Course guide
230997 - SECON - Secure Communications in Fiber-Optic Networks

Last modified: 10/11/2022

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

Degree: **Academic year:** 2022 **ECTS Credits:** 5.0
Languages: English

LECTURER

Coordinating lecturer: Consultar aquí / See here: https://telecos.upc.edu/ca/estudis/curs-actual/professorat-responsables-coordinadors/responsables-assignatura

Others: Consultar aquí / See here: https://telecos.upc.edu/ca/estudis/curs-actual/professorat-responsables-coordinadors/professorat-assignat-idioma

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

Total learning time: 125 h

CONTENTS

1. Fiber-Optic Networks Fundamentals

Description:
Fiber-Optic Communications
- What's an Optical Fiber?
- Brief Historical Perspective
- Fiber-Optic Communications System
The Optical Layer
- Basic Photonic Devices
- Intensity Modulation / Direct Detection (IMDD)
- IQ Modulation / Coherent Detection
- Signal Propagation Through O.F.
Fiber-Optic Networks
- All Optical Networks (AON)
- Optical Networking Essentials
- Software-Defined Networks (SDN)

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

2. Security Issues in Optical Networks

Description:
Network Security
- Security layers
- Security threats
- Security tools
All Optical Networks
- AON vulnerabilities
- Types of attacks
- Network management implications
- Prevention, detection and reaction
Optical Access Networks
- Fiber-to-the-home (FTTH)
- Passive optical networks (PON)
- GPON (ITU-T G.984.3) security
Layer 1 Encryption
- Unbeatable bandwidth and latency (vs. IPSec and MacSec)
- Optical Transport Networks (OTN)
- Commercial Solutions

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
- The Ignored Security Tool
- Unconditional, Computational and Information-Theoretic security
Information-Theoretic security
- Shannon's Perfect Secrecy
- Secure Communication over Noisy Channels
- Channel Coding for Secrecy
- Secret-Key Agreement from Noisy Observations
- Comparison with Classical Cryptography
The thread of quantum computing
- The Quantum Computer
- The Problem
- Quantum Threat Timeline
- From Cbits to Qbits
- Shor's algorithm
Post-quantum cryptography
- Is Cryptography Dead?
- Challenges in Post-Quantum Cryptography
- Comparison to Quantum Cryptography
- Families of Post-Quantum Algorithms
- Post-Quantum Cryptography Standardization

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:
Optical Layer Fundamentals
- Light Properties
- Light-Matter Interaction
- Optical Fibers
- Lasers, Photodetectors and Amplifiers
- Transmitters and Receivers
Secure Communications in Fiber-Optic Networks
- Confidentiality
- Privacy
- Availability
Confidentiality/Authenticity: Optical Encryption
- Optical Code Division Multiplexing (OCDM)
- The Y-00 Stream Cipher
- Optical Key Distribution
- Spatial Division Multiplexing (SDM)

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 mechanics fundamentals
- Quantum key distribution (QKD)

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

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

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.