DEBRE BERHAN UNIVERSITY
INSTITUTE OF TECHNOLOGY
COLLEGE OF COMPUTING

M.Sc. in Computer Networks and Security
[Curriculum]

Debre Berhan, Ethiopial

August 2016

Curriculum for Master of Science Degree in Computer Networks and Security

The Study Program was developed by the Curriculum Development Committee from College of Computing, Institute of Technology, Debre Berhan University

In print:

Samuel Asferaw Demilew (Graduating PhD in Networking)

Yeshialem Gezahegn (MSc)

Getachew Mekuria (MSc)

Sofanyas Yitagesu (MSc)

College of Computing
Institute of Technology
Debre Berhan University
Debre Berhan, Ethiopia
August 2016

Table of Contents

1. INTRODUCTION

Debre Berhan University (DBU) is established as 2nd tier of higher education expansion in the country in the 600 years old historical town of Debre Berhan situated in Amhara Region, North Shoa Zone, 130 km away from Addis Ababa in the north laying foundation stone on 9th May, 2005. Currently, the town is highly vibrant town in all walks of social and industrial development. In addition to existing main road linking the town with Addis Ababa and Dessie, upcoming roads which are under construction: one which connect the town to the port of Djibouti via Anckober and Awash towns, one that connects the town with the country's main road from Addis Ababa to Gojjam and one that connects the town to Mojjo town via Arrarti will make the town another hub in the central part of the country next to Addis Ababa.

The initial intake capacity of the university in Jan. 2007 G.C. was 725 students who joined in to 5 departments with 68 instructors and 7 administrative staffs. But now, the enrolment has significantly increased to more than 14,000 regular, extension and summer students who joined in to 35 departments/ programs in ten colleges, two institutes and eight post graduate programs. Among the two institutions is Institute of Technology which hosts two Schools: School of Engineering and School of Computing. The latter hosts this post graduate program, MSc in Computer Networks and Security.

Currently, the university is staffed with more than 700 (first degree to third degree) academic staffs (276 are on study leave), and more than 500 administrative staffs. In 2015 G.C, the intake capacity of the university has grown to 12,000 regular academic trainees.

Mission of DBU:

- Producing efficient graduates by offering research assisted quality education.
- Undertaking a problem solving research based on national need and benefiting the community with the outcome.
- Offering government and community centred training, consultancy service, transferring technology and undertaking innovation.

Vision of DBU:

- Aspires to be the best university in Ethiopia by 2020.

Values of DBU:

- Shared vision

- Quality service
- Attention to cross-cutting issues
- Diversity
- Professionalism
- Equality
- Effectiveness
- Democracy

2. RATIONALE OF THE CURRICULUM

In the digital era, where all walks of life is becoming totally dependent on the information technology, computer networks and security plays a major role. World is now in the information era which has been and will continue to be profoundly influenced by advances in digital technology with dramatic impact in the field of education, health, business, entertainment, and other service providing systems where they explore ways of taking advantage of computer networks and security technologies in order to expand the repertoire of engineering practice and enhance development means.

To be competitive locally and globally, the Ethiopian Government Development Policy demands extensive use of ICT (Information Communication Technology) in which computer networks and security is a backbone. Hence, the basic rationale for the MSc in Computer Networks and Security program is the prevailing conditions in the country with respect to the need for professionals in computer networks and security, and the future developing trend in the demands for the profession.

The report of the need assessment done by the curriculum committee directly reflects the necessity of this program in the country because the country is engaged in huge ICT projects in different sectors like, e-governance, e-services, etc. The potential organizations that will observe the graduates of this program (banks, ICT agency, Ministry of Finance, universities, Ethiopian Air lines, etc) during need assessment of the program emphasised the importance of contents not only computer network but also network security in the program. As a result, we are attempted to show this not only on the program content but also in the program nomenclature.

During need assessment, firstly, we have observed that to be competitive in their work, many organizations in Ethiopia need skilled, highly educated professionals in Computer Networks and Security. In the country, these days, the number of manufacturing industries, commercial centres, governmental and nongovernmental organizations that use network and network applications are considerably increasing. To work successfully and to be competent, these organizations and enterprises need computer networks and security experts to handle and manage their sophisticated systems confidentially and securely.

Secondly, the number of Computer Science, Information Technology, Electrical and Computer Engineering, etc graduates graduating from all universities in the country is increasing rapidly per annum; so it is becoming inevitable that many shall be seeking higher education. Thirdly, for many of these graduates, it is both necessary to prepare them for doctoral level education and also to achieve their professional goals with practice in dynamically changing trends of information technology. Fourthly, research and academic institutes need young researchers and academicians to look into and contribute their problem solving solutions in the computer networks and security related state-of-the-art technologies so that the gap in scholarly communication among different regions to be filled. Therefore, Debere Berhan University, Institute of Technology, College of Computing was convinced that it is necessary to offer graduate program (MSc. in Computer Networks and Security as a unique program in Ethiopia) in order to provide opportunity to the eligible under graduate professionals to upgrade themselves to higher level and make them available for the development of the country.

3. OBJECTIVE OF THE PROGRAM

3.1 General Objectives

This program provides students with advanced-level of knowledge and skills in Computer Networks and Security at master's level with possible addition of vendor-specific trainings in the curriculum. The focus is on imparting Body of Core Knowledge Areas and evaluation through research by thesis and/or network project design, management and implantation through project in relevant domains. A Master's degree in Computer Networks and Security is highly respected program and graduates from this degree program enjoy an excellent employment rate as it is a backbone for any industries or organizations to stay competitive in the market. Hence, the program has the following general objectives:

- To produce trained professionals in computer networks and security suitable for academia, industries, organizations and enterprises.
- To prepare students to realize the importance of preparedness for emerging network professional opportunities.
- To prepare students to acquire basic artefacts of advance network planning, design, deployment, management and security.
- To educate students on the importance of the quality consciousness, honesty, loyalty and ethical professionalism.
- To produce trained professionals in computer networks and security to fill the gap between the industry and the academics.

3.2 Specific Objectives

This program intends to provide students with the theoretical (research) and practical skills necessary to pursue careers as computer networks and security professionals. The specific objective of the MSc award in Computer Networks and Security is to equip students with an in-depth understanding of advanced technical and academic skills and knowledge for:

- Providing students with a solid foundation in network planning, design, management, system administration, network security, enterprise networks, and network performance.
- The application of Computer Networking and Security technologies in the real world.
- Professional employment or further academic development in the continually expanding areas of computer networks and security technologies.
- Developing key employability skills, such as communication, collaboration, and project management through studio-based and project-based learning.
- Providing for training in design, implementation and administration of high-performance computer network and security infrastructures including examination of the methods, techniques, tools and technologies used to develop and secure such infrastructures.
- Equipping students with network security skills demanded by the digital world.

- Equipping the trainees with not only the general science and skills but also with vendor specific technologies.
- A rigorous theoretical knowledge and understanding of current research issues as well as detailed practical experience of network planning, design, development, implementation, operations, applications, systems and services.
- Skills that will enable students to contribute to future developments in the field of system administration, network design, management and implementation.
- The ability to make a critical evaluation of the theories, techniques and systems used in planning, design, implementation, management, security and disaster recovery of modern communication networks as well as the services they support.
- Skills to embark students in consultancy, developing research as well as problem-solving techniques through practical project experience by extending students' knowledge and skills in a specialized area they will be prepared for careers in advanced research and/or industry.
- The ability to evaluate the performance of wired and wireless computer networks using analytical and/or simulation tools; and manage the implementation of a complete communication design project with high security.
- Knowledge and understanding of the legal, social, ethical and professional issues related to network design and development.

4. STRUCTURE OF THE PROGRAM

The program consists of two years of full-time studies for regular students, giving a total of 42 Credits. The medium of instruction is English.

The curriculum is organized in 4 semesters in 2 years duration. In first year first semester there are 4 courses each with 3 credits (1 theory and 3 theory integrated with lab courses). In first year second semester there are 4 courses each with 3 credits (all theory integrated with lab courses). In second year first semester like first year second semester there are 4 courses each with 3 credits (all theory integrated with lab courses). Second year second semester is dominated by thesis research work and preparation for final year thesis defence.

In addition, to the main course material and thesis work, students are expected to attend a regular program of seminars on specific topics, designed by Computer Networks and Security

(CNS) Lab to extend students knowledge and introduce them to new technologies, applications and research areas. Furthermore, focus on experimental work is ensured through laboratory courses integrated with majority of the courses.

The structure of the four semesters is divided up as shown in the following table:

Year	Semester	Teaching
I	I	1 Theory Course + 3 Theory Integrated with Lab Courses
I	II	4 Theory Integrated with Lab Courses
II	I	4 Theory Integrated with Lab Courses
II	II	Thesis

5. PROGRAM REQUIREMENTS

5.1 Top View of Course Content Areas

The course program comprises of core (compulsory) and elective courses.

5.2 Admission Requirements

Students seeking admission to M.Sc. in Computer Networks and Security program must possess:

i. Completed the academic requirements for the Bachelor Degree in Information Technology, Computer Science or an **equivalent degree** from an accredited higher learning institutions and a Cumulative Grade Point must be a minimum of an Average (CGPA) of 2.00.

ii. Applicant must pass the written and oral entrance examination as prescribed by the university.

iii. Applicant must fully satisfy all the requirement as laid down in academic rule and regulations of Debre Berhan University; and

iv. Produce a letter of recommendation indicating sponsorship for their research work or sign an agreement, if, self sponsored.

v. The maximum number of graduate students to be admitted annually to each program is determined by the CNS Lab and School of Computing council in consultation with the council of graduate studies, based upon the availability of resources and considering its costs effectiveness. However, in any case, the minimum number of students per class shall not be less than 5 students.

vi. Admission shall take place one time in a year on the Semester beginning.

vii. Anyone who wants to join the graduate program can apply. For pedagogical reasons or special requirements of field of study, the School of Computing Academic Commission may set appropriate age limits subject to the approval of the Council of Graduate Studies as per rules and regulation of the Debre Berhan University.

viii. Preference may be given to candidates with at least two years of relevant work experience if he/she qualifies the criteria.

5.3 Graduation Requirements

The graduating candidate (M.Sc. in Computer Networks and Security) must fulfil the following requirements:

a) All candidates must satisfactorily fulfil the general graduation requirements as laid down as in academic rules and regulations of the University School of Graduate Studies

b) Pass all examination in the courses offered in the program with minimum CGPA of 3.00.

c) A graduate student may apply to the CNS Lab and School of Computing Graduate Council to repeat a course in which he/she obtained a "D or F" grades; however, no such course may be repeated more than once.

d) If a graduate student repeating a course in which he/she obtained "D or F", the last grade will be final and it will be marked as repeated.

e) Graduate students repeating courses in which they scored "D or F" grades must register for the courses and carry out all academic activities pertaining to the courses.

f) Successfully defended the graduate thesis

g) Get approval of the university senate.

5.4 Duration of Study

The duration of M.Sc. in Computer Networks and Security program is a minimum of two academic years. However a maximum of four academic years will be permitted on the grounds of force majeure and academic failure on the recommendations of DGC and AC (Academic Council) subject to the fulfilment of special condition laid down by SGS (School of Graduate Studies).

5.5 Teaching-Learning Methods and Strategies

Taking a cue from the dictum of learning which says "You may hear and forget, you may see and remember but you do and learn", action oriented and student-centred learning would be emphasized as the modus operandi while underlining the significance of inducing curiosity for continuous self-learning as the catalyst for effective assimilation of knowledge and its application in concrete situations.

The teaching-learning methods to be adopted, for the transfer and/or acquisition of knowledge and skill development include:

- Classroom gap-lectures backed up by course-work projects, and assignments;
- Lectures by industry professionals and resource persons on a periodic basis;
- Laboratory exercises and practical demonstrations;
- Field visits related to community development/intervention;
- Industrial visits;
- Practical and development oriented network design projects;
- Individual and group seminars/presentations;
- Group tasks/discussions/case studies;

Teaching-Learning Strategies

Teaching-learning strategies for graduates profiles (computing-related cognitive, practical abilities and other transferable skills) are detailed with the corresponding assessment method or methodology as follows:

Computing-related Cognitive Abilities: Students learn knowledge, gain understanding and develop cognitive skills and abilities through self-directed study, resource based learning, small group discussions, small group and individual exercises, laboratory sessions, demonstration software and tools, on-line examples and research thesis. Weekly seminar sessions that provide students with the opportunity to address questions, queries and problems are also part of gaining this ability.

- Traditional lecture delivery,
- Group and individual research, presentations and written reports,
- Laboratory sessions,
- Individual and group design work,
- Individual project: Throughout the program, students are encouraged to undertake independent reading both to supplement and consolidate what is being taught or learned and to broaden their individual knowledge and understanding of the subject.

Assessment of Computing-related Cognitive Abilities: Group and individual coursework; presentations; group and individual reports; and the research thesis assess students' knowledge and understanding:

- Computing-related Practical Abilities: Students gain practical skills through;
- Group and individual research, presentations and written reports,
- Small group and individual exercises,
- Laboratory sessions,
- Individual research thesis,
- Analysis, design and problem solving skills are further developed through various design activities as well as case studies, internships and extensive computer laboratory

sessions. Feedback is given to students on all assessed coursework as well as written exams (in the form of exam reports produced each term).

Assessment of Computing-related Practical Abilities: Students' practical abilities are assessed through group and individual coursework, laboratory tests, examination, and the research thesis:

Transferable skills: Students gain transferable skills through the aforementioned teaching and learning program. These skills are also nurtured through:

- Small group and individual presentations and exercises,
- Laboratory sessions,
- Individual research thesis.

Assessment of Transferable Skills: Students' transferable skills are generally assessed through coursework reports and the thesis report.

