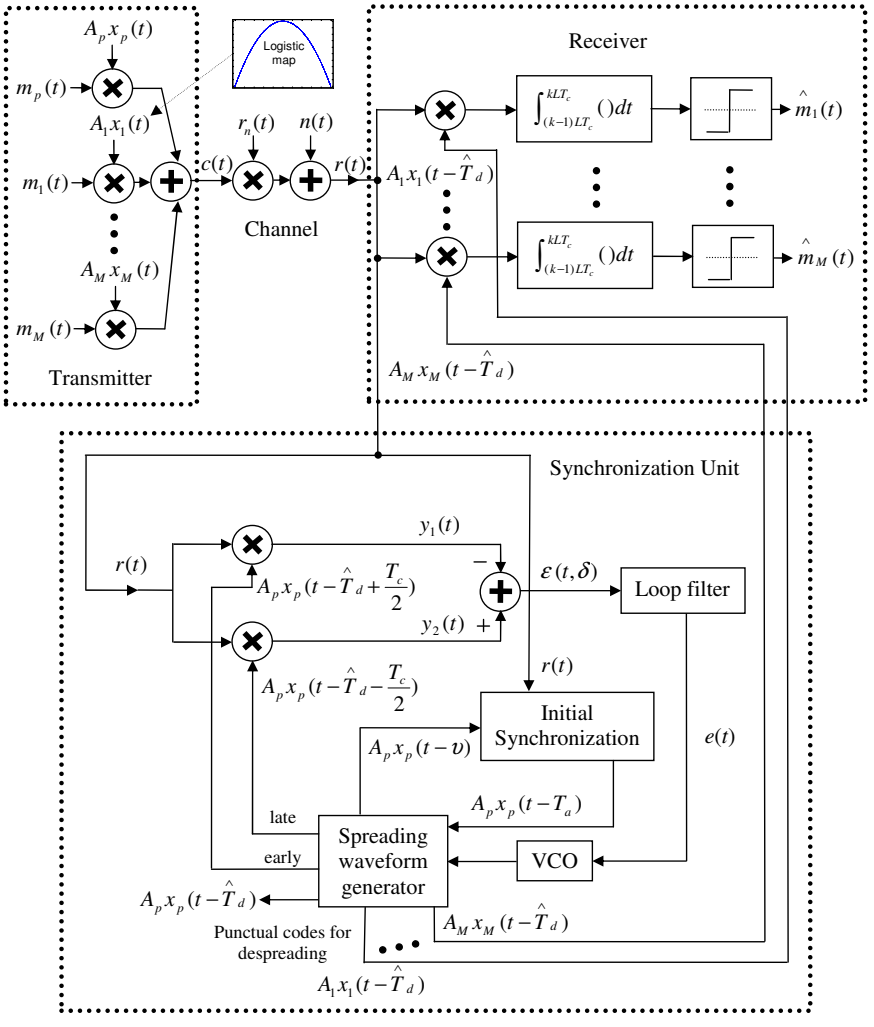


Fig. 7.12 DS-CDMA chaotic communication system with the synchronization unit in the Rayleigh fading channel

The empirical BER curves for the system of Figure 7.12 are shown in Figure 7.13 for 1, 5, 10, 15 and 20 users. The Rayleigh fading envelope, $r_n(t)$, was generated for the velocity of the receiver relative to the transmitter of 55 km/h and the carrier frequency of 900 MHz [73]. For comparison, the theoretical BER curves for the Rayleigh fading channel with the perfect synchronization assumed [10] are also shown. It can be seen from Figure 7.13 that in the Rayleigh fading channel the system fails to satisfy the maximum allowable BER limit of 10^{-3} for any number of users and any E_b / N_o. Furthermore, it can be observed from Figures 7.9 and 7.13 that the system performance in the Rayleigh fading channel degrades more significantly when the perfect synchronization is not assumed than when the perfect synchronization is not assumed without Rayleigh fading. Although the system satisfies the BER level of 10^{-3} for 1-5 users in an AWGN channel it fails for all users in a fading channel. Thus, in comparison, the system in the Rayleigh fading channel is not practical for real world applications. In order to improve the performance in the fading environment techniques used to disperse bursts of error in time, such as block interleaving [10], could be employed.

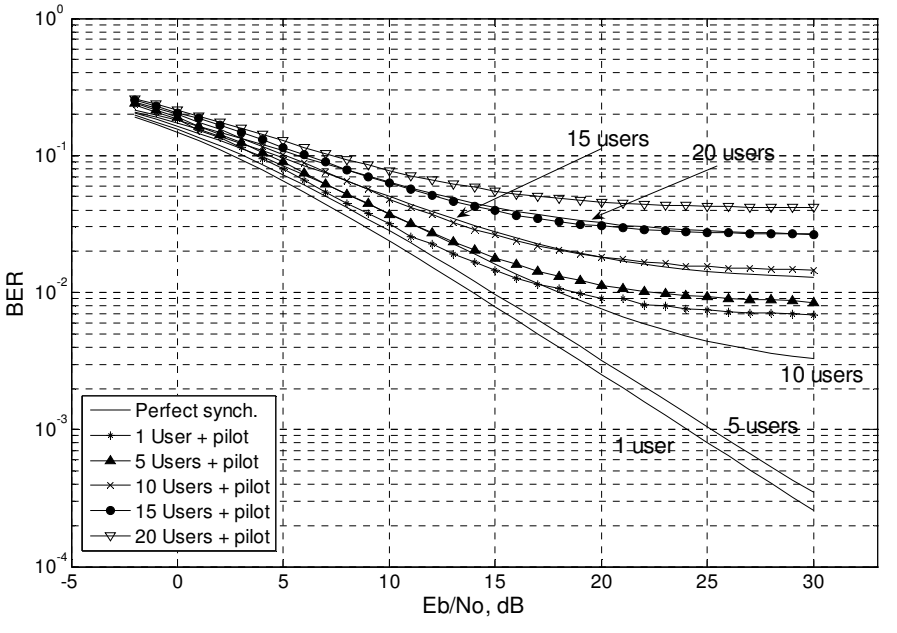


Fig. 7.13 The empirical BER curves of the system of Figure 7.12 in a Rayleigh faded, AWGN channel (marked curves), with T_d varied within the boundaries of equation 7.3.24. The corresponding theoretical curves with perfect synchronization assumed are shown by unmarked curves.

7.4 Code Tracking with a Chaotic Pilot Signal

In this section the code tracking with a chaotic pilot signal in place of the PRBS pilot signal is proposed. Figure 7.14 shows the CBDS-CDMA communication system similar to that of Figure 7.1, but with the chaotic pilot based tracking unit in place of the PRBS pilot based tracking unit.

As in Figure 7.1, $x(t)$ of Figure 7.14 denotes the chaotic spreading signals of amplitude A and spreading factor L, which are multiplied by the binary message

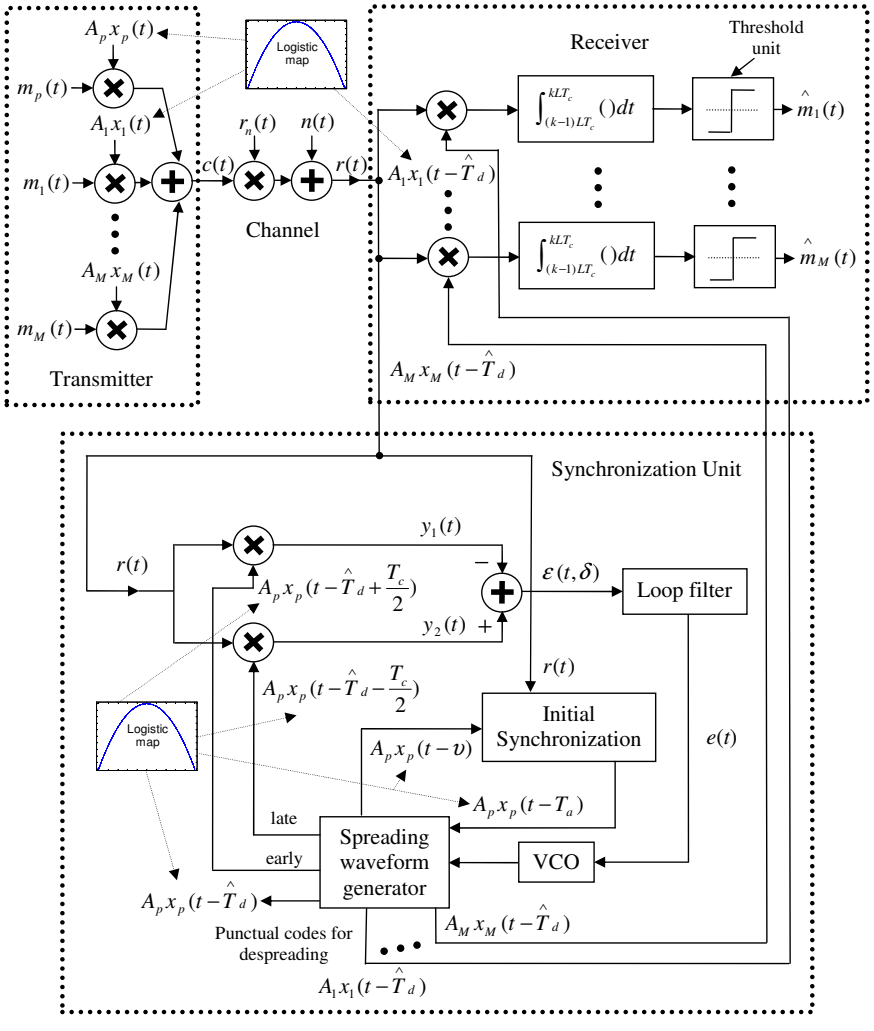


Fig. 7.14 DS-CDMA chaotic communication system with the chaotic pilot based synchronization unit

signals $m(t)$ and then summed up to produce the signal $c(t)$ which is transmitted through the channel. The spreading factor L is defined as the number of chaotic points representing a single bit [63]. $x_p(t)$ denotes the chaotic signal which acts as the periodic or non-periodic, as explained in section 7.4.1, pilot signal used for synchronization purposes. The mutually orthogonal chaotic signals used within the CBDS-CDMA system of Figure 7.14, are produced by the logistic map of equation 7.1.1 [22,15].

The fundamental difference among the proposed system of Figure 7.14 and the corresponding system of Figure 7.1 [15,19] is that the system of Figure 7.14 implements the chaotic pilot signal in place of the PRBS pilot signal.

7.4.1 Theoretical Model of the System

In this subsection the mathematical model of the chaotic pilot based code tracking loop is developed and its validity demonstrated by means of a simulation. Once the chaotic pilot based initial synchronization circuit of Figure 7.14, (as described in section 7.2 [15]), has established the correct time offset to within the pull-in region of the tracking circuit, the tracking circuit is able to take over the synchronization process. As in section 7.3, the code tracking loop with a pull-in region of half a chip length is considered. Therefore, to this end it is assumed that the search parameter Δ of the logistic chaotic map based initial synchronization unit of Figure 1 is equal to a ½. This ensures that the acquired time offset of Figure 7.14, T_a, is accurate to within half a chip length of the exact time offset enabling the tracking circuit to correct the inaccuracy and maintain the correct time offset. Thus, as for PRBS pilot case above, we redefine the incoming time offset η, of section 7.2 [15] as T_d, indicating that the acquisition phase has been finished and that the synchronization unit now has the approximate knowledge of the correct time offset to within half a chip length, as shown in equation 7.3.1.

The tracking circuit examined here utilizes the logistic chaotic map pilot signal in place of the PRBS pilot signal of [15] to produce punctual codes for despreading the received signal $r(t)$. It includes the entire synchronization unit of Figure 7.14 except for the initial synchronization unit. As in section 7.3, the loop filter of Figure 7.14 is essentially an averaging integrator, integrating over the chaotic pilot signal integration period NT_c:

$$e(t) = \frac{1}{NT_c} \int_{-NT_c/2}^{NT_c/2} \varepsilon(t, \delta) dt \tag{7.4.1}$$

where the term δ is defined as the normalized difference among the received signal time offset T_d and the tracking circuit time offset estimate $\hat{T}_d$, that is,

$\delta = (T_d - \hat{T}_d)/T_c$. In equation 7.4.1, N denotes the number of chips in the integration period NT_c.

By keeping in mind that with no fading in the system, (for simplicity of analysis), the received signal $r(t)$ is composed of the mixture of signals of different users, the pilot signal and the noise component $n(t)$:

$$r(t) = c(t) + n(t) = \sum_{i=p}^{M} A_i \, x_i(t - T_d) \, m_i(t - T_d) + n(t) \tag{7.4.2}$$

it is then readily verifiable that equation 7.4.2, as in section 7.3, can be represented as equation 7.4.3 [15]:

$$e(t) = \frac{A_p^2}{NT_c}\left[C_{x_p}\left((\delta - \frac{1}{2})T_c \right) - C_{x_p}\left((\delta + \frac{1}{2})T_c \right) \right] + \frac{1}{NT_c}\int_{-NT_c/2}^{NT_c/2} n_e(t)\, dt \tag{7.4.3}$$

where $n_e(t)$ denotes the AWGN component $n(t)$ and inter-user interferences [15]. In equation 7.4.3, $C_{x_p}(\delta T_c)$ is defined to be the autocorrelation function of the chaotic pilot signal multiplied by the integration period of the tracking loop [15].

As for the PRBS pilot signal, the tracking unit produces punctual codes for despreading the received signal by correlating the early and late replicas of the chaotic pilot signal by the received signal. It then subtracts the two and ensures that the resulting error signal $e(t)$ is constantly forced to zero [15,11]. It is now shown how a punctual time offset $\hat{T}_d$, which matches the received signal time offset T_d, is obtained at discrete time instances. With a correct estimate of T_d, the receiver is able to accurately despread the received signal.

Due to the random like nature of chaotic and PRBS signals, spreading introduces security into the system. However, the fundamental difference between a PRBS signal and a chaotic signal is that a PRBS signal is inherently periodic whereas a chaotic signal is non-periodic. Furthermore, whereas a PRBS signal has only two values, $\pm A_p$ denoting a binary one and a zero, a chaotic signal theoretically may assume an infinite number of amplitudes in a given dynamic range. In case of the logistic chaotic map, used as part of the CBDS-CDMA system proposed here, the dynamic range is ± 1. In any given period of the maximum length PRBS the number of ones always exceeds the number of zeros by one. Because of this inherent property of PRBS signals it is possible to theoretically determine upper and lower bounds of the auto-correlation function of a maximum length PRBS signal, as shown in Figure 7.6 [15]. However, due to the non-periodic

nature of chaotic signals and their constantly changing amplitude, upper and lower limits of the auto-correlation function cannot be determined theoretically and thus need to be determined empirically for every new chaotic signal generated, as explained below.

Figure 7.15 shows the plots of $C_{x_p}\left((\delta-\frac{1}{2})T_c\right)$ and $C_{x_p}\left((\delta+\frac{1}{2})T_c\right)$ functions of equation 7.4.3, and their difference, as well as the plot of $C_{x_p}(\delta T_c)$. It is important to note that plots of Figure 7.15 are valid for non-periodic chaotic pilot signals only when the integration period of the tracking unit [15] is sufficiently large so that $C_{x_p}(T_c)/C_{x_p}(0) \approx C_{x_p}(-T_c)/C_{x_p}(0)$, that is, so that approximate symmetry of the correlation plots exists about the *y* axis. Furthermore, for any periodic pilot signal, that is, any pilot signal (chaotic or other) that reuses the same portion of a signal for every new pilot period, as in section 7.3 [15,19]: $C_{x_p}(-\infty:0) = C_{x_p}(0:\infty)$. Figure 7.6 shows similar plots to those of Figure 7.15 for a maximum length PRBS pilot signal.

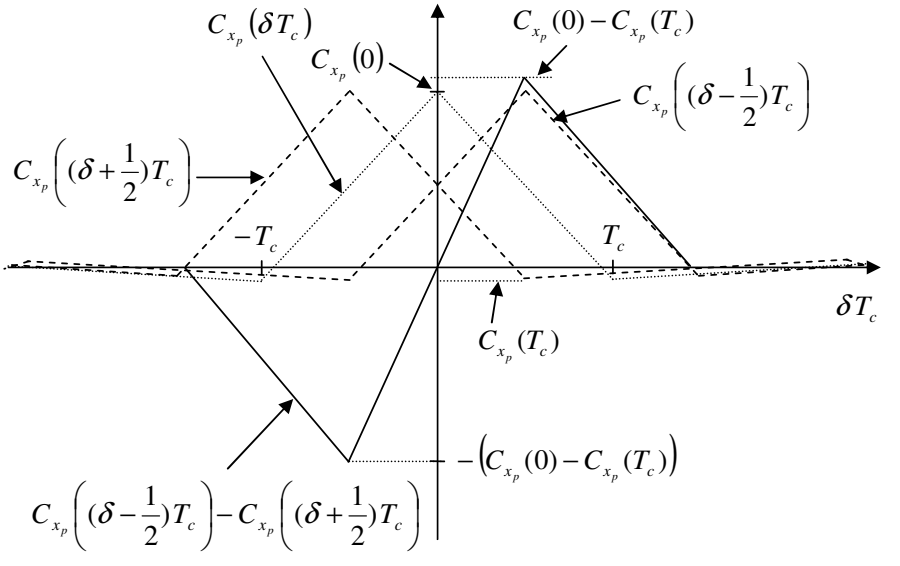


Fig. 7.15 Plot of the early, late, and on-time, chaotic correlation functions

By comparing Figure 7.6 of section 7.3 [15] to Figure 7.15 above, the main difference that should be observed is that for every maximum length periodic PRBS signal the terms $C_{x_p}(0)$ and $C_{x_p}(T_c)$ are constant and equal to $NA_p^2T_c$ and

$-A_p^2 T_c$, respectively, while they vary for chaotic signals with different initial conditions. The following mathematical analysis shows the effect of this on the operation of the tracking loop. For a given tracking period of a chaotic pilot signal, the gradient in the linear region of Figure 7.15 is expressed by equation 7.4.4:

$$m = \frac{C_{x_p}(0) - C_{x_p}(T_c)}{T_c / 2} \tag{7.4.4}$$

Therefore in the linear region, operation of the tracking loop is governed by equation 7.4.5:

$$C_{x_p}\left((\delta - \frac{1}{2})T_c\right) - C_{x_p}\left((\delta + \frac{1}{2})T_c\right) = m\,\delta T_c = \frac{C_{x_p}(0) - C_{x_p}(T_c)}{T_c / 2} \cdot (T_d - \hat{T}_d) \tag{7.4.5}$$

Rearranging equation 7.4.5 to make $\hat{T}_d$ the subject of the formula, equation 7.4.6 is obtained:

$$\hat{T}_d = T_d - \frac{T_c\left[C_{x_p}\left((\delta - \frac{1}{2})T_c\right) - C_{x_p}\left((\delta + \frac{1}{2})T_c\right)\right]}{2\left[C_{x_p}(0) - C_{x_p}(T_c)\right]} \tag{7.4.6}$$

Assuming that the tracking circuit executes a cycle, that is, calculates new values of $C_{x_p}\left((\delta - \frac{1}{2})T_c\right)$, $C_{x_p}\left((\delta + \frac{1}{2})T_c\right)$, $C_{x_p}(0)$ and $C_{x_p}(T_c)$ every T_c seconds [15], equation 7.4.6 can be re-represented by equation 7.4.7:

$$\hat{T}_d(nT_c) = T_d(nT_c) - \frac{T_c\left[C_2(nT_c) - C_1(nT_c)\right]}{2\left[C_0(nT_c) - C_3(nT_c)\right]} \tag{7.4.7}$$

where: $C_0 = C_{x_p}(0)$, $C_1 = C_{x_p}\left((\delta + \frac{1}{2})T_c\right)$, $C_2 = C_{x_p}\left((\delta - \frac{1}{2})T_c\right)$ and $C_3 = C_{x_p}(T_c)$.

Equation 7.4.7 cannot be implemented in practice since it requires the knowledge of the time offset T_d in order to calculate the estimate $\hat{T}_d$ of that time offset in the same time instant [15]. Equation 7.4.7 thus needs to be rewritten in a different form. The procedure of section 7.3 [15] used to rewrite a similar PRBS pilot signals equation in a different form is identical to that for chaotic pilot signals

proposed here and is repeated below for convenience. Under the assumption that the time offset has been acquired successfully to within half a chip period, as denoted by equation 7.3.1 [15], every new subsequent value of the time offset estimate can then be calculated based on its previous estimate in the following manner [15]. Assuming that at the moment of the tracking phase start-up $T_a = T_d$, and substituting it into equation 7.4.7, yields equation 7.4.8:

$$\hat{T}_d(T_c) - T_a = -\frac{T_c\left[C_2 - C_1\right]}{2\left[C_0 - C_3\right]} \tag{7.4.8}$$

Provided that indeed at the tracking phase start-up $T_a = T_d$, $\hat{T}_d(T_c)$ takes the value of T_a since the numerator of the right hand side of equation 7.4.8 goes to zero (refer to Figure 7.15). If however $T_a \neq T_d$, when it was assumed that $T_a = T_d$, then $\hat{T}_d(T_c)$ takes on the actual value of T_d at the start-up of the tracking phase, as the right hand side of equation 7.4.8 generates the difference among the acquired and the actual time offset: $T_a - T_d$, so that equation 7.4.8 takes the form of $\hat{T}_d(T_c) - T_a = -(T_a - T_d)$, resulting in $\hat{T}_d(T_c) = T_d$.

With this thought in mind equation 7.4.8 can be rewritten as equation 7.4.9:

$$\hat{T}_d(nT_c + T_c) = \hat{T}_d(nT_c) - \frac{T_c\left[C_2(nT_c) - C_1(nT_c)\right]}{2\left[C_0(nT_c) - C_3(nT_c)\right]} \tag{7.4.9}$$

where the initial condition is set as: $\hat{T}_d(0) = T_a$.

While for a non-periodic chaotic pilot signal the denominator terms C_0 and C_3 of equation 7.4.9 vary and need to be calculated for every tracking period, in case of a periodic chaotic pilot signal they are constant and need to be calculated only once. Therefore, for a periodic chaotic pilot signal equation 7.4.9 can be rewritten as equation 7.4.10:

$$\hat{T}_d(nT_c + T_c) = \hat{T}_d(nT_c) - \frac{T_c\left[C_2(nT_c) - C_1(nT_c)\right]}{2\left[C_0 - C_3\right]} \tag{7.4.10}$$

Figures 7.16a and 7.16b demonstrate the optimal performance of the periodic chaotic pilot based tracking loop model governed by the control law of equation 7.4.10 when no noise, no fading and no interferences are present. Furthermore, a

similar set of Figures demonstrating successful synchronization is also readily obtainable by executing the control law of equation 7.4.9 for a non-periodic chaotic pilot signal. As in section 7.3 [15], the tracking loop was set to execute 50 cycles, with the incoming time offset T_d varied for the first 35 cycles and set to a constant value, equal to the one of the previous cycle, thereafter. Also as in section 7.3 [15,19], the tracking loop integration period has been set equal to $511 \cdot T_c$ seconds with T_c represented by 8 time units. Choosing the simulation parameters in this way allows one to observe the ability of the tracking loop to actively track the changes in the incoming time offset for the first 35 cycles and then also stabilize at the constant incoming time offset value for the next 15 cycles.

In order for the tracking loop to remain operational and thus ensure the transfer of data between the transmitter and the receiver of Figure 7.14, the range of equation 7.4.11 must be satisfied at all times:

$$-T_c/2 \le \left(\hat{T}_d(nT_c) - T_d(nT_c) \right) \le T_c/2 \tag{7.4.11}$$

Equivalently, in terms of equations 7.4.9 and 7.4.10, the range of equation 7.4.12 must be satisfied at all times:

$$-T_c/2 \le \left(\hat{T}_d(nT_c + T_c) - \hat{T}_d(nT_c) \right) \le T_c/2 \tag{7.4.12}$$

With the range of equations 7.4.11 and 7.4.12 not satisfied, the tracking circuit will no longer be able to track the incoming time offset and the connection among the transmitter and the receiver will inevitably be lost [15]. In this case the time offset will need to be re-acquired by the chaotic pilot based initial synchronization unit of section 7.2 [15] before successful data transfer can take place again.

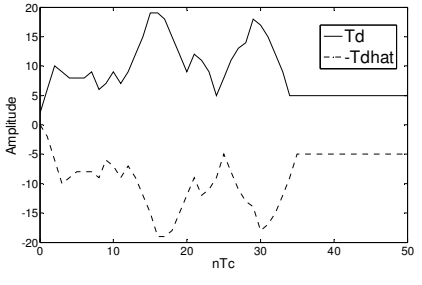


Fig. 7.16a The plot of $T_d(nT_c)$ and $-\hat{T}_d(nT_c)$ vs. nT_c

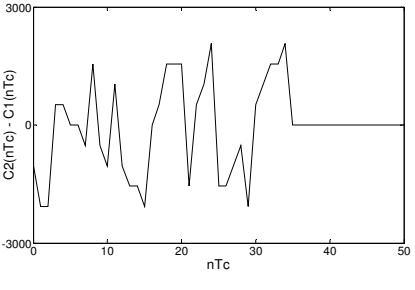


Fig. 7.16b The plot of $C_2(nT_c) - C_1(nT_c)$ vs. nT_c

7.4.2 BER System Performance within AWGN and Rayleigh Fading Channels

In this section, the performance of the chaotic pilot based system of Figure 7.14 is examined under the influence of AWGN, inter-user interferences and Rayleigh multi-path fading during its tracking mode of operation. The performance is evaluated for 1-5, 10, 15 and 20 chaotic users in the system with bit error rate curves [66] for the specified range of the bit energy to noise power spectral density ratio (E_b / N_o). As in section 7.2 [15,19], the spreading factor of 73 chips has been used to represent a single information bit transmitted with the tracking loop integration period of 511 chips, that is, seven times the duration of the information bit. Also, as in section 7.3, the Clarke and Gans flat fading model [73-75] (described in chapter 2) has been used to simulate a multipath Rayleigh fading channel for a velocity of the receiver relative to the transmitter of 55 km/h and a carrier frequency of 900 MHz [73].

The empirical BER curves for the system of Figure 7.14 without Rayleigh multi-path fading are presented in Figure 7.17 for 1-5, 10, 15 and 20 chaotic users on top of the system's periodic chaotic pilot signal whose tracking operation is governed by equation 7.4.10. Similar empirical BER curves for the non-periodic chaotic pilot signal, whose tracking operation is governed by equation 7.4.9, are

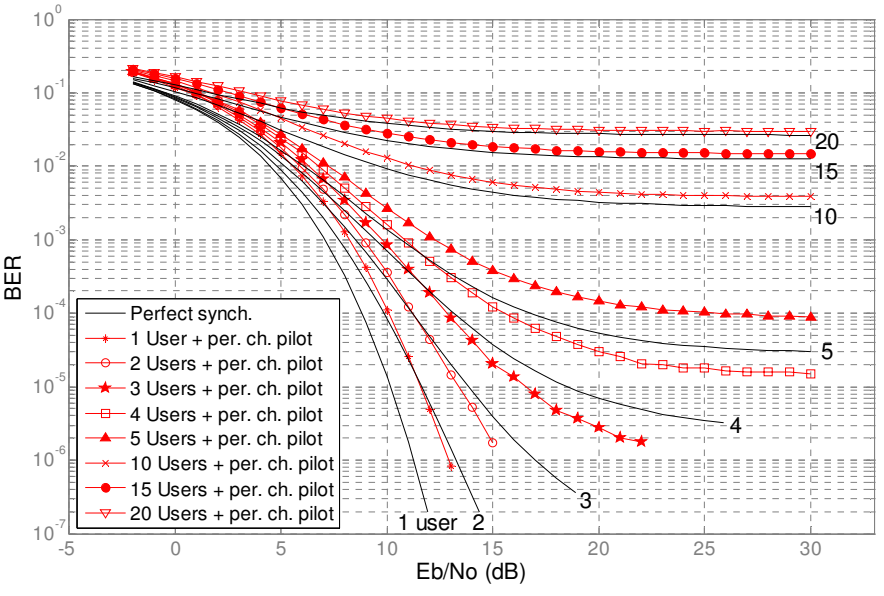


Fig. 7.17 The empirical BER curves of the system of Figure 7.14 when the periodic chaotic pilot signal (marked curves) is used. The corresponding theoretical curves with perfect synchronization assumed are shown by unmarked curves.

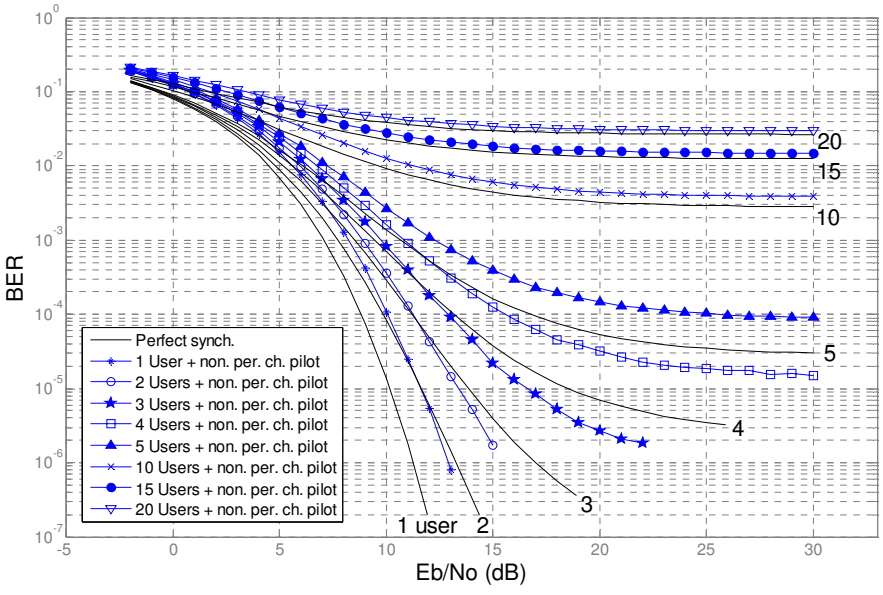


Fig. 7.18 The empirical BER curves of the system of Figure 7.14 when the non-periodic chaotic pilot signal (marked curves) is used. The corresponding theoretical curves with perfect synchronization assumed are shown by unmarked curves.

presented in Figure 7.18. In both cases, the incoming time offset T_d has been uniformly varied within the boundaries of equation 7.4.11. Figures 7.17 and 7.18 also show the corresponding theoretical bit error rate curves without the synchronizing pilot signal, that is, when the perfect synchronization is assumed [55].

Figures 7.17 and 7.18 show that the CBDS-CDMA systems utilising both periodic and non-periodic chaotic pilot signals, respectively, experience degradation in performance as compared to the case when perfect synchronization is assumed. It must also be noted that the theoretical BER curves of Figures 7.17 and 7.18 should be used as a guide only since they are somewhat inaccurate [55], especially at the low values of BER.

Furthermore, it can be observed from Figures 7.17 and 7.18 that for a given E_b / N_o the single user plus the periodic chaotic pilot signal exhibit the best performance due to the lowest interference at the receiver which subsequently causes the tracking unit of Figure 7.14 to generate least error in the time offset estimates. As the number of users increases the inter-user interference inevitably increases, causing further degradation in the performance of the tracking unit, what in turn further degrades the bit error rate. With the decreasing levels of noise, that is with increasing E_b / N_o, the interuser interference dominates, causing the constant bit error rate characterised by the flattening of the BER curves of Figures 7.17 and 7.18.

In Figure 7.19, the BER curves of Figures 7.17 and 7.18 are plotted on the same set of axes for easy comparison. Figure 7.19 shows that there is no noticeable difference in BER performance among the periodic and non-periodic chaotic pilot based CBDS-CDMA systems for any number of users and any E_b / N_o. By assuming that the highest acceptable level of BER equals 10^{-3} [69,70], Figures 7.17, 7.18 and 7.19 show that the E_b / N_o ratio for which the systems' performance is satisfactory for the case of 1, 2, 3, 4, and 5 users is equal to approximately 8, 9, 9.5, 11 and 12 dB, respectively. In the case of 10, 15 and 20 users the BER curves flatten before reaching the BER level of 10^{-3}. Identical behaviour, for the BER level of 10^{-3} and above, has also been observed in section 7.3 [15] for the CBDS-CDMA system utilizing the periodic PRBS pilot signal. The flattening of BER curves above the BER level of 10^{-3} in the case of 10, 15 and 20 users is unacceptable in practice. However, as seen from Figures 7.17 and 7.18, even the perfect synchronization BER curves exceed the BER of 10^{-3} for 10, 15 and 20 users. A possible method to improve the performance in this case would be to use filters specially designed for the chaotic time series [71]. As in section 7.2, the clock synchronization between the transmitter and the receiver is assumed, as is in most cases when evaluating the performance of binary modulation techniques [67,12,63].

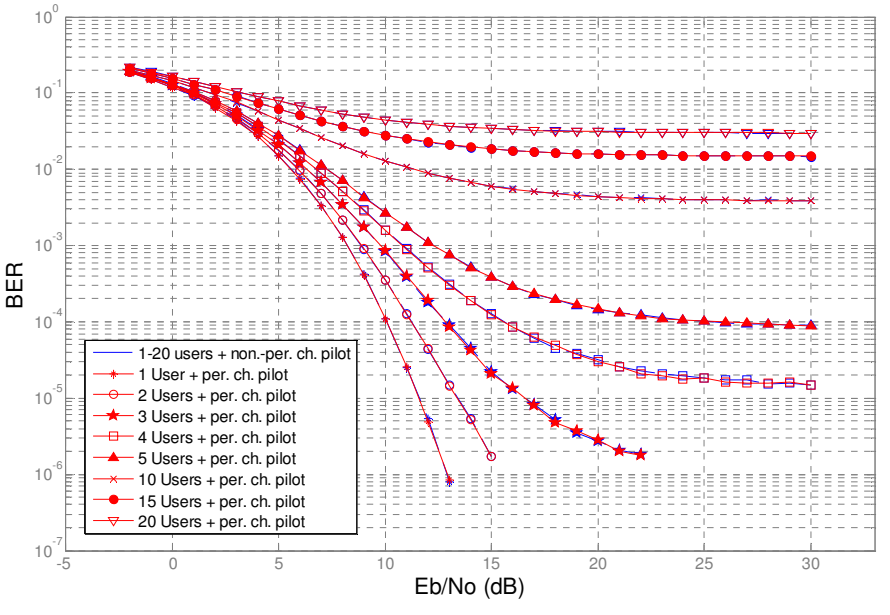


Fig. 7.19 The empirical BER curves of the system of Figure 7.14 when the periodic chaotic pilot signal (solid marked curves) is used, and when the non-periodic chaotic pilot signal (dashed marked curves) is used.

As stated above, the periodic and non-periodic chaotic pilot based CBDS-CDMA systems proposed here exhibit identical behaviour as the periodic PRBS pilot signal based CBDS-CDMA system of section 7.2 [15] at the BER level of 10^{-3} and above. This behaviour is confirmed in Figures 7.20 and 7.21. However, Figures 7.20 and 7.21 also reveal that both periodic and non-periodic chaotic pilot based CBDS-CDMA systems exhibit marginally better performance for a single user plus a chaotic pilot signal than the corresponding PRBS pilot based CBDS-CDMA system at the BER level of 10^{-4} and below. In particular, at the BER level of 10^{-6}, this improvement in performance is approximately equal to 0.175 dB. In other words, for a single user in the system, it requires approximately 0.175 dB more energy per bit to achieve the BER of 10^{-6} using the PRBS pilot based CBDS-CDMA system than the chaotic pilot based CBDS-CDMA systems.

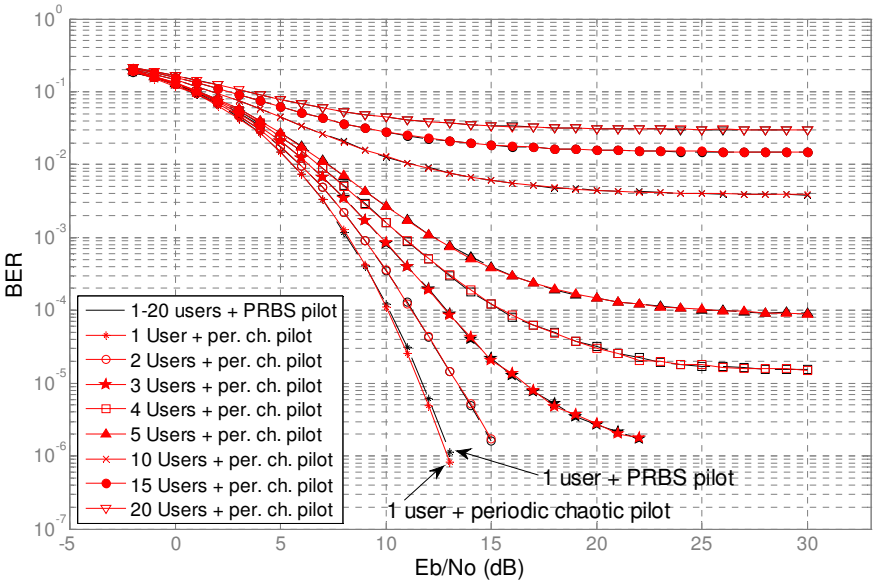


Fig. 7.20 The empirical BER curves of the system of Figure 7.14 when the periodic chaotic pilot signal (solid marked curves) is used, and when the periodic PRBS pilot signal (dashed marked curves) of section 7.3 [15,19] is used.

The BER analysis results for the system of Figure 7.14 in the AWGN and Rayleigh fading channel are shown in Figures 7.22-7.24. As above, the incoming time offset T_d has been uniformly varied within the boundaries of equation 7.4.11. Figure 7.22 shows the empirical BER curves for 1, 5, 10, 15 and 20 users plus the periodic chaotic pilot signal alongside the corresponding theoretical BER curves with perfect synchronization assumed [19]. It can be seen from Figure 7.22 that in the Rayleigh fading channel the system fails to satisfy the maximum

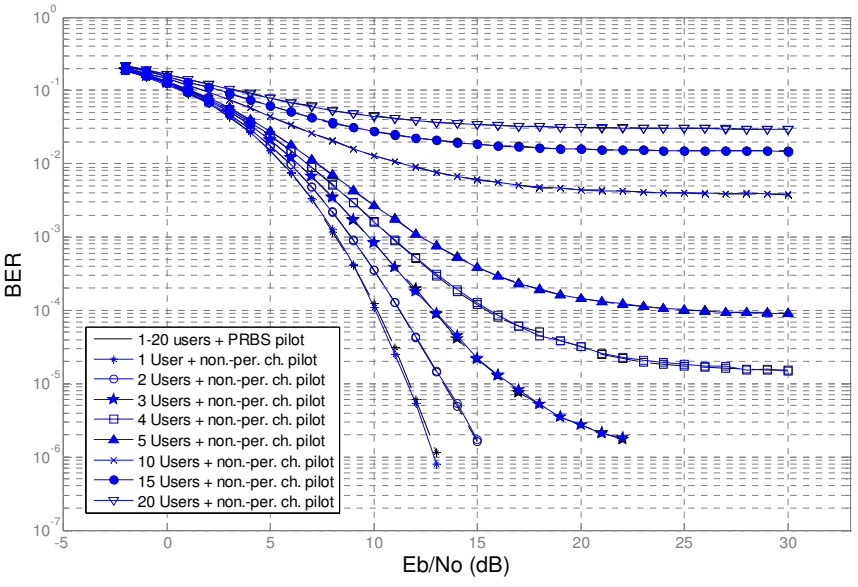


Fig. 7.21 The empirical BER curves of the system of Figure 7.14 when the non-periodic chaotic pilot signal (solid marked curves) is used, and when the periodic PRBS pilot signal (dashed marked curves) of section 7.3 [15,19] is used.

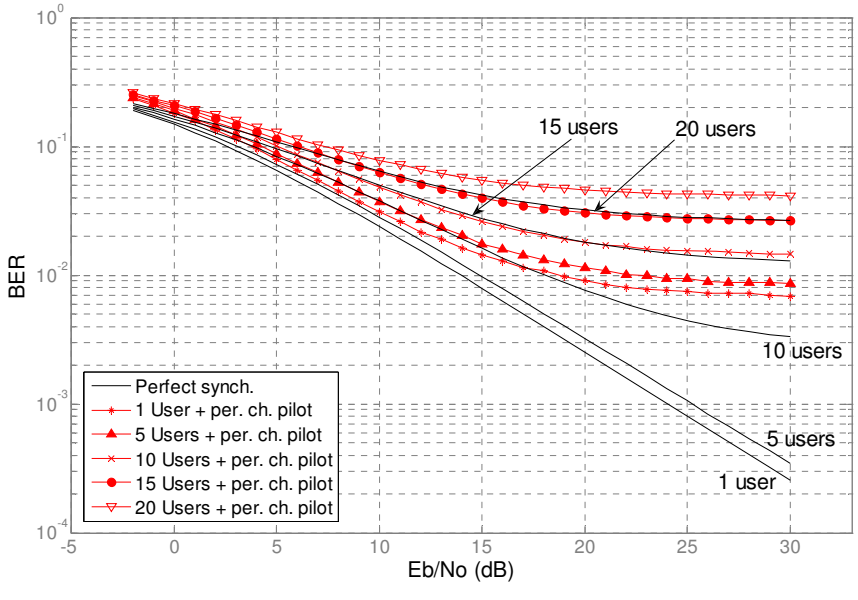


Fig. 7.22 The empirical BER curves of the system of Figure 7.14 in a Rayleigh faded, AWGN channel when the periodic chaotic pilot signal (marked curves) is used. The corresponding theoretical curves with perfect synchronization assumed are shown by unmarked curves.

allowable BER limit of 10^{-3} for any number of users and any E_b / N_o. In Figure 7.23, the corresponding empirical BER curves for the non-periodic chaotic pilot based CBDS-CDMA system are plotted on the same set of axes as the periodic chaotic pilot based CBDS-CDMA system BER curves. It can be observed from Figure 7.23 that the non-periodic chaotic pilot based CBDS-CDMA system exhibits identical behaviour to that of the periodic chaotic pilot based CBDS-CDMA system in the Rayleigh fading channel. Therefore, both chaotic pilot based systems fail to satisfy the maximum allowable BER limit of 10^{-3} for any number of users and any E_b / N_o in the Rayleigh fading channel. Finally, Figure 7.24 shows the corresponding empirical BER curves for the PRBS pilot based CBDS-CDMA system plotted on the same set of axes as the periodic chaotic pilot based CBDS-CDMA system BER curves. It can therefore be observed from Figures 7.23 and 7.24 that both proposed chaotic pilot based CBDS-CDMA systems also match the BER performance of the PRBS pilot based CBDS-CDMA system [19].

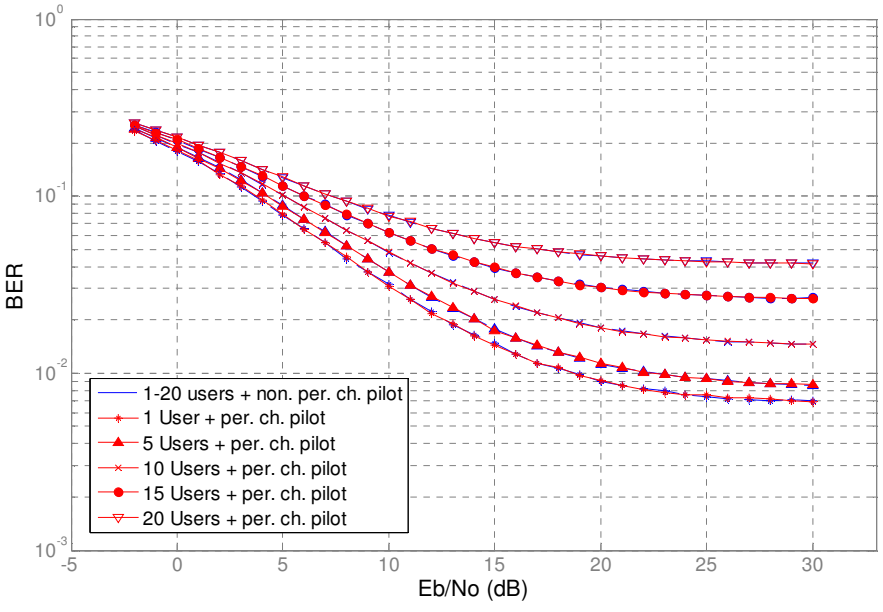


Fig. 7.23 The empirical BER curves of the system of Figure 7.14 in a Rayleigh faded, AWGN channel when the periodic chaotic pilot signal (solid marked curves) is used, and when the non-periodic chaotic pilot signal (dashed marked curves) is used.

In addition, it can be observed from Figures 7.17-7.24 that the systems' performance in the Rayleigh fading channel degrades more significantly when the perfect synchronization is not assumed than when the perfect synchronization is not assumed without Rayleigh fading. Although both chaotic pilot based

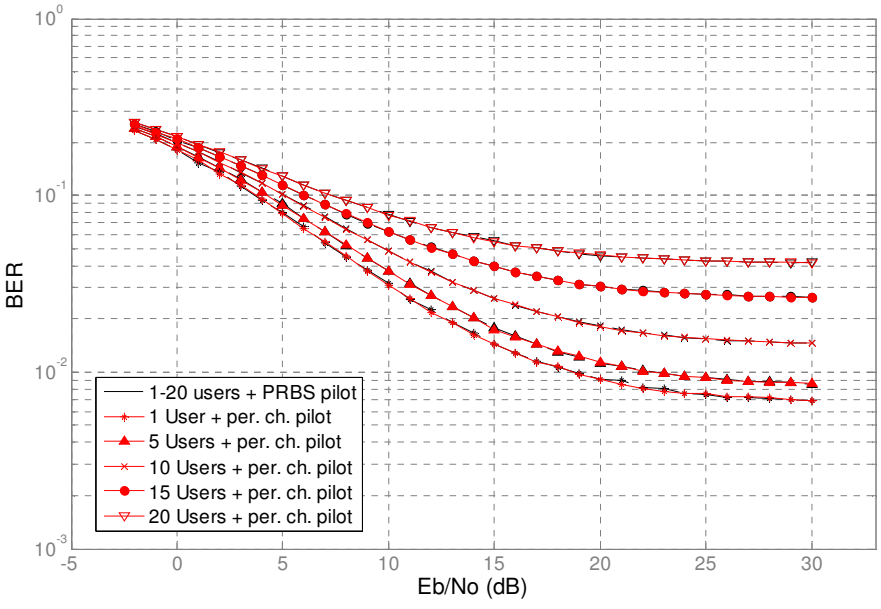


Fig. 7.24 The empirical BER curves of the system of Figure 7.14 in a Rayleigh faded, AWGN channel when the periodic chaotic pilot signal (solid marked curves) is used, and when the periodic PRBS pilot signal (dashed marked curves) of section 7.3 [15,19] is used.

CBDS-CDMA systems satisfy the BER level of 10^{-3} for 1–5 users in an AWGN channel they both fail for all users in the fading channel. Thus, in comparison, the system in the Rayleigh fading channel is not practical for real-world application. To improve the performance in the fading environment, techniques used to disperse bursts of error in time, such as block interleaving [10], could be employed. Furthermore, specialized receiver architectures used to combat fading, such as the rake receiver [10], could also be employed.

