Course guides
230997 - SCFOB - Secure Communications in Fiber-Optic Networks

Last modified: 10/06/2020

Unit in charge: Barcelona School of Telecommunications Engineering
Teaching unit: 739 - TSC - Department of Signal Theory and Communications.

Degree: MASTER'S DEGREE IN CYBERSECURITY (Syllabus 2020). (Optional subject).

Academic year: 2020 **ECTS Credits:** 5.0 **Languages:** English

LECTURER

Coordinating lecturer: Comellas Colome, Jaume

Others: Gene Bernaus, Joan Manuel
Lazaro Villa, Jose Antonio
Spadaro, Salvatore

PRIOR SKILLS

Programing skills
Fundamentals of communication networks

TEACHING METHODOLOGY

Lectures
Laboratory practical work
Individual and group assignments

LEARNING OBJECTIVES OF THE SUBJECT

The main objective of this course is to train students in methods of understanding, evaluating and designing mechanisms for implementing security protocols in fiber optic based networks. The main concepts and specifities of optical networks regarding security issues are introduced and practical solutions are studied.

STUDY LOAD

Type	Hours	Percentage
Self study	86,0	68.80
Hours large group	33,0	26.40
Hours small group	6,0	4.80

Total learning time: 125 h

CONTENTS

1.Introduction

Description:
Fiber Optic networks fundamentals
Multi-layer, multi-domain, network management and control
Need for physical layer security strategies

Full-or-part-time: 9h 30m
Theory classes: 2h
Guided activities: 1h
Self study : 6h 30m

2. Security issues in IP over optical networks

Description:
Nodes and fibers tapping and jamming
Crosstalk attacks
Quality of service (QoS) degrading/disruptive attacks
Disturbances on network control
FTTH networks attacks

Full-or-part-time: 19h
Theory classes: 4h
Guided activities: 2h
Self study : 13h

3. Limitations of Physical Layer-Agnostic Security Technologies

Description:
Types of security
- Unconditional security
- Computational security
- Information-based security
The thread of quantum computing
- Shor's algorithm
- Post-quantum cryptography
High-speed secure communications
- The speed-security trade-off
- State-of-the art

Related activities:
Real time encryption algorithms analysis, simulation and comparison

Full-or-part-time: 29h
Theory classes: 4h
Laboratory classes: 3h
Guided activities: 2h
Self study : 20h

4. Security technologies for the optical layer

Description:
Physical layer security
- The wiretap channel
- Secrecy capacity
Confidentiality/authenticity: optical encryption
- Optical code division multiplexing (OCDM)
- Optical key distribution
- Spatial division multiplexing (SDM)
Privacy: optical steganography
- Chromatic dispersion
- Amplified spontaneous emission (ASE)
Integrity/availability: optical jamming
- Waveband conversion
- Optical chaos-based communications

Full-or-part-time: 29h
Theory classes: 6h
Guided activities: 3h
Self study : 20h

5. Quantum security technologies

Description:
Quantum tools for classic cryptography
- Quantum random number generators (QRNG)
- Quantum noise-randomized ciphers (QNRC)
Quantum cryptography
- Quantum key distribution (QKD)
- Quantum ciphers

Related activities:
Lab Practice: QKD algorithms analysis, simulation and comparison

Full-or-part-time: 38h 30m
Theory classes: 6h
Laboratory classes: 3h
Guided activities: 3h
Self study : 26h 30m

GRADING SYSTEM

Personal assignments (40%), Group assignments (20%), Final exam (40%)

BIBLIOGRAPHY

Basic:
- Bloch, M.; Barros, J. Physical-layer security: from information theory to security engineering. Cambridge: Cambridge University Press, 2011. ISBN 9780521516501.
- Cariolaro, Gianfranco. Quantum Communications [on line]. Cham: Springer, 2015 [Consultation: 25/06/2020]. Available on: http://dx.doi.org/10.1007/978-3-319-15600-2. ISBN 9783319156002.
- Kartalopoulos, Stamatios V. Next generation intelligent optical networks : from access to backbone [on line]. New York: Springer, 2008 [Consultation: 20/05/2020]. Available on: http://dx.doi.org/10.1007/978-0-387-71756-2. ISBN 9780387717555.