5.6 Assessment/Evaluation

Generally, Continuous Assessment out of 50% (like written test, research project work/Lab project work, seminar, individual and group assignment) and final written examination out of 50%, will be used to assess the progress of the trainees but this is subject to nature of the course. The grading system is as per the Debre Berhan University fixed scale ranges for graduate student evaluation system:

Row Mark	Letter Grade	Grade Point
[95, 100]	A+	4.0
[85,95)	A	4.0
[80,85)	A-	3.75
[75,80)	B+	3.5
[70,75)	B	3.0
[65,70)	B-	2.75
[58,65)	C+	2.5
[50,58)	C	2.0
[40,50)	D	1
[0,40)	F	0.0

6. PROGRAM OUTPUT

6.1 Professional Profile

- Possess a body of knowledge that demonstrates understanding of state-of-the-art developments in the area of Computer Networks and Security.
- Be able to investigate and evaluate key network technologies and apply them effectively in an organization
- Exercise critical thinking, and problem-solving ability to tackle complex new problems.
- Be capable of independent professional work with high level of autonomy and accountability.
- Demonstrate significant research, analysis and evaluation skills in the networking discipline.
- Be able to adapt their knowledge and collaborate and communicate with others in a professional setting.
- Know and understand the principles of mobile and wireless communication systems.
- Know, understand and design modern networking systems including the maintenance of security, integrity and confidentiality of data.
- Show critical and analytical thinking in the application of knowledge and/or research in a particular networking system.
- Successful students are expected to go on to become high-level network specialists in fields such as network administration, planning and design, implementation and security.
- Successful completion of this programme will also leave students ideally placed to achieve professional networking certifications.

6.2 Graduate Profile

Successful graduates of this program are expected to acquire advanced knowledge in the field and cognitive thinking and practical skills in Computer Networks and Security. Thus, the department expects graduates to exhibit the following traits:

6.2.1 Knowledge and Understanding

On completion of this program the successful student will have knowledge and understanding of:

- Theoretical and practical knowledge of advanced concepts in networking and security
- Design and implementation of network-based tools
- Advance concepts of mobile communication systems and services
- Current technologies that are used in networking and security industry
- Design and implementation issues of effective security strategies to minimize the effects of attacks.

6.2.2 Cognitive (Thinking) Skills

On completion of this program the successful student will be able to:

- Become a valued expert in high technology with excellent abilities
- Develop interdisciplinary thinking, team orientation and presentation skills
- Use networking tools to analyze complex systems competently
- Gain and explore theoretical and analytical competences for scientific work.
- Acquire skills for developing products and systems in the area of industrial information and communication technology.
- Analyze systems, identify in internetworking problems and effectively apply solutions and tradeoffs.
- Use different research methods to develop policies and select suitable mechanisms to enforce such policies.
- Ensure that networking system design complies with relevant professional, ethical and legal issues.

6.2.3 Practical skills

On completion of the program the successful student will be able to:

- Work in the field and with the general ability to perform tasks of a network engineer.
- Design and implement technical applications of computer network and security systems based on data processing, automation and data transmission, without excluding abilities to work as a researcher, teacher or manager.

- Utilize their network knowledge in other branches of engineering.
- Build networking systems and security to find a solution for a specific task.
- Students achieve good language, communication and cooperation skills and the ability to work in a multidisciplinary and international community.

6.2.4 Excellent Career Prospects

- Multi National Networking Companies e.g. Governmental organizations, NGOs and so on
- Government Organizations such as INSA(Information Network Security Agency)
- Ministry of defence
- Universities and Research organizations.

6.2.5 Educational Outcomes

Students graduating from Computer Networks and Security programs will be able to choose many different roles; network consultants, network project planners, network security consultants, network security project planners, project managers, interface designers, researchers and analysts. Some of the general tasks that a Computer Networks and Security specialist is likely to perform include:

- An ability to apply knowledge of computing and mathematics appropriate to the discipline.
- An ability to analyze a problem, and identify and define the requirements appropriate to its solution.
- An ability to design, implement and evaluate a system, process, component, or program to meet desired needs.
- An ability to work effectively on teams to accomplish a common goal.
- An understanding of professional, ethical, legal, security and social issues and responsibilities.
- An ability to communicate effectively with a range of audiences.
- An ability to analyze the local and global impact of networking and security on individuals, organizations, and society.

- Recognition of the need for and an ability to engage in continuing professional development.
- An ability to use current techniques, skills, and tools necessary for computing practice.
- An understanding of processes that support the delivery and management of networked systems within a specific application environment.
- An ability to use and apply current technical concepts and practices in the core network technologies.
- An ability to identify and analyze user needs and take them into account in the selection, creation, evaluation and administration of computer-based systems.
- An ability to effectively integrate network-based solutions into organizations and enterprises.

7. DEGREE NOMENCLATURE

The degree awarded to students who successfully completes the minimum requirements is as follows:

In English:

“Master of Science in Computer Networks and Security”

In Amharic:

“የሳይንስ ማስተርስ ዲግሪ በኮምፒውተር ኔትወርክስ እና ሴኩሪቲ”

8. PROGRAM RESOURCES

8.1 Staff Profile

Currently, the program is equipped with the following proportion of qualified people:

No	Academic Status	Male	Female	Total	Remark
On Job					
1	Professors	0			
2	Associate Professors	0			
3	Assistant Professor	3	0		2 Waiting for dissertation defence
4	Lecturers	25	3	28	
5	Assistant Lecturers	11	0	11	
6	Graduate Assistants	8	5	13	
On Study Leave					
7	PhD	4	1	5	
8	MSc	14	2	16	

8.2 Material Resources

As to the resource and materials, computer hardware and software resources such as simulation, experimental, visualization and analysis tools, laboratories with local area network and online access facilities, bibliographic laboratory equipped with appropriate information resources and information retrieval tools, laboratory and office rooms equipped with appropriate ICT resources and facilities are available. In addition to the aforementioned resources, there will be full access to digital libraries such as IEEE and ACM in the coming few months.

Currently, the college has 14 computer labs (on average 25 computers/per lab). In addition to these, one Lab room is expected to be organized and reserved (named as “CNS Lab”) in order to meet the requirements for the M.Sc. program in Computer Networks and Security students. Besides, this lab is equipped with tables, chairs white boards, LCD projectors, audio-visual

tools as well as e-Learning resources such as smart boards, ftp server, different network equipments: routers, switches, cables, racks, work stations. Moreover, the program will use the DBU ICT Office labs and network equipment's (i.e. servers, switch, routers, firewalls and so on).

9. QUALITY ASSURANCE AND CURRICULUM REVIEW

Reviewing this curriculum and developing a revised and enhanced version that will match the latest developments in the discipline is the major issue related to quality assurance and have lasting impact. It is essential to engage the broad computing community to review and critique periodically. Moreover, the remaining part of this section lists some of the quality assurance and curriculum review methods:

- Comprehensive examinations and peer assessment of examination papers and teaching methods;
- Periodical workshops (with stakeholders, teachers and graduates);
- Assessments by using survey project works (researches), internships, and link programs;
- Graduates' evaluation of the program;
- Standardization of course offerings through preparation of general course outlines, exam contents, and external audits;
- Annual assessment of the program by the teaching staff;
- Establishing Alumni of Graduates as a mechanism to assess their career development;
- Working closely with the relevant professional associations to assess graduates' performance.

10. PROGRAM COURSE PROFILE

10.1 Course Numbering

The course number comprises 3 alphabets (CNS) and 4 digits (1st, 2nd, 3rd and 4th). The explanation of 3 alphabets and 4 digits illustrated in the tables below:

i) Significance of Letters:

Alphabet	**C**	**N**	**S**
Stands for	Computer	Networks	Security

ii) Significance of Digits:

Digit	1st	2nd	3rd	4th
Significance	M.Sc course	Year of program	Semester of year	Course number of respective semester
Numeric Number	6 ,7	1 or 2	1,2	1,…….n

iii)Illustration:

6	**1**	**1**	**1**
M.Sc	1st Year	1st Semester	1st Course of 1st Semester of 1st year (i.e., Research Methodology in Computing)
6	**1**	**2**	**1**
M.Sc	1st Year	2nd Semester	1st Course of 2nd Semester of First Year (i.e., Wireless Communication and Mobile Computing)
6	**2**	**1**	**1**
M.Sc	2nd Year	1st Semester	1st Course of 1st Semester of 2nd Year (i.e., Computer Network and Security Laboratory)

10.2 Course Sequence

Regular Program						
Year I Semester I						
S.No	**Course Code**	**Course Name**	**Credit Hour**	**ECTS**	**Lecture Hour**	**Lab Hour**
1	CNS 6111	Network Design, Modelling, and Simulation	3	6	32	48
2	CNS 6112	Advanced Computer Networking and Communications	3	6	32	48
3	CNS 6113	Network Programming	3	6	32	48
4	CNS 6114	Cyber law, Security Policies and Ethical Hacking	3	6	32	48
Total Credit Hour and ECTS			12	24		
Year I Semester II						
S.No	**Course Code**	**Course Name**	**Credit Hour**	**ECTS**	**Lecture Hour**	**Lab Hour**
1	CNS 6121	Mobile Computing and Wireless Security	3	6	32	48
2	CNS 6122	Research Methods and Seminar Topics in Computer Networks and Security	3	6	48	0
3	CNS 6123	Advanced Networking and System Administration	3	6	32	48
4	CNS 6124	Biometrics and Cryptography	3	6	32	48
Total Credit Hour and ECTS			12	24		
Year II Semester I						

S.No	Course Code	Course Name	Credit Hour	ECTS	Lecture Hour	Lab Hour
1	CNS 6211	Advanced Computer Network Security	3	6	32	48
2-10	CNS 621(2 , 3, ... or 10)	Elective I	3	6	32/48	48/0
11	CNS 6221	M.Sc. Thesis in Computer Networks and Security	-	-	-	-
Total Credit Hour and ECTS			6	12		
Year II Semester II						
S.No	**Course Code**	**Course Name**	**Credit Hour**	**ECTS**	**Lecture Hour**	**Lab Hour**
1	CNS 6221	M.Sc. Thesis in Computer Networks and Security	6	30	-	-
Total Credit Hour and ECTS			6	30		
Electives						
S.No	**Course Code**	**Course Name**	**Credit Hour**	**ECTS**	**Lecture Hour**	**Lab Hour**
2	CNS 6212	Network Project Management	3	6	32	48
3	CNS 6213	IP Networking and Application	3	6	32	48
4	CNS 6214	Mobile Broadband and Multimedia Networks	3	6	32	48
5	CNS 6215	Social Network Analysis	3	6	32	0
6	CNS 6216	Virtualization and Cloud Computing	3	6	32	48
7	CNS 6217	Web Engineering	3	6	32	48

8	CNS 6118	Distributed Systems	3	6	32	48
Extension Program						
Year I Semester I						
S.No	**Course Code**	**Course Name**	**Credit Hour**	**ECTS**	**Lecture Hour**	**Lab Hour**
1	CNS 6111	Network Design, Modelling, and Simulation	3	6	32	48
2	CNS 6112	Advanced Computer Networking and Communications	3	6	32	48
3	CNS 6113	Network Programming	3	6	32	48
Total Credit Hour and ECTS			9	18		
Year I Semester II						
S.No	**Course Code**	**Course Name**	**Credit Hour**	**ECTS**	**Lecture Hour**	**Lab Hour**
1	CNS 6114	Cyber law, Security Policies and Ethical Hacking	3	6	32	48
2	CNS 6121	Mobile Computing and Wireless Security	3	6	32	48
3	CNS 6122	Research Methods and Seminar Topics in Computer Networks and Security	3	6	48	0
Total Credit Hour and ECTS			9	18		
Year I Summer						
S.No	**Course Code**	**Course Name**	**Credit Hour**	**ECTS**	**Lecture Hour**	**Lab Hour**
1	CNS 6123	Advanced Networking and System Administration	3	6	32	48

2	CNS 6124	Biometrics and Cryptography	3	6	32	48
Total Credit Hour and ECTS			6	12		
Year II Semester I						
S.No	**Course Code**	**Course Name**	**Credit Hour**	**ECTS**	**Lecture Hour**	**Lab Hour**
1	CNS 6211	Advanced Computer Network Security	3	6	32	48
2-10	CNS 621(2 , 3, ... or 10)	Elective I	3	6	32/48	48/0
11	CNS 6221	M.Sc. Thesis in Computer Networks and Security	-	-	-	-
Total Credit Hour and ECTS			6	12		
Year II Summer and Year III						
S.No	**Course Code**	**Course Name**	**Credit Hour**	**ECTS**	**Lecture Hour**	**Lab Hour**
1	CNS 6221	M.Sc. Thesis in Computer Networks and Security	6	30	-	-
Total Credit Hour and ECTS			6	30		

10.3 Course Map for Graduate Profile

10.4 Course Descriptions

==========

Course Title: Network Design, Modelling and Simulation

Course Code: CNS 6111

Credit Hour: 3

Contact Hour per Week: 3 Lecture Hours and 3 Lab Hours

Course Status: Compulsory

Pre-requisite: Undergraduate Computer Networking and Communication course

---

Course Description: This course is designed to give students an understanding of types of computer networks: LANs, VLANs, and WANs; prominent and recent routing algorithms and routing protocols; the network development life cycle; network analysis and design methodology; network design issues: manageability, node placement and sizing; link topology and sizing; routing, forwarding and data dissemination; reliability; data in support of network design; structured enterprise network design; hierarchical tree network design: terminal assignment; concentrator location; mesh topology optimization; traffic flow analysis; analysis of loss and delay in networks; network reliability issues.