7.5 Conclusion

In this chapter, chaotic carriers have been embedded within a practical multi-user DS-CDMA chaotic communication system and its performance evaluated in the presence of noise and interuser interferences. The mutually orthogonal properties between the chaotic time series produced by the logistic map and the PRBS pilot signal have enabled the traditional ideas of the multi-user CDMA sequence synchronization process to be utilized within the multi-user chaos based DS-CDMA (CBDS-CDMA) system. Furthermore, the system has been taken one step further by introducing a chaotic pilot signal in place of the PRBS pilot signal, thus making the CBDS-CDMA system fully chaotic. In this way, the security of CBDS-CDMA systems is significantly improved by eliminating the security threat posed by an inherently different PRBS pilot signal used in the otherwise chaotic

CBDS-CDMA systems. Both phases of the sequence synchronization process, namely the code acquisition and the code tracking, have been proposed and investigated.

The code acquisition phase has been evaluated in terms of the probability of detection and the probability of false alarm at the chip energy to noise power spectral density ratio of -15 dB for the three different pilot signals and varying number of chaotic users in the system. The theoretical upper bound on the probability of detection has been derived and compared to the empirically determined results with the chaotic interferences present. The subsequent empirical curves associated with the increasing number of users in the system have demonstrated the expected degradation in the system performance with the increasing level of interference. In addition, the expected increase of the probability of detection, with the increase in the integration time, has been demonstrated. Furthermore, it has been shown that the best code acquisition performance is achieved when the PRBS is used as the pilot signal as compared to the logistic and Bernoulli chaotic maps.

The mathematical models for the investigation of the code tracking loops have been presented and used to derive the control laws used for the generation of the time offset estimates for PRBS and, periodic and non-periodic chaotic pilot signals. Their validity has then been demonstrated by means of a simulation. The performance of the proposed code tracking circuits has been primarily evaluated in terms of the bit error rate for varying levels of the chaotic interuser interferences, that is, for different numbers of chaotic users in the system. It has been shown that the systems are reasonably robust to noise as compared to the performance under the assumption of perfect synchronization. The overall BER performance degradation in an AWGN channel for a multi-user system is characterised by the flattening of the BER curves at low levels of noise due to the prevailing effects of the interuser interferences.

Furthermore, it has been demonstrated that the CBDS-CDMA communication systems implementing the proposed sequence synchronization schemes, with a single user in the system, in general exhibit better noise performance in terms of the bit error rate than the Pecora – Carroll CS based communication techniques. It was also shown that although the systems are robust to the influence of AWGN and interuser interferences, they all fail to satisfy the maximum allowable bit error rate limit of 10^{-3} in the Rayleigh fading channel, exbhibiting identical BER performance.

Finally, it has been shown that in terms of BER, in the AWGN channel only, the proposed chaotic pilot based CBDS-CDMA systems outperform the PRBS pilot based system for a single user in the system at the BER level of 10^{-4} and below. In particular, an improvement of 0.175 dB has been demonstrated at the BER level of 10^{-6}. Therefore, in addition to the added security, it has been demonstrated that by introducing the chaotic pilot based tracking unit in place of the corresponding PRBS unit makes the CBDS-CDMA system more robust. The BER performance of all systems has been shown to be identical for more than one user in the system.

References

[1] Yamada, T., Fujisaka, H.: Stability Theory of Synchronized Motion in Coupled-Oscillator Systems. II. Progress of Theoretical Physics 70(5), 1240–1248 (1983)

[2] Afraimovich, V.S., Verichev, N.N., Rabinovich, M.I.: Stochastic synchronization of oscillations in dissipative systems. Izvestija Vuzov, Radiofizika 29, 795–803 (1986)

[3] Pecora, L.M., Carroll, T.L.: Synchronization in chaotic systems. Physical Review Letters 64(8), 821–824 (1990)

[4] Murali, K., Lakshmanan, M.: Transmission of signals by synchronization in a chaotic Van der Pol-Duffing oscillator. Physical Review E, Rapid Communications 48(3), R1624–R1626 (1993)

[5] Cuomo, K.M., Oppenheim, A.V.: Circuit Implementation of Synchronized Chaos with Applications to Communications. Physical Review Letters 71(1), 65–68 (1993)

[6] Lu, J., Wu, X., Lü, J.: Synchronization of a unified chaotic system and the application in secure communication. Physics Letters A 305(6), 365–370 (2002)

[7] Pecora, L.M., Carroll, T.L.: Driving systems with chaotic signals. Physical Review A 44(4), 2374–2383 (1991)

[8] Carroll, T.L., Pecora, L.M.: Cascading synchronized chaotic systems. Physica D 67(1-3), 126–140 (1993)

[9] Chua, L.O., Itoh, M., Kocarev, L., Eckert, K.: Chaos synchronization in Chua's circuit. Journal of Circuits, Systems and Computers 3(1), 93–108 (1993)

[10] Lee, J.S., Miller, L.E.: CDMA Systems Engineering Handbook, pp. 18–837. Artech House Publishers, Boston (1998)

[11] Peterson, R.L., Ziemer, R.E., Borth, D.E.: Introduction to Spread Spectrum Communications, pp. 149–495. Prentice Hall, Inc., Upper Saddle River (1995)

[12] Ziemer, R.E., Peterson, R.L.: Introduction to Digital Communication, 2nd edn., pp. 611–615. Prentice Hall, Inc., Upper Saddle River (2001)

[13] Polydoros, A., Weber, C.L.: A Unified Approach to Serial Search Spread-Spectrum Code Acquisition – Part I: General Theory. IEEE Transactions on Communications 32(5), 542–549 (1984)

[14] Polydoros, A., Weber, C.L.: A Unified Approach to Serial Search Spread-Spectrum Code Acquisition – Part II: A Matched – Filter Receiver. IEEE Transactions on Communications Com-32(5), 550–560 (1984)

[15] Jovic, B., Unsworth, C.P., Sandhu, G.S., Berber, S.M.: A robust sequence synchronization unit for multi-user DS-CDMA chaos-based communication systems. Signal Processing 87(7), 1692–1708 (2007)

[16] Hurd, W.J., Anderson, T.O.: Digital Transition Tracking Symbol Synchronizer for LOW SNR Coded Systems. IEEE Transactions on Communications Technology COM-18(2), 141–147 (1970)

[17] Spilker, J.J., Magill, D.T.: The Delay-Lock Discriminator – An Optimum Tracking Device. In: Proceedings of the IRE, vol. 49(9), pp. 1403–1416 (1961)

[18] Nielsen, P.T.: On the Acquisition Behaviour of Binary Delay-Lock Loops. IEEE Transactions on Aerospace and Electronic Systems AES-11(3), 415–418 (1975)

[19] Jovic, B., Unsworth, C.P.: Performance comparison of a multi-user chaos based DS-CDMA synchronisation unit within an AWGN and a Rayleigh fading channel. IET Electronics Letters 43(18), 988–989 (2007)

[20] Davidovici, S., Milstein, L.B., Schilling, D.L.: A New Rapid Acquisition Technique for Direct Sequence Spread-Spectrum Communications. IEEE Transactions on Communications COM-32(11), 1161–1168 (1984)

[21] Polydoros, A., Simon, M.K.: Generalized Serial Search Code Acquisition: The Equivalent Circular State Diagram Approach. IEEE Transactions on Communications COM-32(12), 1260–1268 (1984)

[22] Parlitz, U., Ergezinger, S.: Robust communication based on chaotic spreading sequences. Physics Letters A 188(2), 146–150 (1994)

[23] Heidari-Bateni, G., McGillem, C.D.: A Chaotic Direct-Sequence Spread-Spectrum Communication System. IEEE Transactions on Communications 42(2/3/4), 1524–1527 (1994)

[24] Mazzini, G., Setti, G., Rovatti, R.: Chaotic Complex Spreading Sequences for Asynchronous DS-CDMA – Part I: System Modelling and Results. IEEE Transactions on Circuits and Systems – I: Fundamental Theory and Applications 44(10), 937–947 (1997)

[25] Mazzini, G., Setti, G., Rovatti, R.: Chaotic Complex Spreading Sequences for Asynchronous DS-CDMA – Part II: Some Theoretical Performance Bounds. IEEE Transactions on Circuits and Systems – I: Fundamental Theory and Applications 45(4), 496–506 (1998)

[26] Mazzini, G., Rovatti, R., Setti, G.: Sequence synchronization in chaos – based DS – CDMA systems. In: Proceedings of the 1998 IEEE International Conference on Circuits and Systems (ISCAS 1998), Monterey, CA, May 31- June 3, pp. IV-485–IV-488 (1998)

[27] Setti, G., Rovatti, R., Mazzini, G.: Synchronization Mechanism and Optimization of Spreading Sequences in Chaos-Based DS-CDMA Systems. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences E82-A(9), 1737–1746 (1999)

[28] Mei, W., Li-cheng, J.: A DS – CDMA communication system based on correlation chaotic synchronization. Journal of China Institute of Communications 23(8), 121–127 (2002)

[29] Setti, G., Mazzini, G., Rovatti, R.: Gaussian Characterization of Self-Interference during Synchronization of Chaos Based DS-CDMA Systems. In: Proceedings of the 1998 IEEE International Conference on Electronics, Circuits and Systems (ICECS 1998), Lisboa, Portugal, 7, September 7-10, pp. 231–234 (1998)

[30] Rovatti, R., Setti, G., Mazzini, G.: Statistical Features of Chaotic Maps Related to CDMA Systems Performance. In: Proceedings of the 1998 International Symposium on Mathematical Theory of Networks and Systems (MTNS 1998), Padova, Italy, July 6-10, pp. 385–388 (1998)

[31] Eshima, N., Kohda, T.: Statistical approach to the code acquisition problem in direct-sequence spread-spectrum communication systems. IMA Journal of Mathematical Control and Information 23(2), 149–163 (2006)

[32] Kohda, T., Jitsumatsu, Y., Khan, T.A.: Spread-Spectrum Markovian-Code Acquisition in Asynchronous DS/CDMA Systems. In: Proceedings of the 2003 International Symposium on Circuits and Systems (ISCAS 2003), Bangkok, Thailand, May 25-28, pp. III-750–III-753 (2003)

[33] Jitsumatsu, Y., Kohda, T.: Bit error rate of incompletely synchronised correlator in asynchronous DS/CDMA system using SS Markovian codes. Electronics Letters 38(9), 415–416 (2002)

[34] Eshima, N., Jitsumatsu, Y., Kohda, T.: Markovian SS Codes Imply Inversion-Free Code Acquisition in Asynchronous DS/CDMA Systems. In: Proceedings of the 2004 International Symposium on Circuits and Systems (ISCAS 2004), Bangkok, Thailand, May 23-26, pp. IV-617–IV-620 (2004)

[35] Chen, C.-C., Yao, K.: Design of Spread Spectrum Sequences Using Chaotic Dynamical Systems with Lebesgue Spectrum. In: Proceedings of the 2001 International Symposium on Circuits and Systems (ISCAS 2001), Sydney, Australia, May 6-9, pp. III-149–III-152 (2001)

[36] Fujisaki, H.: On Correlation Values of *M*-Phase Spreading Sequences of Markov Chains. IEEE Transactions on Circuits and Systems – I: Fundamental Theory and Applications 49(12), 1745–1750 (2002)

[37] He, D., Leung, H.: Quasi – Orthogonal Chaotic CDMA Multi – User Detection Using Optimal Chaos Synchronization. IEEE Transactions on Circuits and Systems – II: Express Briefs 52(11), 739–743 (2005)

[38] Rovatti, R., Mazzini, G.: Interference in DS-CDMA systems with exponentially vanishing autocorrelations: Chaos-based spreading is optimal. Electronics Letters 34(20), 1911–1913 (1998)

[39] Rovatti, R., Mazzini, G., Setti, G.: On the Ultimate Limits of Chaos-Based Asynchronous DS-CDMA – I: Basic Definitions and Results. IEEE Transactions on Circuits and Systems – I: Regular Papers 51(7), 1336–1347 (2004)

[40] Rovatti, R., Mazzini, G., Setti, G.: On the Ultimate Limits of Chaos-Based Asynchronous DS-CDMA – II: Analytical Results and Asymptotics. IEEE Transactions on Circuits and Systems – I: Regular Papers 51(7), 1348–1364 (2004)

[41] Mazzini, G., Rovatti, R., Setti, G.: On the Shannon Capacity of Chaos-Based Asynchronous CDMA Systems. In: Proceedings of the 13th International Symposium on Personal, Indoor and Mobile Radio Communications, September 15-18, pp. 2337–2341 (2002)

[42] Mazzini, G., Rovatti, R., Setti, G.: Interference minimisation by auto-correlation shaping in asynchronous DS-CDMA systems: chaos-based spreading is nearly optimal. Electronics Letters 35(13), 1054–1055 (1999)

[43] Rovatti, R., Setti, G., Mazzini, G.: Chaos-Based Spreading Compared to *M*-Sequences and Gold Spreading in Asynchronous CDMA Communication Systems. In: Proceedings of the1997 European Conference on Circuit Theory and Design (ECCTD 1997), Budapest, Hungary, August 30-September 3, pp. 312–317 (1997)

[44] Chen, C.-C., Yao, K., Umeno, K., Biglieri, E.: Design of Spread-Spectrum Sequences Using Chaotic Dynamical Systems and Ergodic Theory. IEEE Transactions on Circuits and Systems – I: Fundamental Theory and Applications 48(9), 1110–1114 (2001)

[45] Fujisaki, H.: On Optimum 3-Phase Spreading Sequences of Simple Markov Chains. In: Proceedings of the 2001 International Symposium on Circuits and Systems (ISCAS 2001), Sydney, Australia, May 6-9, pp. III-229–III-232 (2001)

[46] Penaud, S., Guittard, J., Bouysse, P., Quere, R.: DSP implementation of self-synchronized chaotic encoded decoder. Electronics Letters 36(4), 365–366 (2000)

[47] Hidalgo, R.M., Fernandez, J.G., Rivera, R.R., Larrondo, H.A.: Versatile DSP-based chaotic communication system. Electronics Letters 37(19), 1204–1205 (2001)

[48] Starkov, S.O., Yemetz, S.V.: Digital communication systems, using chaos. In: Proceedings of the 1997 First International Conference on Control of Oscillations and Chaos (COC 1997), St. Petersburg, Russia, August 27-29, pp. 207–210 (1997)

[49] Fleming-Dahl, A.: Chaotic Communications through Arbitrary Attenuation: A Hardware Demonstration. In: Proceedings of the Global Telecommunications Conference (GLOBECOM 2001), San Antonio, TX, November 25-29, pp. 191–196 (2001)

[50] Kamata, H., Endo, T., Ishida, Y.: Secure Communication System Using Chaos via DSP Implementation. In: Proceedings of the 1996 International Symposium on Circuits and Systems (ISCAS 1996), Atlanta, GA, May 12-15, pp. 112–115 (1996)

[51] Lj. Simic, S.: Berber, "Performance Analysis of a Chaos-Based Multi-User Communication System Implemented in DSP Technology". In: Proceedings of the First IEEE International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2006), Sydney, Australia, March 13-16, pp. 1–6 (2006)

[52] Jovic, B., Unsworth, C.P.: Chaos based multi-user time division multiplexing communication system. IET Communications 1(4), 549–555 (2007)

[53] Lau, F.C.M., Tse, C.K.: Chaos-Based Digital Communication Systems, ch. 1, pp. 1–20. Springer, Berlin (2004)

[54] Tam, W.M., Lau, F.C.M., Tse, C.K.: A Multiple Access Scheme for Chaos – Based Digital Communication Systems Utilizing Transmitted Reference. IEEE Transactions on Circuits and Systems – I: Regular Papers 51(9), 1868–1878 (2004)

[55] Tam, W.M., Lau, F.C.M., Tse, C.K., Lawrance, A.J.: Exact Analytical Bit Error Rates for Multiple Access Chaos – Based Communication Systems. IEEE Transactions on Circuits and Systems – II: Express Briefs 51(9), 473–481 (2004)

[56] Sandhu, G.S., Berber, S.M.: Investigation on Orthogonal Signals for Secure Transmission in Multiuser Communication Systems. In: Proceedings of the First IEEE International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2006), Sydney, Australia, March 13-16, pp. 1–6 (2006)

[57] Kennedy, M.P., Kolumban, G., Jako, Z.: Chaotic Modulation Schemes. In: Kennedy, M.P., Rovatti, R., Setti, G. (eds.) Chaotic Electronics in Telecommunications, pp. 163–175. CRC Press LLC, Boca Raton (2000)

[58] Kolumban, G., Kennedy, M.P., Chua, L.O.: The Role of Synchronization in Digital Communications Using Chaos – Part II: Chaotic Modulation and Chaotic Synchronization. IEEE Transactions on Circuits and Systems – I: Fundamental Theory and Applications 45(11), 1129–1140 (1998)

[59] Kolumban, G., Kennedy, M.P., Chua, L.O.: The Role of Synchronization in Digital Communications Using Chaos – Part I: Fundamentals of Digital Communications. IEEE Transactions on Circuits and Systems – I: Fundamental Theory and Applications 44(10), 927–936 (1997)

[60] Kolumban, G., Kennedy, M.P.: The Role of Synchronization in Digital Communications Using Chaos – Part III: Performance Bounds for Correlation Receivers. IEEE Transactions on Circuits and Systems – I: Fundamental Theory and Applications 47(12), 1673–1683 (2000)

[61] Lau, F.C.M., Tse, C.K.: Optimum correlator-type receiver design for CSK communication systems. International Journal of Bifurcation and Chaos 12(5), 1029–1038 (2002)

[62] Zhou, C.S., Chen, T.L.: Extracting information masked by chaos and contaminated with noise: Some considerations on the security of communication approaches using chaos. Physics Letters A 234(6), 429–435 (1997)

[63] Jovic, B., Berber, S., Unsworth, C.P.: A novel mathematical analysis for predicting master – slave synchronization for the simplest quadratic chaotic flow and Ueda chaotic system with application to communications. Physica D 213(1), 31–50 (2006)

[64] Berber, S.M., Jovic, B.: Sequence Synchronization in a Wideband CDMA System. In: Proceedings of the First IEEE International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2006), Sydney, Australia, March 13-16, pp. 1–6 (2006)
[65] Oh, H.-S., Han, D.-S.: An adaptive double – dwell PN code acquisition system in DS – CDMA communications. Signal Processing 85(6), 2327–2337 (2005)
[66] Hanzo, L., Yang, L.-L., Kuan, E.-L., Yen, K.: Single – and Multi – Carrier DS – CDMA Multi – User Detection, Space – Time Spreading, Synchronisation and Standards, pp. 754–772. IEEE press and Wiley, Chichester (2003)
[67] Carroll, T.L., Pecora, L.M.: Using multiple attractor chaotic systems for communication. Chaos 9(2), 445–451 (1999)
[68] Palmore, J., Herring, C.: Computer Arithmetic, Chaos and Fractals. Physica D 42(1-3), 99–110 (1990)
[69] Giger, A.J., Barnett, W.T.: Effects of Multipath Propagation on Digital Radio. IEEE Transactions on Communications COM-29(9), 1345–1352 (1981)
[70] Wehinger, J., Mecklenbrauker, C.F.: Iterative CDMA Multiuser Receiver With Soft Decision-Directed Channel Estimation. IEEE Transactions on Signal Processing 54(10), 3922–3934 (2006)
[71] Jovic, B., Unsworth, C.P., Berber, S.M.: De-noising 'Initial Condition Modulation' Wideband Chaotic Communication Systems with Linear & Wavelet Filters. In: Proceedings of the First IEEE International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2006), Sydney, Australia, March 13-16, pp. 1–6 (2006)
[72] Jovic, B., Unsworth, C.P.: Synchronization of Chaotic Communication Systems. In: Wang, C.W. (ed.) Nonlinear Phenomena Research Perspectives, Nova Publishers, New York (2007)
[73] Rappaport, T.S.: Wireless Communications Principles and Practice, pp. 172–188. Prentice Hall, Inc., Upper Saddle River (1996)
[74] Smith, J.I.: A Computer Generated Multipath Fading Simulation for Mobile Radio. IEEE Transactions on Vehicular Technology VT-24(3), 39–40 (1975)
[75] Arredondo, G.A., Chriss, W.H., Walker, E.H.: A Multipath Fading Simulator for Mobile Radio. IEEE Transactions on Communications COM-21(11), 1325–1328 (1973)

Chapter 8
Chaos Based Multi-user TDM Communication System

This chapter proposes a chaos based multi-user time division multiplexing (TDM) communication system. Its performance is compared to the performance of chaos based direct sequence code division multiple access (DS-CDMA) system in the noisy and Rayleigh fading channels. Initially, the benchmark performance of the systems is investigated in terms of the bit error rate under the assumption of perfect synchronization. The chaotic spreading signals, used to encrypt the binary messages, are generated using the logistic map. The degradation in performance of the systems in the Rayleigh fading channel as compared to the noisy channel is demonstrated. Furthermore, it is shown that in both noisy and Rayleigh fading channels the chaos based multi-user TDM system outperforms the chaos based DS-CDMA system for a larger number of users in the system, while the chaos based DS-CDMA system yields better performance for low number of users in the system. The sequence synchronization unit of chapter 7 is then adapted for the use within the proposed chaos based multi-user TDM communication system and its performance investigated without assuming perfect sequence synchronization. Again, it is shown that the chaos based TDM system outperforms the chaos based DS-CDMA system in the AWGN channel for a larger number of users and vice-versa for low number of users in the system. As for the chaos based DS-CDMA system, it is shown that the proposed chaos based TDM system fails in the Rayleigh fading channel when perfect sequence synchronization is not assumed. To obtain the full characterization of the system, the sequence synchronization is also assumed with the PRBS pilot signal present on top of each signal. The effect of the pilot signal on the performance of the system is thus demonstrated in AWGN and Rayleigh fading channels. Finally, a generalized TDM chaotic communication system, which does not assume perfect synchronization, is proposed and investigated when there is more than one DS-CDMA user per TDM branch in the AWGN channel. In this way, it is shown that allocating more than one DS-CDMA user per TDM branch yields a better BER performance while at the same time increasing the total number of users.

As shown in chapter 6, in many cases when studying chaotic communication systems only single user systems are considered [1-6]. Alternatively, multi-user

B. Jovic: Synchronization Techniques for Chaotic Commun. Syst., SCT 5, pp. 229 – 256.
springerlink.com

chaotic communication techniques, based on the DS-CDMA principle, have been studied in [7-14], demonstrating their robust nature to noise. However, these systems suffer from the inevitable interuser interference which causes the degradation in the bit error rate (BER) performance for a large number of users in the system.

In contrast to chaos based DS-CDMA, chaos based time division multiplexing (TDM) systems do not suffer from interuser interference, when one assumes perfect synchronization between the transmitter and the receiver. Chaos based TDM systems have been investigated in [15-21]. The principles of TDM from a viewpoint of the chaos based spread spectrum communication systems have been discussed in [15]. The synchronization among the multiplexing and de-multiplexing switches of the transmitter and the receiver has been considered and the method of achieving synchronization proposed [15]. In this method, the high frequency signal for rotating the switch is extracted by applying the received chaotic sequence to high pass or bandpass filters. Based on this method, the multi-user chaos based TDM system was proposed in [16,17]. The system was investigated for the two user case using the Pecora-Carroll (PC) self synchronizing properties of the Chua master-slave systems. In [19,20], a chaotic communication scheme based on the principles of chaotic masking was investigated and the possibility of constructing a time division multiple access (TDMA) secure communication system based on this scheme was suggested.

In this chapter, a chaos based TDM technique is proposed and used to transmit the information of multiple users across the same channel [14]. The work presented here is in contrast to [15-21], where the PC synchronization principle is used to encode and decode information. Instead, here the information is encoded and decoded using a correlator transceiver as used in DS-CDMA systems. Synchronization among the spreading sequences between the transmitter and the receiver is initially assumed and the benchmark performance of the system is obtained in terms of the BER curves. It is demonstrated in terms of BER that the chaos based TDM system proposed outperforms the chaos based DS-CDMA system [7,12] for a large number of users in the system in both additive white Gaussian noise (AWGN) and Rayleigh fading channels. Following this, the proposed chaos based TDM system is investigated without the assumption of perfect sequence synchronization in AWGN and Rayleigh fading channels. Again, it is shown that in terms of BER it outperforms the chaos based DS-CDMA system for a large number of users in the system whilst it is outperformed for low number of users in the system. It is also shown that both chaos based TDM and chaos based DS-CDMA systems are insufficiently robust in the Rayleigh fading channel when perfect sequence synchronization is not assumed. Finally, a generalized TDM communication system with more than one DS-CDMA user per TDM branch is proposed and evaluated in the AWGN channel. In this way, the bandwidth efficiency of a DS-CDMA system is combined with the interuser

interference immunity of a TDM system, to allow for an increased number of users in the system while improving the BER performance.

Section 8.1, proposes and presents a chaos based multi-user TDM system under the assumption of perfect sequence synchronization. The principles of operation of the system are explained and its performance evaluated in the AWGN and Rayleigh fading channels. The performance of the system is then compared to that of the DS-CDMA system, demonstrating the superior performance of the TDM system for a large number of users in the system. Section 8.2, evaluates the performance of the TDM system of Section 8.1 without assuming perfect sequence synchronization. Its performance superiority over the corresponding DS-CDMA system is again demonstrated for a large number of users in the system. Finally, a generalized chaos based TDM system is proposed and investigated in the AWGN channel in Section 8.3. It is shown that its bandwidth efficiency and interuser interference immunity, allow for an increased number of users in the system, while improving the BER performance.

8.1 Chaos Based TDM Communication System with Perfect Sequence Synchronization Assumed

In this section, the chaos based TDM communication system is proposed and evaluated in terms of BER in the presence of AWGN, interuser interferences and Rayleigh fading. Its performance is evaluated under the assumption of perfect synchronization within the system.

8.1.1 Chaos Based TDM Communication System

The proposed chaos based TDM communication system with the correlator transceiver is shown in Figure 8.1 [14].

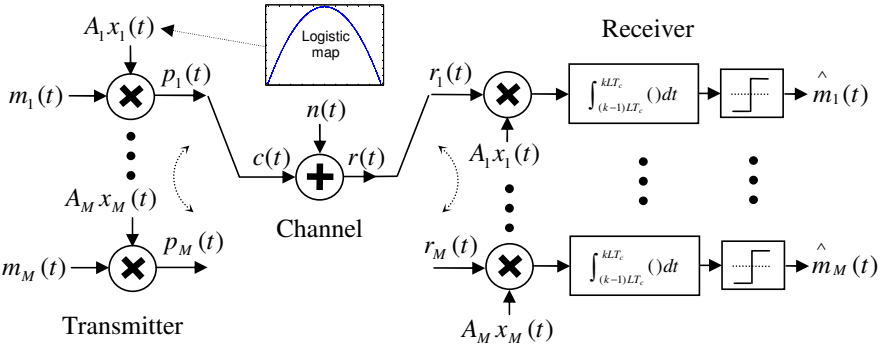


Fig. 8.1 The chaos based TDM communication system

In Figure 8.1, $x(t)$ denotes the chaotic spreading signals which are multiplied by the binary message signals $m(t)$. The products $p(t)$ are then multiplexed to produce the signal $c(t)$ which is transmitted through the channel. As in chapter 7, in order for the spreading waveform generator at the receiver to produce punctual despreading codes the initial conditions of the spreading codes of each of the M users at the transmitter must be available to it. Provided that the chaotic generator at the receiver is identical to that of the transmitter, the initial conditions provide sufficient information to readily regenerate chaotic sequences at the receiver. The received signal $r(t)$ is then de-multiplexed and correlated with the punctual despreading codes. Provided that the power of the noise in the system is low compared to the power of the signal, the correlation value produced at the output of each correlator is positive if the bit is 1, denoted by $m(t) = 1$, is transmitted and negative if the bit is 0, denoted by $m(t) = -1$, is transmitted [7]. As in chapter 7, the chaotic spreading signals have been generated using the logistic map time series of equation 2.1.5, repeated below for convenience as equation 8.1.1 [7]:

$$X_{n+1} = 1 - 2X_n^2 \tag{8.1.1}$$

The logistic map time series is shown in phase-space [22] in Figure 8.1.

The multiplexing, or interleaving, operation at the transmitter side of Figure 8.1 can be represented by equation 8.1.2:

$$c(t) = \sum_{i=1}^{M} p_i(t) \tag{8.1.2}$$

where:

$$p_i(t) = m_i(t)\, A_i x_i(t) = \sum_{j=1}^{L} p_{i\,t}\, \delta(t - M(j-1) - i) \tag{8.1.3}$$

In equation 8.1.3 $\delta(t)$ is the impulse function and L is the spreading factor, that is, the number of chaotic points representing a single bit [6].

The received signal $r(t)$ is represented by equation 8.1.4:

$$r(t) = c(t) + n(t) \tag{8.1.4}$$

where:

$$n(t) = \sum_{i=1}^{M} \sum_{j=1}^{L} n_{i\,t}\, \delta(t - M(j-1) - i) \tag{8.1.5}$$

The individual, de-multiplexed, signals of each of the M users can then be represented by equation 8.1.6:

$$r_i(t) = p_i(t) + n_i(t) = \sum_{j=1}^{L} (p_{i\,t} + n_{i\,t})\, \delta(t - M(j-1) - i) \tag{8.1.6}$$

The received message is recovered by first despreading and then correlating the incoming de-multiplexed received signals by the basis function copy at the receiver, as described by equation 8.1.7:

$$\begin{aligned}\hat{m}_i(t) &= \mathrm{T_h}\left[\int_{(k-1)LT_c}^{kLT_c} r_i(t)\,A_i x_i(t)\,dt\right] \\ &= \mathrm{T_h}\left[\int_{(k-1)LT_c}^{kLT_c} \left\{m_i(t)\,A_i x_i(t) + n_i(t)\right\}\cdot A_i x_i(t)\,dt\right] \\ &= \mathrm{T_h}\left[\int_{(k-1)LT_c}^{kLT_c} m_i(t)\,A_i^2 x_i^2(t)\,dt + \int_{(k-1)LT_c}^{kLT_c} n_i(t) A_i x_i(t)\,dt\right]\end{aligned} \tag{8.1.7}$$

where $\mathrm{T_h}[\ ]$ is the signum function which denotes the thresholding operation and assigns either a -1 or a 1 depending on whether the value in the brackets is negative or positive, respectively [14,23]. If the value in the brackets is equal to zero, the receiver makes a random guess in favour of -1 or 1 [24].

Since the chaotic spreading sequences produced by the logistic map for different initial conditions are highly orthogonal to each other, demonstrated by near zero cross correlation and high autocorrelation in Figures 2.14a and 2.14b, equations 8.1.8a and 8.1.8b hold:

$$\int_{(k-1)LT_c}^{kLT_c} m_i(t)\,A_i^2 x_i^2(t)\,dt > 0 \qquad if \quad m_i(t) = 1 \tag{8.1.8a}$$

$$\int_{(k-1)LT_c}^{kLT_c} m_i(t)\,A_i^2 x_i^2(t)\,dt < 0 \qquad if \quad m_i(t) = -1 \tag{8.1.8b}$$

Provided that the power of noise in the system is comparatively low to the power of the signal causes the noise affected term of equation 8.1.7 to be approximately equal to zero, that is: $\int_{(k-1)LT_c}^{kLT_c} n_i(t) A_i x_i(t)\,dt \approx 0$, so that equation 8.1.7 takes on the form of equations 8.1.9a and 8.1.9b:

$$\hat{m}_i(t) = 1 \qquad if \quad m_i(t) = 1 \tag{8.1.9a}$$

$$\hat{m}_i(t) = -1 \qquad if \quad m_i(t) = -1 \tag{8.1.9b}$$

The bit error rate numerical simulation results of the system of Figure 8.1 are presented for 1-5, 10, 15 and 20 users in Figure 8.2 in the additive white Gaussian noise (AWGN) channel. As in the evaluation of most binary modulation techniques, clock synchronization between the transmitter and the receiver is assumed [25,6]. Also, in order to evaluate the benchmark performance of the system, synchronization among the multiplexing and de-multiplexing switches, as well as the sequence synchronization among the spreading and despreading sequences at the transmitter and the receiver are assumed.

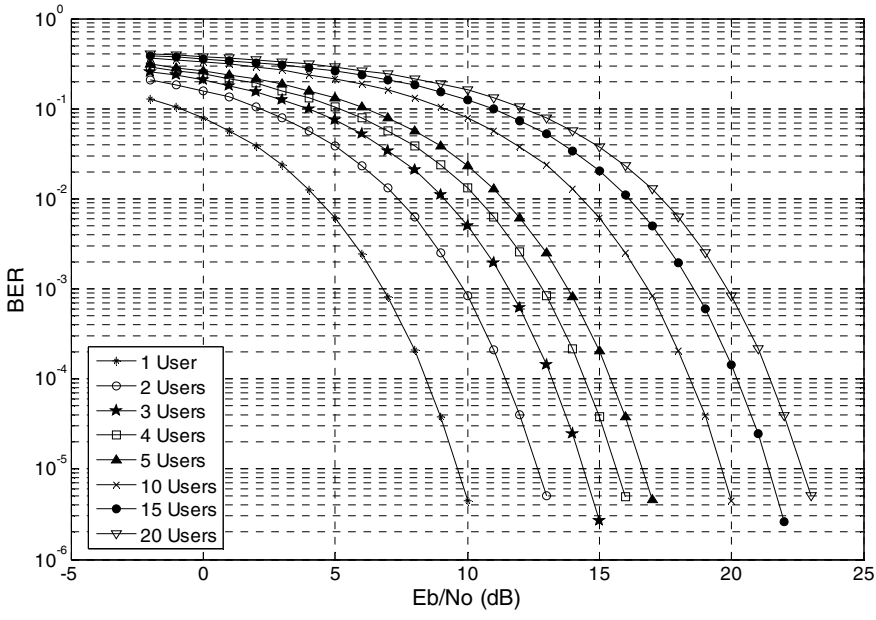


Fig. 8.2 The empirical BER curves of the chaos based TDM system of Figure 8.1 for 1-5, 10, 15 and 20 users

By assuming that the highest acceptable level of BER equals 10^{-3} [26,27], it can be observed from Figure 8.2 that the bit energy to noise power spectral density ratio, E_b / N_o, for which the system performance is satisfactory for the case of 1, 2, 3, 4, 5, 10, 15 and 20 users is equal to approximately 7, 10, 12, 13, 14, 17, 18.5 and 20 dB, respectively. In mobile communications the BER level of 10^{-3} is often used as the target BER [26,27].

8.1.2 Performance Comparison of the Chaos Based TDM to the Chaos Based DS-CDMA System in an AWGN Channel

The chaos based DS-CDMA communication system of [7] with perfect synchronization assumed is shown in Figure 2.15 of chapter 2 [14]. As for the chaos based TDM system of Figure 8.1, the logistic map chaotic signals have been used within the chaos based DS-CDMA system of Figure 2.15 for spreading and despreading.

The bit error rate numerical simulation results of the chaos based TDM system of Figure 8.1, are compared to those of the chaos based DS-CDMA system of Figure 2.15, for 1-5, 10, 15 and 20 users in Figure 8.3 in the AWGN channel.

It can be observed from Figure 8.3 that the E_b / N_o ratio for which the system performance is satisfactory for the case of 1, 2, 3, 4, and 5 users is equal to

approximately 7, 7.5, 8, 9 and 10 dB, respectively. In the case of 10, 15 and 20 users the BER curves flatten, due to the prevailing interuser interferences, before reaching the BER level of 10^{-3}. This is unacceptable in practice [26,27]. In contrast to this, the corresponding BER curves of the chaos based TDM system do not flatten as can be observed from Figure 8.3. Therefore, for a larger number of users, the chaos based TDM system outperforms the chaos based DS-CDMA system. However, for the low number of users, it can be observed from Figure 8.3 that the chaos based DS-CDMA system outperforms the chaos based TDM system at the BER level of 10^{-3}.

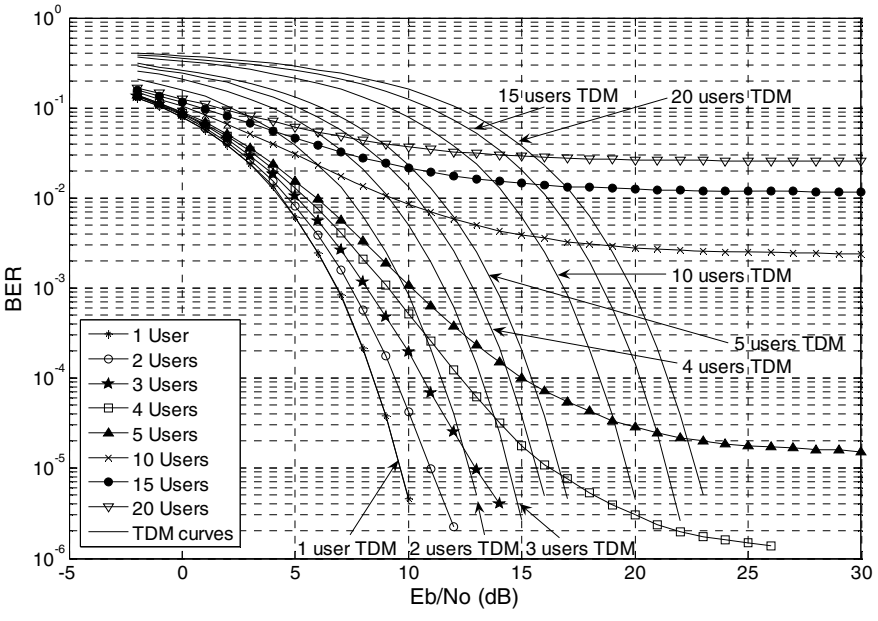


Fig. 8.3 The empirical BER curves of the chaos based DS-CDMA system of Figure 2.15 for 1-5, 10, 15 and 20 users (marked curves), alongside the corresponding empirical BER curves of the chaos based TDM system of Figure 8.1 (unmarked curves).

One of the main characteristics of the DS-CDMA systems is that they are bandwidth efficient and that they offer increased security of transmission [7,24]. However, as seen from Figure 8.3, they suffer from interuser interference which gets more significant for the large number of users. On the other hand, a TDM system does not in general suffer from the interuser interferences, (assuming perfect synchronization), due to the fact that it assigns different time slots to different users [28,29]. However, this characteristic of TDM systems also makes them inefficient of bandwidth, as with each new user introduced into the system the bandwidth inevitably increases. This is because the scheme must squeeze *M* samples derived from *M* independent message sources into a time slot equal to one sampling interval [24]. The purpose of introducing the chaos based TDM system is to eliminate the interuser interference, at the expense of the increased

bandwidth, while still maintaining the security of transmission. Due to the increase in bandwidth, for an increased number of users in the TDM system, the BER performance degrades. The BER performance of a multi-user TDM system can be improved to equal that of a single-user TDM BER performance by increasing the power of each TDM user. However, in the case of the TDM system proposed here the power has been kept constant. The reason for this somewhat unconventional approach is to allow one to directly compare the TDM BER performance to that of the chaos based DS-CDMA system. To this effect, in the case of the multi-user TDM system proposed, E_b denotes the bit power in the BER curves presented. It should be noted, however, that in a real world TDM system the power would be increased to adjust all the multi-user BER curves to the BER curves of the single-user TDM system.

Due to their security of transmission, the chaos based TDM and DS-CDMA systems of subsections 8.1.1 and 2.3.2, respectively, may find applicability in the areas such as mobile military communications [14].

8.1.3 Performance of the Chaos Based TDM System in a Rayleigh Fading Channel

To determine the impact of flat fading on the received signal, the transmitted signal of Figure 8.1 is multiplied by a fading envelope $r_n(t)$. The chaos based TDM system in the Rayleigh fading channel is presented in Figure 8.4 [14].

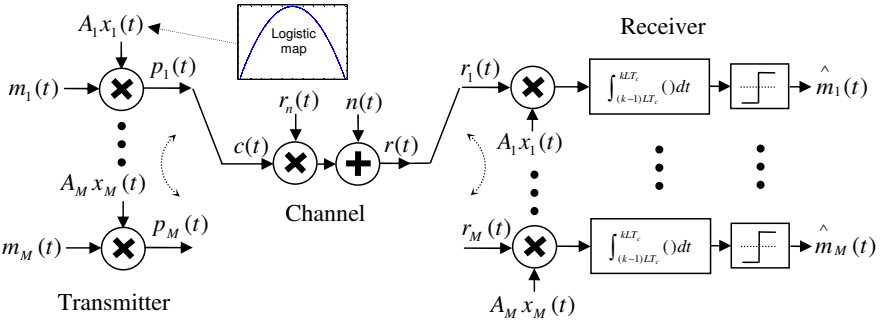


Fig. 8.4 The chaos based TDM communication system in the Rayleigh fading channel

The bit error rate numerical simulation results of the chaos based TDM system of Figure 8.4 for 1-5, 10, 15 and 20 users in the Rayleigh fading channel are shown in Figure 8.5. For comparison, the corresponding curves of the chaos based TDM system in the AWGN channel only are also presented. As in chapter 7, the Rayleigh fading envelope, $r_n(t)$, was generated for the velocity of the receiver relative to the transmitter of 55 km/h and the carrier frequency of 900 MHz [30,31] with $P_r = 1\,\mathrm{W}$.

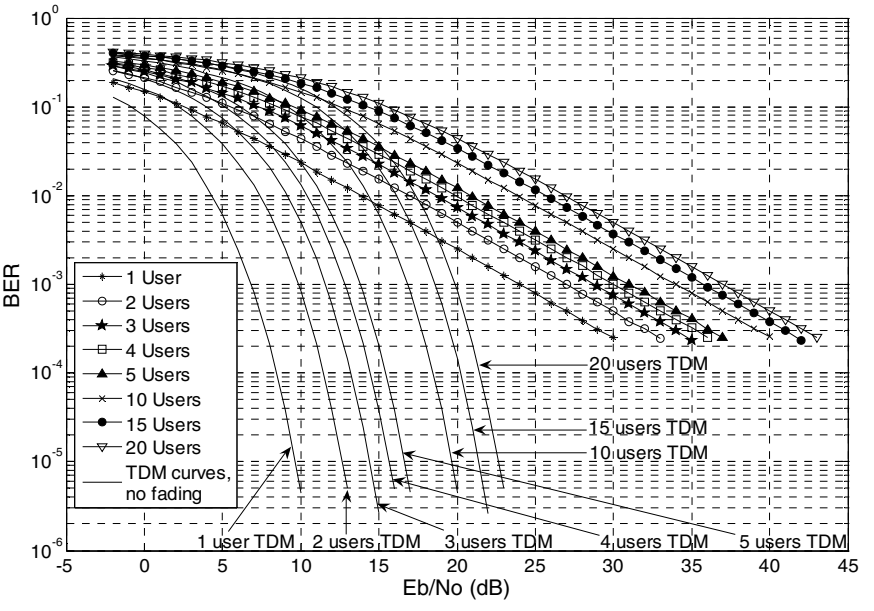


Fig. 8.5 The empirical BER curves of the chaos based TDM system of Figure 8.4 for 1-5, 10, 15 and 20 users (marked curves), alongside the corresponding empirical BER curves of the chaos based TDM system of Figure 8.1 (unmarked curves).

It can be observed in Figure 8.5, that the E_b / N_o for which the system performance is satisfactory for the case of 1, 2, 3, 4, 5, 10, 15 and 20 users is equal to approximately 24, 27, 29, 30, 31, 34, 36 and 37 dB, respectively. By comparing the BER curves of the systems a significant degradation in performance can be observed from Figure 8.5 when the Rayleigh fading is present in the channel.

8.1.4 Performance Comparison of the Chaos Based TDM to the Chaos Based DS-CDMA System in a Rayleigh Fading Channel

The chaos based DS-CDMA system in the Rayleigh fading channel with perfect synchronization assumed is presented in Figure 8.6 [14].

The bit error rate numerical simulation results of the system of Figure 8.6 are presented for 1, 5, 10, 15 and 20 users in Figure 8.7 in the Rayleigh fading channel. Again, the Rayleigh fading envelope, $r_n(t)$, was generated for the velocity of the receiver relative to the transmitter of 55 km/h and the carrier frequency of 900 MHz [30,31] with $P_r = 1\,\mathrm{W}$.

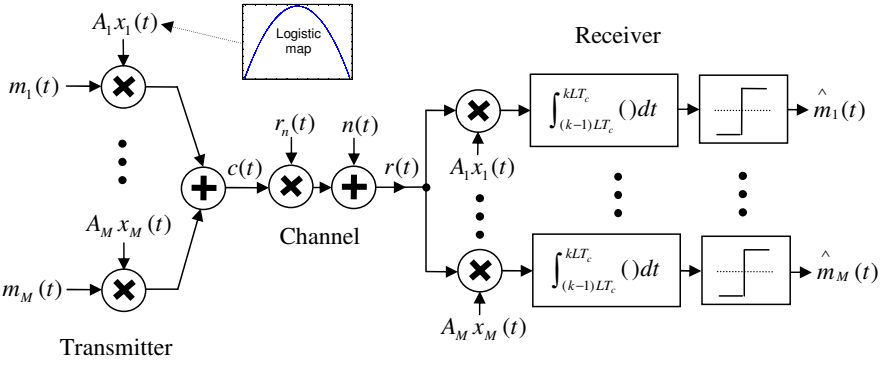


Fig. 8.6 The chaos based DS-CDMA communication system in the Rayleigh fading channel

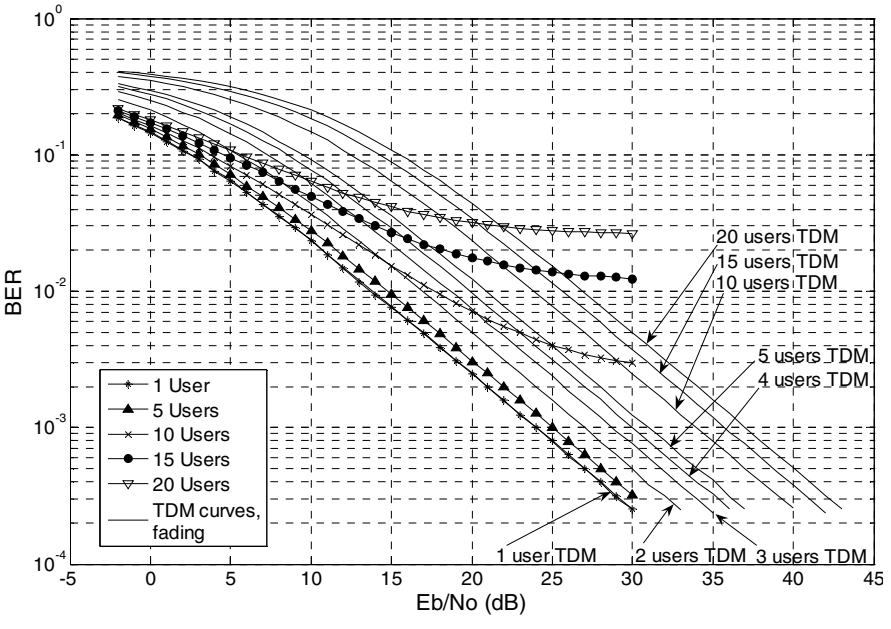


Fig. 8.7. The empirical BER curves of the chaos based DS-CDMA system of Figure 8.6 for 1, 5, 10, 15 and 20 users (marked curves), alongside the corresponding empirical BER curves of the chaos based TDM system of Figure 8.4 (unmarked curves).

