MASTER IN TELECOMMUNICATIONS, NETWORKS AND SECURITY

Main Language of Instruction:
French ☑ English ○ Arabic ○

Campus Where the Program Is Offered: USJ-CST / Lebanese University Rafic Hariri Campus – Hadath

OBJECTIVES

The Master in Telecommunications, Networks and Security prepares engineers and network and security researchers to navigate the global landscape of telecommunications and security. It equips students with the expertise needed for careers in network and security research, network design, telecommunications systems, network administration, multimedia content transmission, and the future of the Internet. This program also lays a solid foundation for students wishing to pursue doctoral studies (PhD) in these fields.

This inter-university degree, awarded in Lebanon, is supported by the collaboration of reputable institutions, which contribute their academic and scientific resources to the training.

This Master's degree is co-delivered by two faculties from two Lebanese universities: **The Faculty of Engineering** at the Lebanese University and the **Faculty of Engineering and Architecture** at the Saint Joseph University of Beirut. The program is offered jointly under the aegis of the Lebanese Ministry of Education and Higher Education.

PROGRAM LEARNING OUTCOMES (COMPETENCIES)

- Acquire and apply advanced knowledge relevant to the discipline.
- Solve critical issues and demonstrate expertise in key areas.
- Innovate and develop solutions for real-world problems.
- Apply new and diversified theoretical and experimental methods relevant to the discipline.
- Conduct independent, original research and contribute to the advancement of knowledge in the field.
- Communicate effectively in both oral and written forms.

ADMISSION REQUIREMENTS

This is a Master 2 program. Candidates who have already completed 60 credits in a relevant Master's degree or hold an engineering degree in telecommunications, computer science, networks, or any related fields will receive first-year credits by equivalence.

PROGRAM REQUIREMENTS

120 credits: Required courses (60 credits), divided over 2 semesters of 30 credits each. Courses granted by equivalence (60 credits)

Required Courses (60 Cr.)
Advanced Network Protocols and Services (3 Cr.). Mobile and Cellular Networks (3 Cr.). Cryptography (3 Cr.). Network Modeling (3 Cr.). Optimization for Networks (3 Cr.). Cloud and Application Architectures (3 Cr.). Security in Networks (3 Cr.). Cybersecurity (3 Cr.). Wireless Networks (3 Cr.). Machine Learning for Networks and Cybersecurity (3 Cr.). Master Thesis (30 Cr.).

SUGGESTED STUDY PLAN

Semester 1

Code	Course Name	Credits
MTRS01S1	Advanced Network Protocols and Services	3
MTRS02S1	Mobile and Cellular Networks	3
MTRS03S1	Cryptography	3
MTRS04S1	Network Modeling	3
MTRS05S1	Optimization for Networks	3
MTRS06S1	Cloud and Application Architectures	3
MTRS07S1	Security in Networks	3
MTRS08S1	Cybersecurity	3
MTRS09S1	Wireless Networks	3
MTRS10S1	Machine Learning for Networks and Cybersecurity	3
	Total	**30**

Semester 2

Code	Course Name	Credits
MTRS01S2	Master Thesis	30
	Total	**30**

COURSE DESCRIPTION

MTRS01S1 Advanced Network Protocols and Services 3 Cr.

This course covers the following topics: Switching, flow and congestion control, error control. Routing protocols (RIP, OSPF, BGP). Addressing and Multipoint Group Management (IGMP). Multipoint routing (DVMRP, PIM). Variants of TCP. Protocols for reliability and congestion control for multipoint. IPv6 evolution. IP mobility. Multihoming and SCTP. Architecture of QoS, IntServ and RSVP, DiffServ, MPLS Service. Quality of service routing, Flow management mechanisms (RED, WFQ, etc.), VoIP.

MTRS06S1 Cloud and Application Architectures 3 Cr.

This course covers the following topics: Cloud Technologies and Services. Cloud Computing, architectures, infrastructures, services, virtualization. Distributed processing and storage. Programming and Application Architectures. Agent and multi-agent systems. Intelligent agents. Peer-to-peer architectures.

MTRS03S1 Cryptography 3 Cr.