Course Objective: Upon successful completion of the course, the students should be able to describe and develop a network model using analysis and simulation; design a new network model to meet requirements for new and existing networks; use quantitative and qualitative techniques to design or upgrade a network; make decisions on the proper network technologies, routing protocols, network topologies, node placement, etc.; troubleshoot and diagnose network problems; identify network issues, risks, bottlenecks, etc.; proficient in using simulation tools such as The ONE, NS2, OPNET, OMNET++, NetLogo management and measurement tools, etc.; learn how to be a good team player by working on a semester-

long project; write a technical report, technical essay describing a subject briefly or elaborately as required; communicate design content, risk assessment, security issues and budgetary considerations to upper-management.

Course Content:

1. Introduction to Network Design, Modelling and Simulation
    1.1. Network Design
    1.1.1. Overview of Network Design
    1.1.2. Design Considerations of Cellular, Radio and Transmission Networks
    1.1.3. Design Models of Data Networks
    1.2. Overview of Modelling and Simulation Tools
    1.2.1. The ONE
    1.2.2. NS2
    1.2.3. OPNET
    1.2.4. OMNET++
    1.2.5. NetLogo
2. The Science of Network Design
    2.1. Network Analysis (Delay, Throughput, Probability Loss, etc.)
    2.2. Network Simulation and NS2
    2.3. Traffic Measurement and Monitoring Tools and Applications
3. The Art of Network Design
    3.1. Making Technology Choices (Ethernet vs. ATM)
    3.2. Ethernet Switching, VLAN and Layer 3 Switching
    3.3. Cabling, Network Components
    3.4. Deployment and Migration
    3.5. Node Placement, Reliability, Redundancy and Routing

3.6. Case Studies of LAN Network Design

4. Mobility Models and Traces

4.1. Mobility Models

4.1.1. Definition and Taxonomy of Mobility Models

4.1.2. Entity Mobility Models

4.1.3. Correlated/Group-based Mobility Models

4.1.4. Human or Sociality-based Mobility Models

4.1.5. Vehicular Mobility Models

4.1.6. Artificial Mobility Models

4.2. Mobility Traces

4.2.1. Overview of Mobility Traces

4.2.2. Trace Collection

4.2.3. Trace Formats

4.2.4. Modelling Contacts from Traces

4.3. Impact of Mobility on Routing Algorithms

4.4. Challenges and Open Issues

5. WAN Network Design

5.1. Centralized and Distributed Network Design

5.2. Star and Tree Topology Networks

5.3. Backbone Networks

5.4. Mesh Networks

6. Network Performance Analysis

6.1. Review of Probability Theory and Graph Theory

6.2. Queuing Theory and Networks of Queues

6.3. Flow and Congestion Control

6.4. Routing-flow Allocation

6.5. Controlled and Random Access techniques in Data Networks

6.6. Performance Analysis of Circuit Switching.

Assessment and Grading System:

- Assignment(s) – 10%
- Case Studies: Seminar(s) – 25%
- Project(s) – 35% (Practical/Laboratory)
- Final Written Examination – 30%
- Grades will be determined according to the University post-graduate rules and regulations.

Textbook and References:

- A-B. Hussein, "Simulation in Computer Network Design and Modeling", Springer, 2012.
- M. Guizani, A. Rayes, B. Khan, and A. Al-Fuqaha, "Network Modeling and Simulation: A Practical Perspective", Wiley Publishing, 2010.
- J. L. Burbank, W. Kasch, and J. Ward, "An Introduction to Network Modeling and Simulation for the Practicing Engineer", IEEE Communications Society, 2011.
- K. Wehrle, M. Günes, and J. Gross "Modeling and Tools for Network Simulation", Springer, 2010.
- S. Karris, "Networks: Design and Management", Orchard Publications, 2006.
- J. McCabe, "Practical Computer Network - Analysis and Design", Morgan Kaufmann Publishers, 1998.
- T. Mann-Rubinson, and K. Terplan, "Network Design: Management and Technical Perspectives", CRC Publisher, 1988.
- R. Breyer, and S. Riley, "Switched, Fast, and Gigabit Ethernet", Macmillan Technical Publishing, Third Edition, 1999.

- P. Oppenheimer, "Top-Down Network Design", Cisco Press, 2001.

==========

Course Title: Advanced Computer Networking and Communications

Course Code: CNS 6112

Credit Hour: 3

Contact Hour per Week: 2 Lecture Hours and 3 Lab Hours

Course Status: Compulsory

Pre-requisite: A basic Undergraduate or equivalent course in Computer Networks/ing and Communications

---

Course Description: This course introduces the students to the world of internetworking. There are in-depth discussions about the application, transport, network and link layers and associated protocols, issues in multimedia networking, overlay networks and peer-to-peer networks, and how quality of service is delivered in an IP network. The course wraps up with a case study, which the students work in groups to discuss, design and present their solutions. Moreover, the course aims to get a strong understanding of fundamental concepts and to get a flavour of more recent research and recent developments in the area.

Course Objective: Up on successful completion of the course, the students will be able to identify the component of an internetworking; describe the functionality of internetworking components; articulate how the internet protocol is implemented in a network; describe how routers and routing protocols operate; describe multimedia networking applications and QoS; describe how real-time interactive application protocols such as RTP, RTCP, etc. works.

Course Content:

1. Introduction to Computer Networks and Communications

    1.1. Overview and History of the Internet

    1.2. Network Edge and Core

1.2.1. End Systems, Access Networks and Links

1.2.2. Circuit Switching, Packet Switching, Network Structures and Architectures

1.2.3. Delay, Loss and Throughput in Packet-Switched Networks

1.3. Overview of OSI and TCP/IP Layer Protocols

2. Application Layer

2.1. Principles of Network Applications

2.2. Web and HTTP

2.2.1. Web server redirection and caching

2.3. FTP, SMTP, POP3, IMAP, DNS

2.4. Socket Programming with TCP/UDP

2.5. Applications Level Issues and Problem: Applications Need their Own Protocols

2.5.1. Name Service and Traditional Applications

2.5.2. Multimedia Applications

2.5.3. Overlay Networks and P2P Networks

2.5.4. Web Server Systems

3. Transport Layer

3.1. Transport Layer Services

3.2. Multiplexing and Demultiplexing

3.3. User Datagram Protocol (UDP) and Transmission Control Protocol (TCP)

3.3.1. Segment Structure

3.3.2. Reliable Data Transfer

3.3.3. Flow Control

3.3.4. Connection Management

3.4. Scheduling, Congestion Control and Avoidance

3.5. TCP Flavors (Prominent Protocols): RENO, NEWRENO, TAHOE, VEGAS, etc.

4. Network Layer

4.1. Introduction to Network Layer

4.2. Virtual Circuit and Datagram Networks

4.3. What's Inside a Router?

4.4. Internet Protocol (IP)

4.4.1. Datagram Format

4.4.2. IPv4 and IPv6 Addressing

4.4.3. Internet Control Message Protocol (ICMP)

4.5. Routing algorithms (Link State, Distance Vector, Hierarchical Routing, etc.)

4.6. Routing in the Internet (RIP, OSPF, BGP, etc.)

4.7. Unicast, Broadcast and Multicast Routing

5. Link Layer

5.1. Introduction, Services, Error Detection and Correction

5.2. Multiple Access Protocols and Link Layer Addressing

5.3. Ethernet and Link Layer Switches

5.4. Point-to-Point Protocol (PPP) and Link Virtualization: ATM, MPLS

6. Multimedia Networking

6.1. Multimedia Networking Applications

6.2. Streaming Stored Audio and Video

6.3. Making the Best Out of Best Effort Service

6.4. Protocols for Real-time Interactive Applications (RTP, RTCP, SIP, etc.)

6.5. VoIP Fundamentals

6.5.1. How Packetized Voice Works and Voice Quality

6.5.2. SIP, Soft Switches and Gateways

6.5.3. PBX Replacement

6.6. Providing Multiple Classes of Service

6.7. Providing QoS Guarantees

7. Next Generation Networking

7.1. Motivation and Challenges

7.2. Self-organizing Networks: (Ad-hoc, Sensors and Mesh Networks; Applications; Communication Support: Information Dissemination, Medium Access Mechanisms; Self-organizing Concepts in Infrastructure-based Networks.)

7.3. New Trends in Computer Networking (PAN, Pervasive Computing, Grid computing, Cloud Computing, etc.)

Assessment and Grading System:

- Case Study (Group Task) – 25%
- Individual Assignment(s) – 15%
- Project (Practical/Lab) – 20%
- Final Written Examination – 40%
- Grades will be determined according to the University post-graduate rules and regulations.

Textbook and References:

- J. F. Kurose, and K. W. Ross, "Computer Networking: A Top-Down Approach", Addison-Wesley, Fourth Edition, 2008.
- A. S. Tannenbaum, "Computer Networks", Prentice Hall, Fourth Edition, 2003.
- B. A. Forouzan, "Data Communications and Networking", McGraw Hill, Third Edition, 2003.
- W. Stallings, "Data and Computer Communications", Prentice Hall, Seventh Edition, 2004.
- W. Stallings, "High-Speed Networks and Internets: Performance and Quality of Service", Prentice Hall, Second Edition, 2002.

==========

Course Title: Network Programming

Course Code: CNS 6113

Credit Hour: 3

Contact Hour per Week: 2 Lecture Hours and 3 Lab Hours

Course Status: Compulsory

Pre-Requisite: A basic undergraduate or equivalent course in Computer Networks/ing and Communications; basic undergraduate or equivalent course in Object-Oriented Programming language(s)

Course Description

This is a course focusing on the programming aspects of computer networks. Covers application layer protocol and how applications use the transport layer; principles and practice of network programming; the client-server model; concurrent processing; introduction to sockets and related functions client and server software design with examples; principles, issues and challenges in e-mail and web application protocols; security protocols; and network life system concepts; overall it cover the network programming in both wired networks and wireless networks. The goal of this course is to understand the current trends of communication protocols, socket programming, inter-process communication, and to understand how network research is done.

Course Objectives: On completion of the course, students should be able to

- Explain a variety of important principles in networking, with a strong focus on the Internet.
- Send and receive data between processes in the UNIX and Internet domains.
- Write programs using the socket interface.
- Explain TCP/IP client-server model of interaction and write networking applications using the client/server technology, and write secure software.

What Students Should Know Prior to this Course?

1. Basic networking constructs, including routers, switches, and hosts
2. Some programming experience, as well as experience with tools such as WireShark and NS2

3. Routing algorithms in the Internet; link-state routing and distance-vector routing; broadcast and multicast routing algorithms.
4. Multi-Protocol Label Switching; requirements, introduction to labels, signaling protocols.
5. Traffic Engineering; Requirements, deployment, prioritizing traffic.
6. Link layer technologies; mulitple access protocols; local area networks; Ethernet and the CSMA/CD protocol.
7. Wireless and mobile networks; introduction, 802.11, mobility management, mobile IP.

Course Contents:

1. Basics on Network Programming:
   - 1.1 Network programming
   - 1.2 Socket programming
   - 1.3 Client/Server applications
   - 1.4 Peer to peer network programming
   - 1.5 Protocols and RFCs
2. Upper layers
   - 2.1 Introduction to Processes
     - 2.1.1 Multitasking, processes, multithreading, threads;
     - 2.1.2 Inter-thread & inter-process communications, network communications
   - 2.2 Client-Server Network Programming
     - 2.2.1 Unicast, multicast, broadcast;
     - 2.2.2 Sockets, RMI, applet-servlet communications;
     - 2.2.3 Ping, e-mail and file transfer; ICMP, SMTP, POP3, IMAP, FTP protocols;
     - 2.2.4 Web traffic: HTTP, HTTPS protocols;
   - 2.3 Client-side Network Programming
     - 2.3.1 Static documents; HTML, XHTML, XML languages
     - 2.3.2 Dynamic documents; Applets, Java Script
   - 2.4 Server-side Network Programming
     - 2.4.1 Database access;
     - 2.4.2 Servlets, JSP, ASP, PHP technologies

2.5 Advanced Network Programming Issues

2.5.1 Firewalls, proxy servers, caches;

2.5.2 Elements of CORBA, J2EE, and .NET technologies

3. Lower layers

3.1 Low Level Issues

3.1.1 IP overview, Data rates, MPLS, hardware vs. software

3.1.2 Router architecture, network device drivers, buffer management.

3.2 Transport Layer

3.2.1 Review of sockets, TCP protocol description

3.2.2 Implementation of TCP, other transport layer protocols (e.g. RTP, RTCP, RTSP)

3.3 Network Layer

3.3.1 Internet routing protocols (RIP, OSPF, BGP).

3.3.2 Router configuration and network administration. IP support for multicast.

3.4 Signalling in Packet Networks

3.4.1 The control plane, why is signalling needed? End-to-end signalling (e.g. SIP)

3.4.2 QoS and resource reservation, signalling in IP networks, MPLS signalling, signalling gateways.

3.5 Advanced Packet Forwarding

3.5.1 Deep packet probes, policy-based routing,

3.5.2 Hardware acceleration, network processors.

Textbooks and References:

- **James Kurose and Keith Ross**. Computer Networking: A Top-Down Approach Featuring the Internet. Addison Wesley: 0321497708

Assessment and Grading System:

- Case Study (Group Task) – 25%
- Individual Assignment(s) – 15%
- Project (Practical/Lab) – 20%
- Final Written Examination – 40%

- Grades will be determined according to the University post-graduate rules and regulations.