It can be observed from Figure 8.7 that the E_b / N_o ratio for which the system performance is satisfactory for the case of 1-5 users is equal to approximately 24-25 dB. In the case of 10, 15 and 20 users the BER curves flatten before reaching the BER level of 10^{-3}. This is unacceptable in practice [26,27]. In contrast to

this, the corresponding BER curves of the chaos based TDM system do not flatten as can be observed from Figure 8.7. Therefore, for a larger number of users, the chaos based TDM system outperforms the chaos based DS-CDMA system in the Rayleigh fading channel from the respect of the BER curves. However, for the case of 1-5 users, it can be observed from Figure 8.7 that in the Rayleigh fading channel the chaos based DS-CDMA system outperforms the chaos based TDM system at the BER level of 10^{-3}.

8.2 Chaos Based TDM Communication System without Assuming Perfect Sequence Synchronization

In this section, the sequence synchronization unit of chapter 7 is incorporated into the chaos based TDM system. The performance of the chaos based TDM communication system is thus evaluated without assuming perfect sequence synchronization. As in the previous sections the performance is evaluated in terms of BER in the presence of AWGN, interuser interferences and Rayleigh fading.

8.2.1 Chaos Based TDM Communication System with the Sequence Synchronization Unit

The chaos based TDM communication system of subsection 8.1.1 with the sequence synchronization unit of chapter 7 incorporated is proposed in Figure 8.8.

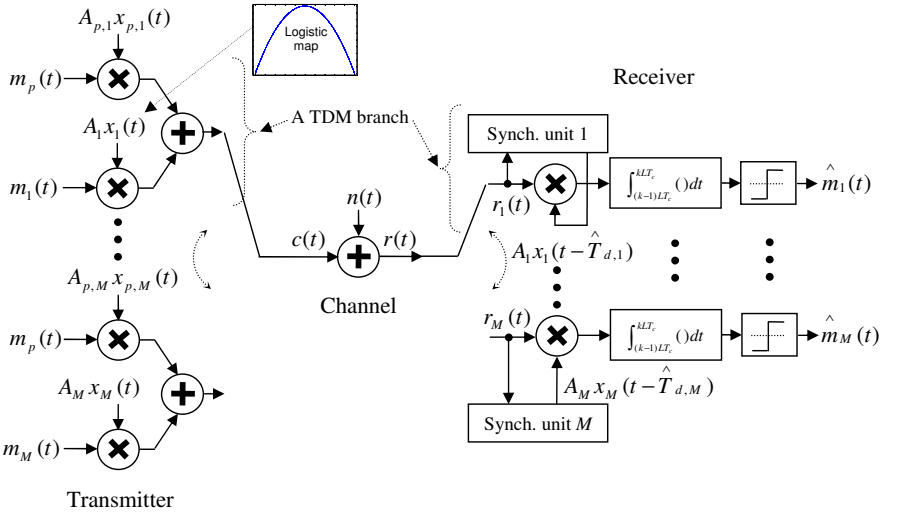


Fig. 8.8 The chaos based TDM communication system with the pilot signals and the sequence synchronization unit

In Figure 8.8, $x(t)$ denotes the logistic map chaotic spreading signals which are multiplied by the binary message signals $m(t)$. In each TDM branch a unique PRBS pilot signal, $x_p(t)$, is introduced for synchronization purposes. The pilot signals are multiplied by $m_p(t)$ which are set at 1 for all time [13,30]. The two products are then summed and multiplexed with the products of the other TDM branches to produce the signal $c(t)$ which is transmitted through the channel. The received signal $r(t)$ is then de-multiplexed and fed into the M separate sequence synchronization units at the receiver. As in chapter 7, the sequence synchronization unit generates the punctual despreading code. The block diagram illustrating a sequence synchronization unit of Figure 8.8 is shown in Figure 8.9.

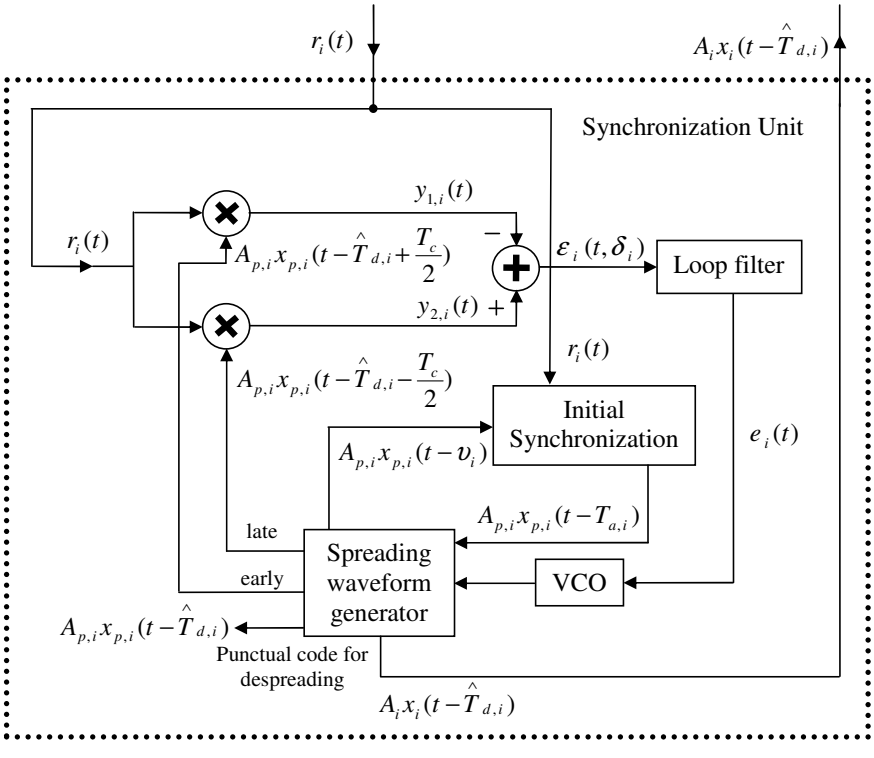


Fig. 8.9 The architecture of the sequence synchronization unit for each of the M users of Figure 8.8, where $\delta_i = (T_{d,i} - \hat{T}_{d,i})/T_c$.

In the case of Figure 8.8, it is assumed that each of the de-multiplexed signals, $r_i(t)$, has its own independent time offset $T_{d,i}$. Therefore, in contrast to the DS-CDMA system of chapter 7, each synchronization unit of Figure 8.8, that is, Figure 8.9, produces a unique time offset estimate $\hat{T}_{d,i}$ for each TDM branch.

With the synchronization within each TDM branch at the receiver achieved, the correlation process takes place.

Provided that the synchronization is accurate and that the power of the noise in the system is low compared to the power of the signal, the correlation value produced at the output of each correlator is positive if the bit is 1, denoted by $m(t) = 1$, is transmitted and negative if the bit is 0, denoted by $m(t) = -1$, is transmitted [7].

The bit error rate numerical simulation results of the system of Figure 8.8 are presented for 1-5, 10, 15 and 20 users in Figure 8.10 in the additive white Gaussian noise (AWGN) channel. In addition, the corresponding empirical BER curves of the system of Figure 8.1, where the perfect synchronization is assumed, are plotted for comparison. An expected degradation in performance can be observed from Figure 8.10 when perfect synchronization is not assumed. Again, as in the evaluation of most binary modulation techniques, clock synchronization between the transmitter and the receiver is assumed [25,6]. Also, synchronization among the multiplexing and de-multiplexing switches at the transmitter and the receiver is assumed.

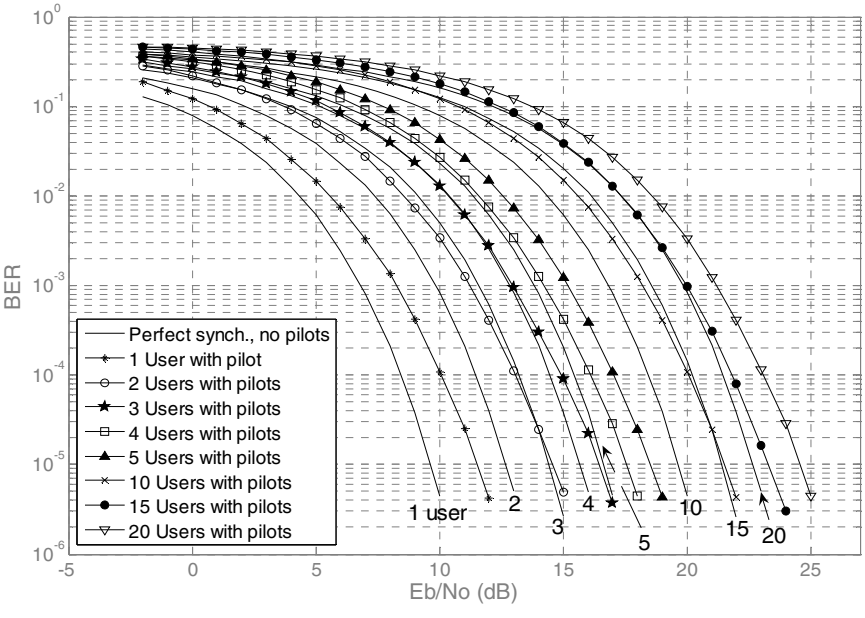


Fig. 8.10 The empirical BER curves of the chaos based TDM system of Figure 8.8 for 1-5, 10, 15 and 20 users (marked curves). The corresponding empirical BER curves of Figure 8.2 with perfect synchronization assumed are shown by unmarked curves.

Again, by assuming that the highest acceptable level of BER equals 10^{-3} [26,27], it can be observed from Figure 8.10 that the E_b / N_o ratio for which the system performance is satisfactory for the case of 1, 2, 3, 4, 5, 10, 15 and 20 users is equal to approximately 8, 11, 13, 14, 15, 18, 20 and 21 dB, respectively.

Therefore, as compared to the perfect synchronization BER curves, it can be observed from Figure 8.10 that at the BER level of 10^{-3} a constant degradation of approximately 1 dB occurs in each case.

The effect of the sequence synchronization error only on the BER performance of the system of Figure 8.8 is now illustrated. This is achieved by assuming perfect sequence synchronization while still keeping the pilot signals within the system of Figure 8.8. The BER curves of the system of Figure 8.8 with the pilot signals intact, but with the perfect sequence synchronization assumed at the receiver, are shown in Figure 8.11.

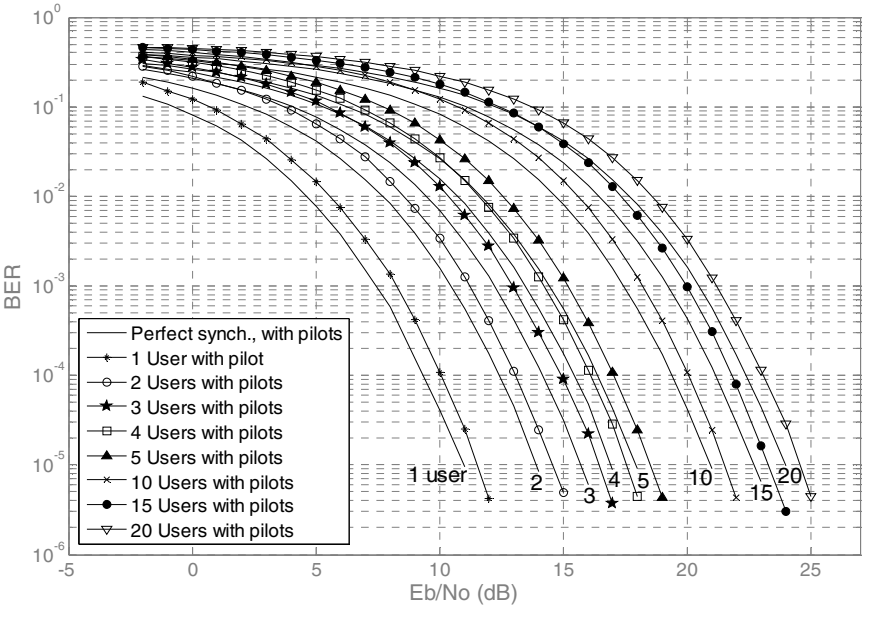


Fig. 8.11 The empirical BER curves of the chaos based TDM system of Figure 8.8 for 1-5, 10, 15 and 20 users (marked curves). The corresponding empirical BER curves of the chaos based TDM system of Figure 8.8, but with perfect synchronization assumed and the pilot signals intact, are shown by unmarked curves.

It can be observed from Figure 8.11 that at the BER level of 10^{-3} the degradation in performance is equal to approximately 0.75 dB in each case. However, by careful observation of Figures 8.10 and 8.11 one can see that as the E_b / N_o increases the corresponding BER curves of Figure 8.10 diverge from each other whereas those of Figure 8.11 do not. The former is due to the interuser interference among the pilot signals and the user signal within each TDM branch causing those BER curves to diverge with the tendency to eventually flatten, as seen in chapter 7. In the latter, the corresponding BER curves do not diverge from each other as in both cases of Figure 8.11 the pilot signals interfere with the user

signals regardless of whether the perfect synchronization is assumed or not. It can thus be concluded from Figures 8.10 and 8.11 that the degradation in the BER performance, caused by the sequence synchronization error only, is approximately constant and equal to 0.75 dB.

8.2.2 Performance Comparison of the Chaos Based TDM to the Chaos Based DS-CDMA System in an AWGN Channel without Assuming Perfect Sequence Synchronization

The chaos based DS-CDMA communication system with the sequence synchronization unit is shown in Figure 7.1 of chapter 7.

The bit error rate numerical simulation results of the chaos based TDM system of Figure 8.8, are compared to those of the chaos based DS-CDMA system of Figure 7.1, for 1-5, 10, 15 and 20 users in Figure 8.12 in the AWGN channel.

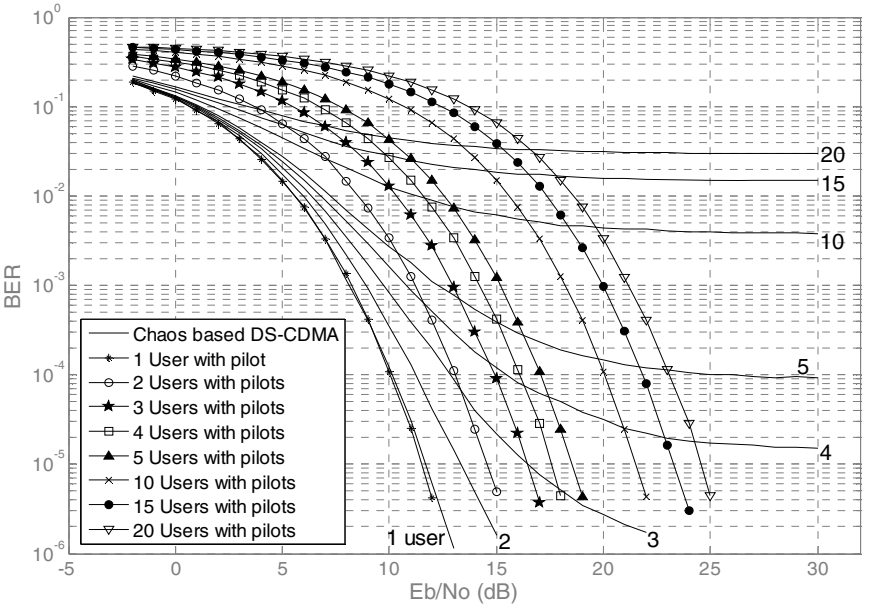


Fig. 8.12 The empirical BER curves of the chaos based TDM system of Figure 8.8 for 1-5, 10, 15 and 20 users (marked curves), alongside the corresponding empirical BER curves of the chaos based DS-CDMA system of Figure 7.1 (unmarked curves).

As in subsection 8.1.2, in the case of 10, 15 and 20 users the chaos based DS-CDMA BER curves flatten, due to the prevailing interuser interferences, before reaching the highest acceptable BER level of 10^{-3}. In contrast to this, the corresponding BER curves of the chaos based TDM system do not flatten. Therefore, for a larger number of users, the chaos based TDM system with the sequence synchronization unit outperforms the corresponding chaos based

DS-CDMA system. Furthermore, it can be observed from Figure 8.12 that the chaos based DS-CDMA system outperforms the chaos based TDM system at the BER level of 10^{-3} for the low number of users in the system. However, by careful observation of Figures 8.3 and 8.12 one can observe that at the BER level of 10^{-3} the performance of the chaos based TDM system degrades less than that of the chaos based DS-CDMA system when perfect synchronization is not assumed.

8.2.3 Performance of the Chaos Based TDM System in a Rayleigh Fading Channel without Assuming Perfect Sequence Synchronization

The chaos based TDM system in the Rayleigh fading channel with the sequence synchronization units of Figure 8.9 is presented in Figure 8.13.

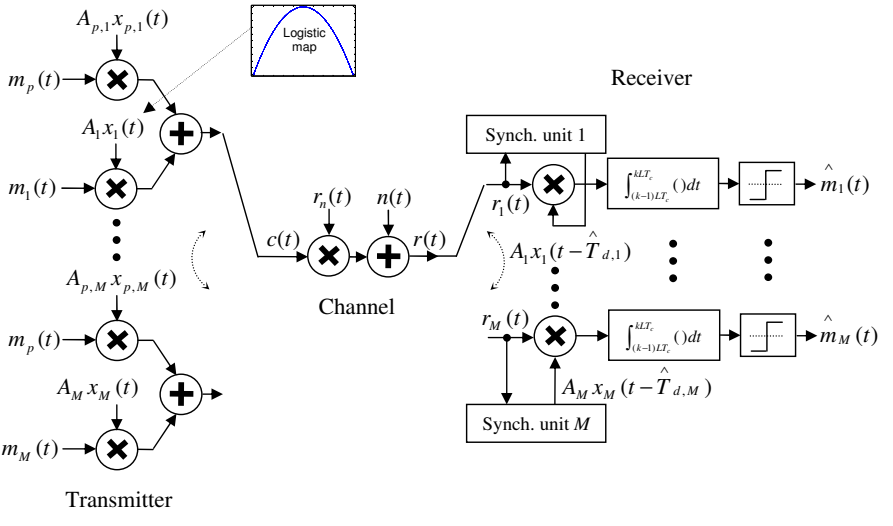


Fig. 8.13 The chaos based TDM communication system with the pilot signals and the sequence synchronization unit in the Rayleigh fading channel

The bit error rate numerical simulation results of the chaos based TDM system of Figure 8.13 for 1-5, 10, 15 and 20 users in the Rayleigh fading channel are shown in Figure 8.14. For comparison, the corresponding curves of the chaos based TDM system in the Rayleigh fading channel with perfect synchronization assumed are also presented. As in subsection 8.1.3, the Rayleigh fading envelope, $r_n(t)$, was generated for the velocity of the receiver relative to the transmitter of 55 km/h and the carrier frequency of 900 MHz [30,31] with $P_r = 1\text{W}$.

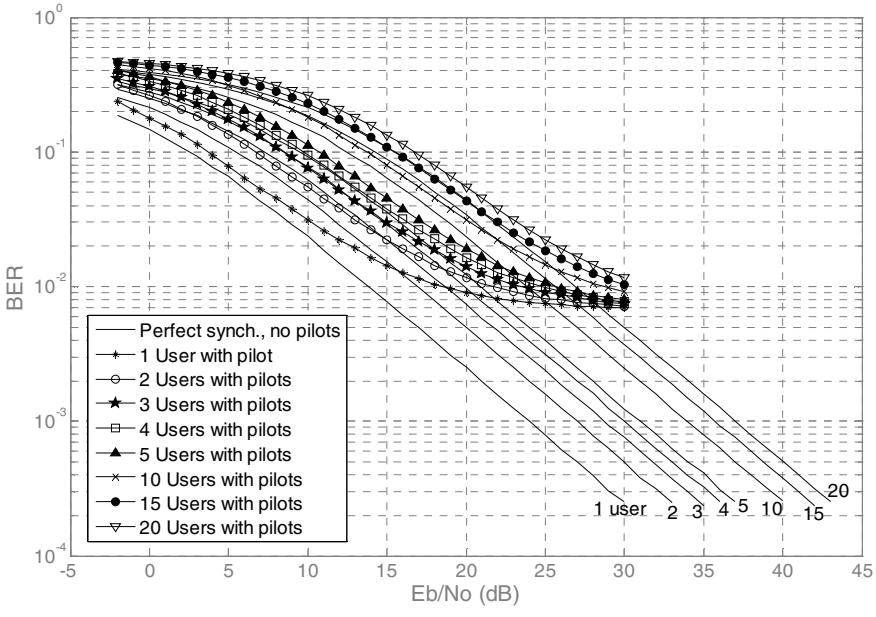


Fig. 8.14 The empirical BER curves of the chaos based TDM system of Figure 8.13 for 1-5, 10, 15 and 20 users (marked curves). The corresponding empirical BER curves of Figure 8.5 with perfect synchronization assumed are shown by unmarked curves.

It can be observed in Figure 8.14, that in all cases the BER curves of the chaos based TDM system of Figure 8.13 flatten before reaching the highest acceptable BER level of 10^{-3}. Therefore, one can observe from Figure 8.14 that without assuming perfect synchronization in the Rayleigh fading channel, the system performance degrades significantly.

By comparing Figures 8.10 and 8.14, it can be observed that although the system satisfies the BER level of 10^{-3} for all users in an AWGN channel, it fails for all users in a fading channel. Thus, in comparison, the system in the Rayleigh fading channel is not practical for real world application. As mentioned in chapter 7, in order to improve the performance in the fading environment techniques used to disperse bursts of error in time, such as block interleaving [30], could be employed.

In the same fashion as in subsection 8.2.1, the effect of the sequence synchronization error only on the BER performance of the system of Figure 8.13 is now illustrated. Again, this is achieved by assuming perfect sequence synchronization while still keeping the pilot signals within the system of Figure 8.13. The BER curves of the system of Figure 8.13 with the pilot signals intact, but with the perfect sequence synchronization assumed at the receiver, are shown in Figure 8.15.

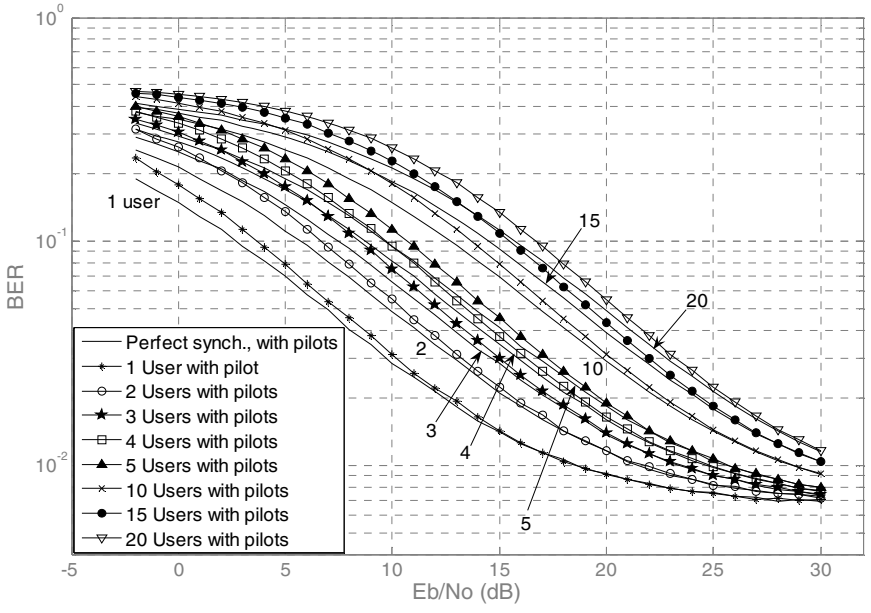


Fig. 8.15 The empirical BER curves of the chaos based TDM system of Figure 8.13 for 1-5, 10, 15 and 20 users (marked curves). The corresponding empirical BER curves of the chaos based TDM system of Figure 8.13, but with perfect synchronization assumed and the pilot signals intact, are shown by unmarked curves.

It can be observed from Figure 8.15 that the BER curves of the system of Figure 8.13 with perfect synchronization assumed also flatten before reaching the BER level of 10^{-3}. It can thus be concluded that the flattening of the BER curves in the Rayleigh fading channel is primarily due to the interuser interference among the pilot signals and the user signal within each TDM branch and not due to the sequence synchronization error. By careful observation of Figure 8.15, one can observe that the BER performance degradation due to the sequence synchronization error only is minimal.

8.2.4 Performance Comparison of the Chaos Based TDM to the Chaos Based DS-CDMA System in a Rayleigh Fading Channel without Assuming Perfect Sequence Synchronization

The chaos based DS-CDMA system in the Rayleigh fading channel with the synchronization unit incorporated is presented in Figure 7.12 of chapter 7.

The bit error rate numerical simulation results of the system of Figure 7.12 are presented for 1, 5, 10, 15 and 20 users in Figure 8.16 in the Rayleigh fading channel.

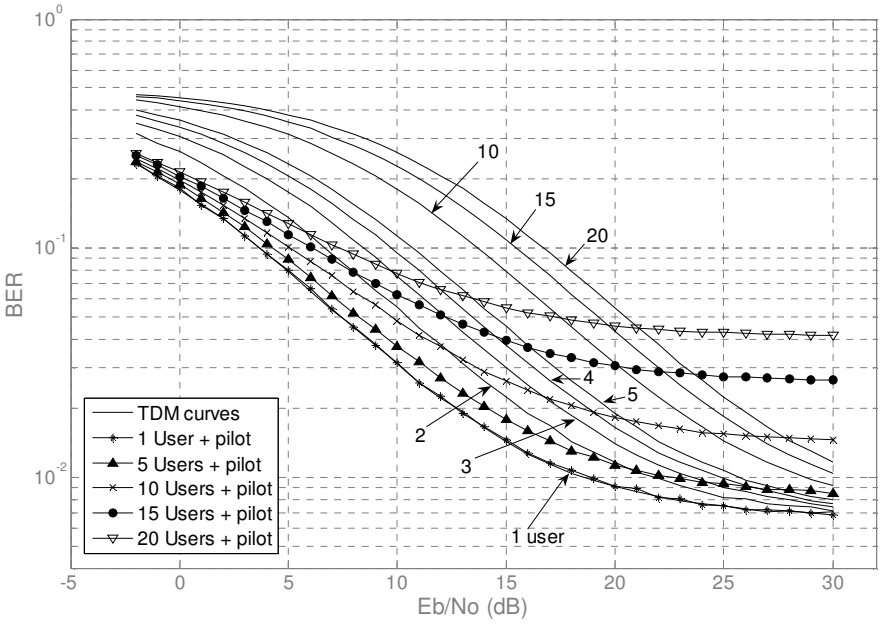


Fig. 8.16 The empirical BER curves of the chaos based DS-CDMA system of Figure 7.12 for 1, 5, 10, 15 and 20 users (marked curves), alongside the corresponding empirical BER curves of the chaos based TDM system of Figure 8.13 (unmarked curves).

It can be observed from Figure 8.16 that the BER performance of the chaos based DS-CDMA system is better for the low number of users in the system (1-5), for E_b / N_o less than approximately 27 dB. Its performance is worse for the large number of users in the system (10, 15, 20), for E_b / N_o greater than approximately 24, 22 and 21 dB, respectively. However, as mentioned previously, one can also observe that both systems fail to satisfy the maximum allowable BER level of 10^{-3} for any number of users in the system.

8.3 Generalized Chaos Based TDM Communication System without Assuming Perfect Sequence Synchronization

In this section, the chaos based TDM communication system of Figure 8.8 is extended to include more than one DS-CDMA user per TDM branch. It is thus shown that in this way the overall number of users in the system can be increased substantially while at the same time improving the BER performance of the system. Its performance is evaluated without assuming perfect sequence synchronization in terms of the bit error rate in an AWGN channel.

8.3.1 Generalized Chaos Based TDM Communication System with the Sequence Synchronization Unit

The generalized chaos based TDM communication system is proposed in Figure 8.17.

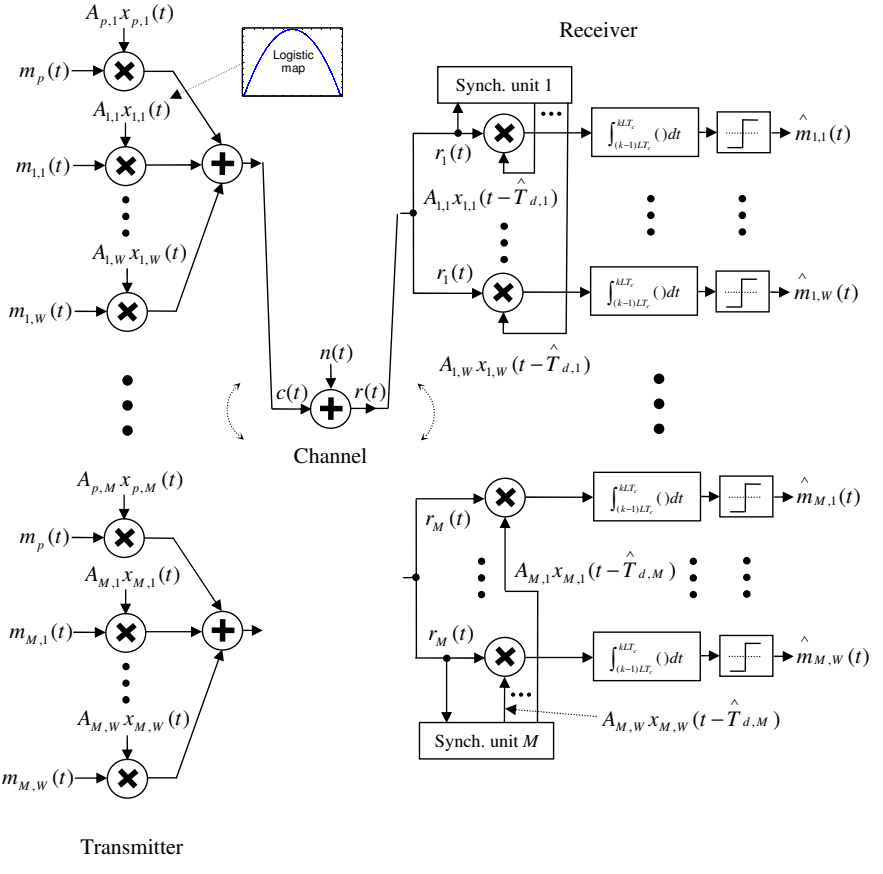


Fig. 8.17 The generalized chaos based TDM communication system with the pilot signals and the sequence synchronization unit

In each TDM branch of the system of Figure 8.17 a unique PRBS pilot signal, $x_p(t)$, is introduced for synchronization purposes. In addition, each of the M TDM branches also contains W users which are modulated in the DS-CDMA manner. These are then multiplexed in the TDM manner to produce the signal $c(t)$ which is transmitted through the channel. As in section 8.2, the received signal $r(t)$

is then de-multiplexed and fed into the *M* separate sequence synchronization units at the receiver. The sequence synchronization unit generates the punctual despreading codes. The block diagram illustrating the sequence synchronization unit of Figure 8.17 is shown in Figure 8.18.

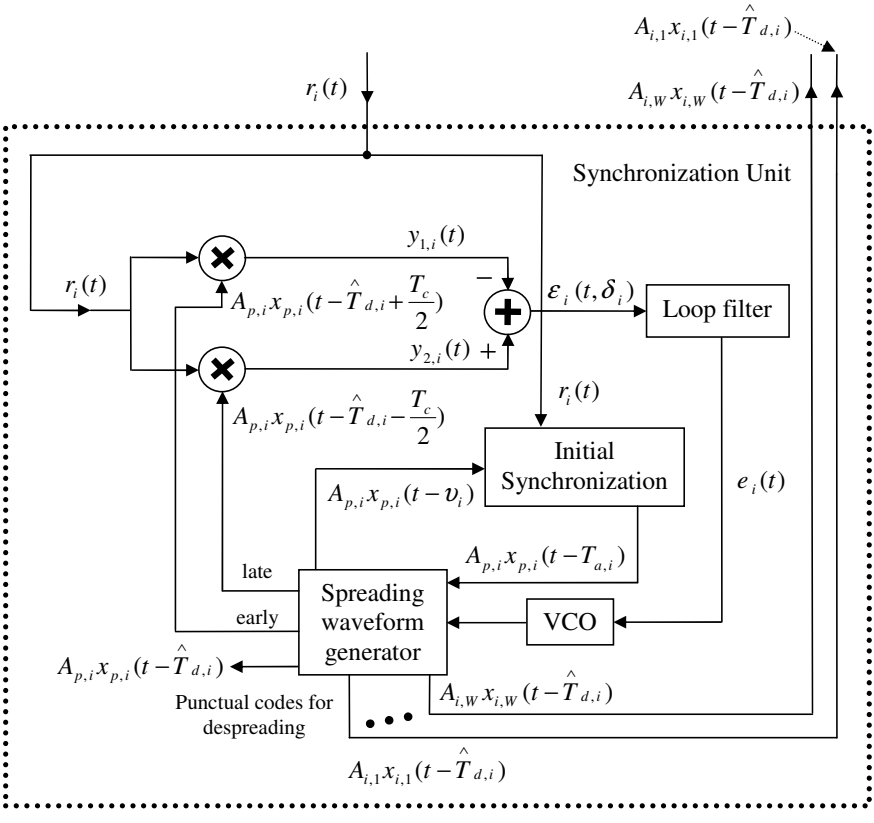


Fig. 8.18 The architecture of the sequence synchronization unit for each of the *M* TDM branches of Figure 8.17, where $\delta_i = (T_{d,i} - \hat{T}_{d,i})/T_c$.

The bit error rate numerical simulation results of the TDM/DS-CDMA system of Figure 8.17 are presented in Figure 8.19 for 1-3 DS-CDMA users per each branch of a 2 TDM branch system. Furthermore, Figure 8.20 shows the BER curves for 1-3 DS-CDMA users per each TDM branch of a 3 TDM branch system. Finally, Figure 8.21 shows Figures 8.19 and 8.20 on the same set of axis.

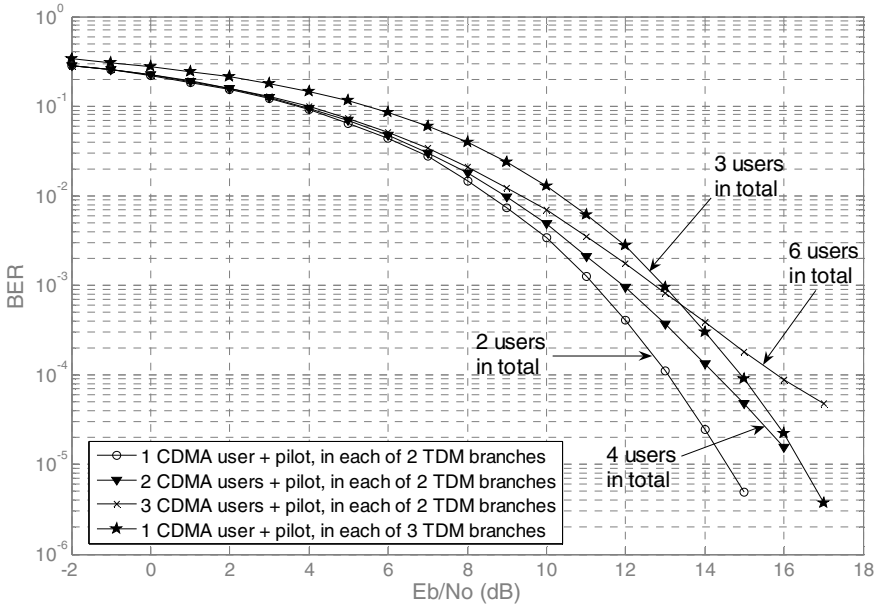


Fig. 8.19 The empirical BER curves of the chaos based TDM/DS-CDMA system of Figure 8.17 for 2, 3, 4 and 6 users in the system.

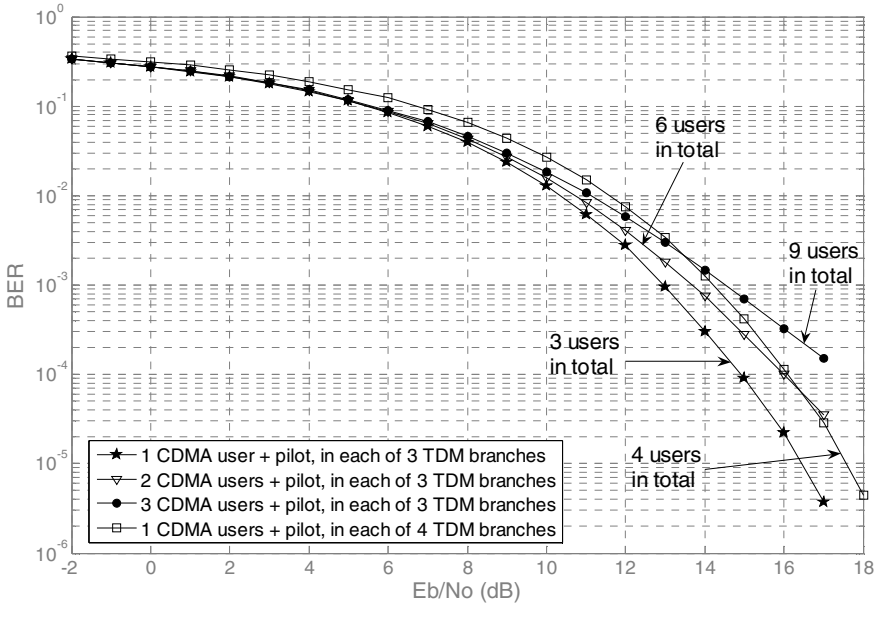


Fig. 8.20 The empirical BER curves of the chaos based TDM/DS-CDMA system of Figure 8.17 for 3, 4, 6 and 9 users in the system.

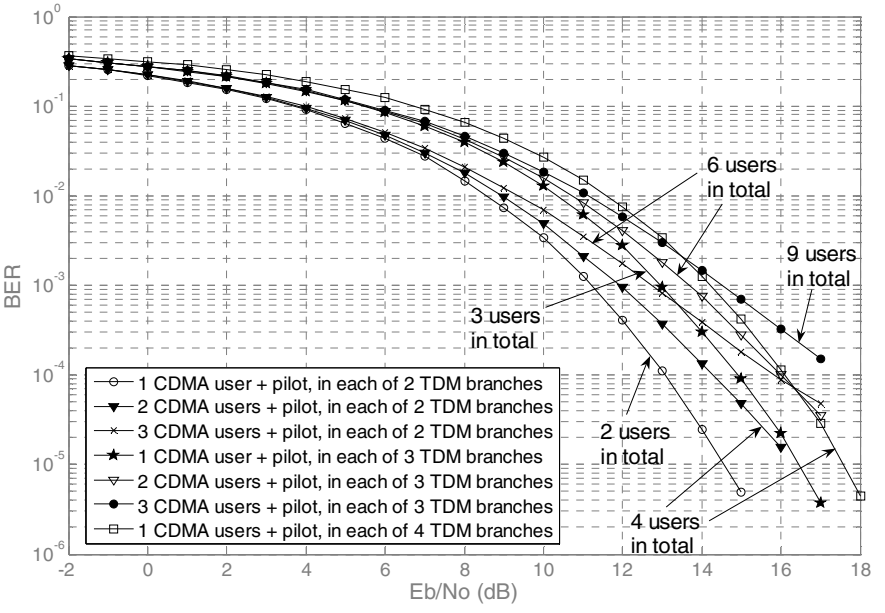


Fig. 8.21. The empirical BER curves of Figures 8.19 and 8.20 plotted on the same set of axes.

It can be observed from Figure 8.19 that at the BER level of 10^{-3} the E_b / N_o ratio for which the system performance is satisfactory for the case of the total of 2, 3, 4 and 6 users is equal to approximately 11, 13, 12 and 12.5 dB, respectively. Thus, at the BER level of 10^{-3} the chaos based TDM system of Figure 8.17 with 2 TDM branches in the system and 3 DS-CDMA users in each branch (6 users in total), outperforms the system with 1 DS-CDMA user in each of the 3 TDM branches (3 users in total). Furthermore, it can be observed that the total of 4 users in the '2 DS-CDMA per 2 TDM' configuration, outperforms the total of 3 users in the '1 DS-CDMA per 3 TDM' configuration by approximately 1dB. Therefore, allocating more than one DS-CDMA user per TDM branch yields a better BER performance while at the same time increasing the total number of users. In this way, the bandwidth efficiency of a DS-CDMA system is combined with the interuser interference immunity of a TDM system, to allow for an increased number of users in the system while improving the BER performance. However, in actual practice TDM systems may often be more bandwidth efficient than CDM based systems. This is due to the signalling formats employed by CDM based systems which are often not optimized for bandwidth efficiency.

In Figure 8.20, a similar scenario to that of Figure 8.19 can be observed. It is shown that at the BER level of 10^{-3} the E_b / N_o ratio for which the system performance is satisfactory for the case of the total of 3, 4, 6 and 9 users is equal to approximately 13, 14, 13.5 and 14.5 dB, respectively. It can be observed that the BER performance degrades by approximately 0.5 dB in the case of the total of 9 users in the '3 DS-CDMA per 3 TDM' configuration as compared to the total of 4 users in the '1 DS-CDMA per 4 TDM' configuration. However, this degradation in the BER performance is minimal compared to the increase in the number of users which in this case is more than two fold.

Finally, the BER curves of Figures 8.19 and 8.20 are plotted in Figure 8.21 on the same set of axes. It can be observed from Figure 8.21 that out of the two possible 6 users configurations the '3 DS-CDMA per 2 TDM' configuration outperforms the '2 DS-CDMA per 3 TDM' configuration by approximately 1 dB at the BER level of 10^{-3}. However, at the E_b / N_o level of approximately 16.5 dB, the '2 DS-CDMA per 3 TDM' configuration starts to outperform the '3 DS-CDMA per 2 TDM' configuration. This is as expected, as the interuser interference which, as seen in chapter 7, is more dominant for more DS-CDMA users starts to flatten the BER curve. Furthermore, an improvement of approximately 2 dB can be observed for the total number of users of 4 in the '2 DS-CDMA per 2 TDM' configuration as compared to the '1 DS-CDMA per 4 TDM' configuration.

As in section 8.2, the clock synchronization and the synchronization among the multiplexing and de-multiplexing switches at the transmitter and the receiver are assumed.

8.3.2 Performance Comparison of the Generalized Chaos Based TDM to the Chaos Based DS-CDMA System in an AWGN Channel without Assuming Perfect Sequence Synchronization

The chaos based DS-CDMA communication system with the sequence synchronization unit is shown in Figure 7.1 of chapter 7.

The bit error rate numerical simulation results of the chaos based TDM system of Figure 8.17 are now compared to those of the chaos based DS-CDMA system of Figure 7.1. In Figure 8.22 the BER results are shown in the AWGN channel.

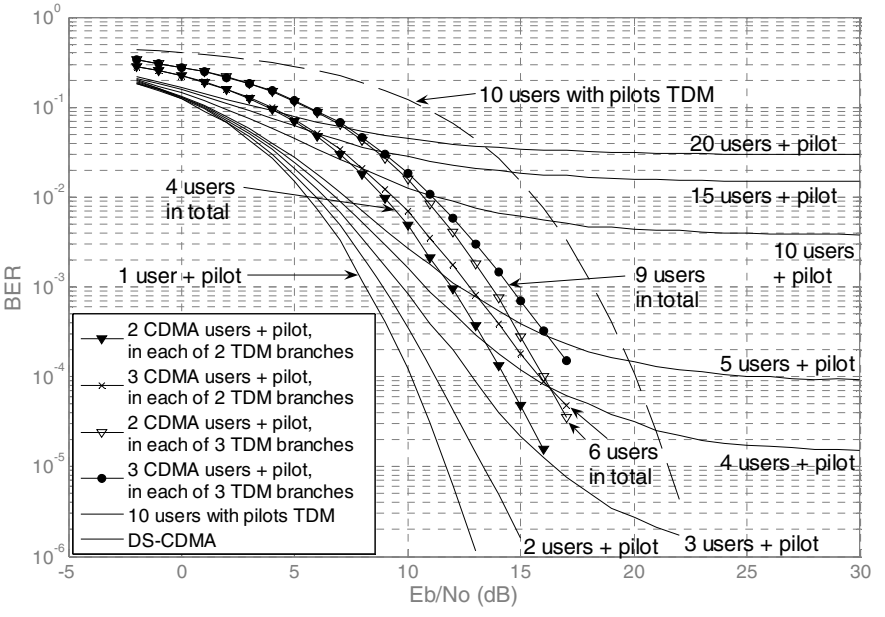


Fig. 8.22 The empirical BER curves of the generalized chaos based TDM system of Figure 8.17 for 4, 6 and 9 users (marked curves). The empirical BER curves of the chaos based DS-CDMA system of Figure 7.1 for 1-5, 10, 15 and 20 users are shown by unmarked curves.

It can be observed from Figure 8.22 that the generalized chaos based TDM system of Figure 8.17 is outperformed by the chaos based DS-CDMA system at the BER level of 10^{-3} for the low number of users (4, 6) in the system. However, the margin by which the generalized system of Figure 8.17 is outperformed is not as large as the margin by which the system of Figure 8.8 is outperformed at the low number of users in the system. Furthermore, one can see from Figure 8.22 that the generalized chaos based TDM system starts to significantly outperform the chaos based DS-CDMA system at the BER levels less than 10^{-3}. As the number of users in the system increases to 9 users, it can be observed from Figure 8.22 that the BER curve of the generalized chaos based TDM system of Figure 8.17 does not flatten. Therefore, for a larger number of users, the generalized chaos based TDM system with the sequence synchronization unit outperforms the corresponding chaos based DS-CDMA system. Furthermore, at the BER level of 10^{-3}, it can also be observed that the generalized chaos based TDM system of Figure 8.17 exhibits a significant improvement over the chaos based TDM system of Figure 8.8 (dashed curve) for a larger number of users in the system.

8.4 Conclusion

In this chapter, a chaos based multi-user TDM system has been proposed and evaluated in terms of the bit error rate. Its performance has been investigated with and without the assumption of perfect sequence synchronization in the noisy and Rayleigh fading channels. Furthermore, the BER performance of the chaos based DS-CDMA system has been compared to the performance of the chaos based multi-user TDM system. The chaotic spreading signals, used to encrypt the binary messages, have been generated using the logistic map. As in chapter 7, the mutually orthogonal properties, between the chaotic time series produced by the logistic map with different initial conditions, have been used to decrypt messages sent across the channel.

Assuming perfect sequence synchronization, it has been shown that in the AWGN and Rayleigh fading channels the TDM system reaches the adopted minimum allowable BER level of 10^{-3} for 1-5, 10, 15 and 20 users in the system. Furthermore, it has been shown that in terms of BER the chaos based multi-user TDM system outperforms the chaos based DS-CDMA system for a large number of users in the system, while the chaos based DS-CDMA system yields better performance for low number of users in the system.