This course covers the following topics: Basics of Security Services. History of Cryptography. Symmetric, Asymmetric Algorithms, Hash Functions. Cryptographic Mechanisms and Techniques. Cryptographic Modes. PKCS standards. Envelopes. PKI. Smart Cards. Cryptography and ASN1. Modern (quantum) cryptography. It is conducted in the cryptographic laboratory with the use of Cryptographic Tools to implement symmetric, asymmetric, hash algorithms, cryptographic modes, cryptographic protocols and security devices.

MTRS08S1 Cybersecurity 3 Cr.

This course introduces cybersecurity and covers the following topics: cybersecurity tools and processes, system administration, operating system and database vulnerabilities, types of cyberattacks, cybersecurity risk analysis, and technical recommendations for cybersecurity.

MTRS10S1 Machine Learning for Networks and Cybersecurity 3 Cr.

This course covers the following topics: Machine Learning, data analysis methods. How-tos for networks and cybersecurity, analysis, how ML can be applied to cybersecurity, attack detection, prevention, and more.

MTRS01S2 Master Thesis 30 Cr.

This thesis serves as an introduction to research techniques and represents the synthesis of six months of research conducted in a company, research center, or laboratory.

MTRS02S1 Mobile and Cellular Networks 3 Cr.

This course covers the following topics: Cellular concepts and functions in mobile networks; Standardization and evolution of mobile networks; LTE and 4G networks (LTE-Advanced and LTE-Advanced Pro): services, radio interface, physical and protocol architectures, physical, transport and logical channels, voice in LTE, management of data flows, management of radio resources, management of security and developments from LTE to LTE-Advanced and LTE-Advanced Pro; recent advances in mobile networks; dimensioning and radio planning of 4G networks; mobile network deployment practices; quality of service and optimization of mobile networks; C-RAN; SDN; Cellular Internet of Things.

MTRS04S1 Network Modeling 3 Cr.

This course covers the following topics: Introduction to teletraffic theory. Memoryless source model (Bernoulli and Poisson) and study of multiplexing and multiple access. Discrete-time and continuous-time Markov chains. Introduction to Queuing Theory). Markovian files of type M/M and applications to modeling in networks. Queuing networks. Product form networks. Traffic and traffic aggregation models. Non-Markovian files (M/G/1 and G/M/1). Problems of performance evaluation and modeling of communication systems. Sizing.

MTRS07S1 Security in Networks 3 Cr.

This course covers the following topics: Network techniques and architectures. Network attacks. Security services and areas. Network security and associated solutions. Tools and equipment (smart cards) for security. Real case studies for network security. Key distribution - PKI - Audit - Components (TPM) - Applications: Ad-hoc networks, RFID, peer-to-peer, electronic directory and messaging, SMIME, etc. Security in fixed and mobile telecom and packet networks (GSM, UMTS, WiMAX).

MTRS05S1 Optimization for Networks 3 Cr.

This course covers the following topics: Mathematical optimization: formulation of an optimization problem, linear optimization problem, convex non-linear optimization problem, integer optimization problem, non-convex non-linear optimization problem. Search for optimal solution: Lagrangian, duality, optimality conditions, complexity, tools and software for optimization.
Algorithms: simplex, branch and bound, gradient and subgradient, primal and dual decomposition, meta-heuristic. Multi-objective optimization: dominance, scalar method, Pareto criterion and utilitarian criterion. Optimization and game theory: non-cooperative games, utility function and optimization, Nash equilibrium, Best Response algorithm. Application of optimization for networks: routing in networks, network sizing, bandwidth allocation and fairness problems, scheduling in wireless networks, power control in wireless networks, selection of wireless access.

MTRS09S1 Wireless Networks 3 Cr.

This course covers the following topics: Classification of wireless networks. WLAN networks: architecture, versions, MAC protocol, QoS. Ad hoc networks: self-configuration, proactive and reactive routing, MAC layer. Vehicular networks: requirements and constraints of intelligent transport systems (ITS), V2I and V2V communications, applications, standards, QoS, mobility models. Sensor networks: WSN architecture, clustering and routing mechanism with energy constraints, low-power communications standards (IEEE 802.15.4, BLE), 6LowPAN and ZigBee. Internet of Things: IoT pillars, IoT elements, IoT applications, communication protocols: MQTT, CoAP, LoRaWAN.