==========

Course Title: Cyber law, Security Policies and Ethical Hacking

Course Code: CNS 6114

Credit Hour: 3

Contact Hour per Week: 2 Lecture Hours and 3 Lab Hours

Course Status: Compulsory

Pre-requisite: Data Communication and Networking at first degree level

---

Course Description:

Course Objective: On successful completion of the module students will be able to:

- Describe elements of computer security and privacy
- Investigate the degree of vulnerability of a computing environment to security threats
- Identify computer security threats in a computing environment and prepare the necessary counter measures for protection
- Deploy security techniques like encryption, cryptography, access control, firewall, etc.
- Develop computer security and privacy policies, procedures and guidelines for a computing environment.
- Develop team work spirit and communication skills

Course Content:

1. Fundamentals of computer security and privacy:
   1.1 Overview,
   1.2 history,
   1.3 vulnerabilities,
   1.4 countermeasures,

1.5 physical security

2. Computer security threats:

2.1 Viruses,

2.2 Worms,

2.3 Trojan horses,

2.4 Crackers,

2.5 Spy-wares …

3. Security Techniques:

3.1 Encryption,

3.2 cryptography,

3.3 access control,

3.4 firewall, …

4. Network security concepts and mechanisms:

4.1 Software security mechanisms,

4.2 programming techniques

5. Secure system planning and administration:

5.1 Analysing risks,

5.2 planning policies and procedures

6. Computer forensics: Legal, ethical and policy issues

7. Ethical Hacking: Ethical Hacking: How to scan, test, hack and secure their own systems, current essential security systems, how perimeter defenses work and then be lead into scanning and attacking their own networks, no real network is harmed, how intruders escalate privileges and what steps can be taken to secure a system, learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation.

Assessment and Grading System:

- Assignment(s) – 15%
- Seminar(s) – 25%
- Project(s) – 30% (Practical/Laboratory)
- Final Written Examination – 30%
- Grades will be determined according to the University post-graduate rules and regulations.

Textbook:

- Rajat Khare, Network Security and Ethical Hacking, Luniver Press, Nov 1, 2006.

References:

- **Jean-Loup Richet 2015. Cybersecurity Policies and Strategies for Cyberwarfare Prevention (Text Book)**
- Pauline C. Reich 2012. Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization
- Reveron, Derek S. 2012. Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Georgetown University Press.
- Text: Hacking Exposed 7: Network Security Secrets and Solutions, Stuart McClure, Joel Scambray, George Kurtz, © 2012, McGraw Hill, ISBN 978-0-07-178028-5. Software: VirtualBox or VMWare Player, Kali Linux.
- D. Russell and G.T. Gangemi, Computer Security Basics, OReilly& Associates, 1991.
- BPB Publications, Security Complete, New Delhi BPB Publications, 1999.
- C. Easttom, Computer Security Fundamentals, Prentice Hall, May 2005.
- W. Stallings, Network Security Essentials, 2nd edition, Prentice Hall, 2003.
- L. Fennelly, Effective Physical Security, Butterworth-heinemann, 2003.
- T. R. Peltier, Information Security Policies, Procedures, and Standards: Guidelines For Effective Information Security Management, Auerbach Publications, 2001.
- E. Michael, Physical Security for IT, DigitalPr, 2004.

- M. Bishop, Computer Security: Art and Science, Addison-Wesley, 2002.
- S. Bosworth and M. E. Kabay, Computer Security Handbook, 4th edition, Willey, 2002.
- M. R. Overly, E-Policy: How to Develop Computer, E-Policy, and Internet Guidelines to Protect Your Company and its Assets, AMACOM, 1998.
- S. A. Thomas, SSL and TLS Essentials: Securing the Web, Wiley, 2000.
- R. J. Anderson, Security Engineer;ing, Ross Anderson, John Wiley & Sons Inc., 2008.

Software Requirement: SNMP, Nmap, Nessus, Nikto, MetaSploit, NetStumbler, C/C++/Java, other cryptographic application tools

==========

Course Title: Mobile Computing and Wireless Security

Course Code: CNS 6121

Credit Hour: 3

Contact Hour per Week: 2 Lecture Hours and 3 Lab Hours

Course Status: Compulsory

Pre-requisite: Advanced Computer Networking and Communication (CNS 6112)

Course Description: This course introduces advanced concepts in wireless communication, mobile computing and wireless security. Required laboratory tools include mobile programming languages (such as Objective C, Java Script, Java, etc.)

Course Objective: At the end of the course, students will be able to know the advanced concepts of wireless communication and mobile computing; explore the architecture of wireless systems; design wireless communication protocols; know the principles of Telecommunication systems and pervasive computing; identify the research topics and conduct researches in the wireless communication and computing areas; develop mobile applications using current mobile programming tools.

Course Content:

1. Wireless and Mobile Technology
    1.1. Overview of Wireless and Mobile Technologies
    1.2. Radio Technologies and Platforms
    1.3. Wireless Communication Algorithms
    1.3.1. Multiple Input Multiple Output (MIMO)
    1.3.2. Cooperative Communications
    1.3.3. Dynamic Spectrum Access (DSA)
    1.3.4. Network Coding
2. Wireless Communication and Mobile Computing Environments
    2.1. Applications, Architectures and Protocol Design Issues
    2.2. Mobility, Disconnection and Scale
    2.3. Data Management
    2.4. Limitations and Research Challenges
3. Telecommunication Systems
    3.1. Fundamentals of Telecom Technologies
    3.1.1. Introductory Topics in Telecom
    3.1.2. Network Topologies
    3.1.3. Quality of Service (QoS) and Standardization
    3.1.4. Models of Telecom Channels
    3.2. Telecom Standards and Advanced Technologies
    3.2.1. Telecom Standards, PSTN and ISDN
    3.2.2. Intelligent Telecom Technologies
    3.2.3. Analysis of Telecom Management Technologies
    3.2.4. Application of Big Data Technologies to Telecom Architecture

3.2.5. Security in Telecom Technologies

4. Emerging Wireless and Mobile Networks

4.1. WLANs and Satellite-based Networks

4.2. Mobile Phone Sensing and Mobile Crowd sensing

4.3. Socially-aware Networks

4.4. Mobile Cloud Computing

4.5. Bio-Inspired Networking

4.6 Cellular Network: 2G, 3G, 4G, LTE and Beyond

5. Security in Wireless and Mobile Networks

5.1 IEEE 802.11 Security: WEP and WPA

5.2 IEEE 802.11 Security: WPA2 and 802.11i

Assessment and Grading System:

- Mobile Application Development Project Report (20%) and Presentation (10%)
- Assignment(s) – 20%
- Final Written Examination – 50%
- Grades will be determined according to the University post-graduate rules and regulations.

Textbook and References:

- M. Guizani, "Wireless Communications and Mobile Computing", Wiley Online Library, Issues: 2006-2015, ISSN: 1530-8677.
- A. Umar, "Mobile Computing and Wireless Communications: Applications, Networks, Platforms, Architectures, and Security", NGE Solutions, 2004.
- Y-K. R. Kwok, and V. K .N. Lau, "Wireless Internet and Mobile Computing: Interoperability and Performance", IEEE Press, 2007.

- "Mobile Computing Principles: Designing and Developing Mobile Applications", Cambridge University Press, 2004.
- A. Boukerche, "Handbook of Algorithms for Wireless Networking and Mobile Computing", CRC Press, 2005.
- M. Schwartz, "Mobile Wireless Communications", Cambridge University Press, 2005.
- I. Stojmenovic, "Handbook of Wireless Networks and Mobile Computing", Wiley Publishing, 2003.
- Recent Research Articles from Top Journals such as IEEE Communication Surveys and Tutorials, Proceedings of the IEEE, International Journal of Wireless Communication and Mobile Computing (WCMC), IEEE Transactions on Mobile Computing, etc.

==========

Course Title: Research Methods and Seminar Topics in Computer Networks and Security

Course Code: CNS 6122

Credit Hour: 3

Contact Hour per Week: 3 Lecture Hours

Course Status: Compulsory

Pre-requisite: None

Course Description: A study of current methods and techniques in computing research, including writing research proposals, conducting research, technical writing and presentations. The major topics includes research in computing, proposal preparation, using resources to conduct research, writing research papers and making presentations, ethical issues. The instructional methods and techniques include traditional lectures with some assignments, student presentations and group problem solving.

Course Objective: Upon completion of the course, the students will be able to describe computing research methods; develop effective research proposal; conduct research

effectively in computer-related fields; use resources to conduct research; organize and prepare technical papers, thesis and presentations; work and cooperate effectively with other research workers on a computing research; aware of the research ethics and other related issues.

Course Content:

Module 1: Research Methods in Computing

1. Introduction and Overview of Research

1.1. What is Research and not Research?

1.2. Scientific Research

1.3. Objectives, Motivations and Significance of Research

1.4. Requirements and Characteristics of Research

1.5. Types and Approaches of Research24

1.6. Research Methods and Problem Solving

1.7. Effective Report Writing Principles and Criteria for Good Research

1.8. Evaluating and Reviewing Research Results

1.9. What is Research in Computing?

2. Processes in Conducting Research

2.1. Overview of Current State of the Art Areas and Techniques in Computing

2.2. Actors, Roles and Relationship

2.2.1. The Student

2.2.2. The Supervisor

2.2.3. The Examiner/Evaluator

2.3. The Process

2.3.1. Developing Research Proposal

2.3.2. Developing Problem Description

2.3.3. Following the Objectives

2.3.4. Presenting and Analyzing the Data

2.3.5. Drawing Conclusion and Identifying Future Work

2.3.6. Presenting and Defending Orally

2.3.7. Preparing Final Research Documentation (Thesis)

2.4. Proposal Preparation

2.4.1. Choosing a Subject Area

2.4.2. Choosing a Problem within the Subject Area

2.4.3. Quality Assurance of Initial Ideas

2.4.4. Write Research Proposal

2.4.5. Sample and More Acceptable Research Proposal Structure

2.4.6. Research Proposal Check-list

2.5. Literature Reviews

2.5.1. Importance and Roles of Literature Review

2.5.2. Skills and Keys to Effective Literature Review

2.5.3. Literature Sources (Journals, Conference Proceedings, Books, Reports, Thesis, etc.)

2.5.4. Literature Review Writing

2.6. Assessment Criteria

3. Resources to Conduct Research

3.1. Digital Libraries (IEEE, ACM, Science Direct, Springer, etc.)

3.2. Documentation Tools (Ex: Latex) and Language Skill

3.3. Team Work

3.4. Datasets

3.5. Simulation, Experimental or Visualization Tools

4. Writing Research Papers and Making Presentations

4.1. Structure of Good Quality Papers, Citations and References

4.2. Making Excellent Presentation

4.3. How to Write Good Quality Thesis and Papers (Journal and Conferences)

5. Research Ethics

5.1. Ethical Issues in Research

5.2. Plagiarism, Falsification, Fabrication

5.3. Academic Honesty Related Issues – Ex. Misleading Authorship

5.4. Other Ethical Issues in Computing

6. Data Collection and Analysis (Presentation of Research Results such as Data Figures)

Textbook and References:

General textbooks are not suitable for this course, but there are a growing number of research papers research published in quality journals such as IEEE and ACM that explore models, frameworks as well as contents in Computing Research Methods to help students to become an expert in computing.

Assessment and Grading System (50%):

- Critical Assessment of Relevant Articles (10%)
- Proposal Writing – Using Latex (30%)
- Review Paper (Survey Paper) – Using IEEE/ACM Latex Standard (10%)
- Grades will be determined according to the University post-graduate rules and regulations.

==========

Module 2: Seminar Topics in Computer Networks and Security

Pre-requisite: None

Module Description: The motivation for this course lies in the interest in providing a broad viewpoint on Computer Networks and Communication by surveying recent developments, major results, and hot topics in today's leading-edge research in Computer Networks. The

main focus of this course is on topics of current interest in Computer Networking and Communications. The course will cover topics such as pervasive, mobile and social computing, Internet of Things, cloud computing, Big data, state of the art networking paradigms such as Vehicular Social Networks, etc.

Module Objective: On successful completion of the course, students will be able to identify current research topics in Computer Networks and Communications and critically discuss research topics in Computer Networks and Communications.

Module Content:

1. Analyze Latest Topics in Computer Networks and Security (such as ad-hoc networks, socially-aware networks, wireless sensor networks (i.e. mobile crowdsensing), vehicular social networks, cloud computing, big data, Internet of Things, etc.)
2. Identify Tools and Techniques for Use in Recent Research Topics in Computer Networks and Security

---

Assessment and Grading System: (50%)

- Assignment on understanding and criticising conference paper or journal Article 1 – 25%
- Assignment on understanding and criticising conference paper or journal Article 2 – 25%
- Grades will be determined according to the University post-graduate rules and regulations.

Textbook and References:

- There is no single text book for the module. It is, thus, recommended that the students read appropriate articles and chapters from the given reading materials (high-quality publications) in addition to their own reading materials.
- Check Appendix for details about research articles.

==========

Course Title: Advanced Networking and System Administration

Course Code: CNS 6123

Credit Hour: 3

Contact Hour per Week: 2 Lecture Hours and 3 Lab Hours

Course Status: Compulsory

Pre-requisite: A basic Undergraduate or equivalent course in Operating Systems and Advanced Computer Networking and Communication (CNS 6112)

Course Description: This course instructs students how to administer and manage a modern network by properly planning and implementing various functions of a Network OS. Key components include how to plan server deployment, server monitoring and maintenance, application and data provisioning, and providing business continuity and availability by proper use of security configuration and backup policies. The course material is designed to provide extensive hands-on experience. Topics include: installation and configuration; the boot process; user and group administration; filesystem administration, including quotas, FACLs, RAID and LVM; task automation; client networking; software management; log files; troubleshooting; Emphasis is also given on storage, file management system, connectivity, security, troubleshooting, archiving, backing up, directory services, remote administration, access control lists.

Course Objective: At the end of the course, students will be able to demonstrate an understanding of the principles, practices and goals of systems administration; perform installation of NOSs and configure the server environment; perform user accounts management and implement security groups; demonstrate an understanding of the configuration and management of data storage; perform network services installation and management; use server and network monitoring software tools; describe the elements of an effective troubleshooting methodology and use a variety of software and hardware tools to diagnose problems; managing user and group account information, software packages,

system services, basic network services (ftp, telnet, ssh etc); troubleshoot and respond to boot problems.