The proposed chaos based TDM system was then investigated without the assumption of perfect sequence synchronization in the AWGN and Rayleigh fading channels. Again, it was shown that in terms of BER the chaos based TDM system outperforms the chaos based DS-CDMA system for a large number of users in the system and vice-versa for low number of users in the system. In order to obtain the full characterization of the system, the sequence synchronization was also assumed with a PRBS pilot signal present on top of each user signal. The effect of the pilot signal on the performance of the system was thus demonstrated in AWGN and Rayleigh fading channels. Furthermore, it was shown that both chaos based TDM and chaos based DS-CDMA systems are insufficiently robust in the Rayleigh fading channel when the perfect sequence synchronization is not assumed.

One of the main characteristics of the DS-CDMA systems is that they are bandwidth efficient and that they offer increased security of transmission. The purpose of introducing the chaos based TDM system was to eliminate the interuser interference, at the expense of the increased bandwidth for an increasing number of users in the system, while still maintaining the security of transmission. In order to mutually exploit the DS-CDMA and TDM benefits, a generalized chaos based TDM communication system with more than one DS-CDMA user per TDM branch was proposed and evaluated in the AWGN channel. In this way, the bandwidth efficiency of a DS-CDMA system has been combined with the interuser interference immunity of a TDM system, to allow for an increased number of users in the system while improving the BER performance.

References

[1] Murali, K., Lakshmanan, M.: Transmission of signals by synchronization in a chaotic Van der Pol-Duffing oscillator. Physical Review E, Rapid Communications 48(3), R1624–R1626 (1993)

[2] Oppenheim, A.V., Wornell, G.W., Isabelle, S.H., Cuomo, K.M.: Signal processing in the context of chaotic signals. In: Proceedings IEEE ICASSP, pp. 117–120 (1992)

[3] Kocarev, L., Halle, K.S., Eckert, K., Chua, L.O., Parlitz, U.: Experimental demonstration of secure communications via chaotic synchronization. International Journal of Bifurcation and Chaos 2(3), 709–713 (1992)

[4] Parlitz, U., Chua, L.O., Kocarev, L., Hale, K.S., Shang, A.: Transmission of digital signals by chaotic synchronization. International Journal of Bifurcation and Chaos 2(4), 973–977 (1992)

[5] Cuomo, K.M., Oppenheim, A.V.: Circuit Implementation of Synchronized Chaos with Applications to Communications. Physical Review Letters 71(1), 65–68 (1993)

[6] Jovic, B., Berber, S., Unsworth, C.P.: A novel mathematical analysis for predicting master – slave synchronization for the simplest quadratic chaotic flow and Ueda chaotic system with application to communications. Physica D 213(1), 31–50 (2006)

[7] Parlitz, U., Ergezinger, S.: Robust communication based on chaotic spreading sequences. Physics Letters A 188(2), 146–150 (1994)

[8] Heidari-Bateni, G., McGillem, C.D.: A Chaotic Direct-Sequence Spread-Spectrum Communication System. IEEE Transactions on Communications 42(2/3/4), 1524–1527 (1994)

[9] Mazzini, G., Setti, G., Rovatti, R.: Chaotic Complex Spreading Sequences for Asynchronous DS-CDMA – Part I: System Modelling and Results. IEEE Transactions on Circuits and Systems – I: Fundamental Theory and Applications 44(10), 937–947 (1997)

[10] He, D., Leung, H.: Quasi – Orthogonal Chaotic CDMA Multi – User Detection Using Optimal Chaos Synchronization. IEEE Transactions on Circuits and Systems – II: Express Briefs 52(11), 739–743 (2005)

[11] Rovatti, R., Mazzini, G.: Interference in DS-CDMA systems with exponentially vanishing autocorrelations: Chaos-based spreading is optimal. Electronics Letters 34(20), 1911–1913 (1998)

[12] Tam, W.M., Lau, F.C.M., Tse, C.K., Lawrance, A.J.: Exact Analytical Bit Error Rates for Multiple Access Chaos – Based Communication Systems. IEEE Transactions on Circuits and Systems – II: Express Briefs 51(9), 473–481 (2004)

[13] Jovic, B., Unsworth, C.P., Sandhu, G.S., Berber, S.M.: A robust sequence synchronization unit for multi-user DS-CDMA chaos-based communication systems. Signal Processing 87(7), 1692–1708 (2007)

[14] Jovic, B., Unsworth, C.P.: Chaos based multi-user time division multiplexing communication system. IET Communications 1(4), 549–555 (2007)

[15] Itoh, M.: Spread Spectrum Communication via Chaos. International Journal of Bifurcation and Chaos 9(1), 155–213 (1999)

[16] Itoh, M., Chua, L.O.: Multiplexing Techniques via Chaos. In: Proceedings of the 1997 IEEE International Symposium on Circuits and Systems (ISCAS 1997), Hong Kong, China, June 9-12, pp. 905–908 (1997)

[17] Itoh, M., Chua, L.O.: Multiplexing Techniques via Chaotic Signals. In: Proceedings of the 1997 European Conference on Circuit Design (ECCTD 1997), Budapest, Hungary, August 31-September 3, vol. 14, pp. 278–283 (1997)
[18] Torikai, H., Saito, T., Schwarz, W.: Multiplex Communication Scheme Based on Synchronization via Multiplex Pulse-Trains. In: Proceedings of the 1998 IEEE International Symposium on Circuits and Systems (ISCAS 1998), Monterey, CA, May 31-June 3, vol. 4, pp. IV-554–IV-557 (1998)
[19] He, Z., Li, K., Yang, L.: TDMA Secure Communication Scheme Based on Synchronization of Chua's Circuits. Journal of Circuits, Systems, and Computers 10(3&4), 147–158 (2000)
[20] Li, K., Liu, J., Yang, L., He, Z.: A Robust Chaotic Digital Secure Communication Scheme. In: Proceedings of the 1999 IEEE Pacific rim Conference on Communications, Computers and Signal Processing (PACRIM 1999), Victoria, BC, August 22-24, pp. 491–494 (1999)
[21] Peng-bo, X., Li, M.: Time Division Multiplexing Signals Transmission via Intermittently Coupled, Synchronized Chaotic System. Journal of Qingdao University 13(2), 45–49 (2000)
[22] Zhou, C.S., Chen, T.L.: Extracting information masked by chaos and contaminated with noise: Some considerations on the security of communication approaches using chaos. Physics Letters A 234(6), 429–435 (1997)
[23] Jordan, D.W., Smith, P.: Mathematical Techniques: An introduction for the engineering, physical, and mathematical sciences, 2nd edn., p. 8. Oxford University Press, Oxford (1997)
[24] Haykin, S.: Communication systems, 4th edn., pp. 61–514. Wiley, New York (2001)
[25] Carroll, T.L., Pecora, L.M.: Using multiple attractor chaotic systems for communication. Chaos 9(2), 445–451 (1999)
[26] Giger, A.J., Barnett, W.T.: Effects of Multipath Propagation on Digital Radio. IEEE Transactions on Communications COM-29(9), 1345–1352 (1981)
[27] Wehinger, J., Mecklenbrauker, C.F.: Iterative CDMA Multiuser Receiver With Soft Decision-Directed Channel Estimation. IEEE Transactions on Signal Processing 54(10), 3922–3934 (2006)
[28] Carlson, A.B.: Communication Systems: An Introduction to Signals and Noise in Electrical Communication, 2nd edn., ch. 8, pp. 330–334. McGraw-Hill, Inc., New York (1975)
[29] Haas, H., McLaughlin, S.: A Dynamic Channel Assignment Algorithm for a Hybrid TDMA/CDMA-TDD Interface Using the Novel TS-Opposing Technique. IEEE Journal on Selected Areas in Communications 19(10), 1831–1846 (2001)
[30] Lee, J.S., Miller, L.E.: CDMA Systems Engineering Handbook, pp. 18–837. Artech House Publishers, Boston (1998)
[31] Rappaport, T.S.: Wireless Communications Principles and Practice, pp. 172–188. Prentice Hall, Inc., Upper Saddle River (1996)

Chapter 9
Chaotic Synchronization Based Multi-user TDM Communication Systems

In this chapter, the chaotic synchronization based multi-user TDM communication systems are proposed and evaluated in terms of BER in AWGN and Rayleigh fading channels. In particular, the proposed systems include the Lorenz and Ueda CPM based TDM systems and the Ueda ICM based TDM systems. It is shown that the ICM based multi-user TDM systems outperform the CPM systems. However, it is also found that both CPM and ICM based TDM systems fail to satisfy the maximum allowable BER level of 10^{-3} in the Rayleigh fading channel. The performance of the ICM and CPM based TDM systems, is then compared to that of the chaos based DS-CDMA and TDM systems of chapters 7 and 8. It is shown that in the AWGN and Rayleigh fading channels the chaos based TDM system of chapter 8 outperforms the CPM and ICM based TDM systems. Furthermore, it is also found that the chaos based DS-CDMA system outperforms the CPM and ICM based TDM systems for low number of users in the system while the opposite is true for large number of users.

In chapter 8, sequence synchronization within the proposed chaos based multi-user TDM system [1] has been achieved through the process of acquisition and tracking of chapter 7 [2]. In contrast to this, in this chapter sequence synchronization within TDM multi-user systems is achieved through the process of chaotic synchronization of chapter 6 [3,4]. In this way, the design principles of the single-user systems of chapter 6 are extended and the new chaotic synchronization based multi-user TDM systems proposed. As in chapter 8, the synchronization among the multiplexing and de-multiplexing switches of the transmitter and the receiver is assumed [1].

As mentioned in chapter 8, chaos based TDM systems have been investigated in [5-11]. The principles of TDM from a viewpoint of the chaos based spread spectrum communication systems have been discussed in [5]. The synchronization among the multiplexing and de-multiplexing switches of the transmitter and the receiver has been considered and the method of achieving synchronization proposed [5]. Based on this method, the multi-user chaos based TDM system was proposed in [6,7]. The system was investigated for the two user case using the Pecora-Carroll (PC) self synchronizing properties of the Chua master-slave systems.

B. Jovic: Synchronization Techniques for Chaotic Commun. Syst., SCT 5, pp. 257–297.
springerlink.com

In this chapter, chaotic parameter modulation (CPM) and initial condition modulation (ICM) based multi-user TDM systems are proposed. The work presented here is similar to [5-11] in that the PC synchronization ideas are used to synchronize the transmitter and the receiver and thus decode the information. In particular, the authors of [6,7] use the PC synchronization within analogue electronic circuits to transmit sinusoidal messages across the noiseless channel. However, in this chapter the information is encoded and decoded using the novel methods of chaotic synchronization proposed in chapters 3 and 5 [3,4]. Furthermore, the performance of the systems in the presence of noise and fading is also evaluated.

In this chapter, it is shown that in terms of BER the ICM based TDM systems outperform the CPM based TDM systems in both AWGN and Rayleigh fading channels. In addition, it is also shown that of the two Ueda ICM based TDM systems proposed, the system with only the master signal x transmitted outperforms the system with both master signals x and y transmitted. However, the BER analysis in the Rayleigh fading channel reveals that both CPM and ICM based systems fail to satisfy the highest acceptable BER level of 10^{-3} for any number of users in the system and any E_b / N_o. Furthermore, two different receiver architectures are implemented on all of the CPM and ICM based TDM systems. These include the predetermined threshold receiver architecture [4,3] and the receiver architecture implementing two slave systems [12,13]. It is shown that in terms of BER only in the case of the Lorenz CPM based TDM system the two slave receiver architecture outperforms the predetermined threshold architecture. Finally, the BER performance of the CPM and ICM based TDM systems is compared to the BER performance of the chaos based DS-CDMA system of chapter 7 [14] and the chaos based TDM system of chapter 8 [1]. It is shown that in both AWGN and Rayleigh fading channels the CPM and ICM based TDM systems are outperformed by the chaos based TDM system of chapter 8. However, it is also shown that the chaos based DS-CDMA system of chapter 7, outperforms the CPM and ICM based systems only for low number of users. For larger number of users in the system, the CPM and ICM based TDM systems outperform the chaos based DS-CDMA system in the AWGN channel.

Section 9.1, proposes and presents the chaotic synchronization based multi-user TDM systems implementing the CPM technique of chapter 6. The principles of operation of the systems are explained and their BER performance evaluated and compared to that of the chaos based DS-CDMA and TDM systems of chapters 7 and 8. The ICM based TDM systems are then proposed in Section 9.2. Their performance is compared to that of the CPM based TDM systems as well as to that of the chaos based DS-CDMA and TDM systems of chapters 7 and 8.

9.1 The CPM Based Multi-user TDM Communication System

In this section, the single-user Lorenz and Ueda CPM based communication systems of subsection 6.2.1 are used to construct the CPM based multi-user TDM communication systems. Their performance is evaluated in terms of BER in the

AWGN and Rayleigh fading channels. Furthermore, their performance is compared to that of the chaos based DS-CDMA system of chapter 7 and TDM system of chapter 8. As mentioned previously, the BER performance of a multi-user TDM system can be improved to equal that of a single-user TDM BER performance by increasing the power of each TDM user. However, in the case of the TDM system proposed here the power has been kept constant so that one can directly compare its BER performance to that of the chaos based DS-CDMA system. To this effect, in the case of the multi-user TDM system proposed, E_b denotes the bit power in the BER curves presented. In contrast to the chaos based DS-CDMA and TDM systems of chapters 7 and 8, the sequence synchronization of the CPM based TDM system is achieved through the process of chaotic synchronization principles of chapters 3 and 6.

9.1.1 The Principles of the CPM Based Multi-user TDM Communication System

The principles of the single-user CPM based chaotic communication system have been outlined in subsection 6.2.1. In this subsection, the principles of the CPM based multi-user TDM chaotic communication system are proposed. The general structure of this system is presented in Figure 9.1.

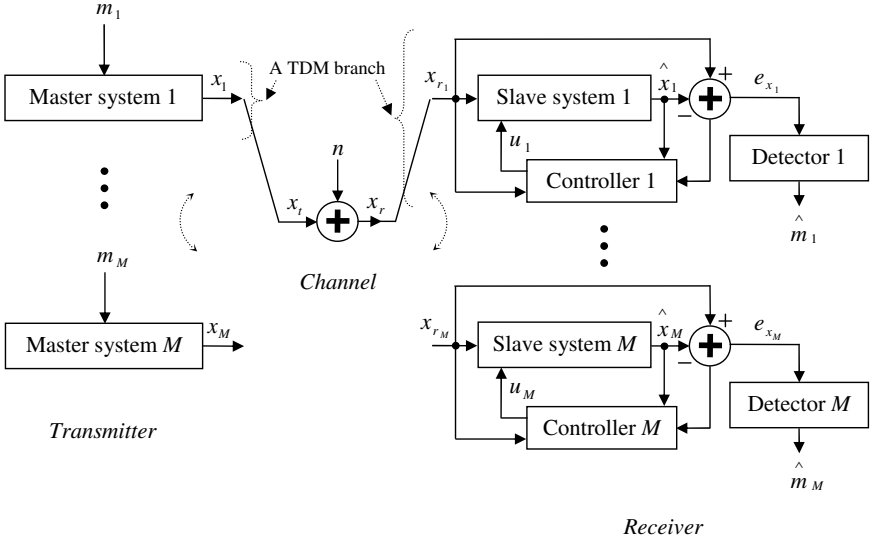


Fig. 9.1 A block diagram of the multi-user TDM chaotic communication system based on the parameter modulation concept

In Figure 9.1, each TDM branch is composed of a chaotic master-slave pair. The principles of operation of a chaotic master-slave pair, within the CPM based communication system, have been described in subsection 6.2.1. The transmitted signal x_t of Figure 9.1 is composed of the interleaved master signals x_1 to x_M, where M denotes the number of users in the system. After passing through the channel, the transmitted signal is received as the signal x_r. As in chapter 8, the received signal is de-multiplexed into M signals, x_{r_1} to x_{r_M}. Each of the de-multiplexed signals is then fed to the appropriate slave system at the receiver. The messages are recovered within each branch of the TDM system following the procedure described in subsection 6.2.1. As discussed in subsection 6.2.1, a requirement for the CPM scheme is for the master-slave system to synchronize for a given driving signal. Therefore, in order to ensure successful recovery of the transmitted bits, each slave system at the receiver must have the knowledge of the corresponding master system parameters. If, however, the knowledge of the parameters is not sufficient, that is, the master-slave system does not synchronize for a given driving signal, the controller is necessary to enforce synchronization. For instance, it has been shown in subsection 6.2.1 that the Lorenz CPM system does not require the controller, whereas the Ueda CPM based system does. Finally, in order to ensure security among different users of the system, it is important to assign different parameter values to each master-slave pair within the TDM system.

In addition to the predetermined threshold receiver used in chapter 6 and Figure 9.1, it is also possible to design the system to include two slave systems within each TDM branch. In this way, the outputs of the two slave systems are used in the symbol detection by comparing the two detector outputs to each other [12,13]. The architecture of a receiver with two slave systems is explained on the Lorenz CPM based TDM communication system in subsection 9.1.2, as well as in section 9.2. It is shown that in certain cases the receivers with two slave systems lead to improved BER performance, whereas in the other cases they do not.

9.1.2 The Lorenz CPM Based TDM Communication System

The concept of parameter modulation on the single-user Lorenz master-slave chaotic system [15,16] was demonstrated in subsection 6.2.1 [3]. The Lorenz CPM based multi-user TDM communication system with the receiver implementing the predetermined threshold principle [4,3] is proposed in Figure 9.2.

In Figure 9.2, the binary message m is equal to 0 or 0.4 depending on whether a binary 0 or 1 is to be transmitted, respectively. To ensure the security between the M users of the system, the parameter b of each master-slave pair is varied in the range $b_1 \ldots b_M \in \{3.5, \ldots, 4.45\}$. Provided that the power of noise in the system is comparatively low to the power of the signal causes the synchronization error, e_x, within each TDM branch to be equal to zero for a master-slave parameter match and non-zero for a mismatch. The principles of operation of a Lorenz master-slave pair, when implemented within a CPM system, have been explained in detail in subsection 6.2.1.

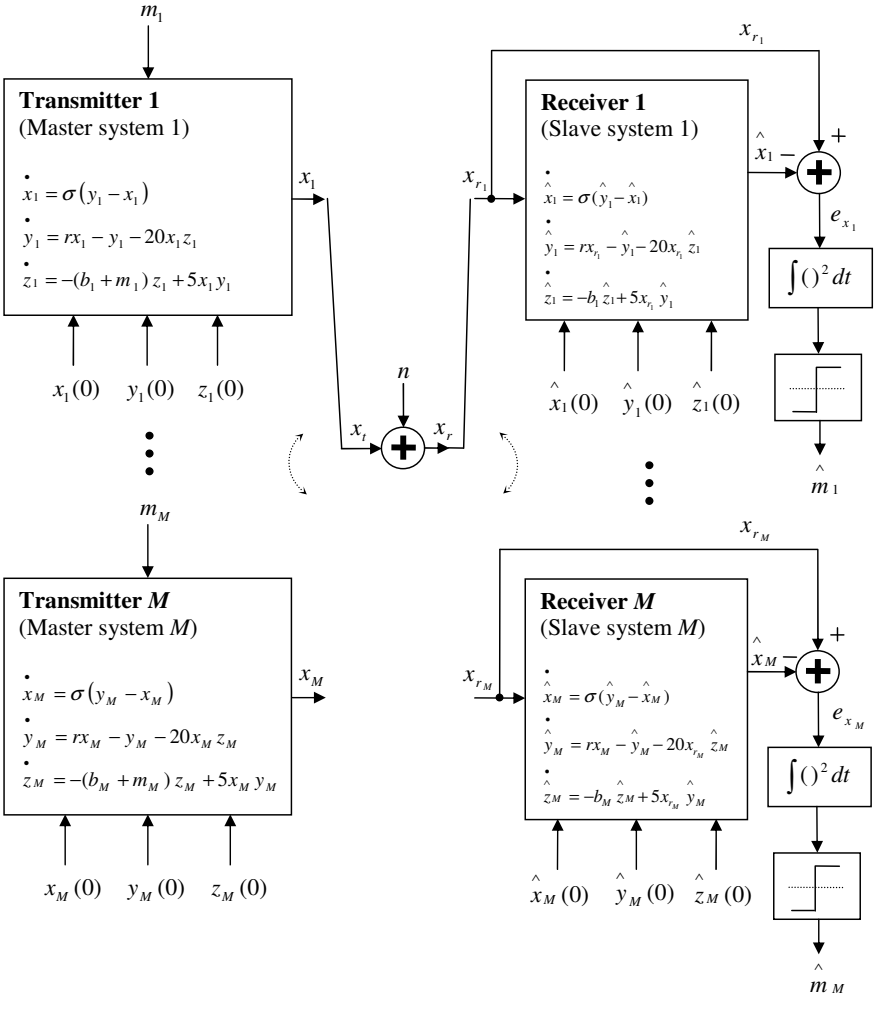


Fig. 9.2 The Lorenz CPM based multi-user TDM communication system in the AWGN channel, implementing the predetermined threshold at the receiver. The parameter values are $\sigma = 16$, $r = 45.6$ and $b_1 \ldots b_M \in \{3.5, \ldots, 4.45\}$.

In Figure 9.3, a similar system to that of Figure 9.2 is shown, however, the receiver of Figure 9.3 implements the two slave systems per each TDM branch. A detailed description of the master-slave pair within a TDM branch is shown in Figure 9.4.

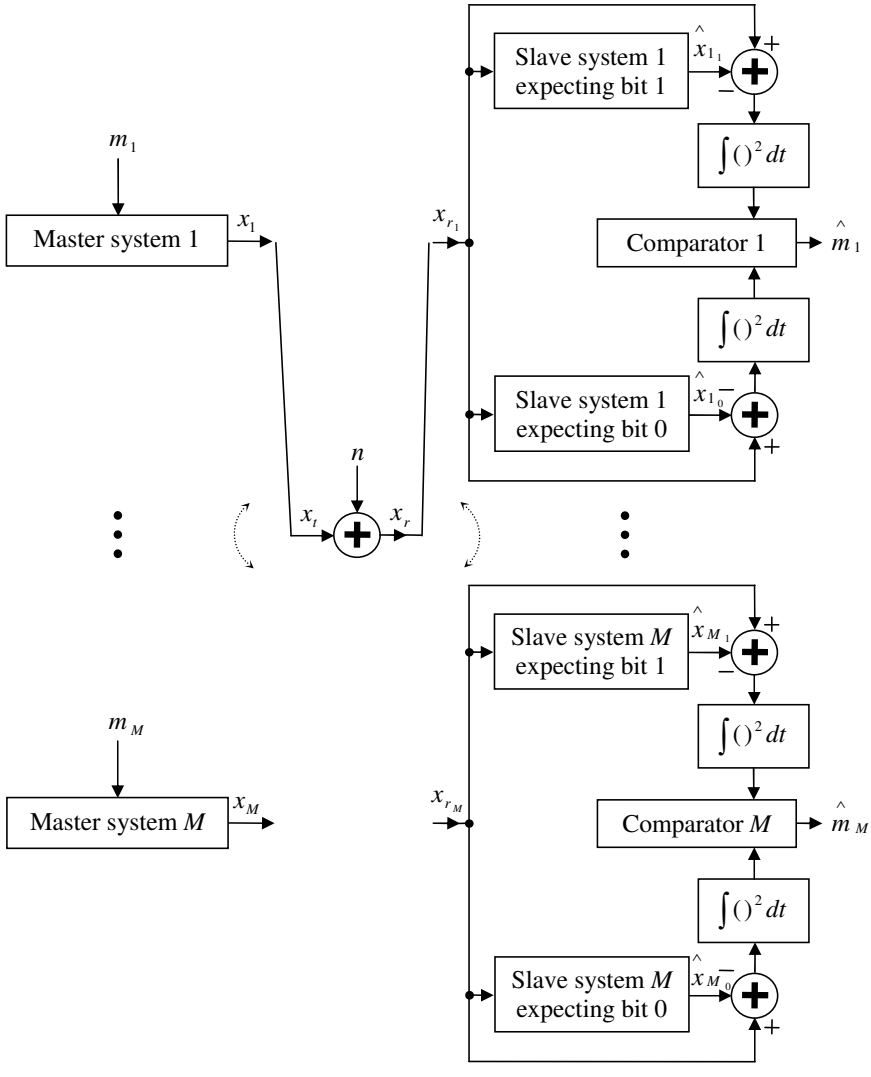


Fig. 9.3 The Lorenz CPM based multi-user TDM communication system in the AWGN channel, implementing the two slaves at the receiver. The parameter values are $\sigma = 16$, $r = 45.6$ and $b_1 ... b_M \in \{3.5, ..., 4.45\}$.

In Figure 9.4, $P_{i,1}$ of the upper slave system is set equal to $P_{i,1} = b_i + m_{i,1}$, where $m_{i,1}$ denotes the binary symbol 1 and is set to $m_{i,1} = 0.4$ for all time. Alternatively, $P_{i,0}$ of the lower slave system is set equal to $P_{i,0} = b_i + m_{i,0}$

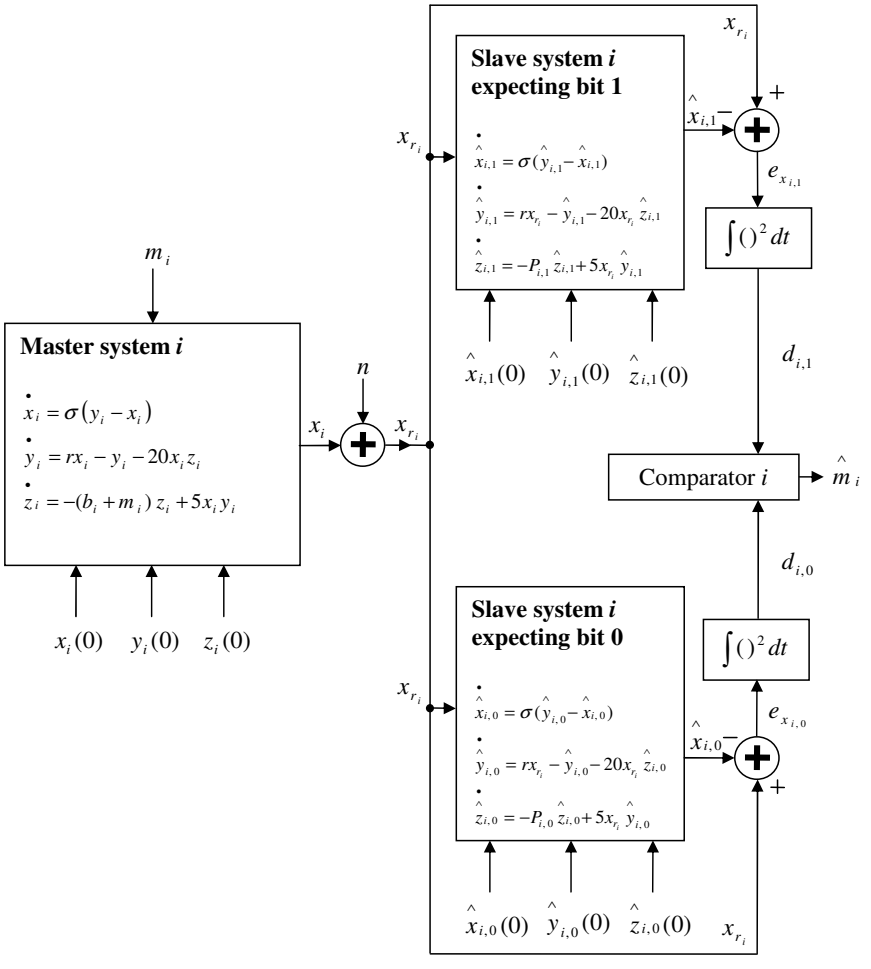


Fig. 9.4 A single branch of the Lorenz CPM based multi-user TDM communication system of Figure 9.3. The parameter values are $\sigma = 16$, $r = 45.6$ and $b_i \in \{3.5,...,4.45\}$.

where $m_{i,0} = 0$ for all time. Therefore, the parameters of the upper slave system are so set to always match those of the master system when bit 1 is transmitted. Alternatively, those of the lower slave system are set to always match those of the master system when bit 0 is transmitted. As discussed in chapter 6, the synchronization occurs provided that the master-slave parameters match and does not if a mismatch occurs. Accordingly, the decision variable $d_{i,1}$ of the upper slave system, with parameters set to match for bit 1, tends to zero when bit 1 is transmitted and does not when bit 0 is transmitted. In contrast, the decision variable $d_{i,0}$ of the lower slave system, with parameters set to match for bit 0, tends to zero when

bit 0 is transmitted and does not when bit 1 is transmitted. Therefore, if $d_{i,1} > d_{i,0}$ for a particular bit, the comparator decides in favour of bit 0 and vice-versa. The transmitted signal x_i, of Figure 9.4, is shown in Figure 9.5 when the series of 10 bits is transmitted, that is, when m_i = [0, 0, 0.4, 0, 0.4, 0.4, 0, 0.4, 0, 0.4], or in binary terms: *message* = [0 0 1 0 1 1 0 1 0 1]. Furthermore, Figure 9.5 also shows the corresponding squared synchronization errors of the two slave systems under noiseless conditions. It can be observed from Figure 9.5 that the slave system with parameters set to match for bit 1 synchronizes to the master system when a bit 1 is transmitted. Similarly, it can be observed that the slave system with parameters set to match for bit 0 synchronizes to the master system when a bit 0 is transmitted. Note that as in chapter 6, the spreading factor of 400 has been used to represent one bit.

The bit error rate numerical simulation result of the single-user system of Figure 9.2 is compared to that of Figure 9.3 in Figure 9.6, in the AWGN channel. It can be observed from Figure 9.6 that the system of Figure 9.3 outperforms the system of Figure 9.2 by approximately 3.5 dB. Therefore, the system of Figure 9.3, which implements the two slave receiver, will be used to obtain the empirical BER simulation results for the Lorenz CPM based multi-user TDM communication system. As before, the clock synchronization, as well as the synchronization among the multiplexing and de-multiplexing switches at the transmitter and the receiver is assumed.

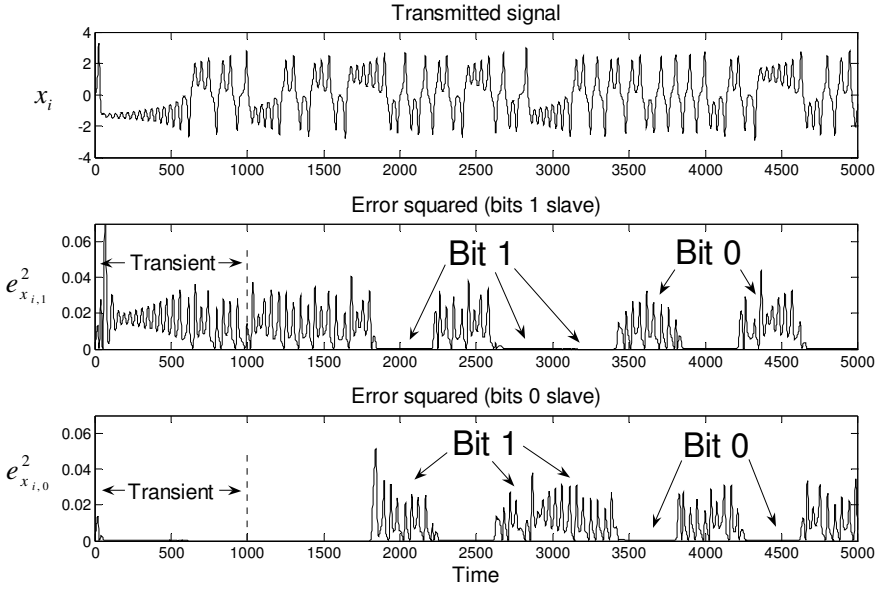


Fig. 9.5 The transmitted signal x_i and the squared synchronization errors $e^2_{x_{i,1}}$ and $e^2_{x_{i,0}}$

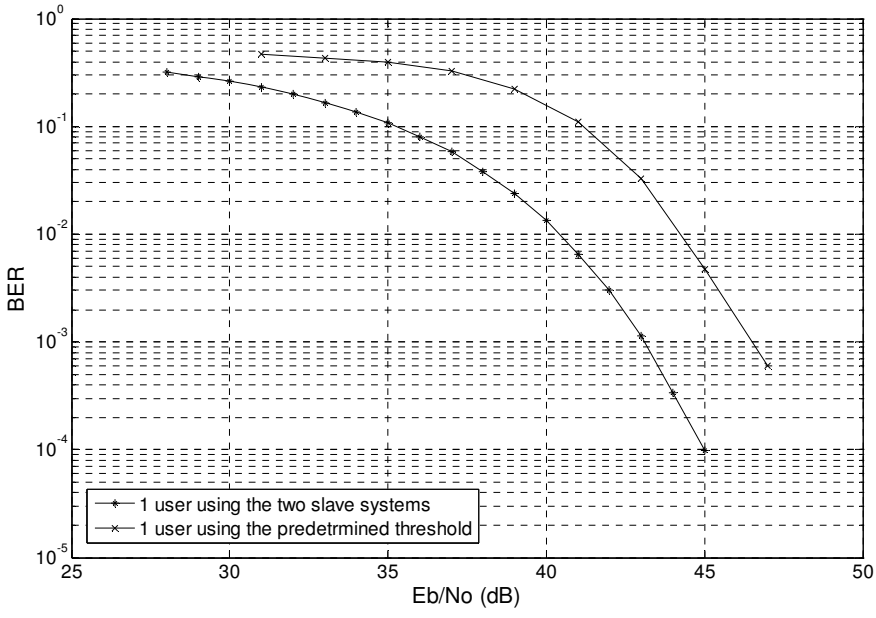


Fig. 9.6 The empirical BER curves of the chaos based TDM system of Figure 9.2 (predetermined threshold) and Figure 9.3 (two-slave receiver) for a single-user in the system.

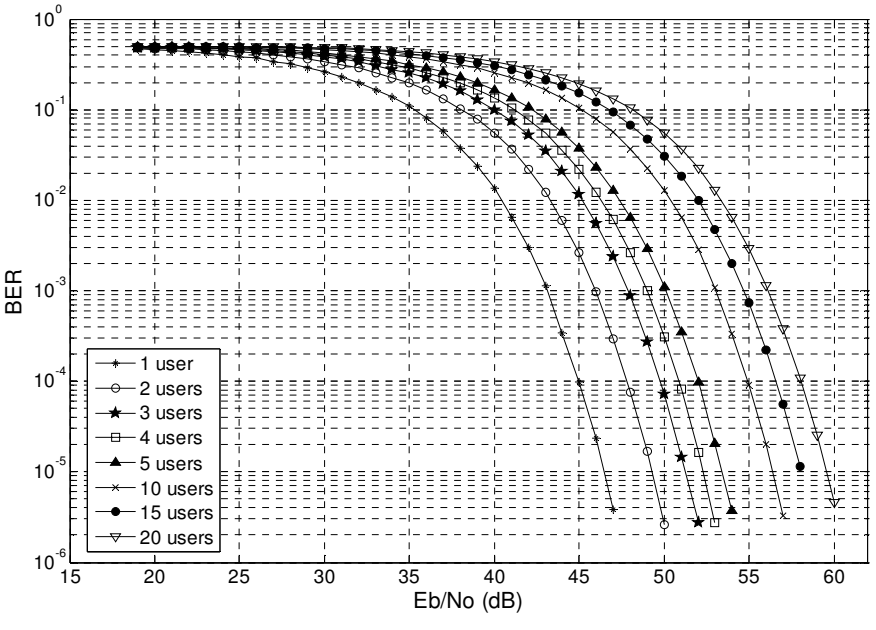


Fig. 9.7 The empirical BER curves of the chaos based TDM system of Figure 9.3 for 1-5, 10, 15 and 20 users

The empirical BER simulation results of the system of Figure 9.3 are shown in Figure 9.7 for 1-5, 10, 15 and 20 users in the AWGN channel. Again, by assuming that the highest acceptable BER level is equal to 10^{-3} [17,18], it can be observed from Figure 9.7 that the E_b / N_o for which the system performance is satisfactory for the case of 1, 2, 3, 4, 5, 10, 15 and 20 users is equal to approximately 43, 46, 48, 49, 50, 53, 55 and 56 dB, respectively.

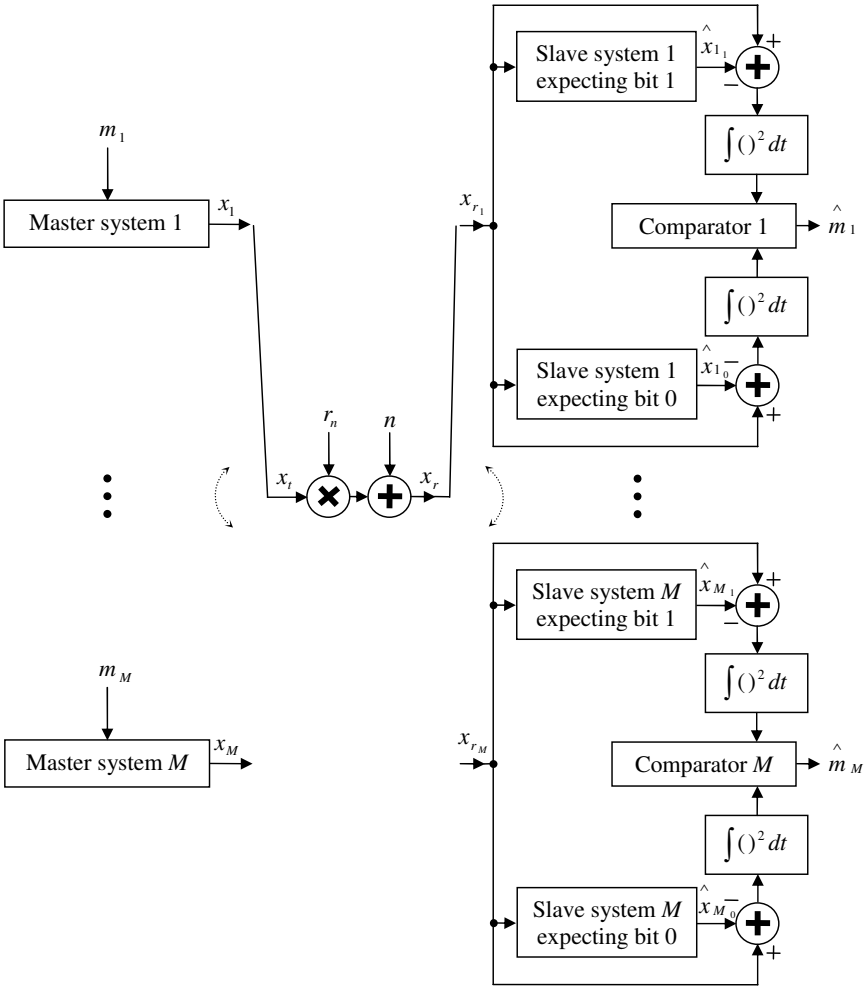


Fig 9.8 The Lorenz CPM based multi-user TDM communication system in the Rayleigh fading channel, implementing the two slaves at the receiver. The parameter values are $\sigma = 16$, $r = 45.6$ and $b_1 ... b_M \in \{3.5, ..., 4.45\}$.

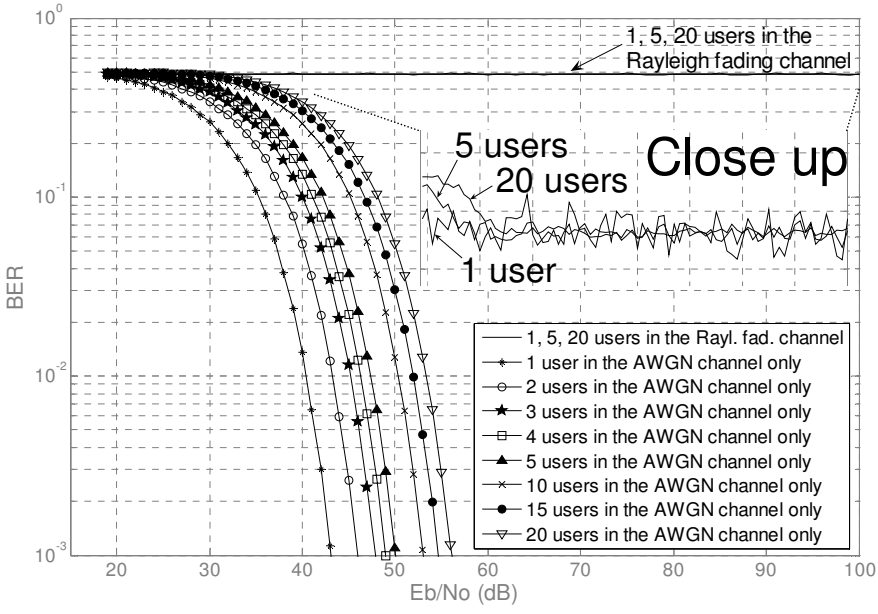


Fig. 9.9 The empirical BER curves of the Lorenz CPM based TDM system of Figure 9.8 for 1, 5 and 20 users (unmarked curves), with the close up. The corresponding empirical BER curves of the system of Figure 9.3 in the AWGN channel only are also shown (marked curves).

The system of Figure 9.3 is shown in Figure 9.8 in the Rayleigh fading channel. Figure 9.9 shows the empirical BER simulation results of the system of Figure 9.8 for 1, 5 and 20 users. It can be observed from Figure 9.9 that the system performance is unsatisfactory in the Rayleigh fading channel for any number of users in the system as the BER curves always remain at the BER level of 0.5. A close up of the BER curves reveals an initial marginal difference among 1, 5 and 20 users in the system. However, this difference is insignificant from a practical point of view.

9.1.3 The Ueda CPM Based TDM Communication System

The single-user Ueda CPM based chaotic communication system of chapter 6, subsection 6.2.2 [4,3], is now used to form a multi-user TDM communication system. The Ueda CPM based multi-user TDM communication system with the receiver implementing the predetermined threshold principle [4,3] is proposed in Figure 9.10.

In Figure 9.10, the binary message m is equal to 0 or 1 depending on whether a binary 0 or 1 is to be transmitted, respectively. The detailed operation of each TDM branch of the system of Figure 9.10 has been explained in subsection 6.2.2. As in subsection 9.1.2, the output of each TDM branch is interleaved to form a

signal x_t which is transmitted through the channel. To ensure security between the M users of the system, the parameters k and B of each master-slave pair are varied in the range $k_1 \ldots k_M \in \{0.03,\ldots,0.13\}$ and $B_1 \ldots B_M \in \{7.4,\ldots,10.3\}$. In contrast to the Lorenz CPM based TDM communication system of Figure 9.2 (9.3), the system of Figure 9.10 requires the controller for each master-slave pair in order to achieve synchronization. Provided that the power of noise in the system

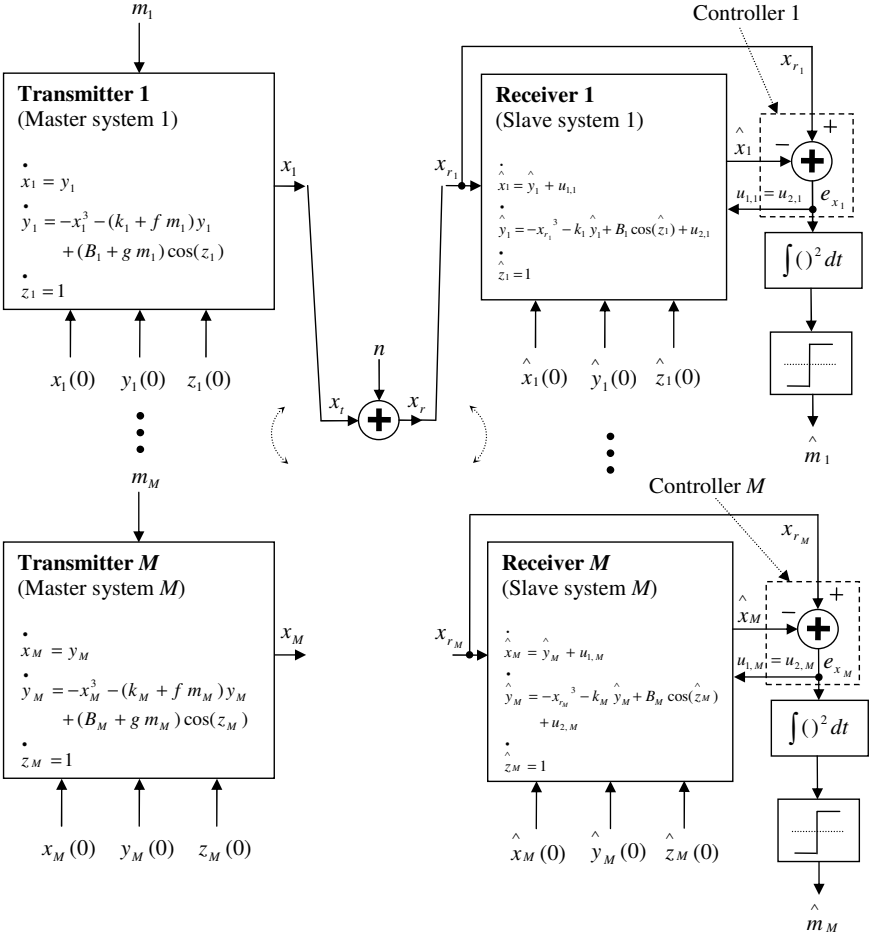


Fig. 9.10 The Ueda CPM based multi-user TDM communication system in the AWGN channel, implementing the predetermined threshold at the receiver. The parameter values are $k_1 \ldots k_M \in \{0.03,\ldots,0.13\}$ and $B_1 \ldots B_M \in \{7.4,\ldots,10.3\}$.

is comparatively low to the power of the signal causes the synchronization error, e_x, within each TDM branch to be equal to zero for a master-slave parameter match and non-zero for a mismatch.

It has been found that in terms of BER, the Ueda CPM based TDM communication system with the receiver based on the predetermined threshold, outperforms the same system with the receiver based on the two slave systems. This is confirmed in Figure 9.11 for the single-user system in the AWGN channel. It can be observed from Figure 9.11 that the system of Figure 9.3 outperforms the similar system based on the two slave receiver by approximately 2-4 dB. Therefore, the system of Figure 9.10, which implements the predetermined threshold, will be used to obtain the empirical BER simulation results for the Ueda CPM based multi-user TDM communication system. As before, the clock synchronization, as well as the synchronization among the multiplexing and de-multiplexing switches at the transmitter and the receiver is assumed.

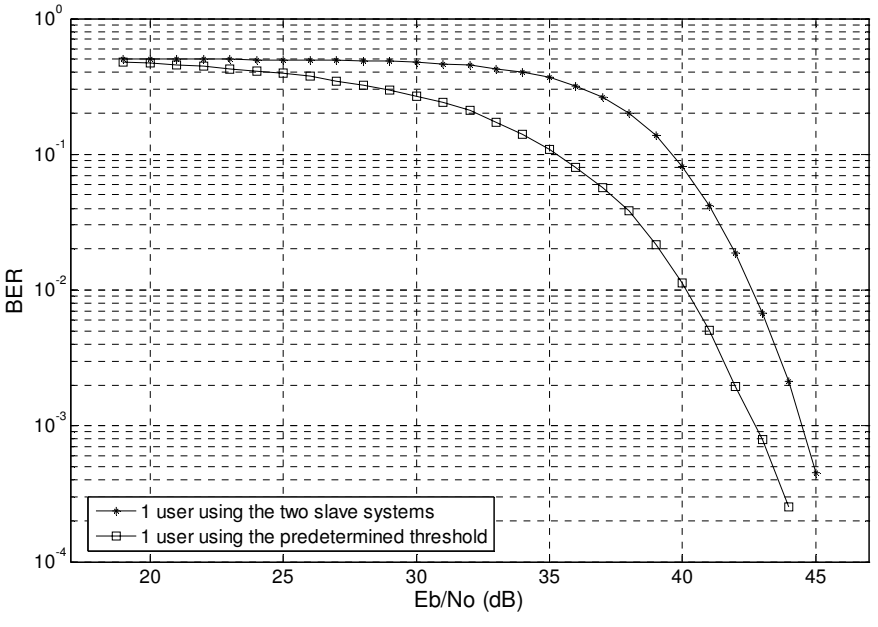


Fig. 9.11 The empirical BER curves of the Ueda CPM based TDM system of Figure 9.10 (predetermined threshold) and the corresponding system with the two-slave receiver for a single user in the system.