Course Content:

1. Introduction to Systems Administration
    1.1. Goals, Philosophy, Challenges and Common Practices
    1.2. Overview of the NOSs
    1.3. Unix-like Systems Vs Windows Systems
    1.4. Linux Distributions and UIs
    1.5. Linux Operations Review
    1.5.1. Filesystem Hierarchy and Standard
    1.5.1.1. Single-rooted hierarchy, Seamless and Extensible Filesystems
    1.5.1.2. Mounting Additional Filesystems
    1.5.1.3. Filesystem Object Oriented Design and Filesystem Standard
    1.5.1.4. Unix File and Directory Permissions
    1.5.2. Essential Shell Commands
    1.5.2.1. Basic File Manipulation Commands and Directory Navigation Commands
    1.5.2.2. Advanced File Manipulation Commands (Init, Processes, and Threads)
    1.5.3. Advanced Shell Features
2. Account and Security Administration, and Access Control (DAC, RBAC)
    2.1. Account and security Administration
    2.1.1. User and Group Concepts, and User Private Group Scheme
    2.1.2. User Administration, Modifying Accounts and Group Administration
    2.1.3. Password Aging and Default User Files
    2.2. Managing files and folder permission
    2.2.1. Managing File Ownership

2.2.2. Controlling Access to files

2.2.3. Managing Disk Quotas

3. File Systems and Management of Data Storages

3.1. File system Administration

3.1.1. Partitioning Disks with fdisk and parted

3.1.2. Creating, Mounting and Maintaining File systems

3.1.3. Swap

3.1.4. Determining Disk Usage With df and du

3.1.5. Configuring Disk Quotas

3.2. Logical Volume Management (LVM) and RAID

3.2.1. Implementing LVM, Creating Logical Volumes (LVs), Manipulating VGs & LVs

3.2.2. Advanced LVM Concepts (i.e. system-config-lvm)

3.2.3. RAID Concepts (Creating and Managing a RAID-5 Array)

4. Software Package Management

4.1. Managing Software

4.2. RPM Features, Architecture and Package Files

4.3. Working With RPMs (Querying, Verifying and Updating)

4.4. Managing Software Dependencies

5. Basic Networking

5.1. Network Configuration (IP Networking and Linux Network Configuration)

5.2. Network Services

5.2.1. RPC-Based Services and INET Super Server

5.2.2. Network Time Services and Sharing Desktops with VNC

5.2.3. Dynamic Host Control Protocol (DHCP)

5.3. Remote Administration with SSH and SCP

5.3.1. Configuration, Telnet Replacement, Secure Copy and Rsync

5.3.2. RSA and DSA Authentication (Password-less Logins)

5.3.3. Remote Command Execution and Port Forwarding

6. Installation of Application Server and Management

6.1. DHCP, DNS, Telnet server; compare with other NOS setup of corresponding network services

6.2. Open SSH: Secure Network Communication

6.3. FTP and Setting-up Mail Servers and Client

6.4. Network Information Service (NIS) and Sharing File systems (NFS)

6.5. SAMBA: Linux and Windows File and Printer Sharing

6.6. DNS/BIND: Tracking Domain Names and Address

6.7. Setting up a Firewall and a Webserver

7. Managing Network Services

7.1. Maintenance Troubleshooting: Common System and Network Problems

7.2. Developing General Strategies

7.3. Resolve Boot Problems, Backup and Restore Data and System Volume

7.4. Using Event Viewer and Troubleshoot Connectivity

8. Systems Security

8.1. Overview, Application Security and Login Security

8.2. Boot Loader Security (LILO and GRUB)

8.3. TCP Wrappers Configuration

8.4. Iptables Firewalling: Preliminaries

8.5. Iptables Scenarios

8.5.1. Packet Filtering

8.5.2. Port-Forwarding/Redirection and NAT/IP Masquerading

8.6. Packet-Processing Model

8.7. Intrusion Detection and Mandatory Access Control (MAC) with LIDS

9. Organizational structure

9.1 Organizational Structure

9.2 Guide for Technical Managers

9.3 Guide for nontechnical managers

9.4 Hiring System administrators

9.5 Firing System Administrators

Assessment and Grading System:

- Assignment(s) – 15%
- Seminar(s) – 25%
- Project(s) – 30% (Practical/Laboratory)
- Final Written Examination – 30%
- Grades will be determined according to the University post-graduate rules and regulations.

Textbook and References:

- The Practice of System and Network Administration, 2nd edition by Limoncelli A. Thomas, Hogan J. Christina, Chalup R. Strata (2007) (Text Book)
- Mark Burgess, "Principles of Network and System Administration", Second Edition, Wiley and Sons, ISBN 0470868074, 2004.
- Michael Palmer, "Hands-On Microsoft Windows Server 2003", Course Technology, Cengage Learning, ISBN-13: 9781423902348, 2003.
- Thomas A. Limoncelli, Christina J. Hogan, and Strata R. Chalup, "The Practice of System and Network Administration", Second Edition, Addison Wesley, ISBN: 0.321-49266.8, 2007.

==========

Course Title: Biometrics and Cryptography

Course Code: CNS 6124

Credit Hour: 3

Contact Hour per Week: 2 Lecture Hours and 3 Lab Hours

Course Status: Compulsory

Pre-requisite: A basic undergraduate or equivalent course in Computer Networks/ing and Communications and basic knowledge of information security

---

Course Description: The course covers the basic concepts of pattern recognition and biometrics, current major biometric technologies, and then analyzes specific case studies from technical, privacy, and social impact viewpoints. The course also offers a critical study of the cryptographic protocols used in many security applications including authentication, authorization, access control and digital commerce. Both commercial practices and federal government policies for classified information will be explored.

Course Objectives:

The purpose of the course is to examine biometric and cryptographic technologies from the viewpoint of systems security administrator, integrator, purchaser, and evaluator. Both biometric and cryptographic systems are very important to the security of systems. So students must understand the fundamentals of these two technologies and be able to competently test and evaluate tools using these technologies, write technical reports on them, do research on them, and understand the process and need of establishing biometrics and cryptographic standards and using them.

Course Requirements

- Regular class attendance. Active class and laboratory participation in all discussions; this means spending some quality time reading and preparing for class and lab meetings and discussions
- One mid-term and a comprehensive final examination will be given. Examination make up will be on Reading Day.
- Individual extra credit assignments for the purpose of propping up a bad grade will not be given.

- Students will be required to sign a contract stating that they will not use knowledge acquired in this course for illegal or unethical purposes. This contract may be released to appropriate authorities should the student be suspected of illegal or unethical computer usage.
- Taking notes is encouraged.
- Each student will write an abstract and make a technical presentation. Students have the freedom to select topics of interest on the condition that they are related to biometrics or cryptography. You can present your past work, technical reports from industry or selected papers from conferences and journals. You can search the ACM digital library or IEEE Explorer on UTC on-line library. You need to provide a page of abstract and a PowerPoint version of slides for the presentation.
- All the presentations must address the following questions.
- How is the problem to be solved?
- What is the author's solution(s)?
- How are the solutions to be evaluated?
- What are the strengths, compared with prior works?
- Do you think there is any weakness in the proposed work?
- Students are encouraged to present at the ACM IEEE Conferences. Please go to the following link for more details of the ACM conference: http://www.utm.edu/staff/jclark/midsouth/

Course Content:

1. Cryptography

1.1 Introduction to Cryptography Traditional Symmetric-key ciphers

1.2 Introduction to Modern Symmetric-Key Ciphers

1.3 Data Encryption Standard (DES)

1.4 Advanced Encryption Standard (AES)

1.5 Encipherment Using Modern Symmetric-Key Ciphers

1.6 Asymmetric-Key Cryptography Message Integrity and Message Authentication

1.7 Cryptography and Hash Functions

1.8 Digital Signature

1.9 Entity Authentication Midterm

1.10 Key Management

1.11 Security Protocols

2. Biometrics

2.1 Introduction to Biometric Technologies

2.2 Fingerprint Biometrics

2.3 Face Biometrics and PCA, LDA

2.4 Voice Biometrics and HMM model

2.5 Handwriting Analysis

2.6 Iris Biometrics and DNA

Software Requirements for Biometrics

1. Microsoft Office (MS Word, MS Excel, MS PowerPoint)

2. IE, Firefox, Google Chrome, MatLab

Assessment and Grading System:

Grades will be based on the following:

30% Laboratory projects

20% A Graduate Project that delivers abstract, 10-page report and a ppt presentation.

50% Final comprehensive examination – covering text material and content of class discussions

Graduate Project

To be able to earn graduate credit for this course, a student must undertake and successfully finish a semester-long graduate project. Students select the topics of interest on the condition that they have research components and are related to biometrics and cryptography, for example, fingerprint biometric, face biometric, voice biometric, handwriting biometric, encryption, key management, or authentication. Projects, based on students' interests, will be approved instructors in the ISA committee consisting of all ISA teaching faculty. Students can search the ACM digital library or IEEE Explorer in UTC on-line library. Students need provide a page of abstract, a project report, and a PowerPoint version of slides for the presentation. All the presentations must address the following questions.

- What is the problem to be addressed?
- What is the authors' solution(s)?
- How did the authors evaluate their scheme(s)?
- What is the strength compared with prior works?

- Do you think there is any weakness in the proposed work?

Textbook and References:

Primary Texts

- Behrouz A. Forouzan. *Cryptography and Network Security*, McGraw Hill, 2008, ISBN: 0-07-287022-2
- Samir Nanavati, Michael Thieme, Raj Nanavati. *Biometrics: Identity Verification in a Network World*, Wiley, 2002, ISBN: 0-471-09945-7
- Paul Reid. *Biometrics for Network Security*, Prentice Hall, 2004, ISBN 0-13-101549-4
- Robert Newman (2013). Security and Access Control Using Biometric Technologies. Course Technology/Cengage Learning, ISBN-10: 1435441052, ISBN-13: 978-1435441057.

References

- David Hook. *Beginning Cryptography with Java*, Wiley, 2005, ISBN: 0-7645-9633-0
- Bill Ball. *Linux in 24 hours*, Sams. Free version of this book is available online. http://www.linux-books.us/linux_general_0009.php
- Paul Reid. *Biometrics for Network Security*. Prentice Hall, 2004, ISBN: 0-13-101549-4
- John Chirillo, Scott Blaul. *Implementing Biometric Security*, Wiley, ISBN 0-7645-2502-6
- Bruce Schneier, *Applied Cryptography*, Wiley, second edition, ISBN: 0-471-11709-9

==========

Course Title: Advanced Computer Network Security

Course Code: CNS 6211

Credit Hour: 3

Contact Hour per Week: 2 Lecture Hours and 3 Lab Hours

Course Status: Compulsory

Pre-Requisite: CNS 6114 Cyber law, Security Policies and Ethical Hacking

---

Course Description: This course takes the students to the in-depth look of computer network security. There are in-depth discussions about the email security, intrusion detection and prevention systems, denial of service detection and prevention, problems of eavesdropping; security in wireless networks; use of router based firewalls as a method to protect Intra-nets, proxy based firewall systems for network security. The course wraps up with a case study, which the students work in groups to discuss, design and present their network security solutions. Moreover, the course aims to students' strong understanding of fundamental concepts and to get a flavour of more recent research and recent developments in computer network security.

Course Objective: Up on successful completion of the course, the students will be able to:

- Have knowledge of the threats faced by computer operating systems, applications and networks that originate from network based attacks, intrusion and misuse.
- Have knowledge of the types of countermeasures that can be put in place in computer systems, networks, and network infrastructures to identify, reduce or prevent problems caused by network attacks or misuse.
- Be capable of making informed choices of the appropriate countermeasures that should be put in place to protect systems from network attacks or misuse and to maintain network security.
- Have a deeper and integrated understanding of selected key topics at the forefront of this field, including recent developments and outstanding issues.
- Have the skills to keep abreast of future developments in network security.
- Be able to undertake practical work that explores techniques covered in this module and comment on their findings.
- Be able to undertake an investigation into areas covered by this module and report on their findings.

Course Content:

1. Email security.

   1.1 Spam: why? ; spam 'click through' rates; targeted spam; spam filtering systems.

   1.2 Phishing attacks; blocking fake sites; browser based defences.

1.3 Email based malware and defences against this.

2. Intrusion detection and prevention systems; honey pots.
3. Denial of Service; Distributed denial of service; Bot-nets; Methods to detect complex denial of service attacks and defences against them.
4. Problems of eavesdropping; security in wireless networks.
5. Use of router based firewalls as a method to protect Intra-nets:

   5.1 De-Militarized Zones,

   5.2 Bastion Hosts;

   5.3 Internal Intra-net firewalls;

   5.4 Personal firewalls.

6. Proxy based firewall systems:

   6.1 Control over which parts of the Internet are accessible;

   6.2 Black-lists and white-lists;

   6.3 Key-word based filtering;

   6.4 Time based controls.

Textbooks and References:

- Christos Douligeris & Dimitrios Nikolaou Serpanos, Network security: current status and future directions, John Wiley and Sons (2007).
- Joseph Migga Kizza, Computer network security, Springer (2005).
- Thomas M. Thomas, Network security first-step, Ed.2, Cisco Press (2004).

Assessment and Grading System:

- Case Study (Group Task) – 25%
- Individual Assignment(s) – 15%
- Project (Practical/Lab) – 20%
- Final Written Examination – 40%

- Grades will be determined according to the University post-graduate rules and regulations.

==========

Course Title: Network Project Management

Course Code: CNS 6212

Credit Hour: 3

Contact Hour per Week: 2 Lecture Hours and 3 Lab Hours

Course Status: Elective

Pre-Requisite: Advanced Computer Networking and Communication (CNS 6112)

Course Description:

Course Objective: On successful completion of the module students will be able to:

- Explain the basic concepts of network design and management.
- Examine the basics of network design.
- Explain the basic concepts of network security.
- Describe the basics of enterprise networks.
- Explain the basic concepts of network management.
- Describe the telecommunications management network.
- Examine SNMP and CMIP.
- Describe the management of broadband networks.
- Describe the tools and applications used for network management.

Course Content:

1. Basics of Network Design and Management: Overview of Network Design and Management, Network Management Model.
2. Network Design: Traffic Engineering on a Telephone Network, Design Considerations of Cellular, Radio, and Transmission Networks, Design Models of Data Networks.

3. Network Security: Basic Concepts of Network Security Authentication Techniques, Access Control, Network Access Control, Network Security Protocols.
4. Enterprise Network: Introduction to Enterprise Networks, Technologies to Connect with Other Networks.
5. Network Management: The Operation, Administration, Maintenance, and Provisioning of a Network, Protocols and Standards for Managing a Network, Interfaces for Managing Individual Devices, Introduction to Operations Support System, Interconnection of OSS.
6. Telecommunications Management Network (TMN): TMN Models, TMN Architecture Styles.
7. Network Management Protocols: Introduction to SNMP, SNMP Architecture, Common Management Information Protocol (CMIP), Common Object Request Broker Architecture (CORBA).
8. Broadband Network Management: ATM Network Management, Broadband Access Network Management, Network Management Tools and Applications, Network Management Tools, Network Management Applications

Text Book and References:

Robert S. Cahn; Wide Area Network Design; Morgan Kaufmann, ISBN 1558604588

Networks: Design and Management; Steven Karris, Orchard Publications, 2006

Assessment and Grading System:

- Case Study (Group Task) – 25%
- Individual Assignment(s) – 15%
- Project (Practical/Lab) – 30%
- Final Written Examination – 30%
- Grades will be determined according to the University post-graduate rules and regulations.

==========

Course Title: IP Networking and Applications

Course Code: CNS 6213

Credit Hour: 3

Contact Hour per Week: 2 Lecture Hours and 3 Lab Hours

Course Status: Elective

Pre-Requisite: Advanced Computer Networking and Communications (CNS 6112)

Course Description:

This course introduces the Internet from both a theoretical and practical perspective. It first examines the architecture and operation of the TCP/IP protocol suit, and shows how information is processed and routed across it. The operation and configuration of routers is discussed alongside the details of protocol operation. The course then discusses the rationale behind the next generation IPv6 protocol, in particular regarding addressing architecture, header functions, and novel protocol concepts. A comparison between IPv4 and IPv6 and transition to the next generation protocol are discussed in depth. The function and implementation of its main support protocols are also covered. The application of these new networking ideas is illustrated by the application of IPv6 to problems in network layer services, especially security. Finally, the course describes the operation and configuration of applications and application-layer protocols, especially Domain Name System (DNS).

Course Objectives: On completion of the course, students should be able to:

- Understand and describe the Internet TCP/IP protocol suite, the protocol operation principles, and solve problems related to its functioning and performance.
- Discuss the client-server approach to networked computing and show where it is appropriate.
- Explain how information is routed across the Internet using different approaches and protocols.
- Describe in general terms and explain the business case and technical case for the next generation IPv6 protocol, its design and network functionality.
- Understand the operation of common applications and application-layer protocols and be able to discuss their configuration and deployment, particularly the DNS.

Course Contents:

1. Review of computer network concepts, layered services and protocols. Local area networks, Ethernets, MAC sub-layer, IP over Ethernet.
2. Internet protocol IPv4: IPv4 addressing, ICMP. ARP, RARP, BOOTP and DHCP.
3. Transport protocols: TCP operation, congestion control algorithms. UDP operation. Performance of computer networks.
4. Internet routing protocols: Static and dynamic routing. Distance-vector routing, link-state routing, convergence, Dijkstra algorithm. Interior and exterior routing protocols, RIP, OSPF, BGP. Multicast addressing and routing: IGMP, IP tunneling, MBONE, PIM.
5. Next generation IPv6 Internet protocol IPv6 addressing architecture. Main header and field functions. Extension headers. Auto-configuration and discovery functions. Comparison with IPv4. Review of IPv6 security concepts, IPv6 security services, transport and tunnel encryption modes. General architecture of IPSec and security headers. ICMPv6 functions. IPv6 mobility.
6. Applications and application-layer protocols. Common Internet services and their configuration. The Domain Name Service (DNS): purpose, installation and configuration.

Textbooks and References:

- HALSAL, F., Computer Networking and the Internet, 5th edition, Addison Wesley; ISBN:0321263588
  - Up-to-date, with background and related topics
- TANENBAUM, A.S., David J Wetherall, Computer Networks, 5th edition, Pearson Education; ISBN: 013255317
  - Good coverage of IPv4 protocol architecture and operation with some basics of IPv6 and network security
- HUITEMA, C., Routing in the Internet, Prentice-Hall; ISBN: 0130226475
  - In-depth discussion of Internet routing techniques by an authority in the field
- HASSAN, M. and JAIN, R., High Performance TCP/IP Networking, Prentice-Hall; ISBN: 0131272578
  - Advanced text on performance of TCP in different network settings
- LOSHIN, P., IPv6: Theory, Protocol, and Practice, 2nd edition, Morgan Kaufmann ISBN: 9781558608108

- Comprehensive text on IPv6 protocol and related issues

- SOLLIMAN, H., Mobile IPv6, Addison Wesley ISBN: 0201788977
  - Relevant text on applications of IPv6 in mobile networks
- PETERSON, L.L. and DAVIE B.S., Computer Networks: A System Approach, 4th edition, Morgan Kaufmann; ISBN: 0123740134
  - Advanced text on computer networks

Assessment and Grading System:

- Case Study (Group Task) – 25%
- Individual Assignment(s) – 15%
- Project (Practical/Lab) – 20%
- Final Written Examination – 40%
- Grades will be determined according to the University post-graduate rules and regulations.

==========

Course Title: Mobile Broadband and Multimedia Networks

Course Code: CNS 6214

Credit Hour: 3

Contact Hour per Week: 2 Lecture Hours and 3 Lab Hours

Course Status: Elective

Pre-requisite: Mobile Computing and Wireless Security (CNS 6121)

Course Description: This course is designed to give students an understanding of mobile broadband communication systems, their evolution, key technological issues and the convergence; transmission techniques and signal processing; MIMO channel modelling and MIMO systems; various broadband wireless multimedia systems; routing and cross-layer design issue of multimedia communication over multi-hop wireless ad-hoc/sensor networks and WLANs; latest advances in QoS provisioning, middleware, mobility management, scheduling and power control.

Course Objective: Upon successful completion of the course, the students should be able to introduce terms and concepts and laying the foundation of a mobile broadband communication system and multimedia systems; describe the basics of multimedia systems such as voice and video; examine multimedia systems over different networking environments such as ad-hoc networks, sensor networks, wireless local area networks, etc.; describe the communication systems and algorithms of broadband multimedia networks and the tools or applications used for high data rates streaming; critically evaluate the various broadband and multimedia components in terms of quality of service metrics.

Course Content:

1. Mobile Broadband Communication

    1.1. Introduction and Evolution

    1.2. Future Trends

    1.3. Key Technological Issues and Ongoing Activities

    1.4. Mobile Broadband Convergence Network

2. Transmission Techniques and Signal Processing

    2.1. Transmission Techniques

    2.1.1. Introduction

    2.1.2. OFDM Systems

    2.1.3. CDMA Systems

    2.2. Signal Processing

    2.2.1. Introduction

    2.2.2. Modulation and Coding

    2.2.3. Equalisation

    2.2.4. Synchronization and Channel State Estimation

    2.2.5. Multi-User Systems and Multi-User Detection

2.2.6. Link Adaptation and Rate-Adaptive Systems

3. MIMO Channel Modelling and Systems

3.1. MIMO Channel Modelling

3.2. MIMO Systems

4. Multimedia Systems

4.1. Design Challenges for Wireless Multimedia Sensor Networks

4.2. Design Challenges for Wireless Multimedia Sensor Networks

4.3. Performance Analysis of Multimedia Traffic over HSDPA

4.4. Interactive Mobile TV Technologies: An Overview

4.5. Multiparty Audio conferencing on Wireless Networks

5. Multimedia Over Ad-hoc, Sensor Networks and WLANs

5.1. Routing for Video Communications over Wireless Ad Hoc Networks

5.2. Unicast and Multicast Video Communication over Wireless Ad-hoc Networks

5.3. Video Communications over Wireless Sensor Networks

5.4. Multimedia QoS Support in IEEE 802.11 Standards

5.5. Peer-Assisted Video Streaming Over WLANs

5.6. Multimedia Services Over Broadband WLAN

6. Quality of Service and Enabling Technologies

6.1. End-to-End QoS Support for Video Delivery Over Wireless Internet

6.2. Handoff Management of Wireless Multimedia Services

6.3. Packet Scheduling in Broadband Wireless Multimedia Networks

6.4. Orthogonal Frequency Division Multiplexing Wireless Communication Systems

---

Assessment and Grading System:

- Assignment(s) – 20%
- Project(s) – 30% (Practical/Laboratory)

- Final Written Examination – 50%
- Grades will be determined according to the University post-graduate rules and regulations.

Textbook and References:

- L. M. Correia, "Mobile Broadband Multimedia Networks: Techniques, Models and Tools for 4G", Elsevier Ltd, 2006.
- Y. Zhang, S. Mao, L. T. Yang, and T. M. Chen, "Broadband Mobile Multimedia: Techniques and Applications", CRC Press, Taylor and Francis Group, 2008.
- B. Bing, "Broadband Wireless Multimedia Networks", Wiley Publishing, 2012.
- S. Paul, "Digital Video Distribution in Broadband, Television, Mobile and Converged", Wiley Publishing, 2011.

==========

Course Title: Social Network Analysis

Course Code: CNS 6215

Credit Hour: 3

Contact Hour per Week: 2 Lecture Hours and 3 Lab Hours

Course Status: Elective

Pre-requisite: A basic Undergraduate or equivalent course in Computer Networks and Communications

---

Course Description: This course will use social network analysis; both its theory and computational tools, to make sense of the social and information networks that have been fuelled and rendered accessible by the internet. Everything is connected: people, information, events and places, all the more so with the advent of online social media. A practical way of making sense of the tangle of connections is to analyze them as networks. In this course students will learn about the structure and evolution of networks, drawing on knowledge from disciplines as diverse as sociology, mathematics, computer science, economics, and physics. Online interactive demonstrations and hands-on analysis of real-world data sets will focus on

a range of tasks: from identifying important nodes in the network, to detecting communities, to tracing information diffusion and opinion formation. Gephi and Pajek are free software tools required for the course.

Course Objective: Upon the successful completion of the course, the students will be able to understand the theoretical and computational tools on social and information networks; apply different tools on online social medias such as Facebook and Twitter to mine and analyze information for decision making; understand the structure and evolution of networks; utilize real-world and synthetic data sets for different tasks such as identifying popular users, detecting communities, tracing data diffusion and opinion formation.

Course Content:

1. Introduction to Social Network Analysis
    1.1. Why Social Network Analysis
    1.2. Software Tools (Gephi and Pajek)
    1.3. Degree and Connected Components
2. Random Graph Models
    2.1. Introduction to Random Graph Models
    2.2. Random Graphs and Alternative Models
    2.3. Models of Network Growth
3. Centrality
    3.1. Degree Betweenness and Closeness
    3.2. Eigen Vector Directed
    3.3. Centrality Applications
    3.4. Power Laws and Data Science
4. Community Structure
    4.1. Community Structure and Detection

4.2. Heuristics for Finding Communities

4.3. Community Finding

5. Small World Networks

5.1. Small World Experiments

5.2. Clustering and Motifs

5.3. Small World Models and Origins of Small Worlds

6. Processed on Networks

6.1. Network Topology and Diffusion

6.2. Complex Contagion

6.3. Innovation and Coordination

6.4. Cool and Unusual Applications

7. Network Resilience

7.1. Introduction to Network Resilience

7.2. Resilience and Assortativity, and Resilience and the Power Grid

---

Assessment and Grading System:

- Assignment(s) – 20%
- Project(s) – 40% (Practical/Laboratory)
- Final Written Examination – 40%
- Grades will be determined according to the University post-graduate rules and regulations.

Textbook and References:

- D. Easley, and J. Kleinberg, "Networks, Crowds, and Markets: Reasoning About a Highly Connected World", Cambridge University Press, 2010.
- J. Scott, "Social Network Analysis", SAGE Publication, 2012.

- C. Prell, "Social Network Analysis: History, Theory and Methodology", SAGE Publication, 2012.
- K. Cherven, "Network Graph Analysis and Visualization with Gephi", Packt Publishing, 2013.
- W. de Nooy, A. Mrvar, and V. Batagelj, "Exploratory Social Network Analysis with Pajek", Cambridge University Press, Second Edition, 2011.

==========

Course Title: Virtualization and Cloud Computing

Course Code: CNS 6216

Credit Hour: 3

Contact Hour per Week: 2 Lecture Hours and 3 Lab Hours

Course Status: Elective

Pre-requisite: Mobile Computing and Wireless Security (IMNW 6121)

Course Description: This course instructs students how to administer and manage a modern network by properly planning and implementing various functions of a Network OS. Key components include how to plan server deployment, server monitoring and maintenance, application and data provisioning, and providing business continuity and availability by proper use of security configuration and backup policies. The course material is designed to provide extensive hands-on experience. Topics include: installation and configuration; the boot process; user and group administration; filesystem administration, including quotas, FACLs, RAID and LVM; task automation; client networking; software management; log files; troubleshooting; Emphasis is also given on storage, file management system, connectivity, security, troubleshooting, archiving, backing up, directory services, remote administration, access control lists.