The empirical BER simulation results of the system of Figure 9.10 are shown in Figure 9.12 for 1-5, 10, 15 and 20 users in the AWGN channel. Again, by assuming that the highest acceptable level of BER equals 10^{-3} [17,18], it can be observed from Figure 9.12 that the E_b / N_o for which the system performance is satisfactory for the case of 1, 2, 3, 4, 5, 10, 15 and 20 users is equal to approximately 42.5, 46, 47.5, 49, 50, 53, 54.5 and 56 dB, respectively.

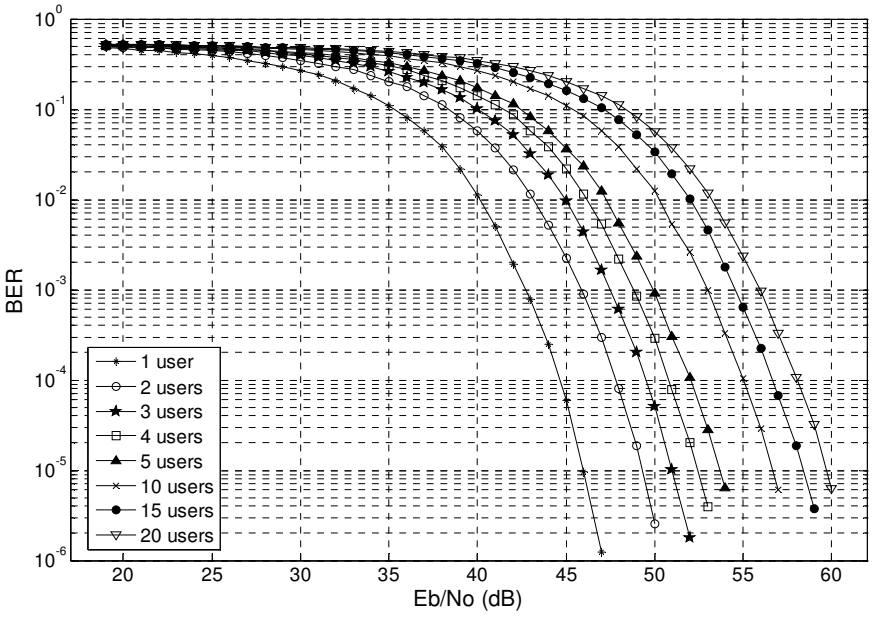


Fig. 9.12 The empirical BER curves of the Ueda CPM based TDM system of Figure 9.10 for 1-5, 10, 15 and 20 users

The system of Figure 9.10 is shown in Figure 9.13 in the Rayleigh fading channel. The empirical BER curves of this system are shown in Figure 9.14 for 1, 5 and 20 users in the system. It can be observed from Figure 9.14 that the system performance is unsatisfactory in the Rayleigh fading channel for any number of users in the system as the BER curves always remain at the BER level of 0.5. A close up of the BER curves reveals no observable difference among 1, 5 and 20 users in the system.

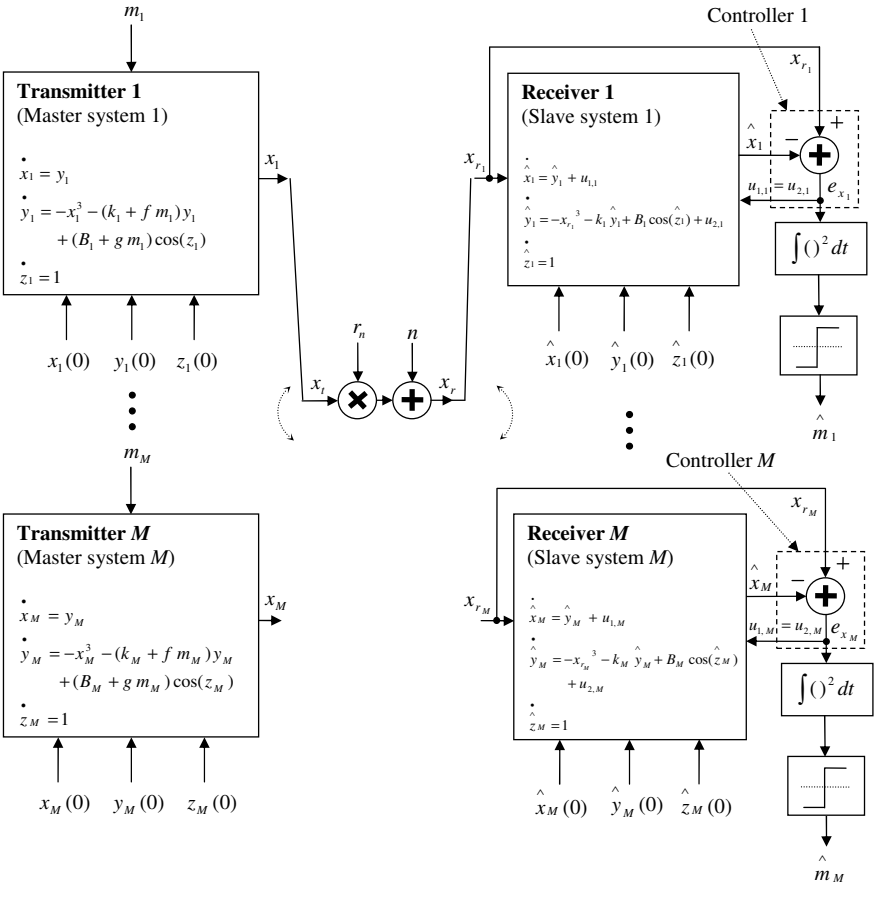


Fig. 9.13 The Ueda CPM based multi-user TDM communication system in the Rayleigh fading channel, implementing the predetermined threshold at the receiver. The parameter values are $k_1 \ldots k_M \in \{0.03,\ldots,0.13\}$ and $B_1 \ldots B_M \in \{7.4,\ldots,10.3\}$.

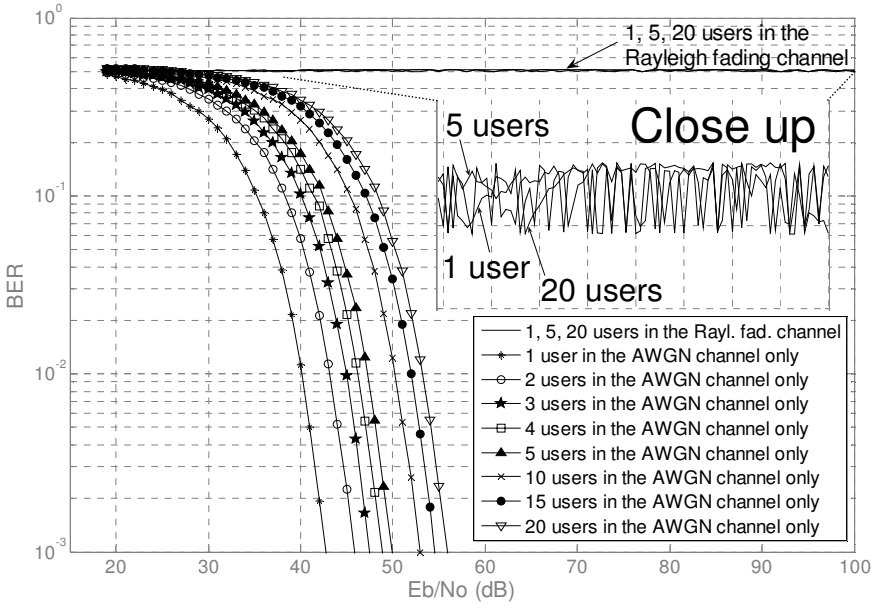


Fig. 9.14 The empirical BER curves of the Ueda CPM based TDM system of Figure 9.13 for 1, 5 and 20 users (unmarked curves), with the close up. The corresponding empirical BER curves of the system of Figure 9.10 in the AWGN channel only are also shown (marked curves).

9.1.4 Performance Comparison of the Lorenz CPM Based to Ueda CPM Based TDM Chaotic Communication System in an AWGN Channel

In this subsection, the BER performance of the Lorenz CPM based multi-user TDM system of Figure 9.3 is compared to the corresponding Ueda CPM based system of Figure 9.10. The performance is compared in the AWGN channel only. It has been observed from Figures 9.9 and 9.14 that in the Rayleigh fading channel both systems exhibit unsatisfactory performance as their respective BER curves remain at 0.5 for any number of users in the system.

In Figure 9.15, the BER numerical simulation results of the Lorenz CPM based TDM system of Figure 9.3 are plotted on the same set of axes with those of the Ueda CPM based TDM system of Figure 9.10.

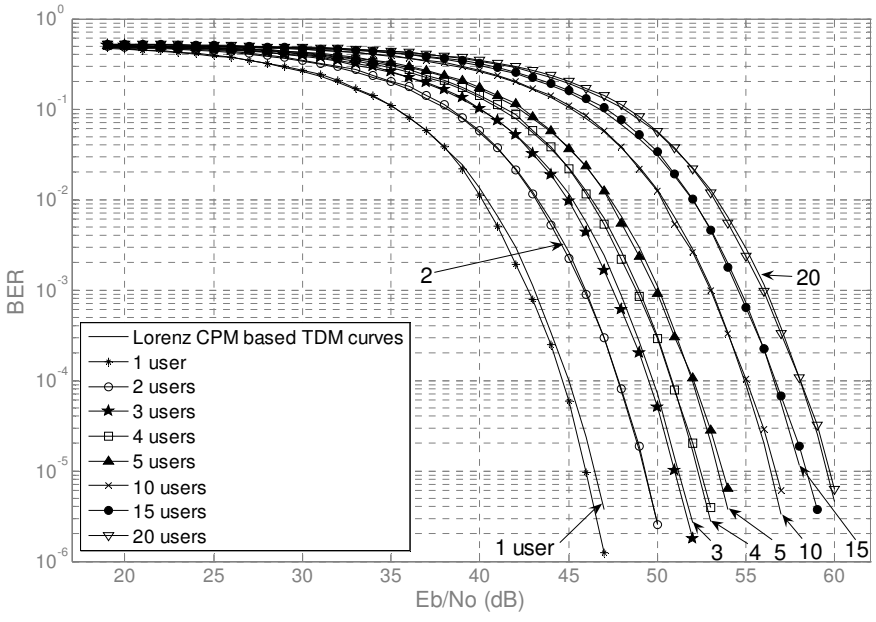


Fig. 9.15 The empirical BER curves of the Ueda CPM based TDM system of Figure 9.10 for 1-5, 10, 15 and 20 users (marked curves), alongside the corresponding empirical BER curves of the Lorenz CPM based TDM system of Figure 9.3 (unmarked curves).

It can be observed from Figure 9.15 that the BER performance of the Lorenz CPM based TDM system is virtually identical to that of the Ueda CPM based TDM system for any number of users in the system.

9.1.5 Performance Comparison of the CPM Based TDM Systems to the Chaos Based DS-CDMA System of Chapter 7 and the Chaos Based TDM System of Chapter 8

In this subsection, the performance of the Lorenz and Ueda CPM based TDM systems is compared to that of the chaos based DS-CDMA system of Figure 7.1 and the chaos based TDM system of Figure 8.8.

In Figure 9.16, the AWGN BER curves of the Lorenz CPM based TDM system of Figure 9.3 and the chaos based DS-CDMA system of Figure 7.1 are plotted on the same set of axes.

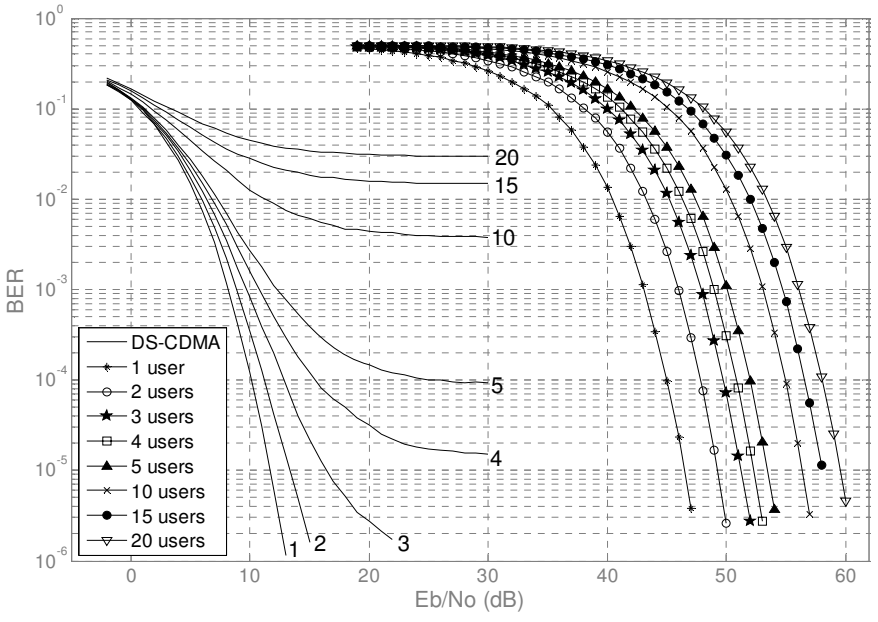


Fig. 9.16 The empirical BER curves of the Lorenz CPM based TDM system of Figure 9.3 for 1-5, 10, 15 and 20 users (marked curves) in the AWGN channel. The corresponding empirical BER curves of the chaos based DS-CDMA system of Figure 7.1 are shown by unmarked curves.

It can be observed from Figure 9.16 that for low number of users in the system (1-5), at the BER level of 10^{-3}, the chaos based DS-CDMA system outperforms the Lorenz CPM based TDM system by approximately 35-38 dB. It can thus be concluded that in terms of BER, for low number of users in the system, the chaos based DS-CDMA system is a superior system. However, for a larger number of users in the system (10, 15, 20), the Lorenz CPM based TDM system outperforms the chaos based DS-CDMA system as its BER curves do not flatten. Note that as the BER performance of the Lorenz and Ueda CPM based TDM systems of sub-sections 9.1.1 and 9.1.2 is essentially identical, the same conclusion can be drawn for the Ueda CPM based TDM system.

Although the Lorenz and Ueda CPM based TDM systems outperform the chaos based DS-CDMA system for large number of users in the system, it should be noted that the two CPM based systems are only functional at the E_b / N_o level of 40-60 dB. Therefore, the two CPM based systems require that the bit energy, E_b, be ten thousand to a million times larger than noise power spectral density, N_o, for the systems to be operational. In the next section it is shown that the ICM based TDM chaotic communication systems are more robust to the influence of AWGN than are the CPM based TDM systems.

In Figure 9.17, the BER curves of the Lorenz CPM based TDM system of Figure 9.3 are compared to those of the chaos based TDM system of Figure 8.8, chapter 8, in the AWGN channel.

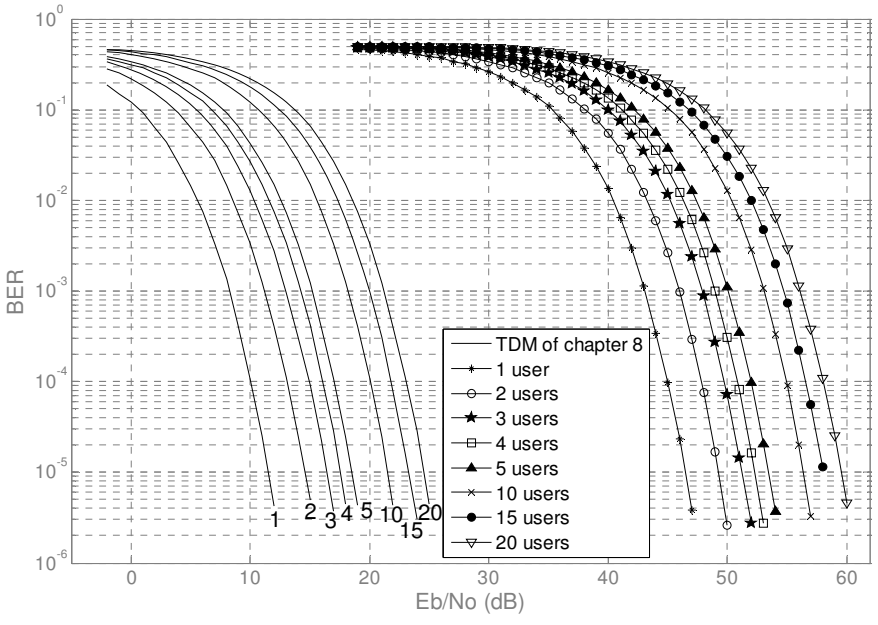


Fig. 9.17 The empirical BER curves of the Lorenz CPM based TDM system of Figure 9.3 for 1-5, 10, 15 and 20 users (marked curves) in the AWGN channel. The corresponding empirical BER curves of the chaos based TDM system of Figure 8.8, chapter 8, are shown by unmarked curves.

It can be observed from Figure 9.17 that at the BER level of 10^{-3}, the chaos based TDM system of Figure 8.8, chapter 8, outperforms the Lorenz (and Ueda) CPM based TDM system of Figure 9.3 (Figure 9.10) by approximately 35 dB. It can thus be concluded that in terms of BER, the chaos based TDM system of chapter 8 is a superior system for any number of users in the system.

A similar BER comparison to that of Figures 9.16 and 9.17 is now performed in the Rayleigh fading channel. In Figures 9.18 and 9.19, the Lorenz CPM based TDM system of Figure 9.8 is compared to the chaos based DS-CDMA system of chapter 7 (Figure 7.12) and to the chaos based TDM system of chapter 8 (Figure 8.13), respectively.

It can be observed from Figures 9.18 and 9.19 that the chaos based DS-CDMA and TDM systems of chapters 7 and 8, respectively, outperform the Lorenz CPM based TDM system of Figure 9.8. Again, the same conclusion can be drawn in regard to the Ueda CPM based TDM system of Figure 9.13 as its BER performance closely resembles that of the Lorenz CPM based TDM system of Figure 9.8.

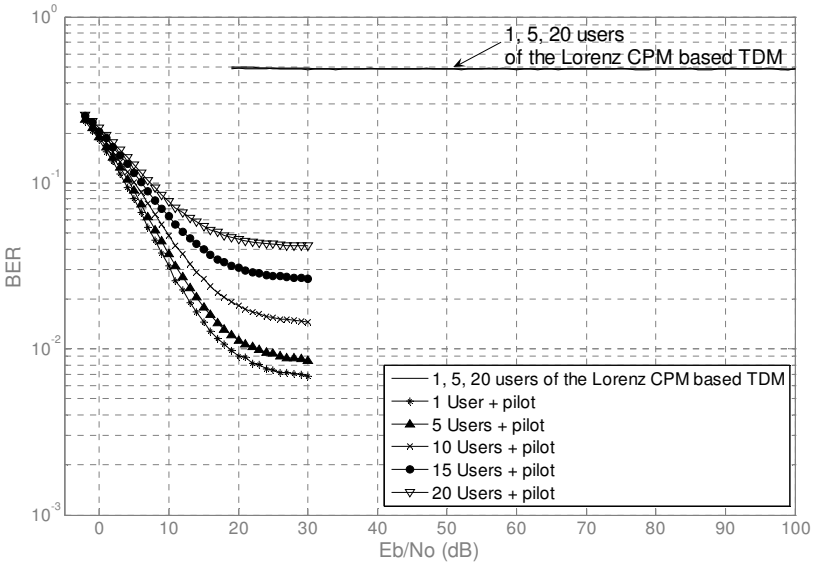


Fig. 9.18 The empirical BER curves of the chaos based DS-CDMA system of Figure 7.12 for 1, 5, 10, 15 and 20 users (marked curves) in the Rayleigh fading channel. The corresponding empirical BER curves of the Lorenz CPM based TDM system of Figure 9.8, are shown by unmarked curves.

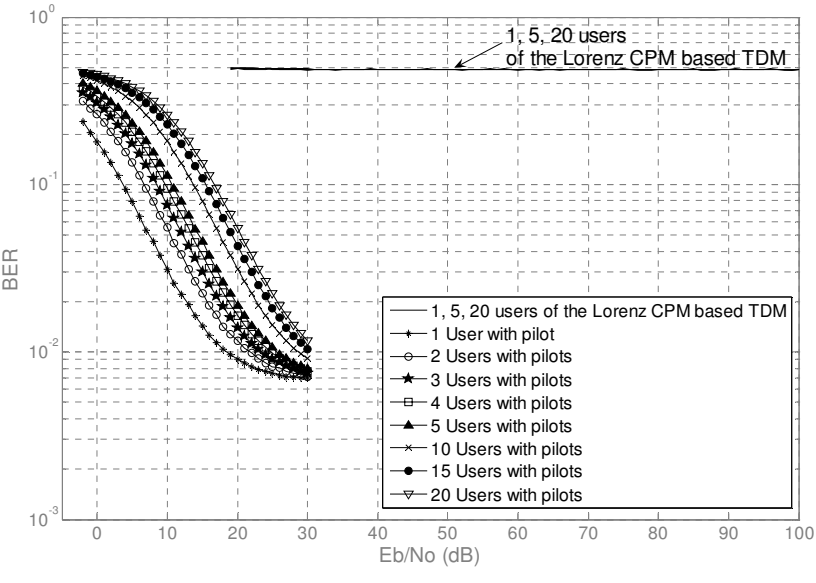


Fig. 9.19 The empirical BER curves of the chaos based TDM system of Figure 8.13 for 1-5, 10, 15 and 20 users (marked curves) in the Rayleigh fading channel. The corresponding empirical BER curves of the Lorenz CPM based TDM system of Figure 9.8, are shown by unmarked curves.

However, as can be observed from Figures 9.18 and 9.19, neither of the systems satisfies the highest acceptable BER level of 10^{-3}. Therefore, the systems are impractical in the Rayleigh fading channel.

9.2 The ICM Based Multi-user TDM Communication System

In this section, the single-user Ueda ICM based chaotic communication system of subsection 6.3.2 [4,3] is used to construct the ICM based multi-user TDM communication system. Furthermore, the single-user Ueda ICM based chaotic communication system with only the master signal x transmitted, as outlined in the appendix [19], is also used to construct an ICM based TDM system. The performance of the two systems is examined and compared in terms of the BER in AWGN and Rayleigh fading channels. As in section 9.1, their performance is then compared to the performance of the chaos based DS-CDMA system of chapter 7 and TDM system of chapter 8. In contrast to the chaos based DS-CDMA and TDM systems of chapters 7 and 8, the sequence synchronization of the ICM based TDM system is achieved through the process of chaotic synchronization principles of chapters 5 and 6.

9.2.1 The Principles of the ICM Based Multi-user TDM Communication System

In subsection 6.3.1, the principles of the single-user ICM based chaotic communication system have been outlined. In this subsection, the principles of the ICM based multi-user TDM chaotic communication system, shown in Figure 9.20, are proposed.

As in Figure 9.1, each TDM branch of an ICM based TDM system of Figure 9.20 is composed of a chaotic master-slave pair. The principles of operation of a chaotic master-slave pair, within an ICM based communication system, have been described in section 6.3. The transmitted signal, x_t, is received as the signal x_r which is then de-multiplexed at the receiver into M signals, x_{r_1} to x_{r_M}, where M denotes the number of users in the system. The multiplexing and de-multiplexing operations of Figure 9.20 are performed in the same manner as for the CPM based TDM systems of subsection 9.1.1. The messages are recovered within each branch by driving each slave system by the corresponding master signal and observing the nature of the error e_x. As discussed in section 6.3, the difference in the master-slave initial conditions governs the synchronization error. Therefore, in order to ensure successful recovery of the transmitted bits, each slave system at the receiver must have the knowledge of the corresponding master system's initial conditions. Furthermore, it should be noted that all the parameters of all the master and slave systems are identical. Finally, in order to ensure security among different users of the system, it is important to assign different initial condition values to each master-slave pair within the TDM system.

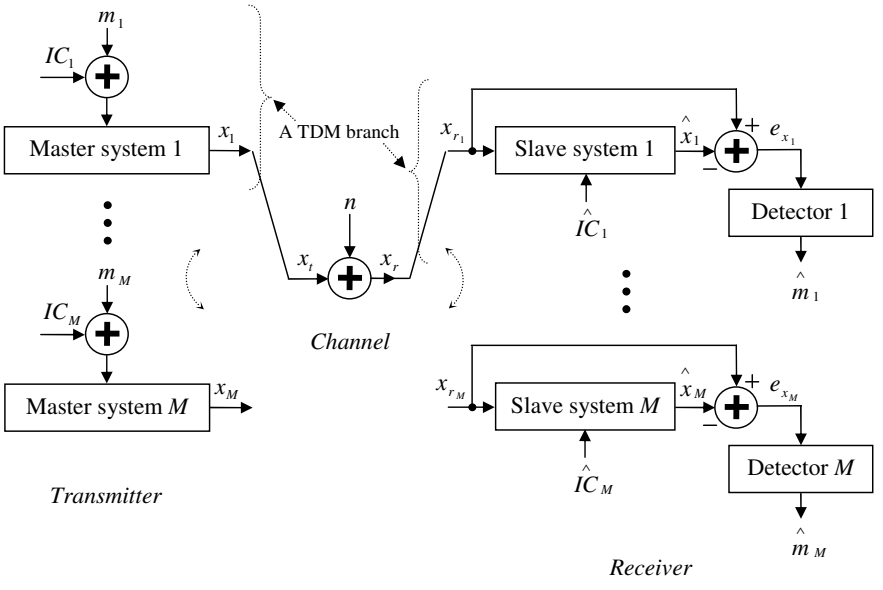


Fig. 9.20 A block diagram of the multi-user TDM chaotic communication system based on the initial condition modulation concept

Besides the predetermined threshold receiver used in chapter 6 and Figure 9.20, it is also possible to design the system to include two slave systems within each TDM branch. As for the CPM based systems, in this way the outputs of the two slave systems are used in the symbol detection by comparing the two detector outputs to each other. The architecture of the receiver with two slave systems is explained on the Ueda ICM based TDM communication system of subsection 9.2.2. However, it is shown that for the ICM based systems examined, the receivers with two slave systems lead to the inferior BER performance.

9.2.2 The Ueda ICM Based TDM Communication System

The Ueda ICM based multi-user TDM communication system with the receiver implementing the predetermined threshold principle [4,3] is proposed in Figure 9.21. The principles of operation of the corresponding single-user system have been presented in the subsection 6.3.2 of chapter 6 [4,3].

In Figure 9.21, the signals $x_1, y_1; \ldots x_M, y_M$ are first multiplexed into the set of signals $s_1 \ldots s_M$ which are in turn multiplexed into the signal s_t. The signal s_t passes through the channel and is received in the form of the signal s_r. The signal s_r is then de-multiplexed into the set of signals $s_{r_1} \ldots s_{r_M}$. Finally, the set

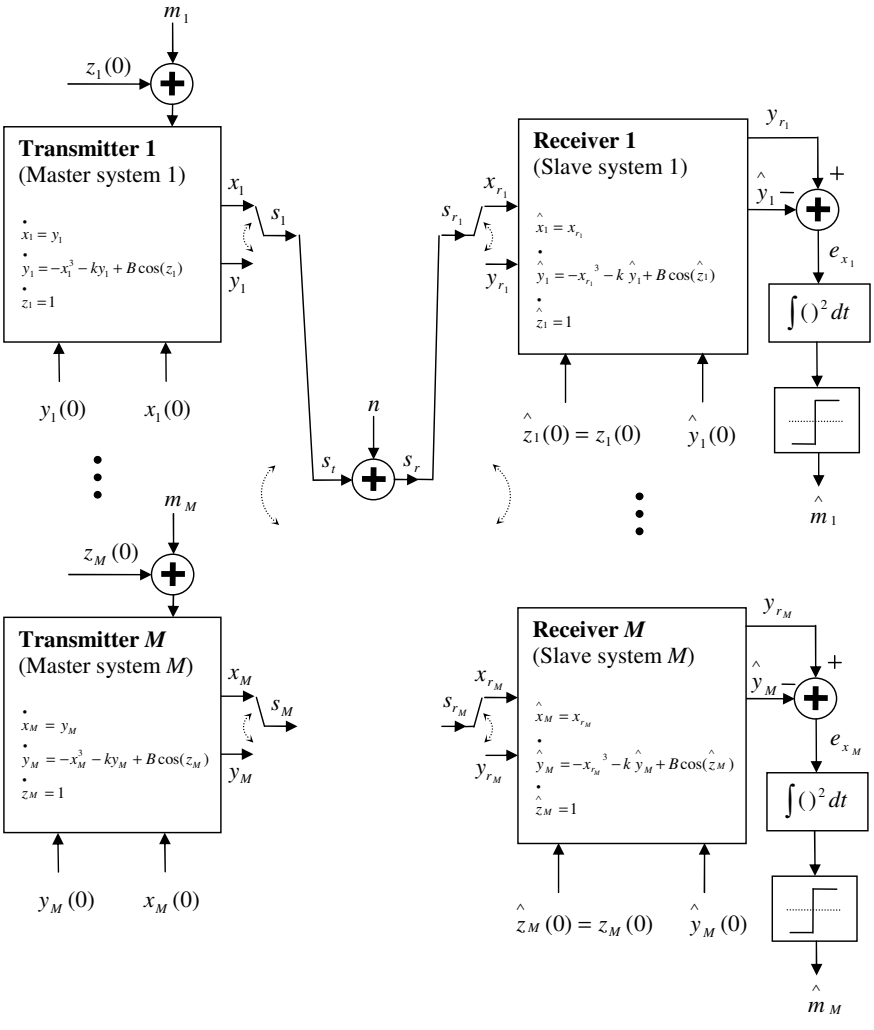


Fig. 9.21 The Ueda ICM based multi-user TDM communication system in the AWGN channel, implementing the predetermined threshold at the receiver. The parameter values are $k = 0.05$, $B = 7.5$.

of signals $s_{r_1} \ldots s_{r_M}$ is de-multiplexed into the set of signals $x_{r_1}, y_{r_1}; \ldots x_{r_M}, y_{r_M}$ of which the signals $x_{r_1} \ldots x_{r_M}$ are used to drive the corresponding slave systems. As explained in subsection 6.3.2, the set of signals $y_{r_1} \ldots y_{r_M}$ is used in conjunction with the output of the slave systems to decode the received information. To ensure the security between the *M* users of the system, the initial conditions of each of the master-slave pairs need to be different

from each other. In Figure 9.21, the bit 0 is represented by $m = 2\pi$ and bit 1 by $m = \pi$ [4,3]. Furthermore, as shown in chapters 5 and 6, it is of crucial importance that the difference among the master-slave z initial conditions be equal to $\pm 2n\pi$, where n is any integer [4]. In this way, it is ensured that for a bit 0 each master-slave pair synchronizes and for a bit 1 it does not, with the synchronization error reaching its maximum possible value. For simplicity, in Figure 9.21, n has

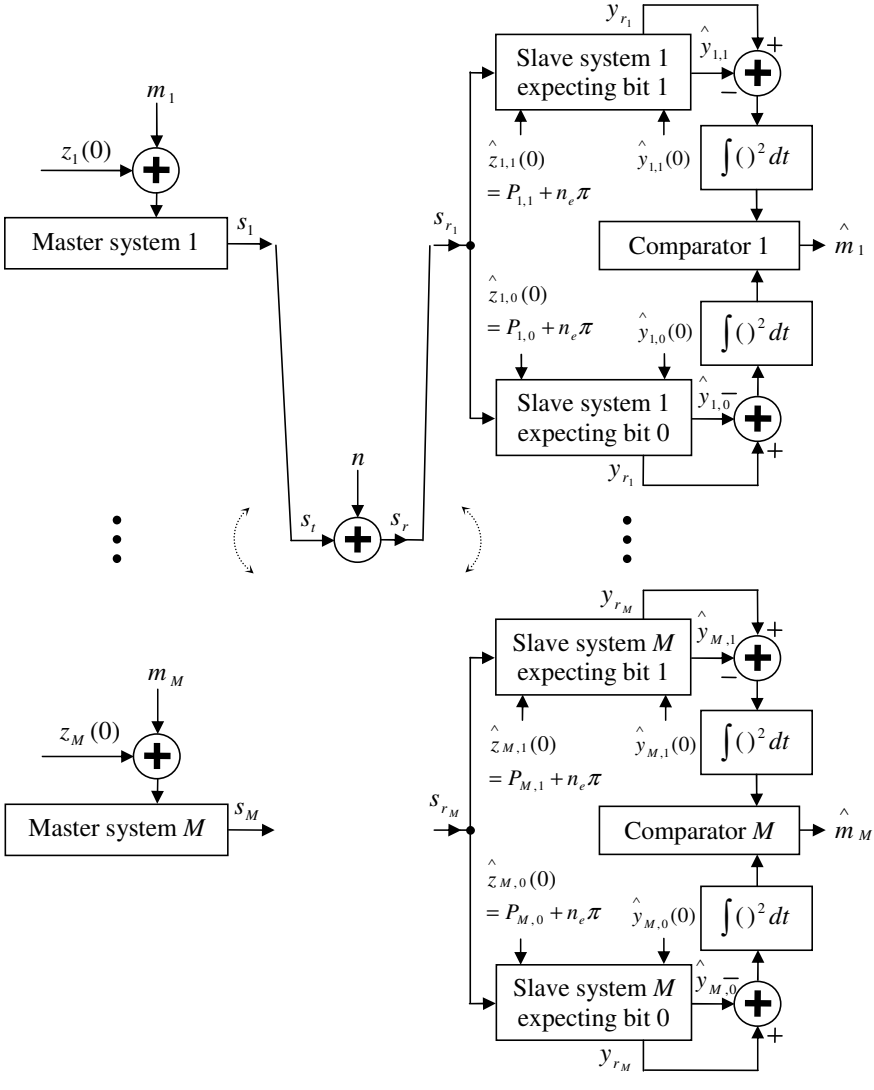


Fig. 9.22 The Ueda ICM based multi-user TDM communication system in the AWGN channel, implementing the two slaves at the receiver, where n_e denotes any even integer.

been set to zero. The principles of operation of a Ueda master-slave pair, when implemented within an ICM system, have been explained in detail in subsection 6.3.2.

In Figure 9.22, a similar system to that of Figure 9.21 is shown, however the receiver of Figure 9.22 implements the two slave systems per each TDM branch. A detailed description of the master-slave pair within a TDM branch is shown in Figure 9.23.

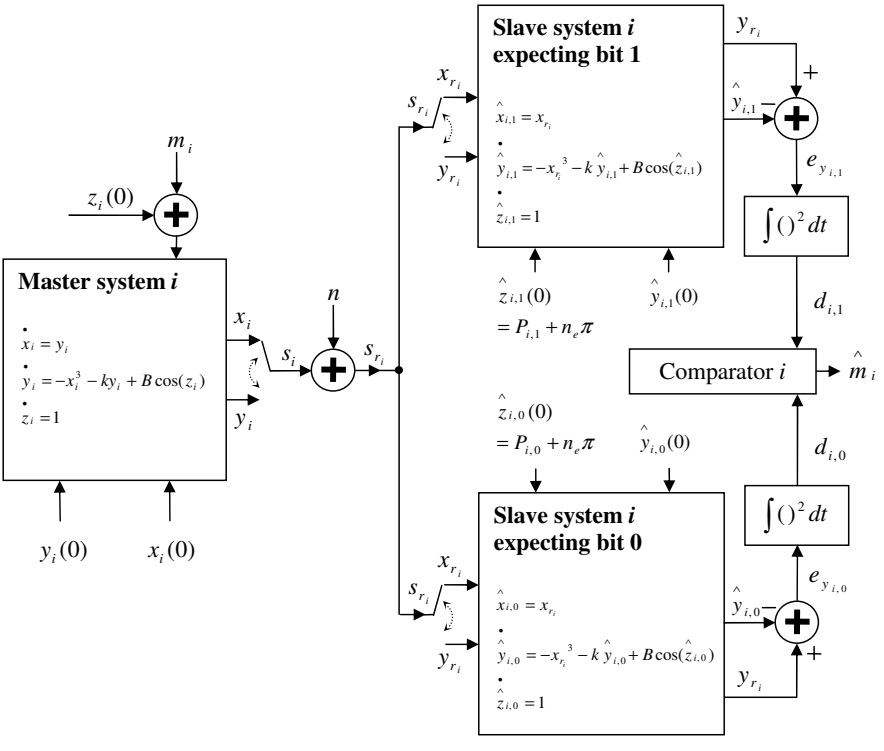


Fig. 9.23 A single branch of the Ueda ICM based multi-user TDM communication system of Figure 9.22, where n_e denotes any even integer. The parameter values are $k = 0.05$, $B = 7.5$.

In Figure 9.23, $P_{i,1}$ of the upper slave system is set equal to $P_{i,1} = z_i(0) + m_{i,1}$, where $m_{i,1}$ denotes the binary symbol 1 and is set to $m_{i,1} = \pi$ for all time. Alternatively, $P_{i,0}$ of the lower slave system is set equal to $P_{i,0} = z_i(0) + m_{i,0}$ where $m_{i,0}$ denotes the binary symbol 0 and is set to $m_{i,0} = 2\pi$ for all time. Therefore, the initial conditions of the upper slave system are so set to always cause synchronization of the master-slave system when bit 1 is transmitted. Alternatively, those

of the lower slave system are set to always cause synchronization of the master-slave system when bit 0 is transmitted. Accordingly, the decision variable $d_{i,1}$ of the upper slave system tends to zero when bit 1 is transmitted and does not when bit 0 is transmitted. In contrast, the decision variable $d_{i,0}$ of the lower slave system tends to zero when bit 0 is transmitted and does not when bit 1 is transmitted. Therefore, if $d_{i,1} > d_{i,0}$ for a particular bit, the comparator decides in favour of bit 0 and vice-versa. The transmitted signal s_i, of Figure 9.23, is shown in Figure 9.24 when the series of 10 bits is transmitted, that is, when m_i = [2π, 2π, π, 2π, π, π, 2π, π, 2π, π], or in binary terms: *message* = [0 0 1 0 1 1 0 1 0 1]. Furthermore, Figure 9.24 also shows the corresponding squared synchronization errors of the two slave systems under noiseless conditions. It can be observed from Figure 9.24 that the slave system, with initial conditions set to cause synchronization for bit 1, indeed synchronizes to the master system when a bit 1 is transmitted. Similarly, it can be observed that the slave system, with initial conditions set to cause synchronization for bit 0, indeed synchronizes to the master system when a bit 0 is transmitted. Note that as in chapter 6, the spreading factor of 400 has been used to represent one bit.

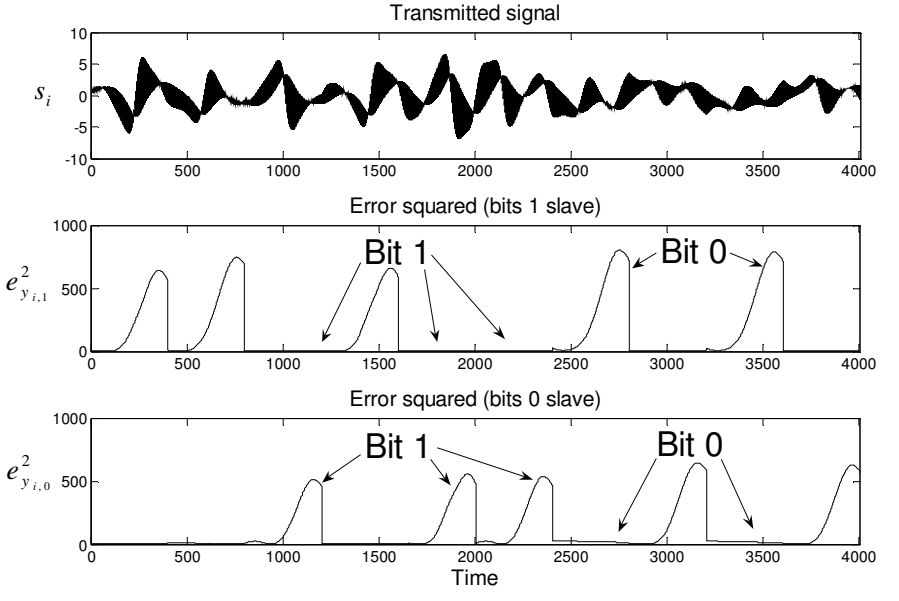


Fig. 9.24 The transmitted signal s_i and the squared synchronization errors $e^2_{y_{i,1}}$ and $e^2_{y_{i,0}}$

The bit error rate numerical simulation result of the single-user system of Figure 9.21 is compared to that of Figure 9.22 in Figure 9.25, in the AWGN channel. It can be observed from Figure 9.25 that the system of Figure 9.21 outperforms the system of Figure 9.22 by approximately 4 dB. Therefore, the system of Figure 9.21, which implements the predetermined threshold, will be used to obtain the empirical BER simulation results for the Ueda ICM based multi-user TDM communication system. Again, the clock synchronization, as well as the synchronization among the multiplexing and de-multiplexing switches at the transmitter and the receiver is assumed.

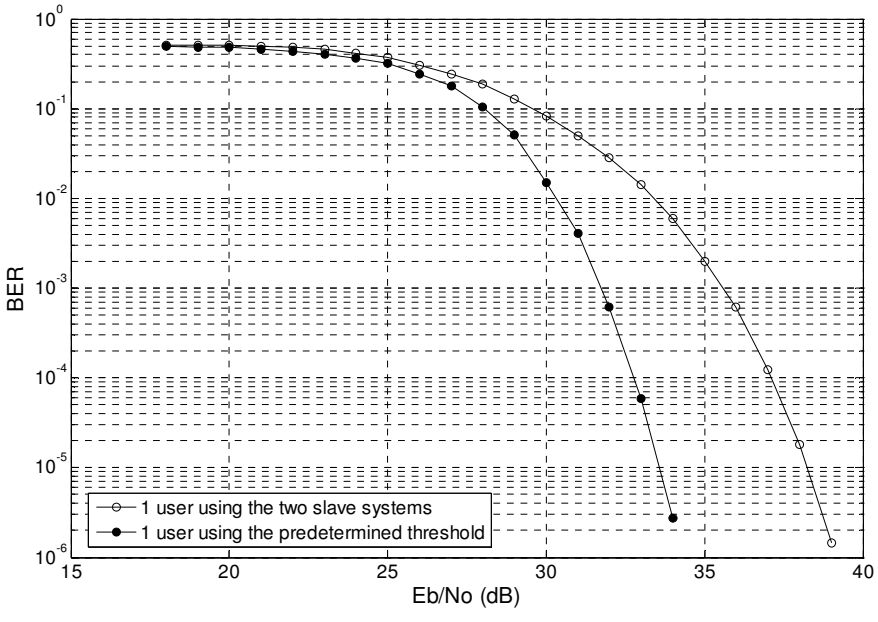


Fig. 9.25 The empirical BER curves of the Ueda ICM based TDM system of Figure 9.21 (predetermined threshold) and Figure 9.22 (two-slave receiver) for a single user in the system.

The empirical BER simulation results of the system of Figure 9.21 are shown in Figure 9.26 for 1-5, 10, 15 and 20 users in the AWGN channel. Again, by assuming that the highest acceptable level of BER equals 10^{-3} [17,18], it can be

observed from Figure 9.26 that the E_b / N_o for which the system performance is satisfactory for the case of 1, 2, 3, 4, 5, 10, 15 and 20 users is equal to approximately 32, 35, 36.5, 38, 39, 42, 43.5 and 44.5 dB, respectively.

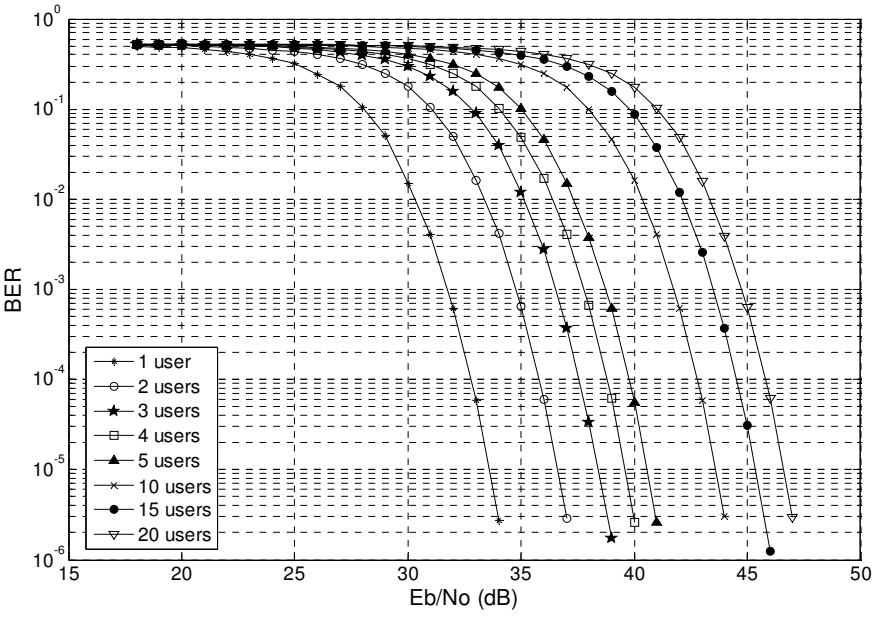


Fig. 9.26 The empirical BER curves of the Ueda ICM based TDM system of Figure 9.21 for 1-5, 10, 15 and 20 users

The system of Figure 9.21 is shown in Figure 9.27 in the Rayleigh fading channel. In Figure 9.28 the empirical BER simulation results of the system of Figure 9.27 are shown for 1, 5 and 20 users. As for the Lorenz and Ueda CPM based TDM systems, it can be observed from Figure 9.27 that the performance of the Ueda ICM based TDM system is also unsatisfactory in the Rayleigh fading channel for any number of users in the system. A close up of the BER curves reveals an initial difference among 1, 5 and 20 users in the system, before the curves settle to the BER level of approximately 0.4. However, as for the CPM based systems, this difference is insignificant from a practical point of view.

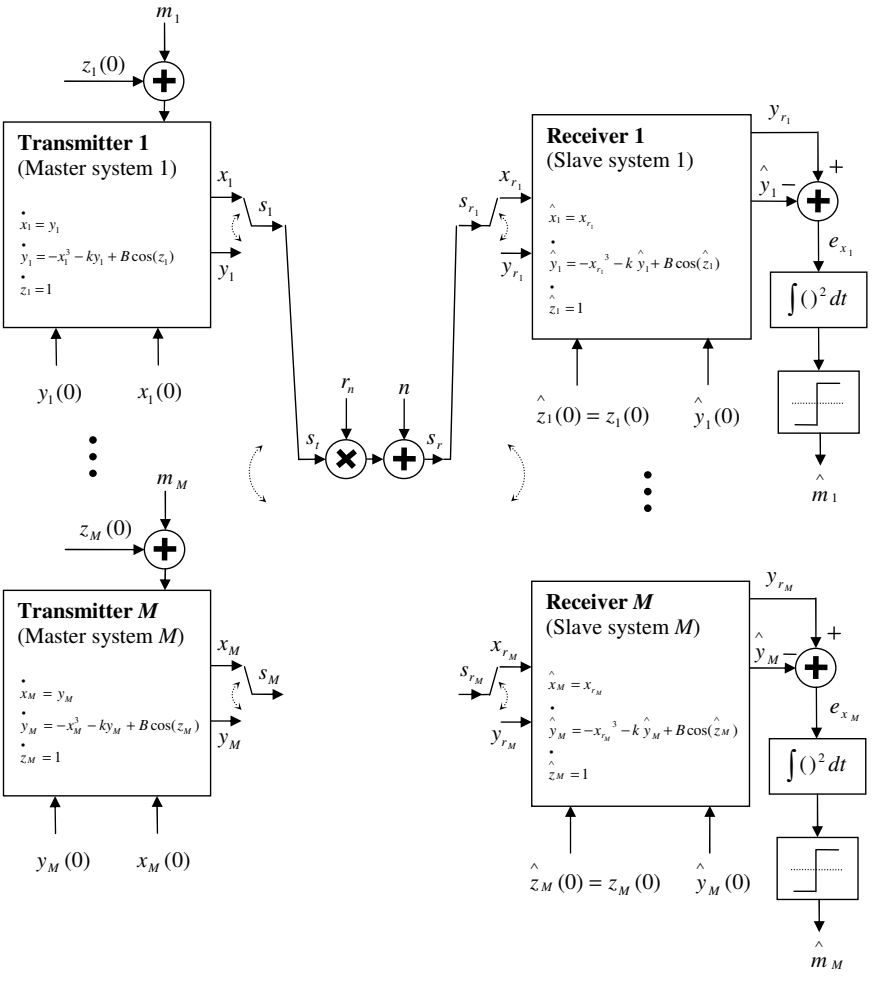


Fig. 9.27 The Ueda ICM based multi-user TDM communication system in the Rayleigh fading channel, implementing the predetermined threshold at the receiver. The parameter values are $k = 0.05$, $B = 7.5$.

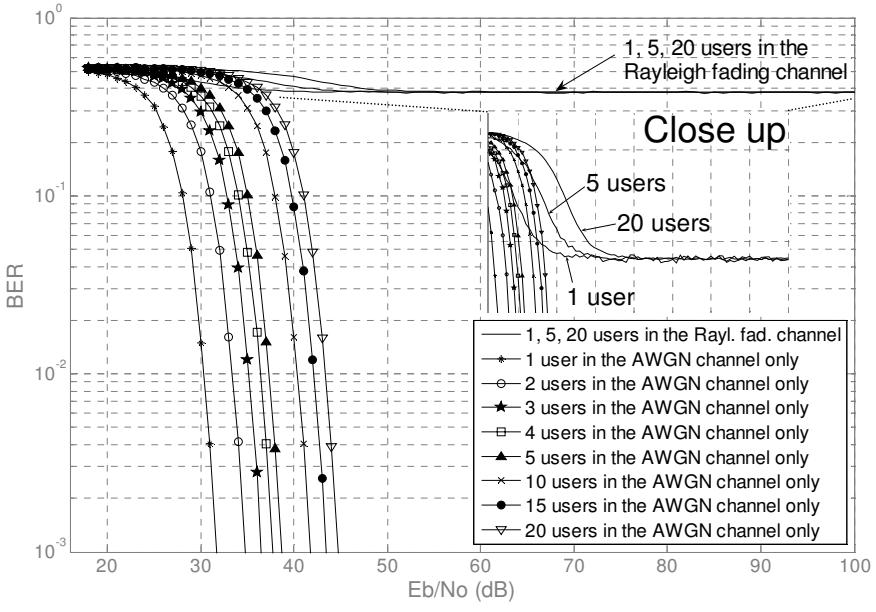


Fig. 9.28 The empirical BER curves of the Ueda ICM based TDM system of Figure 9.27 for 1, 5 and 20 users (unmarked curves), with the close up. The corresponding empirical BER curves of the system of Figure 9.21 in the AWGN channel only are also shown (marked curves).

9.2.3 The Ueda ICM Based TDM Communication System with Only x Transmitted

In this subsection, the Ueda ICM based multi-user TDM system with only the master signal x transmitted, is proposed. The single-user Ueda ICM based chaotic communication system with only the master signal x transmitted, has been presented in the appendix [19]. The Ueda ICM based multi-user TDM communication system with only the master signal x transmitted and the receiver implementing the predetermined threshold principle [4,3], is proposed in Figure 9.29.

In general, the operation of the Ueda ICM based TDM system of Figure 9.29 is identical to that of the system of Figure 9.21, except that the receiver uses only the slave signal $\hat{y}$ to decode the message. This is in contrast to the Ueda ICM based TDM system of Figure 9.21 which uses the synchronization error of the master-slave y signals to decode the message. Therefore, in the case of the system of Figure 9.29, it is not required to transmit the master signal y but only the master signal x which is used to drive the slave system. The detailed operation of each TDM branch of the system of Figure 9.29 has been explained in the appendix. As in subsection 9.1.2, the output of each TDM branch is interleaved to form a signal x_t which is transmitted through the channel.

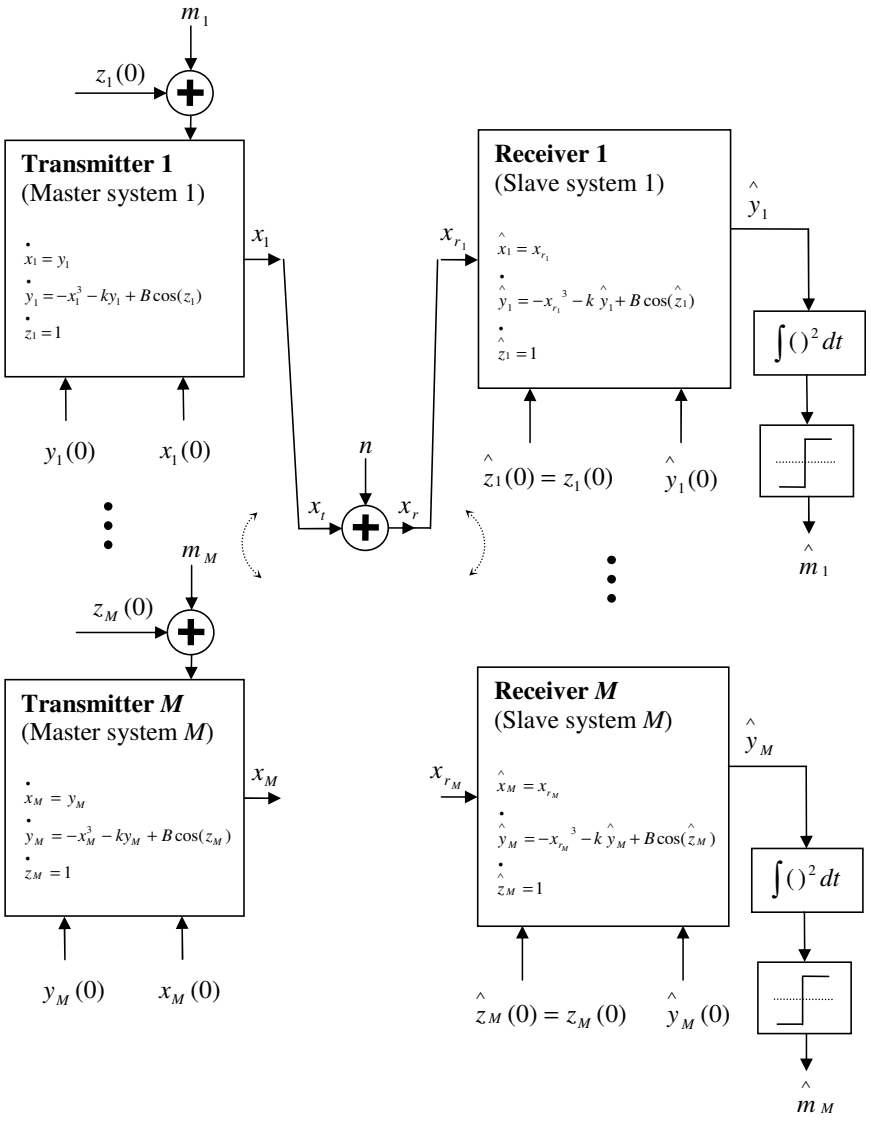


Fig. 9.29 The Ueda ICM based multi-user TDM communication system with only the master signal x transmitted, in the AWGN channel and implementing the predetermined threshold at the receiver. The parameter values are $k = 0.05$, $B = 7.5$.

It has been found that in terms of BER, the Ueda ICM based TDM communication system with only x transmitted and the receiver based on the predetermined threshold, outperforms the same system with the receiver based on the two slave systems. This is confirmed in Figure 9.30 for the single-user system in the AWGN channel. It can be observed from Figure 9.30 that the system of Figure 9.29 outperforms the similar system based on the two slave receiver by approximately 2-4 dB. Therefore, the system of Figure 9.29, which implements the predetermined threshold, will be used to obtain the empirical BER simulation results for the Ueda ICM based multi-user TDM communication system with only x transmitted. Again, the clock synchronization, as well as the synchronization among the multiplexing and de-multiplexing switches at the transmitter and the receiver is assumed.

The empirical BER simulation results of the system of Figure 9.29 are shown in Figure 9.31 for 1-5, 10, 15 and 20 users in the AWGN channel. It can be observed

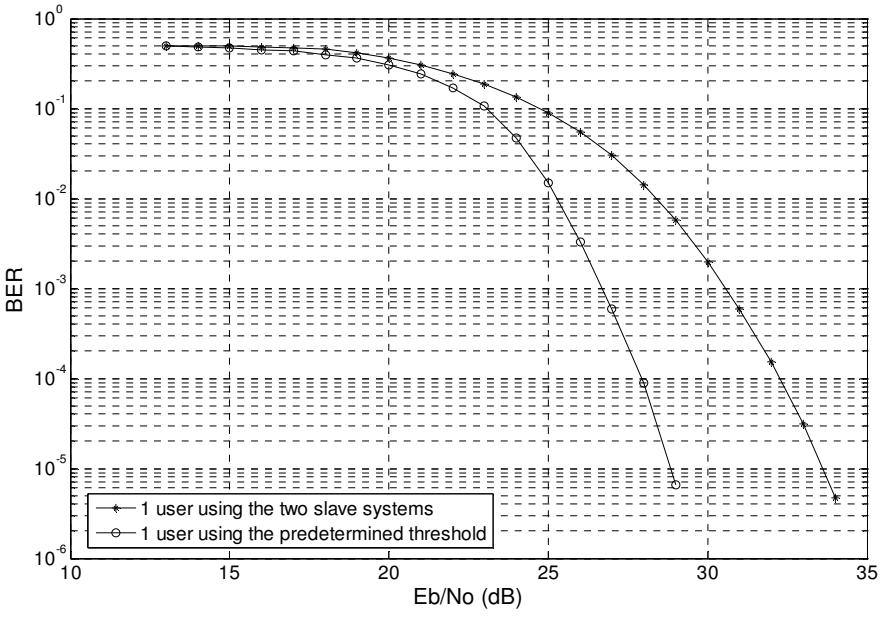


Fig. 9.30 The empirical BER curves of the Ueda ICM based TDM system of Figure 9.29 (predetermined threshold) and the corresponding system with the two-slave receiver, for a single user in the system.

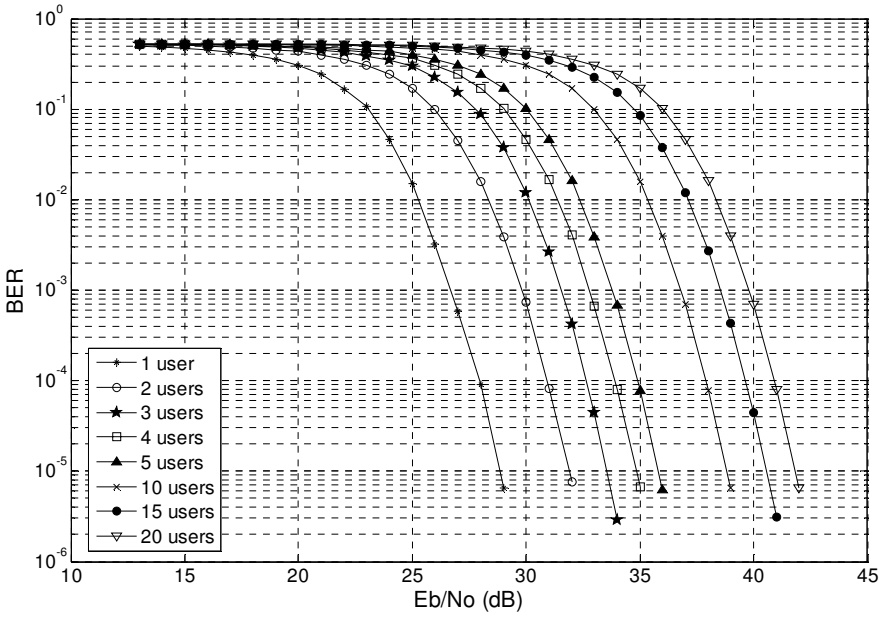


Fig. 9.31 The empirical BER curves of the Ueda ICM based TDM system of Figure 9.29 for 1-5, 10, 15 and 20 users

from Figure 9.31 that at the highest acceptable BER level of 10^{-3} [17,18], the E_b / N_o for which the system performance is satisfactory for the case of 1, 2, 3, 4, 5, 10, 15 and 20 users is equal to approximately 42.5, 46, 47.5, 49, 50, 53, 54.5 and 56 dB, respectively.

The system of Figure 9.29 is shown in Figure 9.32 in the Rayleigh fading channel. The empirical BER curves of this system are shown in Figure 9.33 for 1, 5 and 20 users in the system. Again, it can be observed from Figure 9.33 that the system performance is unsatisfactory in the Rayleigh fading channel for any number of users in the system as the BER curves always remain at the BER level of approximately 0.4. A close up of the BER curves reveals an initial difference among 1, 5 and 20 users in the system, before the curves settle to the BER level of approximately 0.4. Furthermore, it should be observed by careful inspection of Figures 9.28 and 9.33 that in the Rayleigh fading channel the Ueda ICM based TDM system marginally outperforms the Ueda ICM based TDM system with only the master signal x transmitted. However, this difference is insignificant from a practical point of view.

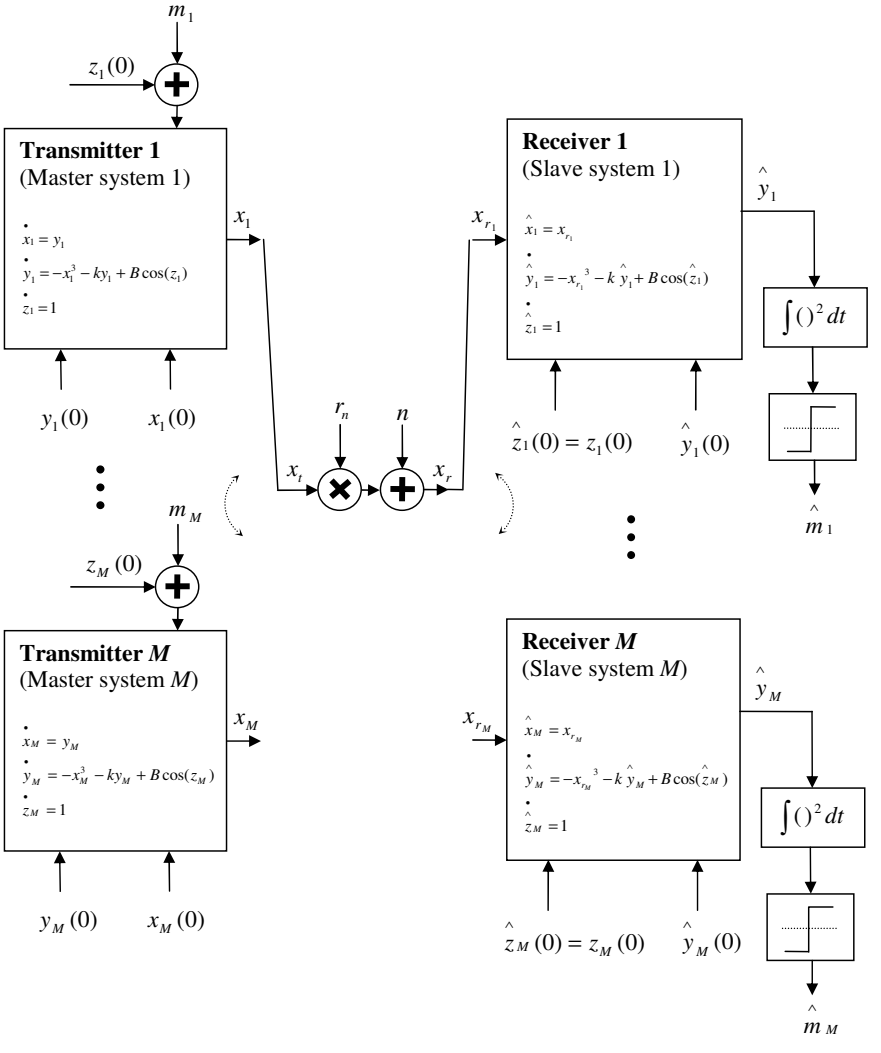


Fig. 9.32 The Ueda ICM based multi-user TDM communication system with only the master signal x transmitted in the Rayleigh fading channel, implementing the predetermined threshold at the receiver. The parameter values are $k = 0.05$, $B = 7.5$.

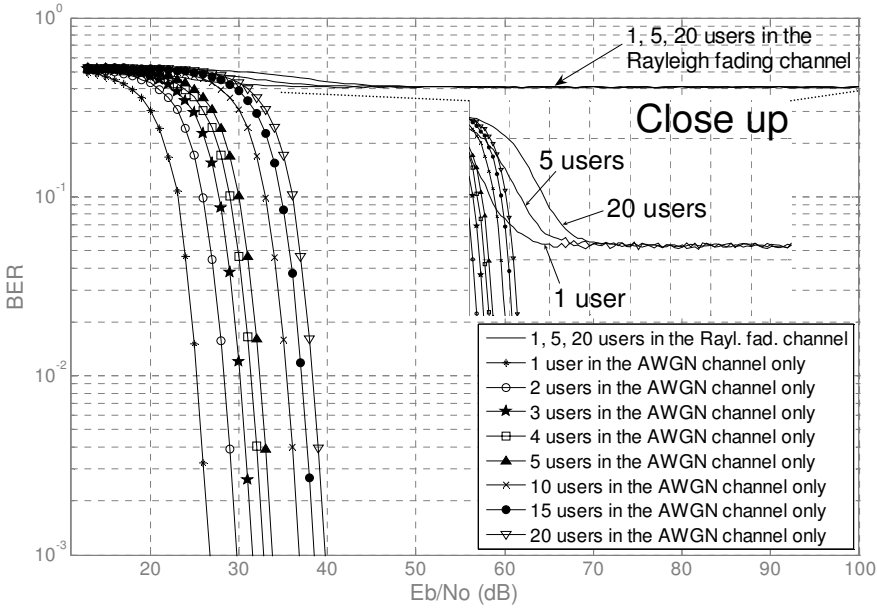


Fig. 9.33 The empirical BER curves of the Ueda ICM based TDM system of Figure 9.32 for 1, 5 and 20 users (unmarked curves), with the close up. The corresponding empirical BER curves of the system of Figure 9.29 in the AWGN channel only are also shown (marked curves).

9.2.4 Performance Comparison of the Ueda ICM Based TDM Chaotic Communication Systems in an AWGN Channel

In this subsection, the BER performance of the Ueda ICM based multi-user TDM chaotic communication system of subsection 9.2.2 is compared to that of the similar system of subsection 9.2.3 but with only x transmitted. The BER curves of the two systems in the AWGN channel for 1-5, 10, 15 and 20 users are plotted on the same set of axes in Figure 9.34. It can be observed from Figure 9.34 that the Ueda ICM based TDM system with only x transmitted of Figure 9.29, outperforms the Ueda ICM based TDM system of Figure 9.21 by approximately 5 dB for any number of users in the system. In general, Figure 9.34 shows that the system with only x transmitted can accommodate approximately three times the number of users as compared to the system of Figure 9.21 for any given BER level. A further advantage of the system with only x transmitted is the resulting reduced overall complexity of the system. This can be observed by comparing Figures 9.21 and 9.29.

It has already been observed from Figures 9.28 and 9.33 that in the Rayleigh fading channel both systems exhibit unsatisfactory performance as their respective BER curves remain at approximately 0.4 for any number of users in the system.

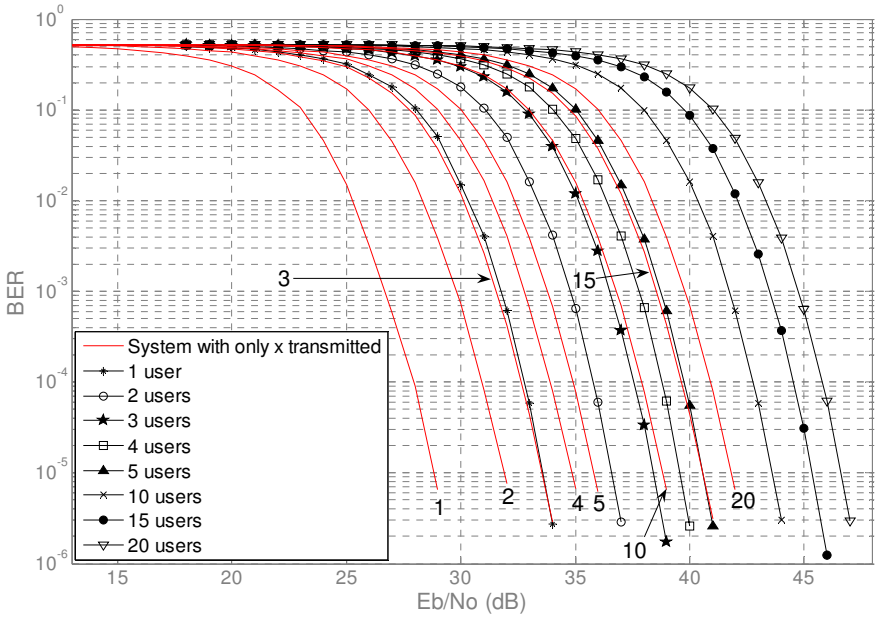


Fig. 9.34 The empirical BER curves of the Ueda ICM based TDM system of Figure 9.21 for 1-5, 10, 15 and 20 users (marked curves). The corresponding empirical BER curves of the Ueda ICM based TDM system with only x transmitted of Figure 9.29 are shown by unmarked curves.

9.2.5 Performance Comparison of the ICM Based TDM Systems to the CPM Based TDM Systems of Section 9.1

In this subsection, the performance of the Ueda ICM based TDM systems is compared to that of the Lorenz CPM based TDM systems of section 9.1. It has been shown in section 9.1 that the AWGN BER performance of the Lorenz and Ueda CPM based TDM systems is virtually identical. Therefore, as before, the BER curves of the Lorenz CPM based TDM system will only be used in the analysis. Furthermore, it has been shown that the Ueda ICM based TDM system, with only x transmitted, of Figure 9.29, outperforms the Ueda ICM based TDM system of Figure 9.21 by approximately 5 dB. Thus, the BER curves of only the Ueda ICM based TDM system of Figure 9.29 will be used in the analysis.

In Figure 9.35, the AWGN BER curves of the Lorenz CPM based TDM system of Figure 9.3 and the Ueda ICM based TDM system of Figure 9.29, are plotted on the same set of axes.

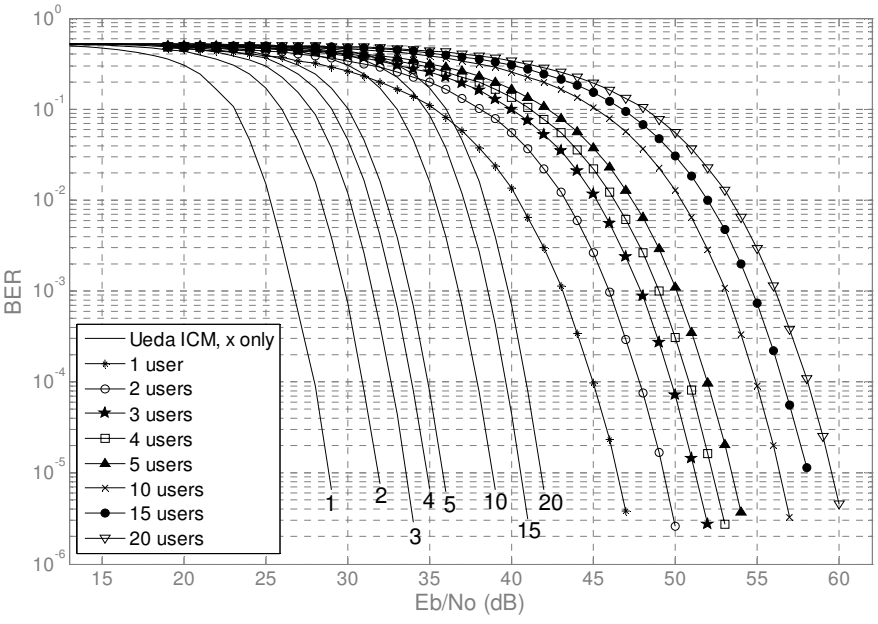


Fig. 9.35 The empirical BER curves of the Lorenz CPM based TDM system of Figure 9.3 for 1-5, 10, 15 and 20 users (marked curves) in the AWGN channel. The corresponding empirical BER curves of the Ueda ICM based TDM system, with only the master signal x transmitted, of Figure 9.29, are shown by unmarked curves.

It can be observed from Figure 9.35 that the Ueda ICM based TDM system, with only the master signal x transmitted, of Figure 9.29, outperforms the Lorenz (and Ueda) CPM based TDM system by approximately 16 dB at the BER level of 10^{-3}. It can thus be concluded that in terms of BER in the AWGN channel, the Ueda ICM based TDM system is a superior system.

As shown in section 9.1 and above, it should be noted that in the Rayleigh fading channel both CPM and ICM based TDM systems fail in terms of BER.

9.2.6 Performance Comparison of the ICM Based TDM Systems to the Chaos Based DS-CDMA of Chapter 7 and Chaos Based TDM System of Chapter 8

In this subsection, the BER performance of the Ueda ICM based TDM systems is compared to that of the chaos based DS-CDMA system of Figure 7.1 and chaos based TDM system of Figure 8.8.

In Figure 9.36, the AWGN BER curves of the Ueda ICM based TDM system of Figure 9.29 and the chaos based DS-CDMA system of Figure 7.1 are plotted on the same set of axes.

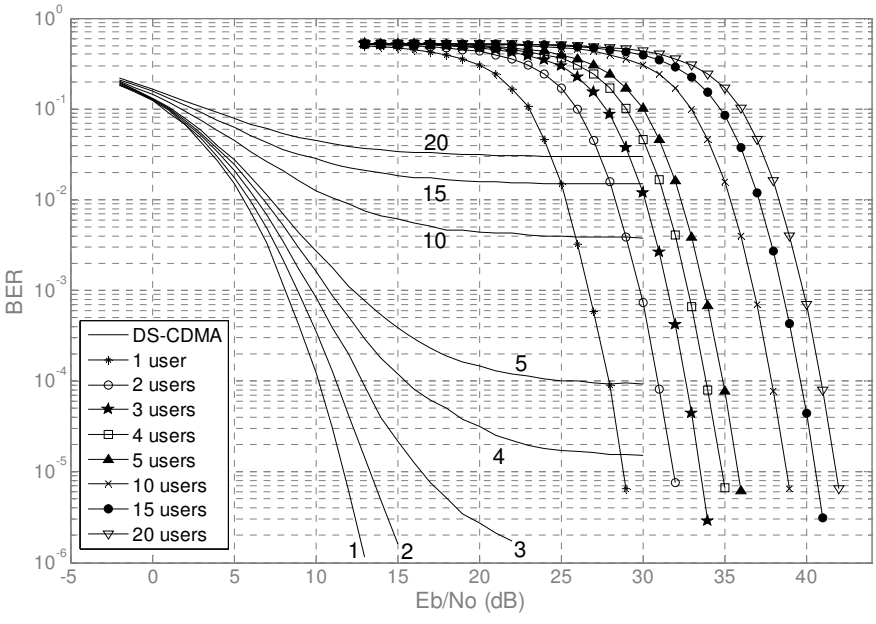


Fig. 9.36 The empirical BER curves of the Ueda ICM based TDM system, with only x transmitted, of Figure 9.29 for 1-5, 10, 15 and 20 users (marked curves) in the AWGN channel. The corresponding empirical BER curves of the chaos based DS-CDMA system of Figure 7.1 are shown by unmarked curves.

It can be observed from Figure 9.36 that for 1-5 users in the system, at the BER level of 10^{-3}, the chaos based DS-CDMA system outperforms the Ueda ICM based TDM system, with only x transmitted, by approximately 18, 21, 22, 22 and 22 dB, respectively. As for the CPM systems, it can thus be concluded that for low number of users in the system, the chaos based DS-CDMA system is a superior system in terms of BER. However, it should also be observed that the ICM based TDM chaotic communication systems are more robust to the influence of AWGN than are the CPM based TDM systems of section 9.1. Due to the prevailing inter-user interference among the DS-CDMA users, the BER curves for the 10, 15 and 20 users flatten before reaching the highest acceptable BER level of 10^{-3}. In contrast to this, for a larger number of users in the system (10, 15, 20), the Ueda ICM based TDM system outperforms the chaos based DS-CDMA systems as its BER curves do not flatten but reach the BER level of 10^{-3}.

In Figure 9.37, the AWGN BER curves of the Ueda ICM based TDM system, with only x transmitted, of Figure 9.29, are compared to those of the chaos based TDM system of Figure 8.8.

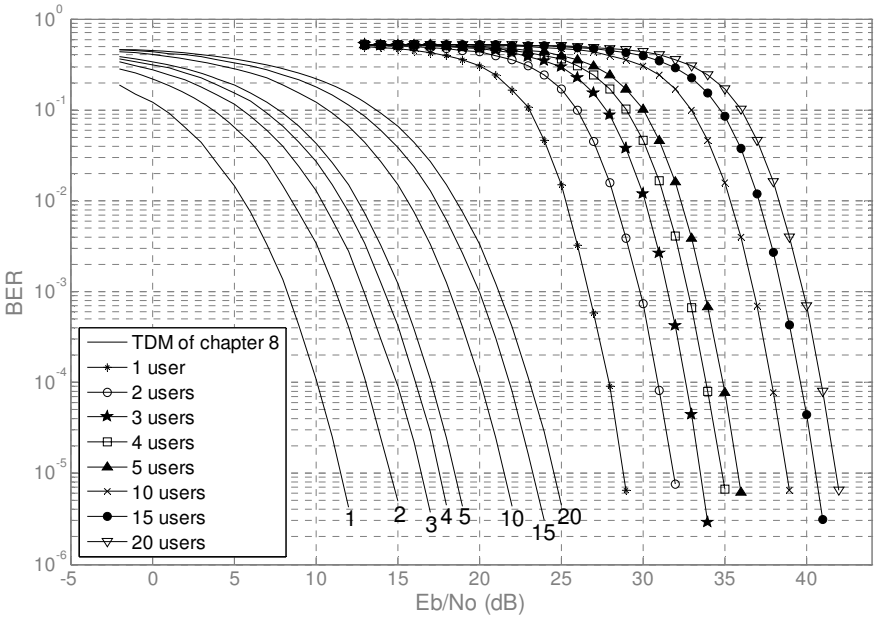


Fig. 9.37 The empirical AWGN BER curves of the Ueda ICM based TDM system, with only x transmitted, of Figure 9.29, for 1-5, 10, 15 and 20 users (marked curves). The corresponding empirical BER curves of the chaos based TDM system of Figure 8.8, chapter 8, are shown by unmarked curves.

Figure 9.37 shows that at the BER level of 10^{-3}, the chaos based TDM system of Figure 8.8, chapter 8, outperforms the Ueda ICM based TDM system with only x transmitted, of Figure 9.29, by approximately 18.5 dB for 1-5, 10, 15 and 20 users in the system. It can thus be concluded that in terms of BER, the chaos based TDM system of chapter 8 is a superior system for any number of users in the system.

It can be readily observed by comparing Figures 9.28 and 9.33 to Figures 9.18 and 9.19, that the Rayleigh fading performance of the Ueda ICM based TDM systems is inferior to that of the chaos based DS-CDMA system of chapter 7 and the chaos based TDM system of chapter 8.

9.3 Conclusion

In this chapter, the chaotic synchronization based multi-user TDM systems have been proposed and evaluated in terms of BER in AWGN and Rayleigh fading channels. In particular, the proposed systems include the Lorenz and Ueda CPM based TDM systems and the Ueda ICM based TDM systems. It has been shown that in terms of BER, the ICM based TDM systems outperform the CPM based TDM systems in both AWGN and Rayleigh fading channels. Furthermore, it has

been found that the Ueda ICM based TDM system with only the master signal x transmitted, outperforms the Ueda ICM based TDM system with both master signals x and y transmitted. However, the BER analysis in the Rayleigh fading channel has revealed that both CPM and ICM based systems fail to satisfy the highest acceptable BER level of 10^{-3} for any number of users in the system and any E_b / N_o. In addition, two different receiver architectures have been implemented and evaluated in terms of BER on all of the CPM and ICM based TDM systems. These include the predetermined threshold receiver architecture and the receiver architecture implementing the two slave systems. It has been shown that in terms of BER only in the case of the Lorenz CPM based TDM system the two slave receiver architecture outperforms the predetermined threshold architecture.

Furthermore, the BER performance of the CPM and ICM based TDM systems has been compared to the BER performance of the chaos based DS-CDMA system of chapter 7 and the chaos based TDM system of chapter 8. Again, the comparison has been conducted in both AWGN and Rayleigh fading channels. It has been shown that in terms of BER the chaos based DS-CDMA system of chapter 7, outperforms the CPM and ICM based TDM systems for low number of users in the AWGN channel. However, for larger number of users in the system, the BER curves of the chaos based DS-CDMA system flatten before reaching the highest acceptable BER level of 10^{-3}. In contrast to this, the BER curves of the CPM and ICM based TDM systems do not flatten and thus outperform the chaos based DS-CDMA system for larger number of users. Furthermore, it has been shown that the chaos based TDM communication system of chapter 8, outperforms the CPM and ICM based TDM systems for any number of users and any E_b / N_o. Finally, it has been shown that the chaos based DS-CDMA system of chapter 7 and the chaos based TDM system of chapter 8; outperform the CPM and ICM based TDM systems in the Rayleigh fading channel. Therefore, it can be concluded that in general, the multi-user chaotic communication systems based on the acquisition and tracking synchronization scheme of chapter 7, are more robust to AWGN and Rayleigh fading than those based on the principles of chaotic synchronization of chapters 3, 5 and 6.

References

[1] Jovic, B., Unsworth, C.P.: Chaos based multi-user time division multiplexing communication system. IET Communications 1(4), 549–555 (2007)

[2] Tam, W.M., Lau, F.C.M., Tse, C.K.: A Multiple Access Scheme for Chaos – Based Digital Communication Systems Utilizing Transmitted Reference. IEEE Transactions on Circuits and Systems – I: Regular Papers 51(9), 1868–1878 (2004)

[3] Jovic, B., Unsworth, C.P.: Synchronization of Chaotic Communication Systems. In: Wang, C.W. (ed.) Nonlinear Phenomena Research Perspectives. Nova Publishers, New York (2007)

[4] Jovic, B., Berber, S., Unsworth, C.P.: A novel mathematical analysis for predicting master – slave synchronization for the simplest quadratic chaotic flow and Ueda chaotic system with application to communications. Physica D 213(1), 31–50 (2006)
[5] Itoh, M.: Spread Spectrum Communication via Chaos. International Journal of Bifurcation and Chaos 9(1), 155–213 (1999)
[6] Itoh, M., Chua, L.O.: Multiplexing Techniques via Chaos. In: Proceedings of the 1997 IEEE International Symposium on Circuits and Systems (ISCAS 1997), Hong Kong, China, June 9-12, pp. 905–908 (1997)
[7] Itoh, M., Chua, L.O.: Multiplexing Techniques via Chaotic Signals. In: Proceedings of the 1997 European Conference on Circuit Design (ECCTD 1997), Budapest, Hungary, August 31-September 3, pp. 278–283 (1997)
[8] Torikai, H., Saito, T., Schwarz, W.: Multiplex Communication Scheme Based on Synchronization via Multiplex Pulse-Trains. In: Proceedings of the 1998 IEEE International Symposium on Circuits and Systems (ISCAS 1998), Monterey, CA, May 31-June 3, vol. 4, pp. IV-554–IV-557 (1998)
[9] He, Z., Li, K., Yang, L.: TDMA Secure Communication Scheme Based on Synchronization of Chua's Circuits. Journal of Circuits, Systems, and Computers 10(3&4), 147–158 (2000)
[10] Li, K., Liu, J., Yang, L., He, Z.: A Robust Chaotic Digital Secure Communication Scheme. In: Proceedings of the 1999 IEEE Pacific rim Conference on Communications, Computers and Signal Processing (PACRIM 1999), Victoria, BC, August 22-24, pp. 491–494 (1999)
[11] Peng-bo, X., Li, M.: Time Division Multiplexing Signals Transmission via Intermittently Coupled, Synchronized Chaotic System. Journal of Qingdao University 13(2), 45–49 (2000)
[12] Chen, G., Dong, X.: From chaos to order: Methodologies, Perspectives and Applications, pp. 598–614. World Scientific Publishing Co. Pte. Ltd., Singapore (1998)
[13] Reddell, N.F., Welch, T.B., Bollt, E.M.: A covert communication system using an optimized wideband chaotic carrier. In: MILCOM Proceedings, vol. 2, pp. 1330–1334 (2002)
[14] Jovic, B., Unsworth, C.P., Sandhu, G.S., Berber, S.M.: A robust sequence synchronization unit for multi-user DS-CDMA chaos-based communication systems. Signal Processing 87(7), 1692–1708 (2007)
[15] Cuomo, K.M., Oppenheim, A.V.: Circuit Implementation of Synchronized Chaos with Applications to Communications. Physical Review Letters 71(1), 65–68 (1993)
[16] Cuomo, K.M., Oppenheim, A.V., Strogatz, S.H.: Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications. IEEE Transactions on Circuits and Systems – II. Analog and Digital Signal Processing 40(10), 626–633 (1993)
[17] Giger, A.J., Barnett, W.T.: Effects of Multipath Propagation on Digital Radio. IEEE Transactions on Communications COM-29(9), 1345–1352 (1981)
[18] Wehinger, J., Mecklenbrauker, C.F.: Iterative CDMA Multiuser Receiver With Soft Decision-Directed Channel Estimation. IEEE Transactions on Signal Processing 54(10), 3922–3934 (2006)
[19] Jovic, B., Unsworth, C.P., Berber, S.M.: De-noising 'Initial Condition Modulation' Wideband Chaotic Communication Systems with Linear & Wavelet Filters. In: Proceedings of the First IEEE International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2006), Sydney, Australia, March 13-16, pp. 1–6 (2006)

Chapter 10
Novel Bit Power Spectrum Measures for Improved Security in Chaotic Communication Systems

In this chapter, the general approach to master-slave chaotic map synchronization of chapter 4 is demonstrated on the $\Re^2$ Burgers' map master-slave system. A Burgers' map CPM based chaotic communication system is then designed using the method of chapter 6. Primarily, however, the security of the proposed Burgers' map and the existing CPM, as well as of the ICM, chaotic communication systems is evaluated. The security is evaluated in terms of the average power of the bits transmitted using the newly developed measures, termed the bit power parameter spectrum (BPPS) and the bit power initial condition spectrum (BPICS). It is shown that due to the largest bit power overlap region of the chaotic carriers of the transmitted bits, (overlap within BPPS and BPICS), the Ueda ICM based chaotic communication system is more secure than the CPM based chaotic communication systems.

With the development of secure communication techniques based on the concept of chaotic synchronization, eavesdropping techniques have also been developed in parallel [1-13], highlighting the lack of security in many of the proposed systems. The eavesdropping techniques include those based on the prediction attacks [1-4], short-time zero-crossing rate (STZCR) attacks [5], generalized synchronization attacks [6,7], return map attacks [8,9], spectral analysis attacks [10-12], and parameter estimation attacks [13], among other.

In [1] Stark and Arumugam demonstrated that it is possible to extract a deterministic signal from a chaotic time series when the two are added together as in the CM scheme. Given that the dynamics of the chaotic background are known it has been shown that the deterministic signal can be recovered even when the ratio of the deterministic to chaotic signals is as low as $10^{-10}:1$ increasing to $10^{-5}:1$ with the unknown dynamics.

It has been shown in [2] that using the multi-step prediction technique the message hidden within the chaotic carrier can be extracted for the three different kinds of message signals embedded within the chaotic carrier. Here the basic idea in extracting the hidden message, from the chaotic communication system based on the CM principle, is to predict the carrier from the received signal, then subtract the predicted carrier from this received signal and thus reveal the hidden message.

The STZCR technique has been used in [5] to show the vulnerability in the security of the CPM scheme when implemented on the Chua circuit [14].

B. Jovic: Synchronization Techniques for Chaotic Commun. Syst., SCT 5, pp. 299–316.
springerlink.com

In [6] eavesdropping is achieved through the concept of generalized synchronization where the unauthorised receiver attempts to synchronize to the received signal, with limited success, and thus decode the message. Here the eavesdropper uses the set of parameters at the slave side which neither correspond to bit 0 nor bit 1, but is still able to retrieve the message successfully due to the significant difference in synchronization errors corresponding to bits 0 and 1. The GS eavesdropping attack presented in [6] is also used in [7] to demonstrate the security weakness within the CPM chaotic communication system based on the adaptive observer synchronization scheme of [15].

In [8] the authors show that the eavesdropper can extract the hidden messages within chaotic communication systems based on CM and CPM schemes due to the fact that any perturbations of the carrier signal influence the attractors of the return map.

The spectrogram of the received signal, followed by mathematical morphological filters, is used in [10] to extract the message from the CPM based chaotic communication system of [14]. Furthermore, in [12], the security of the CM chaotic communication system, based on the synchronization of two chaotic systems of different order [16], is examined showing that the hidden message can be directly extracted from the received signal by simply high pass filtering it.

Finally, in [13], the eavesdropping technique of parameter estimation has been used to break into the chaotic communication system based on the phase synchronization [17], while implementing the CPM scheme to encode binary information.

In perhaps the broadest of terms the chaotic communication eavesdropping techniques, in the literature today, can be divided into those which directly extract the transmitted message without the knowledge of the dynamics of the transmitter [2-7,10-12], and those which make certain assumptions about the dynamics of the transmitter before attempting the extraction of the message [6,7,12,13]. In this chapter, initially the method of implementing the synchronized master-slave system within a CPM based secure chaotic communication system of chapter 6 is demonstrated on the $\Re^2$ Burgers' chaotic map [18,19]. Following this, the eavesdropping message extraction technique which assumes no knowledge of the dynamics of the transmitter is investigated in relation to the proposed and the existing CPM and ICM based communication systems. The message extraction technique developed here is based on the average power of the received signal which for a secure system must be equal for both bits 0 and 1. The carrier signal powers of bits 0 and 1 must be equal, or very nearly equal, to each other to eliminate the possibility of recognising the transmitted message from different carrier powers [7]. It is shown that in terms of the bit power security, the Burgers' map CPM based chaotic communication system can be optimized and thus outperforms the Lorenz CPM based chaotic communication system.

Section 10.1 presents the design of the nonlinear control laws for the synchronization of the Burgers' chaotic map master-slave system. The method of implementing the synchronized Burgers' master-slave system within a CPM based secure chaotic communication system is then demonstrated. In section 10.2, the security of the proposed and the existing CPM, as well as of the ICM, chaotic

communication systems is evaluated in terms of BPPS and BPICS, that is, in terms of the average power of the bits transmitted.

10.1 Communication System Based on the Synchronization of Burgers' Map Master-Slave Chaotic System

In this section, the general approach to the design of the synchronized chaotic maps of chapter 4 is applied to the $\Re^2$ Burgers' chaotic map master-slave system. As in chapter 6, the synchronized system is then used to design the Burgers' map CPM based chaotic communication system. However, in contrast to the $\Re^1$ Cubic map CPM based system of chapter 6, this section demonstrates the process of implementing the $\Re^2$ Burgers' chaotic map within a CPM based communication system. As will be shortly demonstrated, the $\Re^2$ Burgers' map has been chosen for the design as only the single master signal is required to synchronize the master and slave systems.

The Burgers' map [18,19] is given by equation 10.1.1:

$$\begin{aligned} X_{n+1} &= aX_n - Y_n^2 \\ Y_{n+1} &= bY_n + X_n Y_n \end{aligned} \tag{10.1.1}$$

With the parameters $a = 0.75$ and $b = 1.75$ the system is chaotic. Figures 10.1a and 10.1b show the time series and the chaotic map, respectively.