Course Objective: Upon the accomplishment of this course, students will be able to know the basic concepts of Cloud Computing and current trends; know the differences among three cloud technologies; know what information needs to be collected from the clients before

deciding to place an application into the cloud; know the basic concepts of virtualization and current trends; explain procedures, problems and concepts of the three most common virtualization products; list the physical requirements for a physical virtualization server to meet a company's specific virtualization needs; list, discuss and compare the advantages and disadvantages of each of the three most popular VM products; analyze the TCO and change-over costs for a potential VM installation; determine a working quantity of configurable resources for the initial creation of a virtualized operating system such as XP or Win7 or Win8 (RAM, storage, etc.).

Course Content:

1. Introduction to Cloud Computing

    1.1. Cloud Computing Definition and Characteristics (elasticity, multi-tenant, on-demand, ubiquitous, access, usage metering, self-service, sla-monitoring, etc.)

    1.2. Basic Concepts of Cloud Computing and Current Trends

    1.3. Three Cloud Technologies

    1.4. What Does the Client Really Want to Accomplish? (Should everything be in the Cloud?)

    1.5. Cloud Support Software-commercial Products and Vendors: methods, pricing, licensing and maintenance contracts

    1.6. SharePoint

2. Cloud Service Models

    2.1. Infrastructure as a Service (IaaS)

    2.2. Platform as a Service (PaaS)

    2.3. Software as a Service (SaaS)

3. Basics of Virtualization

    3.1. Virtualization Defined and What should/should not be Virtualized?

    3.2. Versions and Licensing, Is it Economical? (TCO, setup costs; long term costs/savings)

3.3. Disaster Potentials and Recovery Strategies

3.4. Comparing Virtualization Technologies

3.5. VMware Server - (version, costs of product, creating VM)

3.6. Citrix: Products list, Xen Server, and Xen Center (create and customize virtual machines)

3.7. Microsoft Virtual PC (VPC console- create and customize virtual machines)

3.8. Microsoft Hyper-V (using Win 2008 r2 create and customize virtual machines)

3.9. Virtual Box- (create and customize virtual machines)

4. Applying Virtualization

4.1. Managing the Virtualization Server

4.2. Server backup methods

4.3. Migrations

4.4. Desktop Virtualization (strong hands-on component)

4.5. Network and Storage Virtualization

5. Building the Virtual Infrastructure

5.1. Form-factor and Hardware Architecture Choices

5.2. Vendor Choices

5.3. Planning

5.4. Deployment

5.5. Maintenance

6. Cloud Security

6.1. DHCP, DNS, Telnet server; compare with other NOS setup of corresponding network services

6.2. Cloud Security Challenges

6.3. Cloud Security Approaches: Encryption, Tokenization/Obfuscation, Cloud Security Alliance Standards, Cloud Security Models and Related Patterns

6.4. Cloud Security in Mainstream Vendor Solutions

6.5. Mainstream Cloud Security Offerings: Security Assessment, Secure Cloud architecture Design

---

Assessment and Grading System:

- Assignment(s) – 15%
- Seminar(s) – 25%
- Project(s) – 30% (Practical/Laboratory)
- Final Written Examination – 30%
- Grades will be determined according to the University post-graduate rules and regulations.

Textbook and References:

- B. Furht, A. Escalante, "Handbook of Cloud Computing", Springer, 2010.
- N. Benmessaoud, C. J. Williams, U. M. Mudigonda, "Network Virtualization and Cloud Computing", Mitch Tulloch - Series Editor, 2014.
- M. Portney, "Virtualization Essentials", John Wiley & Sons, 2012.
- Recent Research Articles from Top Journals such as IEEE Transaction on Cloud Computing, and others.

==========

Course Title: Web Engineering

Course Code: CNS 6217

Credit Hour: 3

Contact Hour per Week: 2 Lecture Hours and 3 Lab Hours

Course Status: Elective

Pre-requisite: Advanced Computer Networking and Communications (CNS 6112)

Course Description: This course is designed to provide students with a solid understanding of a pragmatic process for engineering Web-based applications. Web applications are complex systems that deliver a plethora of features to a large number of users (including developers), and also exhibit unique behaviours and demands in terms of performance, scalability, usability, and security. This course will discuss the limits of current web technologies, information and service architectures, and content management. Covering every important aspect of a WebApp development, the course presents proven methods for requirements gathering and analysis, design, testing, project planning, change and content management.

Course Objective: Upon completion of this course, students will be able to identify the challenges with the existing web technologies and predict features of next generation web-based systems; understand an agile and adaptable approach to the development of next generation WebApps—systems that are more complex, more functional, and more significant than any that exist today; communicate, formulate and plan the web engineering process; analyze and model WebApps, identify and apply the different approaches to web design; construct and deploy web-based systems and WebApps; understand and use design patterns, technologies, tools and testing mechanisms; implement content management systems and some other evolving web technologies.

Course Content:

1. Web-Based Systems and Web Engineering
    1.1. The Web and Web Applications
    1.2. Evolution and Attributes of WebApps
    1.3. Overview of Web Engineering
    1.4. Agile and WebE Framework
    1.5. Components of Web Engineering
    1.6. Web Engineering Best Practices
2. Web Engineering Process

7.6.4. Security and Performance Testing

8. Change and Content Management

8.1. Overview and Attributes of Change

8.2. Change Management for Web Engineering

8.3. Content Management System (CMS)

8.4. Criteria for Implementing CMS

9. Future Directions

9.1. The Changing Nature of the Web and Web Apps

9.2. Evolving Web Technologies and Web 2.0

9.3. The Future and Changing Nature of Web Engineering

Assessment and Grading System:

- Assignment(s) – 15%
- Seminar(s) – 25%
- Project(s) – 30% (Practical/Laboratory)
- Final Written Examination – 30%
- Grades will be determined according to the University post-graduate rules and regulations.

Textbook and References:

- R. Pressman, and D. Lowe, "Web Engineering: A Practitioner's Approach", McGraw-Hill Education, 2008.
- W. Suh, "Web Engineering: Principles and Techniques", Idea Group Inc., 2005.
- R. Sebesta, "Programming the World Wide Web", 2009.

==========

Course Title: Distributed Systems

Course Code: CNS 6218

Credit Hour: 3

Contact Hour per Week: 2 Lecture Hours and 3 Lab Hours

Course Status: Elective

Pre-requisite: None

Course Description: The course introduces the main principles underlying distributed systems: processes, communication, naming, synchronization, consistency and fault tolerance. Furthermore, students will be familiar with some of the main paradigms in distributed systems: Object-based systems, MapReduce and file systems. Class will be run seminar-style; each student will read research papers that will be discussed in class. They will read papers that cover the theory of distributed systems as well as the implementation of systems to support distributed computing.

Course Objective: On the completion of the course, students will be able to understand the fundamentals of distributed computing and be able to design and develop distributed systems and applications; explain how communication is handled in distributed systems; realize issues and difficulties in clock synchronization over several machines; learn the different methods and frameworks such as MapReduce that are used in handling consistency and replication and how fault tolerant systems are built.

Course Content:

1. Introduction to Distributed Systems

1.1. Introduction and Goals of Distributed Systems

1.2. Types of Distributed Systems

2. Architectures and Processes in Distributed Systems

2.1. Architectural Styles and System Architectures

2.2. Threads and Their Implementation

2.3. Anatomy of Clients, Servers and Design Issues

2.4. Process Migration and Scheduling

3. Communication and System Design

3.1. Network Protocols and Standards

3.2. Remote Procedure Call

3.3. Message-Oriented Communication

3.4. Stream-Oriented Communication

3.5. Multicast Communication

4. Naming and Synchronization

4.1. Names, Identifiers, and Addresses

4.2. Flat, Structured and Attributed-based Naming

4.3. Clock Synchronization and Logical Clocks

4.4. Mutual Exclusion

4.5. Election Algorithms

5. Consistency Management and Replication

5.1. Overview of Consistency Management and Replication

5.2. Data-Centric Consistency Models

5.3. Client-Centric Consistency Models

5.4. Replica Management and Prominent Replication Protocols

5.5. Consistency Protocols

6. Fault Tolerance and Grid Computing

6.1. Introduction to Fault Tolerance

6.2. Process Resilience

6.3. Reliable Client-Server and Group Communications

6.4. Distributed Commit and Recovery

7. Distributed Object-based Systems

7.1. Distributed Objects and Object Servers

7.2. CORBA Object References

7.3. Globe Object References

7.4. MapReduce

8. Cluster Computing and Distributed File Systems

8.1. Cluster-Based Distributed File Systems

8.2. Remote Procedure Calls in Network File System

8.3. File-Oriented Communication

Assessment and Grading System:

- Lab Assignment(s) – 25%
- Seminar(s) – 25%
- Final Written Examination – 50%
- Grades will be determined according to the University post-graduate rules and regulations.

Textbook and References:

- A. S. Tanenbaum, and M. V. Steen, "Distributed Systems, Principles and Paradigms", Second Edition, Prentice Hall, 2007.
- A. S. Tannenbaum, "Computer Networks", Prentice Hall, Fourth Edition, 2003.
- S. Mullender, "Distributed Systems", Second Edition, Addison-Wesley, 1993.
- G. Coulouris, J. Dollimore, and T. Kindberg, "Distributed Systems: Concepts and Design", Third Edition, Addison-Wesley, ISBN: 0201619180, 2000.

==========

Course Title: Computer Networking and Security Laboratory

Course Code: CNS 6219

Credit Hour: 3

Contact Hour per Week: 2 Lecture Hours and 3 Lab Hours

Course Status: Elective

Pre-Requisite: Advanced Computer Networking and Communications (CNS 6112), Network Programming (CNS 6113), Network Management, Security, and Ethical Hacking, Network Design, Modelling and Simulation (CNS 6122), Advanced Computer Network and System Administration (CNS 6123), Advanced Computer Network Security (CNS 6124)

Course Description: In this course, students will learn how to put "principles into practice," in a hands-on-computer-networking and security lab course. The course will cover router and end-system labs in the areas of Single Segment IP Networks, Multiple Segment IP Networks and Static Routing, Dynamic Routing Protocols (RIP, OSPF and BGP), LAN switching, Transport Layer Protocols: UDP and TCP, NAT, DHCP, DNS, and SNMP. The labs are due at a rate of roughly one lab per week. A short pre-lab Q&A, as well as lab writeups, are required for each lab.

These labs will be done in a networked lab setting with a few racks each of which consists of 4 Cisco2600-series routers or Juniper MX104 routers, 4 hubs, and 4 Linux hosts. We will additionally have a few labs with Pica8 software-defined networking (SDN) switches or the Juniper switches in SDN mode. **Software-defined networking has been changing the landscape of the networking industry in recent years, so the recently added SDN routers and labs will expose students to the underlying concepts.**

The labs are self-paced (do them in the lab at a time of your own choosing), and so *you will need to be motivated, conscientious, and organized in order to complete this course successfully*. There will be formal lectures by the instructor, but these will primarily refresh conceptual networking material that you would have already covered in the prerequisite for this course.

Course Objectives: On completion of the course, students should be able to:

- Explore, map, and analyze realistic TCP/IP networks using a variety of diagnostic software tools.
- Implement, test and maintain common firewall types and architectures in a simulated (E-banking setting).

- Implement, test, maintain and demonstrate Single Segment IP Networks, Multiple Segment IP Networks and Static Routing, Dynamic Routing Protocols (RIP, OSPF and BGP), LAN switching, Transport Layer Protocols: UDP and TCP, NAT, DHCP, DNS, and SNMP.
- Implement, test, maintain and demonstrate cryptography and network security.

Course Contents:

1. Computer Networking Lab: The module will cover router and end-system labs in the areas of Single Segment IP Networks, Multiple Segment IP Networks and Static Routing, Dynamic Routing Protocols (RIP, OSPF and BGP), LAN switching, Transport Layer Protocols: UDP and TCP, NAT, DHCP, DNS, and SNMP. The labs are due at a rate of roughly one lab per week. A short pre-lab Q&A, as well as lab writeups are required for each lab.
2. Cryptography and Network Security Lab: The module will cover Cryptography and Network Security Labs: openssl, encryption, decryption, cryptography, network attack vectors, anti-virus and spyware exercises, Microsoft baseline security analyzer exercise, perimeter defense: firewalls, password cracking exercise; Network diagramming exercise, Router exercise, wireless networking exercise, protocols, encapsulation exercise, NMap exercise, DNS/FTP/Telnet exercise, Firewall exercise, intrusion detection/prevention systems, IDS/IPS exercise.

Text Book and References:

Mastering Networks: An Internet Lab Manual by Jorg Lieberherr, University of Virginia; Magda El Zarki , University of California , Irvine . ISBN: 0-201-78134-4. Publisher: Addison-Wesley. Copyright: 2004.

Online References:

- http://moodle.umass.edu (for course management), http://piazza.com (for discussions)
- **http://www.tcpip-lab.net/links/** - Listing of links referenced in prelabs, indexed by lab number
- **http://www.cs.virginia.edu/~itlab/book/** - Book website setup by one of the authors
- **http://www.cs.virginia.edu/~itlab/book/errata.html** - List of Errata (printing errors) in the book
- **http://www-edlab.cs.umass.edu/cs491g/2010** - Course webpage from Spring 2010.

- **http://www-net.cs.umass.edu/491g/** - Course webpage from Spring 2011.
- Quick reference for **Linux commands**
- Online Linux **MAN pages**
- Some commonly used tools:
  - tcpdump **command syntax** and **examples**
  - Wireshark **website**
  - Wireshark video tutorials: **display filters** and **capture filters** (especially from 3:50 minutes into the video)

Assessment and Grading System:

- Case Study/ Lab Assignment(s) (Group Task) – 20%
- Individual Lab Assignment(s) – 20%
- Project (Practical/Lab) – 40%
- Final Written Examination – 20%
- Grades will be determined according to the DBU university post-graduate rules and regulations.

==========

Course Title: Thesis in Computer Networks and Security

Course Code: CNS 6221

Credit Hour: 6

Course Status: Compulsory

Pre-requisite: Completion of the Two-Semester Core Courses [Read the Student Manual]

Course Description: This course is intended to provide a practical skill in carrying out research and documenting and presenting the findings in a selected area of Computer Networks and Communications. This course starts in 2nd year 1st semester where students identify research problem and develop research proposal; in 2nd year 2nd semester, students work on the implementation and analysis of the results and possibly look for publication.

Course Objective: At the end of this thesis students will be able to know how to read and understand published papers and other materials related to the thesis title; understand and apply issues related to research in Computer Networks and Communications; write technical reports in the form of journal, conference and workshop papers and thesis; present and defend research findings.

Course Content:

The student investigates an original work including a study of its possible implications, potential applications, and its relationship to previous related works reported in the literature. Contributions and results from this investigation are synthesized and compiled into a thesis presenting the new idea and presented to an examining committee, to be organized by the College.

Assessment and Grading System:

- Grades will be determined according to the university post-graduate rules and regulations.

Textbook and References:

- Articles published in high quality journals and conference proceedings related to the area of the title of the thesis, books, reading materials from the web, etc.

==========

==========

11. Appendix

11.1 Computer Networks and Security Lab (CNS Lab) Student Manual

11.1.1 Basic Information

Welcome to the Computer Networks and Security Lab (CNS Lab) based in College of Computing, Institute of Technology, Debre Berhan University, Debre Berhan, Ethiopia.

The mission of CNS Lab is to create innovation through conducting interdisciplinary, application-driven academic research in networking and security. The laboratory is interested in a broad spectrum of cutting-edge research into social computing, big data, wireless communication, mobile computing, cyber-physical systems, cryptography and relevant areas, from both theoretical and practical foundations, through design and implementation, to real-world applications, as well as education.

- Full name of the Lab: Computer Networks and Security Lab, College of Computing, Institute of Technology, Debre Berhan University, Debre Berhan, Ethiopia.
- Short name of the Lab: CNS Lab
- URL (website): http://dbu/iot/coc/cnslab.edu.et (will be deployed soon)
- Address: First floor, Building (will be identified soon by the college), College of Computing, Institute of Technology, Dbere Berhan University, Dbere Berhan, Ethiopia.
- Supervisor(s): Should be at least PhD holder in Computer Networks and academic staff.

11.1.2 Daily Management

- The lab will have its own Director, one with at least MSc holder and academic staff.
- All lab members are one family, and hence should take care of each other in everyday life.
- The Assistant Director (among the Masters Students) will help the Supervisor to handle everyday management issues, including e.g. equipments and social activities.
- Normally, study and work facilities will be provided by the Supervisor. Send your request to Assistant Director if you need something (for study/work). Valuable

equipments (e.g. computers) bought by the lab are property of the Institute, and must be returned by the time of graduation.

- Every lab member is encouraged to establish a homepage on the website of the lab. It is free.
- Anytime you enrol to or leave from the CNS Lab, ask for permission from the Supervisor in advance.
- The lab will have an FTP server to store various materials for study and work. There will be an FTP Manager (among the Masters Students) who will be assisted by Lab Director or Supervisor. Every lab member can get a unique/private account from the FTP Manager.
- All relevant electronic academic materials (including e.g. full papers, e-books, thesis, datasets, software tools, etc) collected by any lab member should be shared with others. Upload useful materials to the FTP server.
- Distribution of internal materials of the lab without permission is forbidden.
- All research outcomes (e.g. papers, data, source codes, software/tools, relevant documents, etc) must be archived onto the FTP server.

11.1.3 Literature (Research Article) Search

The Institute of Technology or Computing College will provide access portals to two major academic databases in the world (IEEE and ACM digital libraries), from where full texts of scientific papers can be downloaded (on campus) for free.

Very important databases (search and read papers from these databases, especially papers published in TOP journals and TOP conferences in recent 5 years):

- Nature, Scientific Reports: http://www.nature.com
- Science: http://www.sciencemag.org/
- PNAS: http://www.pnas.org/
- PLoS One (Open Access): http://www.plosone.org/
- Physical Review X (Open Access): http://prx.aps.org/
- IEEE Xplore: http://ieeexplore.ieee.org
- ACM Portal: http://portal.acm.org/portal.cfm

- Google and Google Scholar: http://www.google.com/; http://scholar.google.com/
- Microsoft Academic Search: http://academic.research.microsoft.com/
- Springer Link: http://www.springerlink.com
- Elsevier: http://www.sciencedirect.com/
- etc

11.1.4 Research Activities

In the first year of your enrolment:

- Download materials from the Lab FTP server; Learn how to do good research, and how to write good papers, etc (more materials are available on the Internet);
- Report to the Lab Supervisor about what you have read;
- Enhance your capability of reading and writing (in English) as much as possible;
- Search relevant papers (some will be available on the FTP server).
- Read A LOT (of papers on certain topics)! Normally over 100 papers in total should be read, among which at least 40 should be read very carefully (intensive reading). The focus must be on high-quality papers published in TOP/Important journals and TOP conferences in recent 5 years.
- By the end of the first year (August), upload all papers you have read to the FTP server (the name of the folder will be specified later). The Supervisor will check with you to ensure that you have read a lot as instructed.
- Write a SURVEY paper to summarize the state-of-the-art of an emerging topic. This could be a long survey paper or a short tutorial. Good papers might be considered for submission to journals.
- Discuss with lab members about your masters research topics, and identify the research issue you will work on.
- Write your RESEARCH PROPOSAL using the template (12.3) and send it to the Supervisor via email by the end of September.
- Give a presentation on your research proposal. You need to defence it to the Lab community and to your advisor.

In the second year of your enrolment:

- Work on specific research issue (according to research proposal) and obtain original innovative research result/outcome;
- Discover/identify NEW problem, propose NEW solution (e.g. a theory, an algorithm, a protocol, a method, a tool, etc) for the problem, and get NEW data (e.g. simulation or experiment results) to evaluate the performance of the solution;
- Enhance your capability of doing research independently on: leading a team, writing high-quality thesis, writing research/project proposal, thesis etc;
- Write your Master's THESIS using the template that will be provided by the Lab;
- Apply for graduation given that all Program Requirements are satisfied and approved by the Supervisor;
- Send your thesis to your Supervisor; In case of failure in this phase, revise your thesis and do it again until success. You have to pass your supervisor and pre-defence (committee organized by the College) at least a month before the time of graduation.
- Your thesis will be sent out (by the College) for peer-review after you pass the pre-defence. The review process takes about a month in most cases.
- If you pass the peer-review, prepare for the (final) official defence of your M.Sc. thesis. In case of success, congratulations! Revise your thesis and send it to the Supervisor for approval. Submit the final version to the College, and wait for your Masters.
- Pay special attention to the quality of the papers you read and cite (in your thesis). The majority of them should be from TOP/Important journals/conferences and be published in the past 5 years.
- **Any forms of plagiarism and self-plagiarism are forbidden, under any circumstances. Any forms of other scientific misconduct (e.g. fabrication and falsification) are also forbidden.**
- As a general rule, EVERY sentence of a paper should/must be written by the student; EVERY figure/table should/must also be produced by the students.
- It is not allowed to copy any content (including e.g. text/sentences, figures, tables, data, etc) (directly) from others (even you put citations there)!

- Cite references properly wherever necessary, but do not cite useless references (which are not really referred to).
- Students who are found to have engaged in scientific misconduct will be punished seriously and might be kicked out of the Lab and the University.
- Lab members are encouraged to attend various academic activities such as academic day, group meeting, weekly progress report, semi-annual research plan and monthly progress report (templates will be available).
- Each year, the Outstanding Contribution Award (a certificate plus a certain amount of money) will be granted (by the Lab) to one student (of the Lab) with most outstanding performance in research and service. Students who have ever violated rules stated in this document in the year are not eligible for this Award. To become a candidate, send (via email) an application statement along with an outline of your contributions and outcomes in research of the year to the Director of the lab by the end of December. Normally the recipient/s will be announced in early January, and the bonus and certificate will be presented in the next semester.

11.1.5 Others

- Any suggestions/comments (on any related issues) are welcome.
- This manual is revised and compiled with permission from the producer and copyright holder Prof. Feng Xia (Dalian University of Technology) first by Ahmedin Mohammed (PhD) Wolo University and customised by Debre Berhan University. It is not for distribution. Do not use any content of this manual anywhere else without permission by the copyright owner.

11.2 List of Important and Top Journals/Conferences

Students are encourages to read related papers recently published in these important and top journals and conferences. List of Important and Top Journals include:

- Nature (World BEST)
- Science (World BEST)
- PNAS: Proceedings of the National Academy of Sciences
- Nature Communications

- Science Advances
- Proceedings of the IEEE
- Scientific Reports (Nature)
- ACM Computing Surveys
- IEEE Communications Surveys and Tutorials
- ACM Transactions on Information Systems
- IEEE Transactions on Knowledge and Data Engineering
- IEEE Transactions on Mobile Computing
- IEEE Transactions on Parallel and Distributed Systems
- IEEE Transactions on Computers
- IEEE/ACM Transactions on Networking
- IEEE Transactions on Computational Social Systems
- IEEE Transactions on Big Data
- IEEE Transactions on Systems, Man, and Cybernetics: Systems
- IEEE Transactions on Human-Machine Systems
- IEEE Transactions on Cybernetics
- IEEE Transactions on Network Science and Engineering
- IEEE Transactions on Learning Technologies
- IEEE Transactions on Vehicular Technology
- IEEE Transactions on Intelligent Transportation Systems
- IEEE Transactions on Emerging Topics in Computing
- IEEE Transactions on Cloud Computing
- ACM Transactions on Intelligent Systems and Technology
- ACM Transactions on the Web
- ACM Transactions on Internet Technology
- Journal of the Association for Information Science and Technology (Wiley)

- Information Systems (Elsevier)
- Information Sciences (Elsevier)
- The Computer Journal (Oxford)
- Nature Physics
- Communications of the ACM
- IEEE Computer
- Any other IEEE/ACM Transactions/Journals/Magazines
- Any other Journals with IF (Impact Factor) >= 2.0

List of Top Conferences include:

- International Joint Conference on Artificial Intelligence (IJCAI)
- ACM Joint Conference on Digital Libraries (JCDL)
- ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD)
- ACM Conference on Information and Knowledge Management (CIKM)
- IEEE International Conference on Computer Communications (INFOCOM)
- AAAI Conference on Artificial Intelligence (AAAI)
- International World Wide Web Conference (WWW)

11.3 CNS Lab Masters Research Proposal Template

Your Full Name

Month, Year

1. Research/Thesis Title

Should be descriptive of focus, concise, eye-catching

2. Research Summary

A short abstract of research; about 300 words summarizing **What? Why?** and **How?** you are proposing to undertake this research.

3. Research Background and Motivation

To provide background information relating to the context of your study: in the background try to persuade the reader that the study will be useful/interesting; this may include reference to a 'gap' in the research literature, the need to apply certain ideas in a new context, or to the significance of your particular topic (i.e. research problem); address why this topic is still a problem warranting your research (this leads you to stating your research questions).

4. Research Goals and Research Questions/Issues

To state clearly and succinctly the purpose of the study (should logically follow from the above research problem statement); to outline the SMART objectives and key research questions; the purpose is expressed in terms of the broader context of the study; the research question(s) (usually What, How, Why, or What if) should be few, so that the focus is manageable.

5. Review of the Literature

To show that you are aware of significant writers/researchers in the field, and to indicate which issues/topics you will focus on in your review (this may change later); to show that you can be judicious in your selection of issues to focus on and take an approach of critical inquiry; how this project relates to prior work in the area (including your own, if relevant).

6. Research Design/Methodology and Proposed Solution

Be detail (as much as possible) on your proposed approach/solution (idea) for the research question/issue: description of the work you'd like to do; describe the research plans; what approach will be proposed to address the research question/issue? How the anticipated objectives will be accomplished; a thoroughly detailed plan is preferable; includes your understandings of the nature of knowledge and how this affects your choice of research approach; How to evaluate the performance of your approach?

Will you be doing this research on your own or with others?

7. Outline of Contributions

What are the major contributions? These may relate closely to Research Goals

8. Expected Outcomes

Predict the expected outcomes and innovations; what you will deliver by the end of the research: what new algorithm/protocol/method/architecture? prototype? real application/system (with documents)?

9. Timetable

Divide the research into discrete tasks, milestones, or phases; depict the tasks and the stages/times for their completion; this may take the form of a chart, timeline or flowchart (or any other)

10. Proposed Thesis Structure (if available)

Describe the focus of each proposed chapter; each chapter's proposed content is described in a few lines or a small paragraph, or a proposed table of contents is presented

11. References (include only highly related ones, rather than all)

List of works that have been consulted so far and appear to be useful; most of them should be good (SCI-indexed) journal or (IEEE/ACM) conference papers published in recent years.

Note:

1. The purpose of the proposal is to help you (as Masters Student) to focus and define your research plans. These plans are not binding, in that they may well change substantially as you progress in the research. However, they are an indication of your direction and discipline as a researcher. They also help you as direction to your work to obtain your M.Sc.

2. There is no requirement on the length of the proposal, as long as you can address the issues clearly.

3. Rename the file: researchProposal-YourFirstName-Year.doc/x