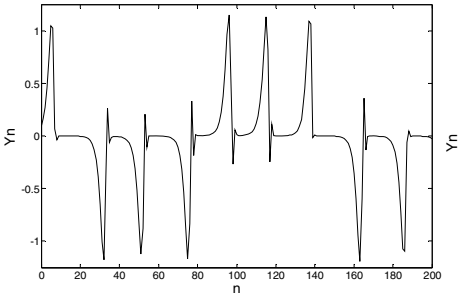


Fig. 10.1a The Burgers' map chaotic time series, Y_n

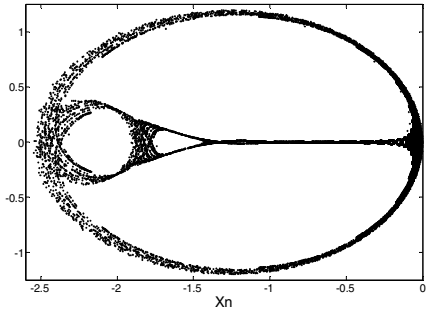


Fig. 10.1b The Burgers' map

The design procedure of the synchronizing nonlinear control laws of the Burgers' map CPM based chaotic communication system of Figure 10.2 is now explained. Let the error be defined by equation 10.1.2:

$$e_{1n} = \hat{X}_n - X_n \tag{10.1.2a}$$

$$e_{2n} = \hat{Y}_n - Y_n \tag{10.1.2b}$$

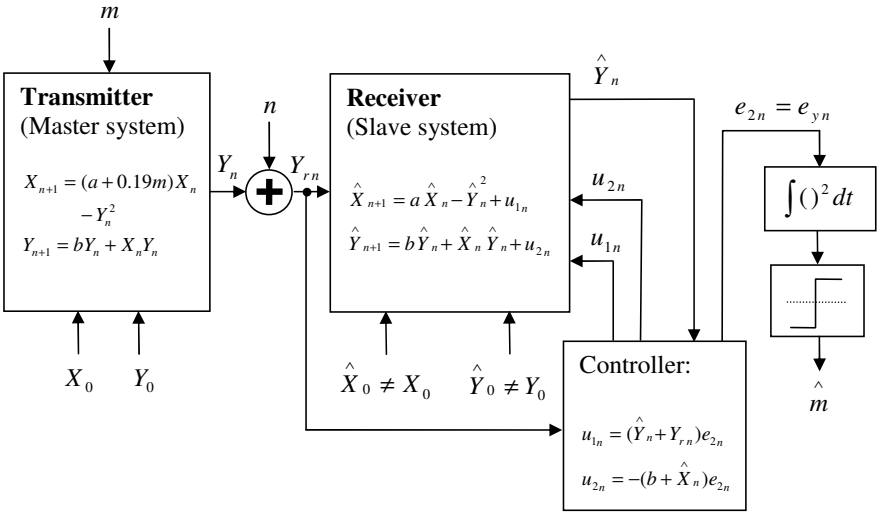


Fig. 10.2 The Burgers' map chaotic communication system based on the parameter modulation concept

In order to demonstrate the design of the controller of Figure 10.2 assume no noise in the system. It follows then that: $Y_{rn} = Y_n$. The difference error, (the error system), can then be represented by equation 10.1.3:

$$\begin{aligned} e_{1n+1} &= \hat{X}_{n+1} - X_{n+1} = a\hat{X}_n - aX_n - \hat{Y}_n^2 + Y_n^2 + u_{1n} \\ e_{2n+1} &= \hat{Y}_{n+1} - Y_{n+1} = b\hat{Y}_n - bY_n + \hat{X}_n\hat{Y}_n - X_nY_n + u_{2n} \end{aligned} \tag{10.1.3}$$

Equation 10.1.3 can also be represented by equation 10.1.5, keeping in mind the identities of equation 10.1.4:

$$\begin{aligned} -\hat{Y}_n^2 + Y_n^2 &= -\hat{Y}_n e_{2n} - Y_n e_{2n} \\ \hat{X}_n\hat{Y}_n - X_nY_n &= Y_n e_{1n} + \hat{X}_n e_{2n} \end{aligned} \tag{10.1.4}$$

$$\begin{aligned} e_{1n+1} &= \hat{X}_{n+1} - X_{n+1} = ae_{1n} + e_{2n}(-\hat{Y}_n - Y_n) + u_{1n} \\ e_{2n+1} &= \hat{Y}_{n+1} - Y_{n+1} = Y_n e_{1n} + e_{2n}(b + \hat{X}_n) + u_{2n} \end{aligned} \tag{10.1.5}$$

With theorem 2 of chapter 4 in mind, matrix equation 10.1.6 is formed:

$$e_{n+1} = A_n e_n + U_n e_n \tag{10.1.6}$$

where: $A_n = \begin{bmatrix} a_{11n} & a_{12n} \\ a_{21n} & a_{22n} \end{bmatrix}$, $U_n = \begin{bmatrix} u_{11n} & u_{12n} \\ u_{21n} & u_{22n} \end{bmatrix}$ and $e_n = \begin{bmatrix} e_{1n} \\ e_{2n} \end{bmatrix}$.

Therefore:

$$e_{n+1} = \begin{bmatrix} a_{11n} & a_{12n} \\ a_{21n} & a_{22n} \end{bmatrix} e_n + \begin{bmatrix} u_{11n} & u_{12n} \\ u_{21n} & u_{22n} \end{bmatrix} e_n \tag{10.1.7}$$

Modifying equation 10.1.5 to fit the matrix form of equation 10.1.7, equation 10.1.8 is obtained:

$$e_{n+1} = \begin{bmatrix} a & -\hat{Y}_n - Y_n \\ Y_n & b + \hat{X}_n \end{bmatrix} e_n + \begin{bmatrix} u_{\mathrm{i}n} & u_{\mathrm{ii}n} \\ u_{\mathrm{iii}n} & u_{\mathrm{iv}n} \end{bmatrix} e_n \tag{10.1.8}$$

where: $u_{1n} = u_{\mathrm{i}n} e_{1n} + u_{\mathrm{ii}n} e_{2n}$ and $u_{2n} = u_{\mathrm{iii}n} e_{1n} + u_{\mathrm{iv}n} e_{2n}$.

Therefore:

$$B = A_n + U_n = \begin{bmatrix} a & -\hat{Y}_n - Y_n \\ Y_n & b + \hat{X}_n \end{bmatrix} + \begin{bmatrix} u_{\mathrm{i}n} & u_{\mathrm{ii}n} \\ u_{\mathrm{iii}n} & u_{\mathrm{iv}n} \end{bmatrix} = \begin{bmatrix} a + u_{\mathrm{i}n} & -\hat{Y}_n - Y_n + u_{\mathrm{ii}n} \\ Y_n + u_{\mathrm{iii}n} & b + \hat{X}_n + u_{\mathrm{iv}n} \end{bmatrix} \tag{10.1.9}$$

Following theorem 2 of chapter 4, the control laws can be chosen in the following manner:

$$\begin{aligned} u_{\mathrm{i}n} &= 0 \\ u_{\mathrm{ii}n} &= \hat{Y}_n + Y_n \\ u_{\mathrm{iii}n} &= 0 \\ u_{\mathrm{iv}n} &= -(b + \hat{X}_n) \end{aligned} \tag{10.1.10}$$

With the control laws of equation 10.1.10, the matrix *B* of equation 10.1.9 takes the form of equation 10.1.11:

$$B_n = \begin{bmatrix} a & 0 \\ Y_n & 0 \end{bmatrix} \tag{10.1.11}$$

It is then readily verifiable that the eigenvalues of matrix B_n of equation 10.1.11 are equal to 0 and *a*. Furthermore, the theorem 2 of chapter 4, requires matrix *B* to be constant. As the matrix *B* is a function of *n*, it must also be ensured that $\|B_{n+1} - B_n\|$ remains bounded to guarantee global asymptotic stability which is the requirement for synchronization. The fact that $\|B_{n+1} - B_n\|$ remains bounded is demonstrated by equation 10.1.12 (10.1.13):

$$B_{n+2} B_{n+1} B_n = \begin{bmatrix} a & 0 \\ Y_{n+2} & 0 \end{bmatrix} \begin{bmatrix} a & 0 \\ Y_{n+1} & 0 \end{bmatrix} \begin{bmatrix} a & 0 \\ Y_n & 0 \end{bmatrix} = \begin{bmatrix} a^3 & 0 \\ a^2 Y_n & 0 \end{bmatrix} \to 0 \quad \text{as } a = 0.75 \tag{10.1.12}$$

that is:

$$B_{n+i}B_{n+(i-1)}\ldots B_n e_n = \begin{bmatrix} a & 0 \\ Y_{n+i} & 0 \end{bmatrix}\begin{bmatrix} a & 0 \\ Y_{n+(i-1)} & 0 \end{bmatrix}\cdots\begin{bmatrix} a & 0 \\ Y_n & 0 \end{bmatrix} = \begin{bmatrix} a^{i+1} & 0 \\ a^i Y_n & 0 \end{bmatrix} \to 0$$

$\forall\ |a| < 1$, and as $i \to \infty$. (10.1.13)

Therefore, as stated in equation 10.1.13, in order for the master and slave systems of Figure 10.2 to synchronize, the parameter a must be kept within the unit circle in z domain.

The control laws u_{1_n} and u_{2_n} are therefore given by equations 10.1.14 and 10.1.15, and incorporated into Figure 10.2.

$$u_{1_n} = u_{\mathrm{i}_n} e_{1_n} + u_{\mathrm{ii}_n} e_{2_n} = (\hat{Y}_n + Y_n) e_{2_n} \tag{10.1.14}$$

$$u_{2_n} = u_{\mathrm{iii}_n} e_{1_n} + u_{\mathrm{iv}_n} e_{2_n} = -(b + \hat{X}_n) e_{2_n} \tag{10.1.15}$$

The important feature of the master-slave system of Figure 10.2 is that it only requires the master signal Y_n to synchronize the master and slave systems. This fact is of particular importance for communications as only one signal needs to be transmitted thus reducing the required bandwidth and complexity [20-22].

The functionality of the control laws, given by equations 10.1.14 and 10.1.15, is demonstrated in Figure 10.3 from which synchronization of both master-slave signals can be observed.

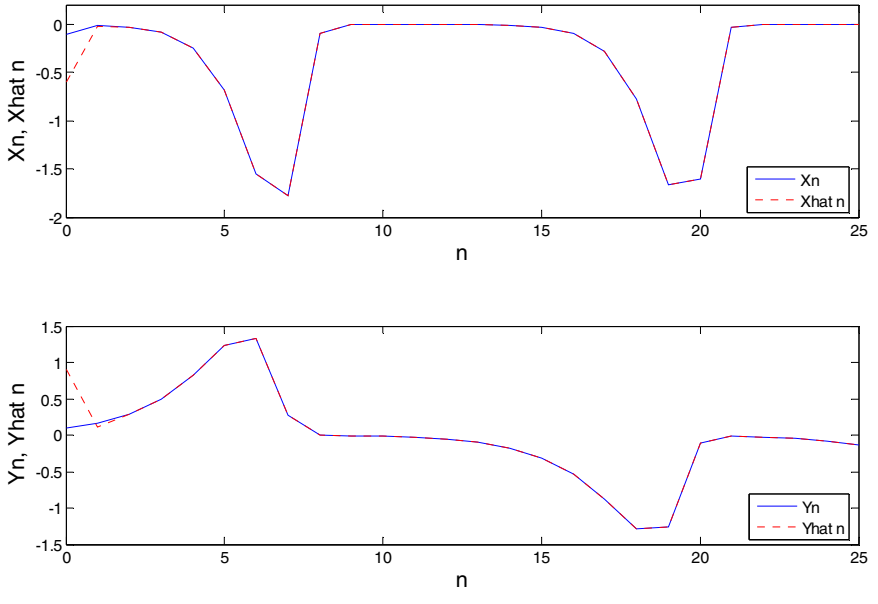


Fig. 10.3 Synchronization of the master-slave Burgers' chaotic signals.

In Figure 10.2, the master system parameter set of $a = 0.015$ and $b = 1.75$ has been chosen to represent a bit 0. The master system parameter set of $a = 0.205$ and $b = 1.75$ has been chosen to represent a bit 1. The reasoning behind such choice of parameters is clarified in the next section. Note that the message *m* of Figure 10.2 takes on the values of 0 and 1 depending on the polarity of a bit transmitted. The slave system parameters are set for all time at $a = 0.015$ and $b = 1.75$, so that synchronization at the receiver side signals a bit 0 and de-synchronization signals a bit 1. Both parameter sets, $a = 0.015$ and $b = 1.75$, and $a = 0.205$ and $b = 1.75$ generate chaotic behaviour in the system [19].

The transmitted signal Y_n is shown in Figure 10.4 when the series of 10 bits is transmitted, that is, when *m* = [0 0 1 0 1 1 0 1 0 1]. Figure 10.4 also shows the corresponding squared synchronization error, e_{yn}^2, under noiseless conditions. The received bits are detected by squaring and integrating the error e_{yn}. The output of the integrator is then compared to the predetermined threshold and the decision is made whether a bit 0 or a bit 1 was sent. Note that as in chapter 6, the spreading factor of 400 has been used to represent one bit. A transient period of 10 chips has been allowed for the case of Figure 10.4. During the transient period there is no data transmission taking place.

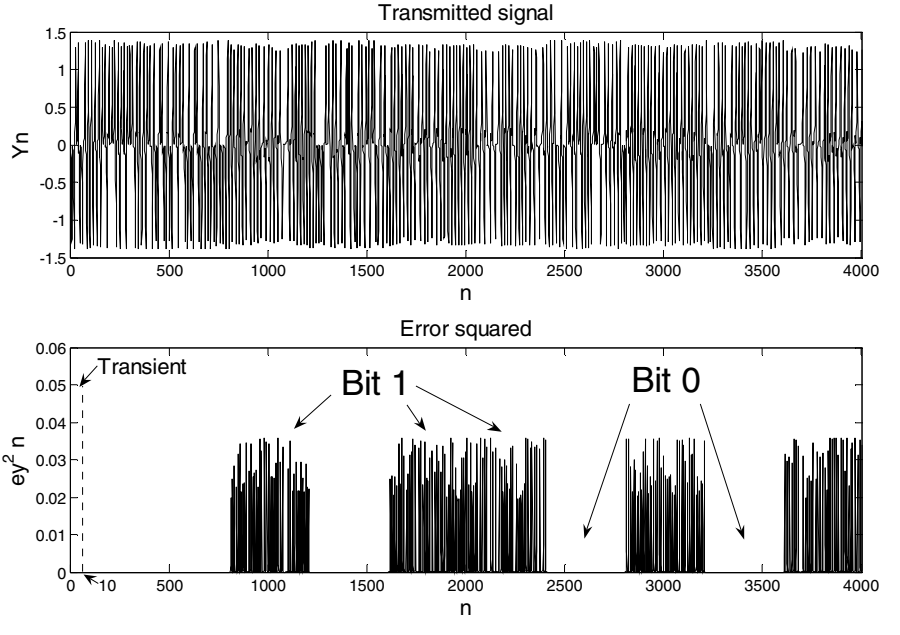


Fig. 10.4 The transmitted signal Y_n and the squared synchronization error e_{yn}^2

10.2 Bit Power Security Issues of Chaotic Communication Systems

In this section, high security regions and insecure regions of the Burgers' map and Lorenz flow CPM based chaotic communication systems are identified using a newly developed measure called the 'Bit Power Parameter Spectrum' (BPPS) [23]. The BPPS measure is based on determining the power of the transmitted bits encrypted within the chaotic carriers of the system. Furthermore, a similar measure to BPPS, termed the 'Bit Power Initial Condition Spectrum' (BPICS), is proposed and used to evaluate the security of the Ueda ICM based [21,20] chaotic communication system.

10.2.1 Security Evaluation of the Burgers' Map CPM Based Chaotic Communication System

For any secure chaotic communication system it is imperative that the power of the chaotic carriers representing bits 0 and 1 be approximately equal to avoid the possibility of decoding information by a third party simply based on the average powers of the chaotic carriers [7]. In order to perform the security analysis on the Burgers' map communication system of Figure 10.2, and thus explain the choice of the modulating parameters, the average power of the chaotic carriers representing bits 0 and 1 is now analysed. To do so the average power of a number of bits (1024) is first calculated and the mean of those powers and the corresponding standard deviation found. A number of points are then obtained for a number of different sets of chaotic parameters and the average power graph, with the error bars, versus the varied parameter, plotted. A pseudo random binary sequence (PRBS) generator has been used to model the transmitted bits. The plots have been produced with the concept of security in mind. If the average power of the chaotic carriers of bits 0 and 1 are different during the same transmission, with the confidence intervals which do not overlap, then the security of the system based on those carriers is jeopardized. This security measure has been termed the 'Bit Power Parameter Spectrum' (BPPS) [23].

Figure 10.5 shows the BPPS of the chaotic carriers representing the bits transmitted. For the bits 1 the parameter b is always kept constant at 1.75 with the parameter a varied in steps of 0.01 from $a = 0$ to $a = 0.75$. For the case of Figure 10.5 bits 0 are represented by the parameter values: $a = 0.6$ and $b = 1.75$ at all times. Bits 1 must then be represented by some other parameter values in order to achieve successful communication. From Figure 10.5 it can be observed that the average power of the chaotic carriers is approximately the same, (and the deviation of this power), when the parameter a is kept in the region: $0 < a < 0.22$, whereas it differs drastically outside of this region. Therefore, choosing the

parameter sets for bits 0 and 1 anywhere outside this region would jeopardize the security of the system. Thus, choosing the parameter values: $a = 0.6$ and $b = 1.75$ to represent bits 0 is not suitable for the security reasons. In order to remedy this let the parameter values representing bits 0 be: $a = 0.015$ and $b = 1.75$. In this case, Figure 10.6 is obtained. From Figure 10.6 it is observed that the carrier powers of the bits 0 and 1 have approximately equal values thus offering increased security over the choice of parameters of Figure 10.5.

Based on the findings of Figure 10.6, it is now shown that choosing the parameter set: $a = 0.015$ and $b = 1.75$, to represent bits 0, and the parameter set, $a = 0.205$ and $b = 1.75$, to represent bits 1, produces the best performance in terms of the bit error rate (BER). In Figure 10.7, the BER vs. the bit energy to noise power spectral density ratio (E_b / N_o) curves have been plotted. Figure 10.7 demonstrates the progressive improvement represented by the BER curves with the parameter a varied in the secure region of Figure 10.6 from $a = 0.0625$ up to $a = 0.205$ in steps of 0.0475. The parameter b has been set to 1.75 for both bits 0 and 1. The parameter a representing bit 0 has been set to: $a = 0.015$. Note that the best BER performance is achieved by choosing the parameter sets, representing bits 0 and 1, to be as far apart as possible from each other within the secure region of Figure 10.6. Also note further improvement in the BER curve, marked by the open circles, as one exits the secure region [23].

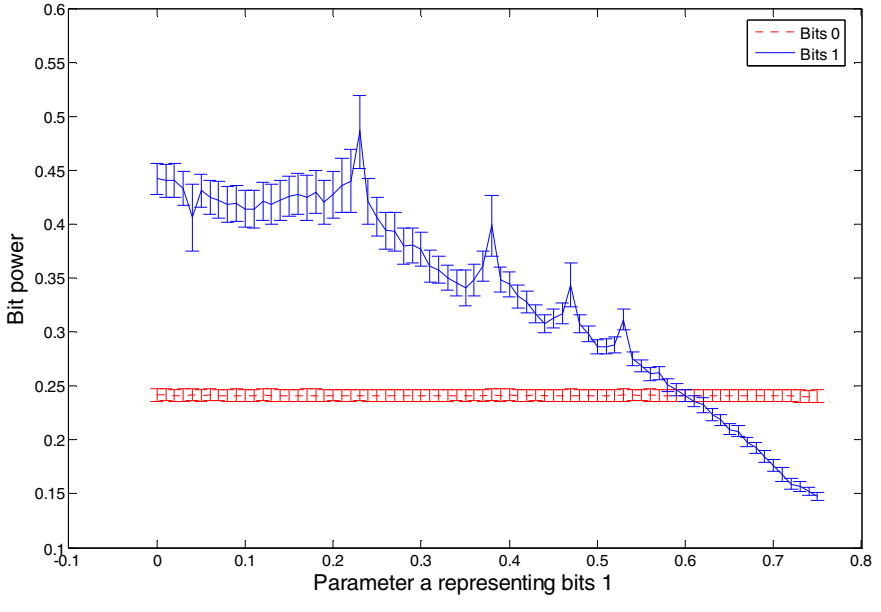


Fig. 10.5 The BPPS within the Burgers' CPM based chaotic communication system when the bits 0 are represented by the parameter set: a = 0.6, b = 1.75.

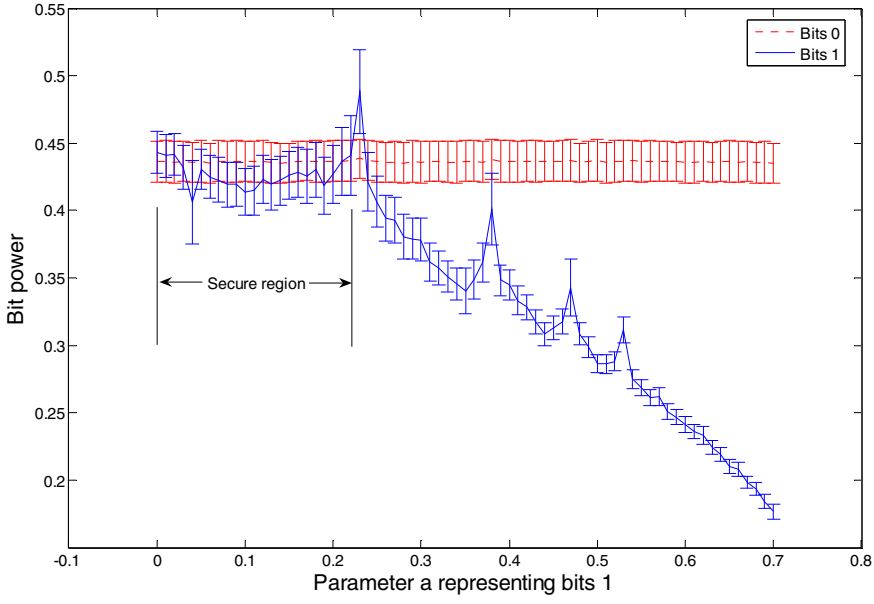


Fig. 10.6 The BPPS within the Burgers' CPM based chaotic communication system when the bits 0 are represented by the parameter set: a = 0.015, b = 1.75.

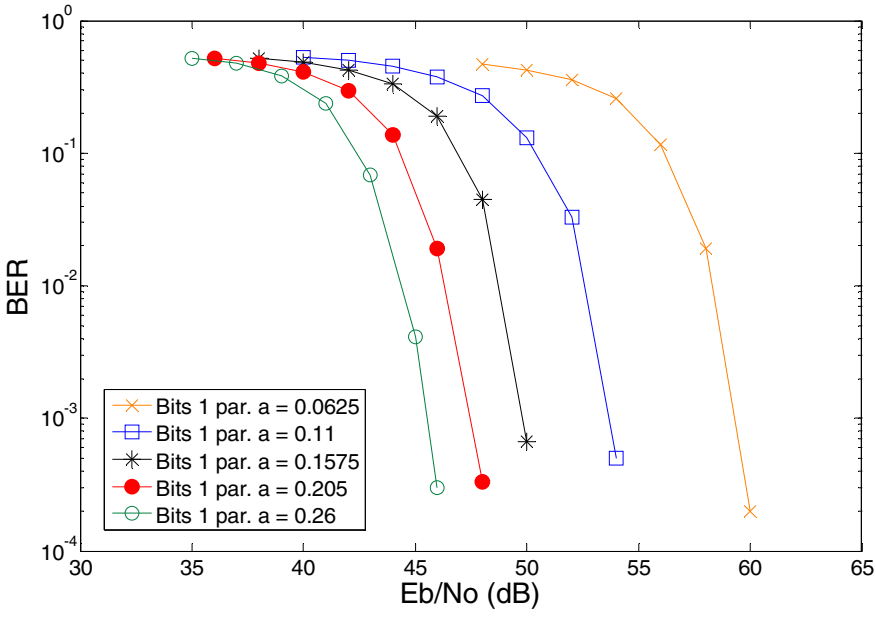


Fig. 10.7 The secure region BER curves of the chaotic communication system based on the parameter modulation of the Burgers' chaotic map with the progressively increasing bits 1 parameter *a*.

Figure 10.8 illustrates the effect on security caused by choosing inappropriate parameter sets which produce chaotic carriers of different power [23]. In case of Figure 10.8 bits 0 have been represented by the parameter set of $a = 0.6$ and $b = 1.75$, while bits 1 have been represented by the parameter set of $a = 0.205$ and $b = 1.75$. The average power of the transmitted signal of Figure 10.8 has been evaluated using the sliding window of 400 chips in length (the spreading factor of a single bit). The sliding window is then shifted one chip in time and the average power evaluated again. This process is repeated until the end of the transmitted signal. It can be observed from Figure 10.8 that the average power of the chaotic carriers of the transmitted bits oscillates periodically with the change of the binary message. In contrast to Figure 10.8, Figure 10.9 illustrates the effect on security caused by choosing the appropriate parameter sets which produce chaotic carriers of approximately equal power. In case of Figure 10.9, bits 0 have been represented by the parameter set of $a = 0.015$ and $b = 1.75$, while bits 1 have been represented by the parameter set of $a = 0.205$ and $b = 1.75$.

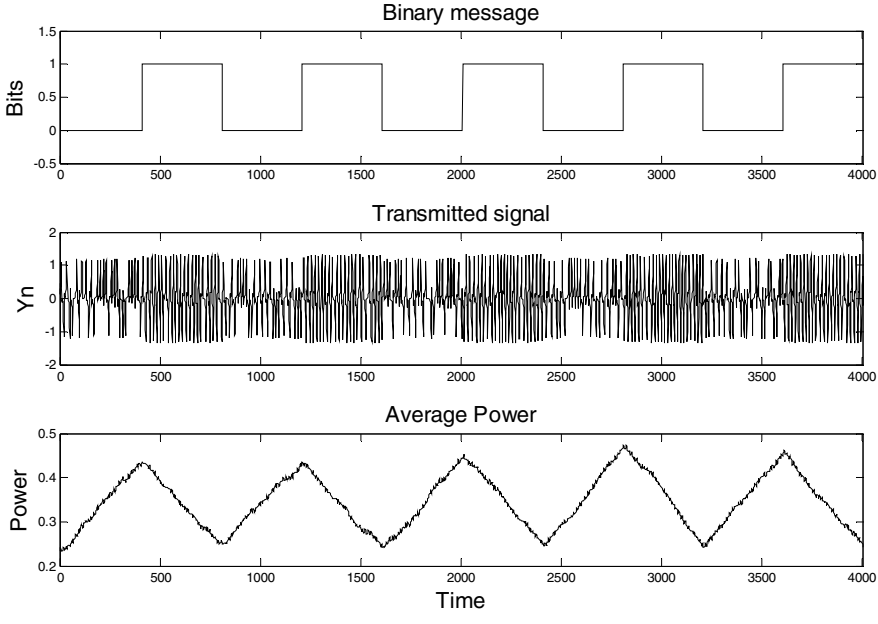


Fig. 10.8 The binary message, the transmitted signal Y_n and the average power of the transmitted signal. Bits 0 parameter set: $a = 0.6$ and $b = 1.75$. Bits 1 parameter set: $a = 0.205$ and $b = 1.75$.

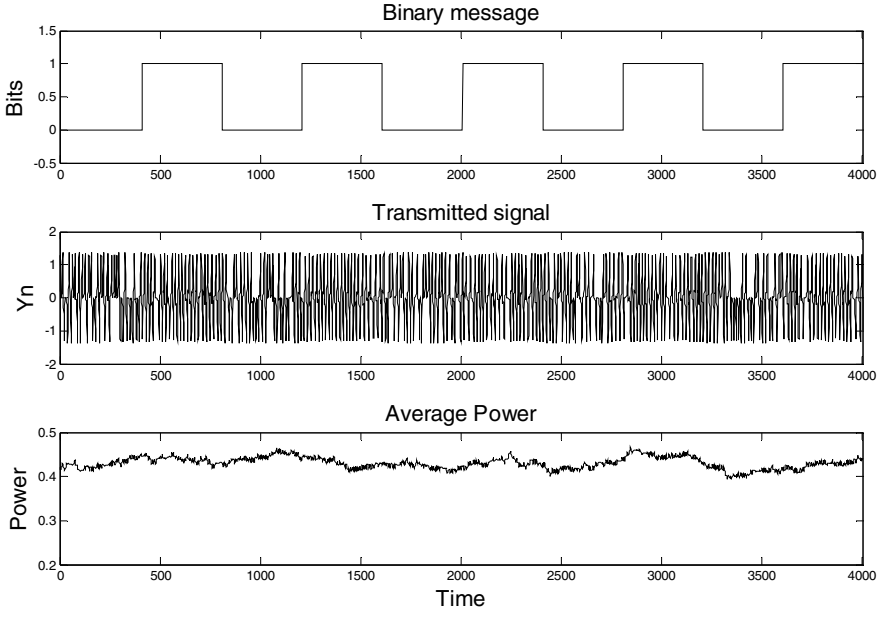


Fig. 10.9 The binary message, the transmitted signal Y_n and the average power of the transmitted signal. Bits 0 parameter set: a = 0.015 and b = 1.75. Bits 1 parameter set: a = 0.205 and b = 1.75.

10.2.2 Security Evaluation of the Lorenz CPM Based Chaotic Communication System

In subsection 6.2.1 of chapter 6, the Lorenz CPM based chaotic communication system has been presented [24]. The Lorenz system is a classical nonlinear dynamical system that is often used to highlight chaotic applications. Here it is shown that the communication system of [24], although chaotic, is not as secure as originally thought [24]. In this scheme the binary message is used to alter the parameter b of the master (transmitter) between 4 and 4.4 depending on whether a bit 0 or bit 1 is to be transmitted. However, at the slave (receiver) side the parameter b is fixed at 4 for all time. Thus, the synchronization either occurs or does not, depending on the state of the parameter b at the transmitter (master) side. The other Lorenz parameters, namely σ and r, are fixed at 16 and 45.6, respectively. For these parameter values the system is chaotic. In order to implement the CPM scheme the authors of [25] have scaled the Lorenz chaotic system to allow for the limited dynamic range of the operational amplifiers. This system, based on the PC synchronization concept, is presented in Figure 6.7 of

chapter 6. A similar BPPS plot as that of Figures 10.5 and 10.6 is plotted in Figure 10.10 but for the Lorenz CPM based chaotic communication system of [25]. In this case the parameter b of the bits 1 is varied from 0.1 to 10 in steps of 0.1 with the other parameters being fixed at the constant values specified above. From Figure 10.10 one can see that there are no secure regions where one can operate the system as the power of the bits 1 increases, almost linearly, with the parameter b. Therefore, to minimise the impact on the security, the parameters b representing bits 0 and 1, must be kept as close to each other as possible.

It can thus be concluded that the Burgers' map CPM based communication system is more secure than the Lorenz based CPM system.

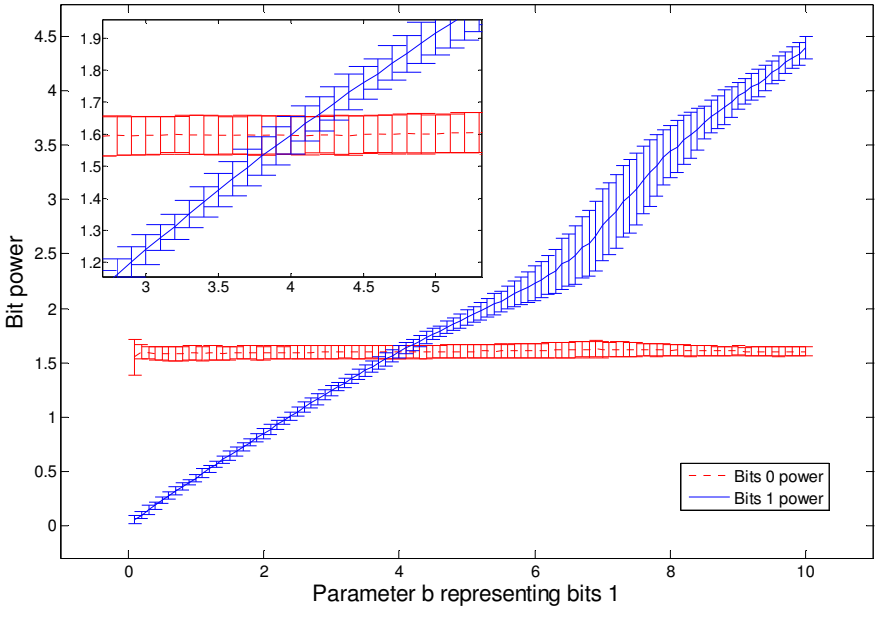


Fig. 10.10 The BPPS within the Lorenz CPM based chaotic communication system. The close up is shown in the upper left hand corner.

10.2.3 Security Evaluation of the Ueda ICM Based Chaotic Communication System with Only x Transmitted

The demodulation of the received signal of the Ueda ICM based system of chapter 6, section 6.3.2, is achieved by observing the synchronization error of the master-slave y signals. If this error tends to zero, it is concluded by the receiver that bit 0 was sent. It is concluded that bit 1 was sent if the steady state error is sinusoidal,

that is, not zero. However, it has also been shown in the appendix [21] that it is sufficient to only observe the behaviour of the slave signal y in order to successfully discriminate among the binary symbols 0 and 1. In this case it is required to only transmit the driving transmitter (master) signal x, thus reducing the required bandwidth. In this subsection, a similar security analysis to the BPPS analysis of subsections 10.2.1 and 10.2.2 is performed on the Ueda ICM based system with only the master signal x transmitted. The detailed operation of this system is outlined in the appendix [21]. Its structure is shown in Figure 10.11, where the message m varies among 2π and π, depending on whether bit 0 or bit 1 is to be transmitted, respectively. The bit power security analysis of the system of Figure 10.11 is shown in Figure 10.12. In order to produce Figure 10.12, the power of a number of bits (1024) has first been calculated and the mean of those powers and the corresponding standard deviation found. This has been done for a certain set of initial conditions. A number of points have then been obtained for a number of different sets of initial conditions and the average power graph, with the error bars, versus the varied initial condition plotted. Accordingly, this security measure has been termed the 'Bit Power Initial Condition Spectrum' (BPICS).

For the bits 1 the initial condition is varied in steps of 0.05 from $1+\pi$ to $1+2\pi$. For the case of Figure 10.12 bits 0 are represented by the initial condition value of $1+2\pi$ at all time. Note that bit 1 can then at no time be represented by $1+2\pi$ but a value very near this value has been used since using the value of $1+2\pi$ makes bits 0 and 1 identical to the receiver. From BPICS of Figure 10.12 it can be observed that the average power of the chaotic carriers is approximately the same for any initial conditions representing bits 1. This ensures the security of transmission as a third party cannot eavesdrop on to the system by trying to discriminate bits 0 and 1 from the power of the transmitted signal x. Furthermore, as can be observed from BPICS of Figure 10.12, the bit powers are essentially identical when the bits 1 are represented by $1+\pi$ and bits 0 by $1+2\pi$. Therefore, choosing sets of initial conditions separated by $\pm 2n\pi$ and $\pm n\pi$, for bits 0 and bits 1, respectively, not only produces the largest bit separation in symbol space [20,21], but also the maximum security from the bit power point of view. In addition to Figure 10.12, Figure 10.13 shows the absolute difference of the mean and standard deviation of the average powers of bits 0 and 1. Due to the lowest absolute difference of the mean and standard deviations of the average powers, two regions exist, as indicated in Figure 10.13, where the security is at its peak.

By comparing Figures 10.6, 10.10 and 10.12 it can be observed that the Ueda ICM based chaotic communication system of Figure 10.11 offers more security than the CPM based chaotic communication systems of Figures 10.2 and 6.7 due to the largest bit power overlap region.

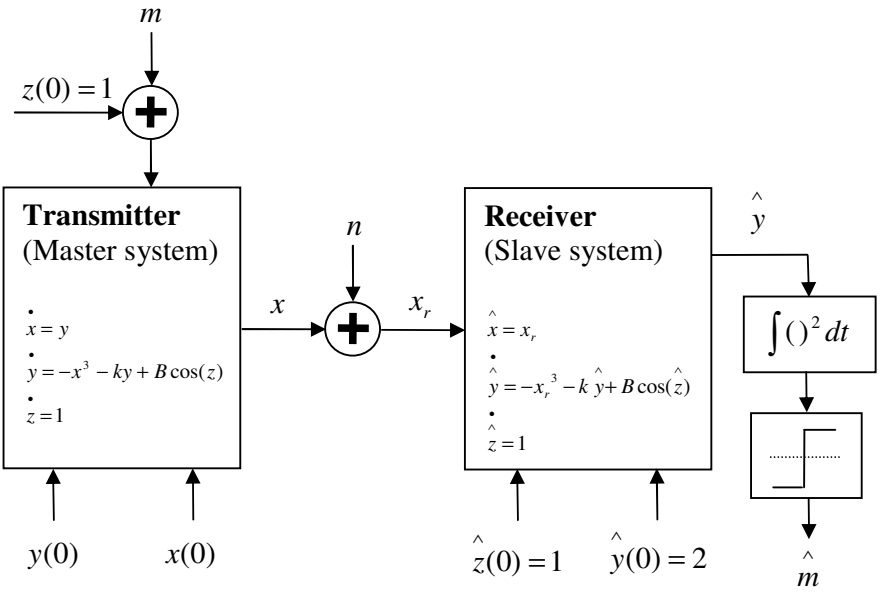


Fig. 10.11 The Ueda chaotic communication system, based on the initial condition modulation of [20], but with only x transmitted [21].

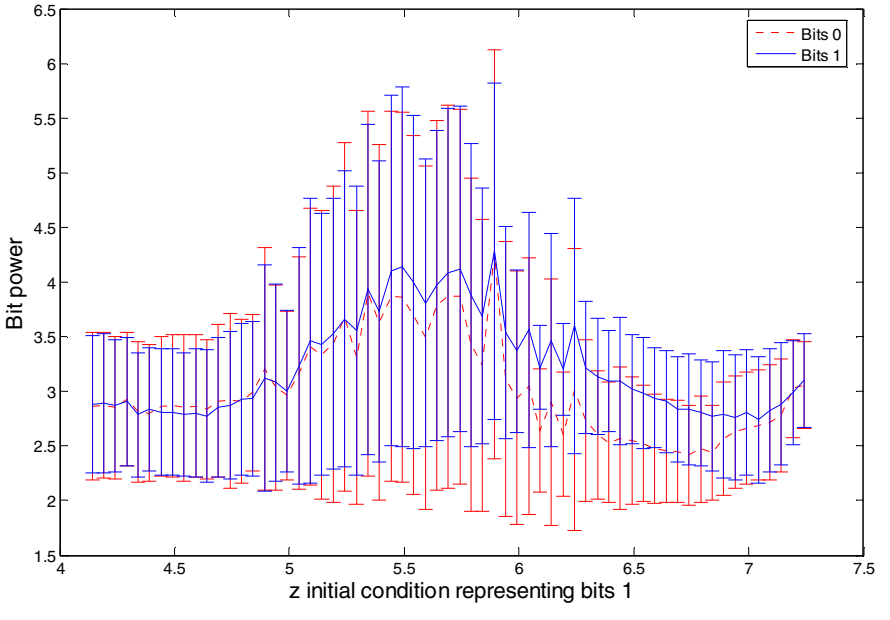


Fig. 10.12 The BPICS within the Ueda ICM based chaotic communication system.

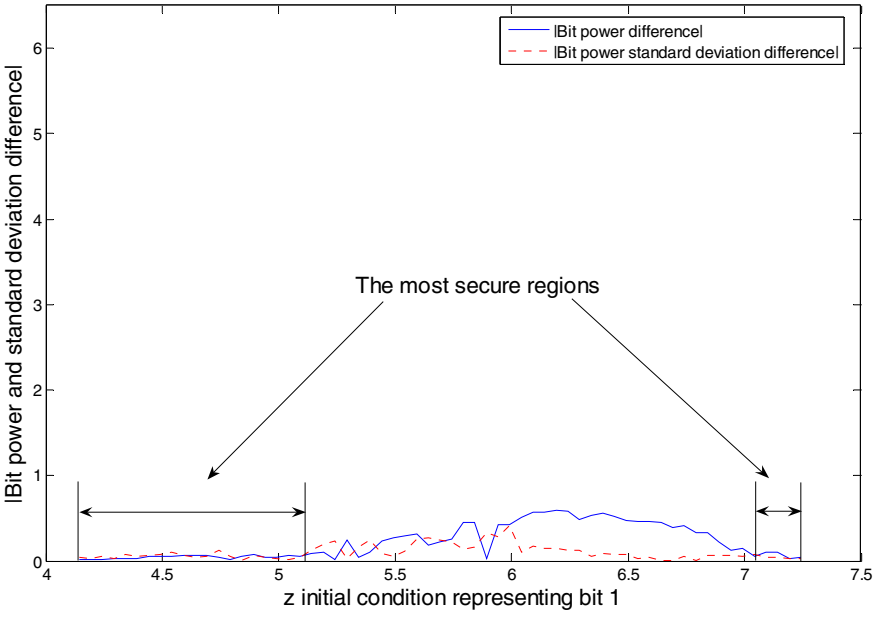


Fig. 10.13 The absolute difference of the mean and standard deviation of the average powers of bits 0 and 1

10.3 Conclusion

In this chapter, the security of the proposed, as well as of the existing chaotic communication systems, has been evaluated in terms of the average power of the chaotic carriers of the bits transmitted. In order to do so, the two new measures have been developed. These have been termed the 'Bit Power Parameter Spectrum' (BPPS) and the 'Bit Power Initial Condition Spectrum' (BPICS) measures and used for security evaluation of CPM and ICM based communication systems, respectively.

Initially, the method of implementing the synchronized master-slave system within a CPM based secure chaotic communication system has been demonstrated on the two dimensional Burgers' map. The nonlinear control laws have been designed in such a way to force the synchronization among the master and slave systems using only one signal of the master system. This is of particular importance for communications as only one signal needs to be transmitted thus reducing the required bandwidth.

The security of the Burgers' and the Lorenz CPM, as well as of the Ueda ICM, chaotic communication systems has then been evaluated. The security of the proposed and the existing systems has been evaluated in terms of the average power of the chaotic carriers of the bits transmitted, that is, in terms of the BPPS and the BPICS. It has been shown that due to the largest BPPS and BPICS overlap region of the chaotic carriers of the transmitted bits, the Ueda ICM based chaotic

communication system is more secure than the CPM based chaotic communication systems. Furthermore, it has been shown that the BER performance of the CPM based chaotic communication system, implementing Burgers' map system, can be optimized. The optimization is achieved by choosing the parameter sets, representing bits 0 and 1, to be as far apart as possible within the secure operating region. Thus, BPPS and BPICS measures developed here prove very useful in the design of secure chaotic communication systems.

References

[1] Stark, J., Arumugam, B.V.: Extracting Slowly Varying Signals from a Chaotic Background. International Journal of Bifurcation and Chaos 2(2), 413–419 (1992)
[2] Short, K.M.: Steps Toward Unmasking Secure Communications. International Journal of Bifurcation and Chaos 4(4), 959–977 (1994)
[3] Short, K.M.: Unmasking a Modulated Chaotic Communications Scheme. International Journal of Bifurcation and Chaos 6(2), 367–375 (1996)
[4] Short, K.M.: Signal Extraction from Chaotic Communications. International Journal of Bifurcation and Chaos 7(7), 1579–1597 (1997)
[5] Yang, T.: Recovery of Digital Signals from Chaotic Switching. International Journal of Circuit Theory and Applications 23(6), 611–615 (1995)
[6] Yang, T., Yang, L.B., Yang, C.M.: Breaking Chaotic Switching Using Generalized Synchronization: Examples. IEEE Transactions on Circuits and Systems – I: Fundamental Theory and Applications 45(10), 1062–1067 (1998)
[7] Álvarez, G., Montoya, F., Romera, M., Pastor, G.: Breaking parameter modulated chaotic secure communication system. Chaos, Solitons and Fractals 21(4), 783–787 (2004)
[8] Pérez, G., Cerdeira, H.A.: Extracting Messages Masked by Chaos. Physical Review Letters 74(11), 1970–1973 (1995)
[9] Li, S., Álvarez, G., Chen, G.: Breaking a chaos-based secure communication scheme designed by an improved modulation method. Chaos, Solitons and Fractals 25(1), 109–120 (2005)
[10] Yang, T., Yang, L.B., Yang, C.M.: Breaking chaotic secure communication using a spectrogram. Physics Letters A 247(1-2), 105–111 (1998)
[11] Álvarez, G., Montoya, F., Romera, M., Pastor, G.: Breaking Two Secure Communication Systems Based on Chaotic Masking. IEEE Transactions on Circuits and Systems – II: Express Briefs 51(10), 505–506 (2004)
[12] Álvarez, G., Hernández, L., Muñoz, J., Montoya, F., Li, S.: Security analysis of communication system based on the synchronization of different order chaotic systems. Physics Letters A 345(4-6), 109–120 (2005)
[13] Álvarez, G., Montoya, F., Pastor, G., Romera, M.: Breaking a secure communication scheme based on the phase synchronization of chaotic systems. Chaos 14(2), 274–278 (2004)
[14] Parlitz, U., Chua, L.O., Kocarev, Lj., Hale, K.S., Shang, A.: Transmission of digital signals by chaotic synchronization. International Journal of Bifurcation and Chaos 2(4), 973–977 (1992)
[15] Feki, M.: An adaptive chaos synchronization scheme applied to secure communication. Chaos, Solitons and Fractals 18(1), 141–148 (2003)

[16] Bowong, S.: Stability analysis for the synchronization of chaotic systems with different order: application to secure communications. Physics Letters A 326(1-2), 102–113 (2004)
[17] Chen, J.Y., Wong, K.W., Cheng, L.M., Shuai, J.W.: A secure communication scheme based on the phase synchronization of chaotic systems. Chaos 13(2), 508–514 (2003)
[18] Sprott, J.C.: Chaos and Time-Series Analysis, pp. 230–440. Oxford University Press, Oxford (2003)
[19] Whitehead, R.R., MacDonald, N.: A chaotic mapping that displays its own homoclinic structure. Physica D 13(3), 401–407 (1984)
[20] Jovic, B., Berber, S., Unsworth, C.P.: A novel mathematical analysis for predicting master – slave synchronization for the simplest quadratic chaotic flow and Ueda chaotic system with application to communications. Physica D 213(1), 31–50 (2006)
[21] Jovic, B., Unsworth, C.P., Berber, S.M.: De-noising 'Initial Condition Modulation' Wideband Chaotic Communication Systems with Linear & Wavelet Filters. In: Proceedings of the First IEEE International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2006), Sydney, Australia, March 13-16, pp. 1–6 (2006)
[22] Haykin, S.: Communication systems, 4th edn., pp. 61–514. Wiley, New York (2001)
[23] Jovic, B., Unsworth, C.P.: Improving Security in Chaotic Spread Spectrum Communication Systems with a Novel 'Bit Power Parameter Spectrum' Measure. In: Proceedings of the International Conference on Security and Cryptography (SECRYPT 2007), Barcelona, Spain, July 28-31, pp. 273–280 (2007)
[24] Jovic, B., Unsworth, C.P.: Synchronization of Chaotic Communication Systems. In: Wang, C.W. (ed.) Nonlinear Phenomena Research Perspectives. Nova Publishers, New York (2007)
[25] Cuomo, K.M., Oppenheim, A.V.: Circuit Implementation of Synchronized Chaos with Applications to Communications. Physical Review Letters 71(1), 65–68 (1993)

Chapter 11
Conclusions and Future Directions

11.1 Conclusions

In this book, sequence synchronization techniques for single and multiple-access chaotic communication systems have been investigated. In particular, the techniques of sequence synchronization studied include those based on the principles of Pecora-Carroll (PC) chaotic synchronization and those based on the principles of traditional DS-CDMA synchronization.

Based on the principles of PC chaotic synchronization, the novel approaches to chaotic synchronization were proposed and used to design new single-user chaotic communication systems. These new chaotic communication systems include those based on the chaotic parameter modulation (CPM) and initial condition modulation (ICM) techniques. Furthermore, the principles of time division multiplexing (TDM) were used to obtain the CPM and ICM based multi-user TDM systems. The performance of all of the proposed and the existing systems was evaluated in terms of the bit error rate (BER) in the additive white Gaussian noise (AWGN) and the Rayleigh fading channels. Furthermore, it was shown that by implementing certain linear and wavelet filters, one can improve the BER performance of the ICM based systems in the AWGN channel.

The sequence synchronization of chaotic communication systems based on the DS-CDMA principles was then proposed. It was shown how the mutually orthogonal properties between the logistic map chaotic time series and the PRBS pilot signal enable the traditional ideas of the multi-user CDMA sequence synchronization process to be utilized within the multi-user chaos based DS-CDMA system. Furthermore, the system was taken one step further by introducing a chaotic pilot signal in place of the PRBS pilot signal, thus making the CBDS-CDMA system fully chaotic and eliminating the security threat posed by an inherently different PRBS pilot signal. Both phases of the sequence synchronization process, namely the code acquisition and the code tracking, were proposed and investigated. It was shown that in terms of BER the chaos based DS-CDMA systems outperform the CPM and ICM based TDM systems for low number of users in the AWGN channel. However, for larger number of users in the system, the BER curves of the chaos based DS-CDMA systems flatten before reaching the adopted highest acceptable BER level of 10^{-3}. In contrast to this, the BER curves of the CPM and ICM based TDM systems do not flatten and thus outperform the chaos based DS-CDMA system for large number of users. In

B. Jovic: Synchronization Techniques for Chaotic Commun. Syst., SCT 5, pp. 317–324.
springerlink.com

addition, it was found that the chaos based DS-CDMA system outperforms the ICM and CPM based TDM systems in the Rayleigh fading channel. However, they all fail to satisfy the highest acceptable BER level of 10^{-3} in the Rayleigh fading channel. Finally, it was shown that in terms of BER, in the AWGN channel only, the proposed chaotic pilot based CBDS-CDMA systems marginally outperform the PRBS pilot based system for a single user in the system at the BER level of 10^{-4} and below.

In addition to the CPM and ICM based TDM systems and the chaos based DS-CDMA system, the chaos based TDM system with the DS-CDMA correlator receiver was also proposed. It was shown that this system outperforms the CPM and ICM based TDM systems for any number of users. However, the system was outperformed by the chaos based DS-CDMA systems for low number of users and vice versa for large number of users.

In order to mutually exploit the DS-CDMA and TDM benefits, a generalized chaos based TDM communication system with more than one DS-CDMA user per TDM branch was proposed and evaluated in the AWGN channel. In this way, the bandwidth efficiency of a DS-CDMA system was combined with the interuser interference immunity of a TDM system, to allow for an increased number of users in the system while improving the BER performance.

In general, it can be concluded that the multi-user chaotic communication systems based on the acquisition and tracking synchronization scheme, are more robust to AWGN and Rayleigh fading than those based on the principles of chaotic synchronization.

Finally, the security of the proposed, as well as of the existing chaotic communication systems, was evaluated in terms of the average power of the chaotic carriers of the bits transmitted. In order to do so, the two new measures were developed. These were termed the 'Bit Power Parameter Spectrum' (BPPS) and the 'Bit Power Initial Condition Spectrum' (BPICS) measures. Using these measures, it was shown that chaotic communication systems can be optimized in terms of security.

In chapter 1, the three main categories of the multi-user mobile communication systems (FDMA, TDMA and CDMA), as well as some of their hybrids, were introduced. Furthermore, the disturbances encountered within the physical transmission channel, such as the additive white Gaussian noise and Rayleigh fading, were presented. The concept of the bit error rate, which is used to measure the effects of the channel imperfections on the transmitted signal, was then outlined. In addition, the procedure of evaluating the bit error rate was then demonstrated when noise and fading are present in the channel. Finally, the motivation of the book was stated by demonstrating the importance of synchronization among the transmitter and the receiver through its effect on the BER performance of the system.

In chapter 2, the phenomenon of chaos was introduced. The Lyapunov exponents which are used to diagnose and characterize the system were then presented. Furthermore, the two different approaches of implementing chaotic systems within secure communication systems were outlined. These include

chaotic communication systems based on the principles of chaotic synchronization and those based on the DS-CDMA principle. Finally, some of the filtering techniques that can be used within chaotic communication systems were briefly introduced.

Chapter 3 examined synchronization of chaotic systems. The concept of the Pecora-Carroll chaotic synchronization was described and its properties examined in terms of the conditional Lyapunov's exponents and Lyapunov's direct method. These demonstrate two different, yet most common approaches to the analysis of chaotic synchronization. Furthermore, Lyapunov's direct method was then used to show a general approach to the design of nonlinear controllers for the master-slave chaotic systems.

In chapter 4, a method of designing the nonlinear control laws for the synchronization of the chaotic map master-slave systems was proposed. The nonlinear control laws were designed in such a way to ensure that the eigenvalues of the error system matrix always fall within the unit circle in the z domain. This ensures the global asymptotic stability of the error system and thus causes the master-slave system of any complexity to synchronize. The general approach to the master-slave chaotic map synchronization was demonstrated on the $\Re^1$ cubic map master-slave system, the $\Re^2$ tinkerbell map master-slave system and the Lorenz $\Re^3$ chaotic map master-slave system. Furthermore, it was shown that it is always possible to achieve instant synchronization, within a single iteration of the master-slave system, when the control laws are designed in such a way to reduce the error system matrix to zero.

In chapter 5, the master-slave synchronization properties of the simplest quadratic chaotic flow and the Ueda chaotic system were investigated by a newly proposed mathematical analysis. It was shown that when the z signal drives, the synchronization error of the simplest quadratic master-slave y signals is constant whereas the synchronization error of the master-slave x signals increases linearly. Using numerical simulations, in conjunction with mathematical analysis, it was demonstrated that the simplest quadratic master-slave chaotic flow does not synchronize when the y signal drives; however, the synchronization error of the master-slave z signals tends to a constant value which is predictable and can be expressed as a combination of the master-slave x signals' initial conditions and the system's parameter value. It was found that the simplest quadratic master-slave chaotic flow synchronizes when the x signal drives.

Furthermore, it was found that the Ueda master-slave chaotic system does not synchronize when the master y or the master z signal drives. However, it was shown that the master-slave y signals do synchronize under certain conditions when the master x signal drives. When the signal x drives, mathematical manipulation of the system's dynamics allows one to determine a useful mathematical expression for the error of the master-slave y signals. This expression, along with the numerical simulations, allows one to predict that if the difference between the master-slave z signals' initial conditions equals $\pm 2n\pi$, the master-slave y signals will always synchronize. When the y signal drives, the synchronization error is constant and was mathematically expressed.

In general, it can be concluded that the synchronization properties of chaotic systems, in particular Pecora-Carroll synchronization properties, do not necessarily have to be investigated by Lyapunov's stability theory, or by evaluation of conditional Lyapunov exponents. Instead, direct mathematical analysis can be used in certain cases, as was demonstrated in chapter 5 for the simplest quadratic chaotic flow and the Ueda chaotic system.

In chapter 6, several chaotic communication systems with the receiver based on chaotic synchronization were described. These include the chaotic communication schemes of chaotic masking, chaotic modulation and the new chaotic communication scheme of initial condition modulation.

It was shown how Lyapunov's direct method, presented in chapter 3, can be used in the design of the CPM based communication systems. In particular, this was shown on the Ueda master-slave chaotic system.

Furthermore, a method of implementing the synchronized chaotic map master-slave system of chapter 4 within a CPM based secure communication system, was demonstrated on the $\mathfrak{R}^1$ cubic map. It was shown that instant synchronization within the chaotic map CPM based communication system allows for the highest level of discrimination among bits 0 and 1.

On the basis of findings of chapter 5, a secure communication system based on the initial condition modulation of the chaotic carrier by the binary message was then proposed. In particular, this system utilizes a novel approach to the master-slave synchronization properties of the three chaotic flows investigated. The empirical BER curves for the proposed communication systems were then produced and compared to the empirical BER curve of the Lorenz CPM based communication system, demonstrating a significant improvement. It was shown that the communication system based on the simplest quadratic master-slave chaotic flow exhibits the best performance in terms of BER, as compared to the other two proposed systems based on the Ueda and the simplest piecewise linear master-slave chaotic flows. From the security point of view it was observed that the communication system based on the Ueda master-slave chaotic system may be the most secure of the three systems proposed.

Finally, the overall performance of the chaotic parameter and initial condition modulation techniques was examined and compared in the presence of AWGN. It was shown in terms of BER that the ICM based chaotic communication systems exhibit better noise performance than the CPM based ones. Furthermore, it was shown on the Ueda ICM based chaotic communication system that the denoising techniques can be used to further improve the BER performance. The denoising techniques, including linear and wavelet filters, were presented in the appendix.

In chapter 7 chaotic carriers were embedded within a practical multi-user DS-CDMA chaotic communication system and its performance evaluated in the presence of noise and interuser interferences. It was shown how the mutually orthogonal properties between the chaotic time series produced by the logistic map and the PRBS pilot signal enable the traditional ideas of the multi-user CDMA sequence synchronization process to be utilized within the multi-user chaos based DS-CDMA (CBDS-CDMA) system. Furthermore, the system was taken one step further by introducing a chaotic pilot signal in place of the PRBS

pilot signal, thus making the CBDS-CDMA system fully chaotic. In this way, the security of CBDS-CDMA systems is significantly improved by eliminating the security threat posed by an inherently different PRBS pilot signal used in the otherwise chaotic CBDS-CDMA systems. Both phases of the sequence synchronization process, namely the code acquisition and the code tracking, were proposed and investigated.

The code acquisition phase was evaluated in terms of the probability of detection and the probability of false alarm at the chip energy to noise power spectral density ratio of -15 dB for the three different pilot signals and varying number of chaotic users in the system. The theoretical upper bound on the probability of detection was derived and compared to the empirically determined results with the chaotic interferences present. The subsequent empirical curves associated with the increasing number of users in the system have demonstrated the expected degradation in the system performance with the increasing level of interference. In addition, the expected increase of the probability of detection, with the increase in the integration time, was demonstrated. Furthermore, it was shown that the best code acquisition performance is achieved when the PRBS is used as the pilot signal as compared to the logistic and Bernoulli chaotic maps.

The mathematical models for the investigation of the code tracking loops were presented and used to derive the control laws used for the generation of the time offset estimates for PRBS and, periodic and non-periodic chaotic pilot signals. Their validity was then demonstrated by means of a simulation. The performance of the proposed code tracking circuits was primarily evaluated in terms of the bit error rate for varying levels of the chaotic interuser interferences, that is, for different numbers of chaotic users in the system. It was shown that the system is reasonably robust to noise as compared to the performance under the assumption of perfect synchronization. The overall BER performance degradation in an AWGN channel for a multi-user system is characterised by the flattening of the BER curves at low levels of noise due to the prevailing effects of the interuser interferences.

Furthermore, it was demonstrated that the CBDS-CDMA communication systems implementing the proposed sequence synchronization schemes, with a single user in the system, in general exhibit better noise performance in terms of the bit error rate than the Pecora-Carroll CS based communication techniques. It was shown that although the systems are robust to the influence of AWGN and interuser interferences, they all fail to satisfy the maximum allowable bit error rate limit of 10^{-3} in the Rayleigh fading channel, exbhibiting identical BER performance.

Finally, it was shown that in terms of BER, in the AWGN channel only, the proposed chaotic pilot based CBDS-CDMA systems outperform the PRBS pilot based system for a single user in the system at the BER level of 10^{-4} and below. In particular, an improvement of 0.175 dB was demonstrated at the BER level of 10^{-6}. Therefore, in addition to the added security, it was demonstrated that by introducing the chaotic pilot based tracking unit in place of the corresponding

PRBS unit makes the CBDS-CDMA system more robust. The BER performance of all systems was shown to be identical for more than one user in the system.

In chapter 8, a chaos based multi-user TDM system was proposed and evaluated in terms of the bit error rate. Its performance was investigated with and without the assumption of perfect sequence synchronization in the noisy and Rayleigh fading channels. Furthermore, the BER performance of the chaos based DS-CDMA system was compared to the performance of the chaos based multi-user TDM system. The chaotic spreading signals, used to encrypt the binary messages, were generated using the logistic map. As in chapter 7, the mutually orthogonal properties, between the chaotic time series produced by the logistic map with different initial conditions, were used to decrypt messages sent across the channel.

Assuming perfect sequence synchronization, it was shown that in the AWGN and Rayleigh fading channels the TDM system reaches the adopted minimum allowable BER level of 10^{-3} for 1-5, 10, 15 and 20 users in the system. Furthermore, it was shown that in terms of BER the chaos based multi-user TDM system outperforms the chaos based DS-CDMA system for large number of users in the system, while the chaos based DS-CDMA system yields better performance for low number of users in the system.

The proposed chaos based TDM system was then investigated without the assumption of perfect sequence synchronization in the AWGN and Rayleigh fading channels. Again, it was shown that in terms of BER the chaos based TDM system outperforms the chaos based DS-CDMA system for large number of users in the system and vice-versa for low number of users in the system. In order to obtain the full characterization of the system, the sequence synchronization was also assumed with the PRBS pilot signal present on top of each user signal. The effect of the pilot signal on the performance of the system was thus demonstrated in AWGN and Rayleigh fading channels. Furthermore, it was shown that both chaos based TDM and chaos based DS-CDMA systems are insufficiently robust in the Rayleigh fading channel when the perfect sequence synchronization is not assumed.

In order to mutually exploit the DS-CDMA and TDM benefits, a generalized chaos based TDM communication system with more than one DS-CDMA user per TDM branch was proposed and evaluated in the AWGN channel. In this way, the bandwidth efficiency of a DS-CDMA system was combined with the interuser interference immunity of a TDM system, to allow for an increased number of users in the system while improving the BER performance.

In chapter 9, the chaotic synchronization based multi-user TDM systems were proposed and evaluated in terms of BER in AWGN and Rayleigh fading channels. In particular, the proposed systems include the Lorenz and Ueda CPM based TDM systems and the Ueda ICM based TDM systems. It was shown that in terms of BER, the ICM based TDM systems outperform the CPM based TDM systems in both AWGN and Rayleigh fading channels. Furthermore, it was found that the Ueda ICM based TDM system with only the master signal x transmitted, outperforms the Ueda ICM based TDM system with both master signals x and y transmitted. However, the BER analysis in the Rayleigh fading channel revealed

that both CPM and ICM based systems fail to satisfy the highest acceptable BER level of 10^{-3} for any number of users in the system and any E_b / N_o. In addition, two different receiver architectures were implemented and evaluated in terms of BER on all of the CPM and ICM based TDM systems. These include the predetermined threshold receiver architecture and the receiver architecture implementing the two slave systems. It was shown that in terms of BER only in the case of the Lorenz CPM based TDM system the two slave receiver architecture outperforms the predetermined threshold architecture.

Furthermore, the BER performance of the CPM and ICM based TDM systems was compared to the BER performance of the chaos based DS-CDMA system of chapter 7 and the chaos based TDM system of chapter 8. Again, the comparison was conducted in both AWGN and Rayleigh fading channels. It was shown that in terms of BER the chaos based DS-CDMA system of chapter 7, outperforms the CPM and ICM based TDM systems for low number of users in the AWGN channel. However, for larger number of users in the system, the BER curves of the chaos based DS-CDMA system flatten before reaching the highest acceptable BER level of 10^{-3}. In contrast to this, the BER curves of the CPM and ICM based TDM systems do not flatten and thus outperform the chaos based DS-CDMA system for larger number of users. Furthermore, it was shown that the chaos based TDM communication system of chapter 8, outperforms the CPM and ICM based TDM systems for any number of users and any E_b / N_o. Finally, it was shown that the chaos based DS-CDMA system of chapter 7 and the chaos based TDM system of chapter 8; outperform the CPM and ICM based TDM systems in the Rayleigh fading channel. Therefore, it can be concluded that in general, the multi-user chaotic communication systems based on the acquisition and tracking synchronization scheme of chapter 7, are more robust to AWGN and Rayleigh fading than those based on the principles of chaotic synchronization of chapters 3, 5 and 6.

In chapter 10, the security of the proposed, as well as of the existing chaotic communication systems, was evaluated in terms of the average power of the chaotic carriers of the bits transmitted. In order to do so, the two newly proposed measures were used. These were termed the 'Bit Power Parameter Spectrum' (BPPS) and the 'Bit Power Initial Condition Spectrum' (BPICS) measures.
Initially, the method of implementing the synchronized master-slave system within a CPM based secure chaotic communication system was demonstrated on the two dimensional Burgers' map. The nonlinear control laws were designed in such a way to force the synchronization among the master and slave systems using only one signal of the master system. This is of particular importance for communications as only one signal needs to be transmitted thus reducing the required bandwidth.

The security of the Burgers' and the Lorenz CPM, as well as of the Ueda ICM, chaotic communication systems was then evaluated. The security of the proposed and the existing systems was evaluated in terms of the average power of the chaotic carriers of the bits transmitted, that is, in terms of the BPPS and the BPICS. It was shown that due to the largest BPPS and BPICS overlap region of

the chaotic carriers of the transmitted bits, the Ueda ICM based chaotic communication system is more secure than the CPM based chaotic communication systems. Furthermore, it was shown that the BER performance of the CPM based chaotic communication system, implementing Burgers' map system, can be optimized. The optimization is achieved by choosing the parameter sets, representing bits 0 and 1, to be as far apart as possible within the secure operating region.

11.2 Future Directions

Wide scale research into chaotic communications was triggered by the discovery that chaotic systems can be synchronized, which is a necessary requirement for many communication systems. However, due to the lack of sufficiently robust synchronization techniques, the chaotic communication systems have thus far only been of academic interest. In order for the chaotic communication systems to become of practical interest, more robust synchronization techniques must be developed for the future. In this book, the techniques for robust synchronization of chaotic communication systems have been developed, thus powering the way for future research in this area.

Furthermore, with the development of secure communication techniques based on the concept of chaotic synchronization, eavesdropping techniques have also been developing.

Eavesdropping techniques such as those based on the prediction attacks, short-time zero-crossing rate (STZCR) attacks, generalized synchronization attacks, return map attacks, spectral analysis attacks, parameter estimation attacks, among other, highlight the lack of security in many of the proposed systems. For secure chaotic communication systems of the future it is also necessary to seriously address the practical issues of eavesdropping.

Appendix

This appendix investigates de-noising techniques in connection with chaotic synchronization based communication systems. An alternate version of the Ueda ICM based chaotic communication system of section 6.3.2, chapter 6, is proposed and evaluated in the presence of noise, demonstrating a significant improvement. It is then shown that the running average finite impulse response (FIR) filter, and the hard-threshold filtering techniques in Haar and Daubechies wavelet domain can be used to significantly improve performance of the proposed chaotic communication system.

The motivation of this appendix is to investigate the performance of filtering techniques when applied to chaotic synchronization based communication systems [1]. Noise removal from chaotic time series has been attempted by a number of researchers [1-8], among others, and is still an active area of research. Filtering methods include linear filters [3] and different wavelet techniques [1,2,4-6], among other. In this appendix, the running average FIR filter and hard-threshold filtering (de-noising) technique in Haar and Daubechies wavelet domain [9,1] are presented. These are then applied to the proposed low complexity Ueda ICM based chaotic communication system similar to that of section 6.3.2 [10], but with only the master signal x transmitted [1]. It is shown in terms of the bit error rate that the filtering techniques presented significantly improve the performance of the proposed chaotic communication system [1]. Time series plots and phase space diagrams [11] are also used to pictorially represent the effect of the filtering.

Sections A1 and A2 present the Haar and Daubechies wavelet transforms, respectively. The principle of hard-thresholding in wavelet domain is then introduced in section A3. Section A4 proposes a low complexity Ueda ICM based chaotic communication system with only the master signal x transmitted. Furthermore, the developed filters are then applied to the proposed communication system showing a significant improvement in terms of BER as compared to the same non-filtered system.

A1 Haar Wavelet Transform

A wavelet transform is based on the approximation of a time domain function *'f'* in the time-frequency domain. The Haar wavelet transform uses two consecutive time domain values of function *'f'* to represent them by one wider step and one wavelet [9,1] in the new domain, that is, time-frequency domain. The wider step measures the average while the wavelet measures the difference between the two consecutive values and divides this difference by two.

The forward Haar wavelet transform is given by equations A1.1a and A1.1b, and the inverse Haar wavelet transform by equations A1.2a and A1.2b [9,1].

$$a_k^{l+1} = \frac{a_{2k-1}^l + a_{2k}^l}{2}, \qquad c_k^{l+1} = \frac{a_{2k-1}^l - a_{2k}^l}{2} \qquad \text{(A1.1a,b)}$$

$$a_{2k-1}^{l} = a_k^{l+1} + c_k^{l+1}, \qquad a_{2k}^{l} = a_k^{l+1} - c_k^{l+1} \tag{A1.2a,b}$$

In equations A1.1 and A1.2, '*a*' designates the average coefficients and '*c*' the wavelet coefficients. The average and wavelet coefficients are organised into the *Average* and *Wavelet* matrices of the form shown below.

$$Average = \begin{bmatrix} a_1^1 & a_2^1 & a_3^1 & a_4^1 \\ a_1^2 & a_2^2 & 0 & 0 \\ a_1^3 & 0 & 0 & 0 \end{bmatrix}$$

$$Wavelet = \begin{bmatrix} c_1^1 & c_2^1 & c_3^1 & c_4^1 \\ c_1^2 & c_2^2 & 0 & 0 \\ c_1^3 & 0 & 0 & 0 \end{bmatrix}$$

A2 Daubechies Wavelet Domain

Unlike the Haar wavelet transform which exhibits jump discontinuities in the signal transformation, Daubechies wavelet transform is a smoother approximation based on the Daubechies basis function [9]. The forward Daubechies wavelet transform is given by equations A2.1a and A2.1b, and the inverse by equations A2.2a and A2.2b [1] (note that in [9] printing errors have caused erroneous equations, here they have been revised).

$$a_{k+1}^{l+1} = \frac{1}{2} \cdot (h_0 \cdot a_{2k+1}^{l} + h_1 \cdot a_{2k+2}^{l} + h_2 \cdot a_{2k+3}^{l} + h_3 \cdot a_{2k+4}^{l}) \tag{A2.1a}$$

$$c_{k+1}^{l+1} = \frac{1}{2} \cdot (h_3 \cdot a_{2k+1}^{l} - h_2 \cdot a_{2k+2}^{l} + h_1 \cdot a_{2k+3}^{l} - h_0 \cdot a_{2k+4}^{l}) \tag{A2.1b}$$

$$a_{k+1}^{l} = h_2 \cdot a_k^{l+1} + h_1 \cdot c_k^{l+1} + h_0 \cdot a_{k+1}^{l+1} + h_3 \cdot c_{k+1}^{l+1} \tag{A2.2a}$$

$$a_{k+2}^{l} = h_3 \cdot a_k^{l+1} - h_0 \cdot c_k^{l+1} + h_1 \cdot a_{k+1}^{l+1} - h_2 \cdot c_{k+1}^{l+1} \tag{A2.2b}$$

A3 Hard-Thresholding in the Wavelet Domain

The underlying idea of the hard-threshold filtering technique is based on looking at the average power of the wavelet scales, that is, at each row of the *Wavelet* matrix. Hard-thresholding in the wavelet domain involves deletion of certain wavelet scales where noise exists, but signal does not [9]. In other words, provided that the pure signal does not contain significant average power in certain row of the *Wavelet* matrix, but when mixed with noise the average power increases in that particular row, then this row can be set to zero in its entirety.

A4 Application to Communications

A4.1 Overview of the Ueda ICM Based Chaotic Communication System

In chapter 6 [10], a digital communication system based on the initial condition modulation of the chaotic carrier by the binary message to be transmitted was proposed. The demodulation process at the receiver is based on the synchronization of one of the master-slave signals. Due to the smooth nature of the transmitted signal at the bit transitions, it was argued in section 6.3.2 that the Ueda chaotic communication system is the most secure out of the systems examined. In case of the Ueda chaotic communication system, when the master x signal drives, demodulation at the receiver is based on the chaotic synchronization properties of the master-slave y signals, governed by equation A4.1 [10].

$$y(t_o) - \hat{y}(t_o) = A - k\int_{t=0}^{t=t_o} (y(t) - \hat{y}(t))dt + 2B\sin(\phi)\sin(t_o + \Omega) \tag{A4.1}$$

where: $\phi = \dfrac{z - \hat{z}}{2} = \dfrac{z(0) - \hat{z}(0)}{2}$ and $\Omega = \phi + \hat{z}(0) + \pi/2$.

Again, in equation A4.1, '^' above the y signal represents the slave y signal. It has been shown in chapter 5, section 5.3 [10], that equation 5.1 settles to steady state behaviour, governed by its third term, as time tends to infinity. As the third term of equation A4.1 is governed by the initial conditions of the master-slave z signals, $z(0)$ and $\hat{z}(0)$, respectively, it has been shown that equation A4.1 can be used to demodulate the received binary message, given that the binary message is represented by the difference of the master-slave z initial conditions [10]. Furthermore it has also been shown that the separation of the binary symbols in their symbol space is largest when the difference among the master-slave z initial conditions is equal to $\pm 2n\pi$ and $\pm n\pi$, depending on whether binary 0 or binary 1 are transmitted, respectively.

In order to implement equation A4.1 at the receiver (slave) side, it is required to transmit both the driving transmitter (master) signal x, and the master signal y.

A4.2 Low Complexity Ueda ICM Based Chaotic Communication System with Only x Transmitted

It is now shown how the Ueda chaotic communication system of section 6.3.2 [10] can be reduced in complexity, while at the same time improving the noise performance. In section 6.3.2 [10], demodulation of the received signal is achieved by observing the synchronization error of the master-slave y signals. If this error tends to zero, it is concluded by the receiver that bit 0 was sent. It is concluded that bit 1 was sent if the steady state error is sinusoidal, that is, not zero. Here it is graphically shown (Figure A2) that it is sufficient to only observe the behaviour of the slave signal y in order to successfully discriminate among the binary symbols 0 and 1. In this case it is required to only transmit the driving transmitter (master) signal x, thus reducing the required bandwidth. Such a communication system is presented in Figure A1.

In Figure A1 the message m is varied among 2π and π, depending on whether bit 0 or bit 1 is to be transmitted, respectively. In order to ensure continuity of the smooth nature of the transmitted signal x, as well as to avoid periodicity of chaotic sequences representing bit 0 and bit 1, the initial conditions of x (y), for every new bit transmitted, are chosen as the final values of the chaotic carrier (signal) of the preceding bit [10]. Note that in Figure A1, n represents the additive white Gaussian noise (AWGN).

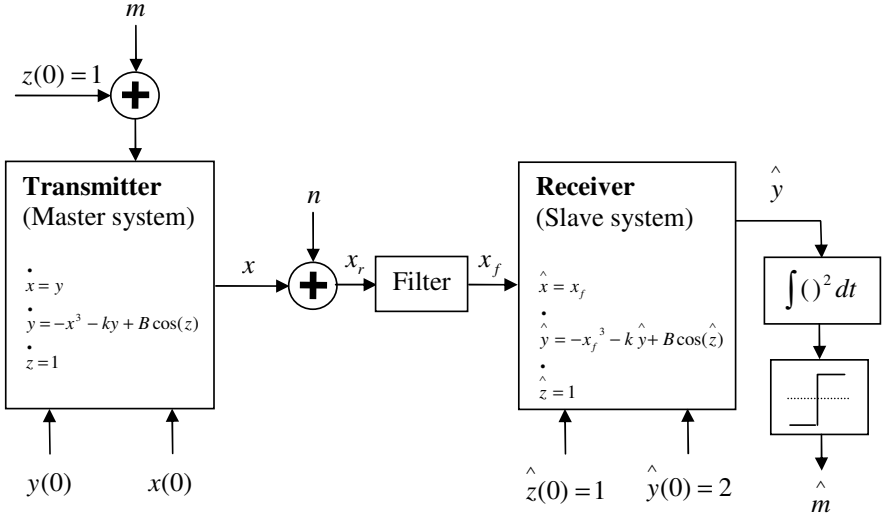


Fig. A1 The Ueda chaotic communication system, based on the initial condition modulation of [10], but with only x transmitted [1].

The transmitted signal x and the squared slave signal $\hat{y}$ are shown in Figures A3a and A2, respectively, when $m = [2\pi,\ 2\pi,\ \pi,\ 2\pi,\ \pi,\ \pi,\ 2\pi,\ \pi,\ 2\pi,\ \pi]$, or in binary terms: *message* = [0 0 1 0 1 1 0 1 0 1]. From Figure A3a, observe the smooth nature of the transmitted signal x. In Figure A2 the dominant peaks represent bits 1.

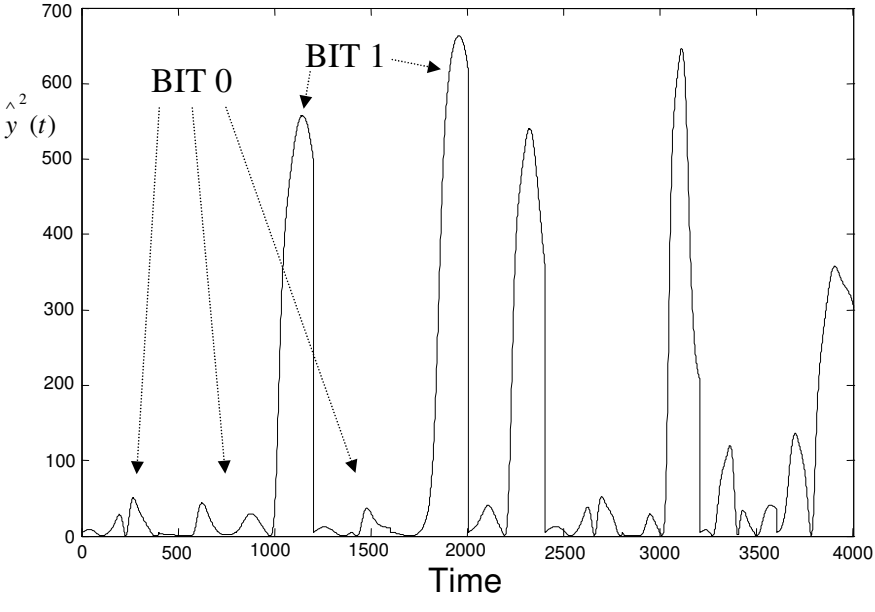


Fig. A2 Slave signal $\hat{y}$ squared

In order to compare the performance of the Ueda chaotic communication system of Figure A1 to the Ueda chaotic communication system of Figure 6.22, chapter 6, an empirical BER curve has been produced and shown in Figure A5 by the open circles. As in the evaluation of most binary modulation techniques, clock synchronization among the transmitter and receiver has been assumed [10]. The spreading factor, that is, the number of chaotic points representing each bit has been chosen to be 400 [10]. For comparison, the BER curves of the Lorenz CPM based system of Figure 6.7, as well as of the BPSK system, have been produced and denoted by the crosses and the solid line, respectively.

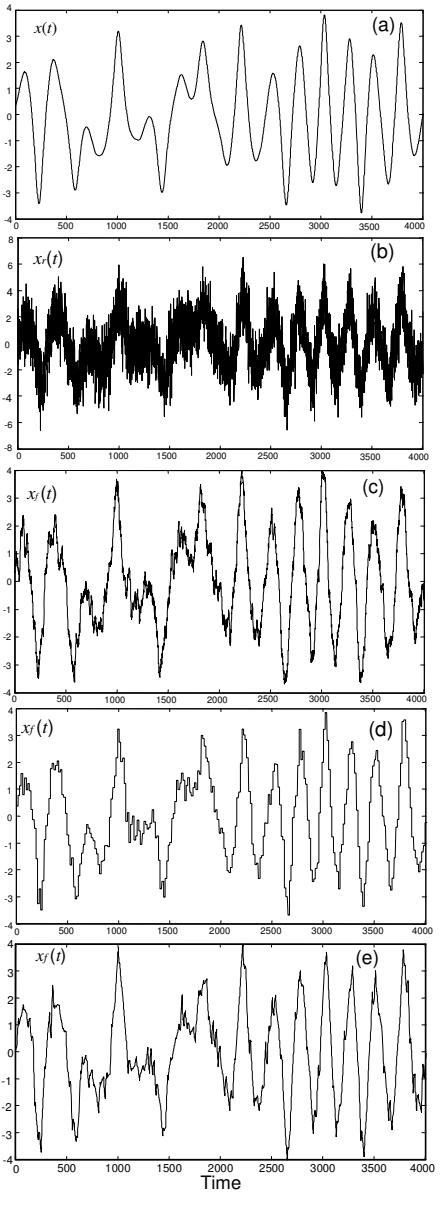


Fig. A3 (a) Transmitted signal *x*, (b) Received signal *xr* at *Eb/No* = 25 dB, (c) FIR filtered signal *xf*, (d) Haar filtered signal *xf*, (e) Daubechies filtered signal *xf*

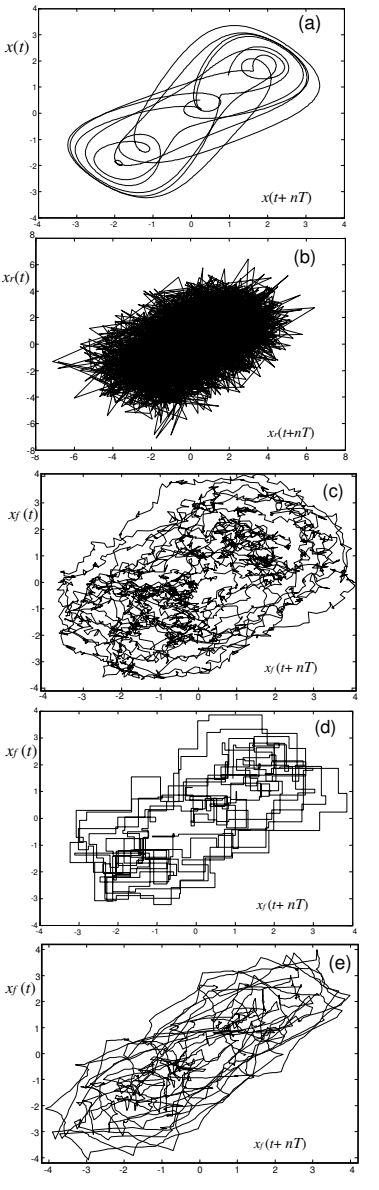


Fig. A4 Ueda strange attractor: (a) Clean, (b) at *Eb/No* = 25 dB, (c) FIR filtered, (d) Haar filtered, (e) Daubechies filtered

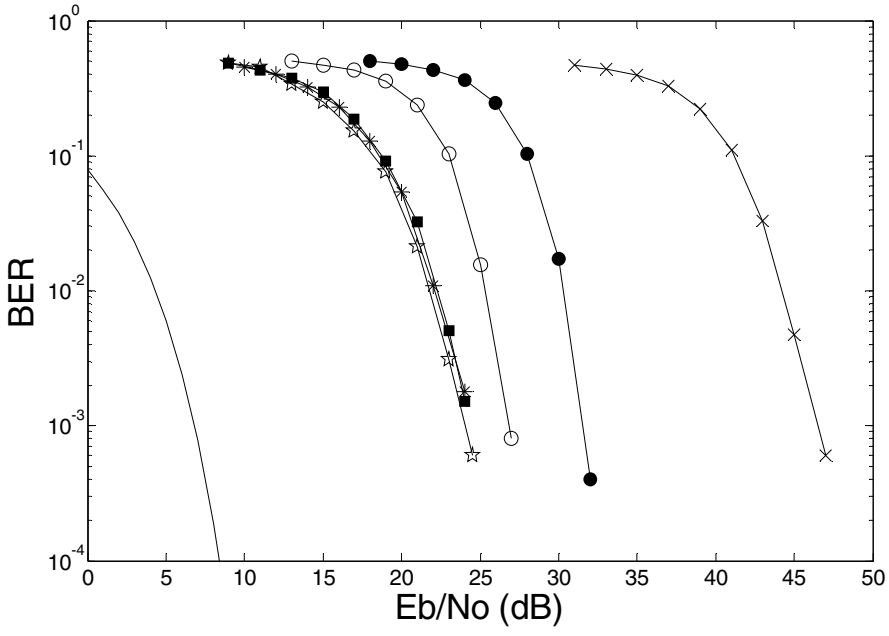


Fig. A5 The BER curves: (a) the solid line is for the theoretical BPSK, (b) the pentagram stars are for the running average FIR filtered system of Figure A1, (c) the asterisks are for the Haar filtered system of Figure A1, (d) the solid squares are for the Daubechies filtered system of Figure A1, (e) the open circles are for the non filtered system of Figure A1, (f) the solid circles are for the Ueda initial condition modulation system introduced in [10], (g) the crosses are for the Lorenz chaotic parameter modulation system introduced in [1].

A4.3 Running Average FIR Filtering

In [3] it has been reported that the linear filters can be used to filter non-linear systems. It is now shown that the noise performance of the system proposed in subsection A4.2 can be further improved by using the running average finite impulse response (FIR) filter [12] to filter the received signal $x_r(t)$.

The noisy Ueda chaotic signal x at E_b / N_o of 25 dB is shown in Figure A3b. The corresponding filtered signal is shown in Figure A3c. The Ueda strange attractor is shown in Figure A4a, followed by the noisy and filtered Ueda strange attractor at E_b / N_o of 25 dB in Figures A4b and A4c, respectively.

From these a clear improvement in the filtered signal can be noticed as compared to the noisy one. The effect of this filtering technique on the communication system of Figure A1 is demonstrated in Figure A5 by the bit error rate (BER) curve marked by the pentagram stars. Comparing this BER curve to the BER curve of the system of Figure A1 without filter (marked by the open circles), an improvement of 3-4 dB can be observed.

A4.4 Filtering in the Haar Wavelet Domain

Figure A6 shows the Ueda chaotic signal *x* in the Haar wavelet domain, for three different noise levels, and for the case when there is no noise. From Figure A6, it can be seen that the first five rows of the *Wavelet* matrix can be hard-threshold to zero at bit energy to noise power spectral density ratio (E_b / N_o) of 20 dB and 15 dB and the first four rows at E_b / N_o of 25 dB.

The Haar filtered Ueda chaotic signal *xf* is shown in Figure A3d. The Haar filtered Ueda strange attractor is presented in Figure A4d. The prominent edge effects can be observed in Figure A4d. These edge effects can be explained in the following manner. Each row of the *Wavelet* matrix is a rough approximation of the row above it, for example, second row is a rough approximation of the first row. Hard-threshold to zero of the first four rows of the *Wavelet* matrix allows lower rows to estimate the upper rows.

In Figure A5 the BER curve of the system of Figure A1, when filtered in the Haar wavelet domain, is represented by the asterisks. It demonstrates an improvement of about 3-4 dB as compared to the non-filtered one (open circles).

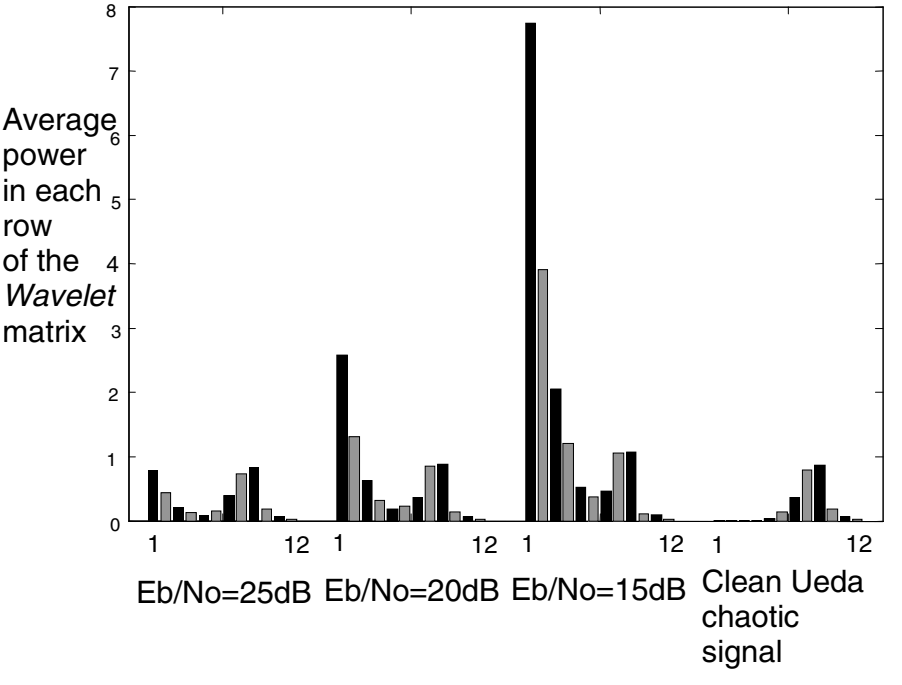


Fig. A6 Average power of the coefficients in each row of the Haar *Wavelet* matrix for the noise polluted signal, where E_b / N_o is 25 dB, 20 dB and 15 dB, and for the clean Ueda chaotic signal *x*

A4.5 Filtering in the Daubechies Wavelet Domain

Figure A7 shows the Ueda chaotic signal x in Daubechies wavelet domain, for three different noise levels, and for the case when there is no noise. From Figure A7 it can be seen that for the Ueda chaotic signal x the first five rows of the *Wavelet* matrix can be hard-threshold to zero at E_b / N_o of 20 dB and 15 dB, and the first four rows at E_b / N_o of 25 dB.

The Daubechies filtered time series and the corresponding chaotic attractor are shown in Figures A3e and A4e, respectively. As with Haar, using the Daubechies filtering technique to filter $xr(t)$, and thus produce $xf(t)$, improves the BER curve of the system of Figure A1 by 3-4 dB, as is demonstrated in Figure A5 by the curve marked by the solid squares.

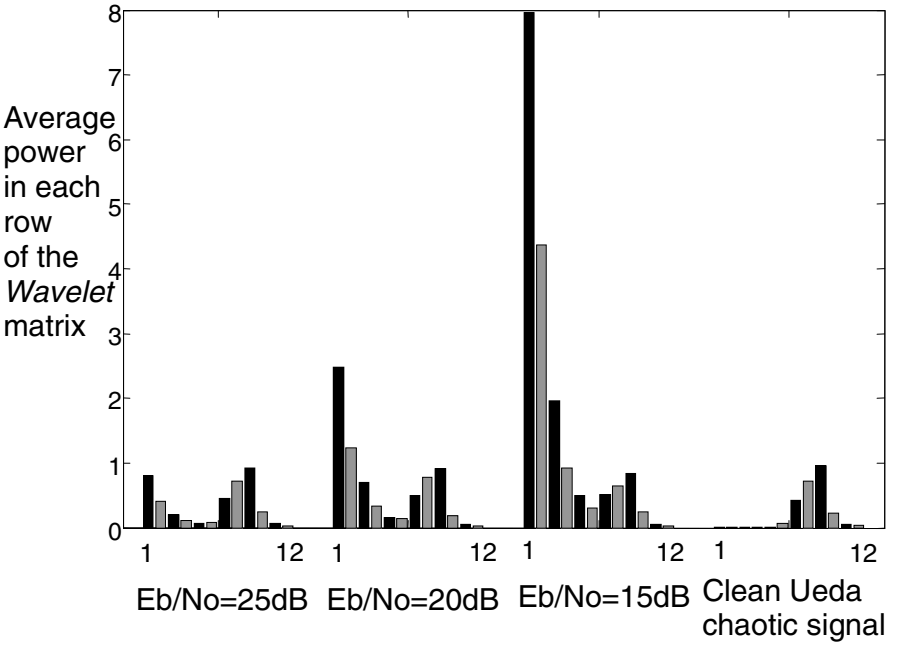


Fig. A7 Average power of the coefficients in each row of the Daubechies *Wavelet* matrix for the noise polluted signal, where E_b / N_o is 25 dB, 20 dB and 15 dB, and for the clean Ueda chaotic signal x

A4.6 Results and Discussions

The bit error rate curves demonstrating the noise performance of the aforementioned communication systems are displayed in Figure A5. The Ueda initial condition modulation chaotic communication system with only the master

signal x transmitted (open circles), exhibits an improvement in the BER curve of approximately 5 dB as compared to the Ueda chaotic communication system of section 6.3.2 [10] (full circles). The three filtering techniques presented above all improve the BER curve of the non-filtered system of Figure A1 by 3-4 dB with the running average FIR filter exhibiting marginally better performance than the Haar and Daubechies filtering techniques.

From Figure A5 it is noted that for the Ueda chaotic communication system of Figure A1 (open circles) it requires 18-19 dB less energy per bit to achieve the same probability of error as compared to the Lorenz based chaotic parameter modulation system of Figure 6.7, section 6.2.1 [13] (crosses). Filtering techniques improve the performance even further. The system of Figure 6.7 could not be efficiently filtered, using the aforementioned filtering techniques, due to the very low levels of noise in its operating region, with an attempt at filtering worsening the performance.

A5 Conclusion

It has been shown that the herein proposed alternative of the secure Ueda ICM based chaotic communication system of section 6.3.2, but with only x transmitted, exhibits a significant improvement in terms of the bit error rate. The running average FIR filter and the hard-threshold wavelet de-noising techniques, in Haar and Daubechies wavelet domain, have been described. Furthermore, these have then been applied to the proposed secure communication system, demonstrating another significant improvement in the bit error rate curve. In [3], it has been mentioned that the linear filters can be used to filter non-linear systems. Here, this has been demonstrated by applying the running average FIR filter within a chaotic synchronization based communication system. It has also been shown that smooth chaotic time-series of the Ueda chaotic communication system can be successfully filtered in wavelet domain, using hard-threshold to zero filtering technique. Despite the fact that filtering in wavelet domain introduces edge effects the dynamics of the strange attractor seem to be well preserved. Filtering in Daubechies wavelet domain exhibits smoother edge effects on the strange attractor than filtering in Haar wavelet domain.

References

[1] Jovic, B., Unsworth, C.P., Berber, S.M.: De-noising 'Initial Condition Modulation' Wideband Chaotic Communication Systems with Linear & Wavelet Filters. In: Proceedings of the First IEEE International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2006), Sydney, Australia, March 13-16, pp. 1–6 (2006)

[2] Grzesiak, M.: Wavelet filtering of chaotic data. Nonlinear Processes in Geophysics 7, 111–116 (2000)

[3] Broomhead, D., Huke, J., Muldoon, M.: Linear Filters and Nonlinear Systems. Journal of the Royal Statistical Society 54(2), 373–382 (1992)

[4] Roy, M., Kumar, V., Kulkarni, B., Sanderson, J., Rhodes, M., Stappen, M.: Simple denoising algorithm using wavelet transform. AIChE Journal 45(11), 2461–2466 (1999)
[5] Constantine, W., Reinhall, P.: Wavelet-based in-band denoising technique for chaotic sequences. International Journal of Bifurcation and Chaos 11(2), 483–495 (2000)
[6] Boccalleti, S., Guiaquinta, A., Arecchi, F.: Adaptive recognition and filtering of noise using wavelets. Physical Review E 55(5), 5393–5397 (1997)
[7] Lee, C.: Noise reduction methods for chaotic signals with application to secure communications, PhD thesis, Georgia institute of technology (1995)
[8] Carroll, T.L.: Approximating chaotic time series through unstable periodic orbits. Physical Review E 59(2), 1615–1621 (1999)
[9] Nievergelt, Y.: Wavelets made easy, chs. 1, 2 and 3. Birkhauser, Boston (1999)
[10] Jovic, B., Berber, S., Unsworth, C.P.: A novel mathematical analysis for predicting master – slave synchronization for the simplest quadratic chaotic flow and Ueda chaotic system with application to communications. Physica D 213(1), 31–50 (2006)
[11] Abarbanel, H.: Analysis of Observed Chaotic Data, p. 120, 125. Springer, New York (1996)
[12] Sprott, J.C.: Chaos and Time-Series Analysis, pp. 230–440. Oxford University Press, Oxford (2003)
[13] Cuomo, K.M., Oppenheim, A.V.: Circuit Implementation of Synchronized Chaos with Applications to Communications. Physical Review Letters 71(1), 65–68 (1993)

Index

D