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

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
Lazo Villa, Jose Antonio
Spadaro, Salvatore

PRIOR SKILLS

Programming 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 specificities of optical networks regarding security issues are introduced and practical solutions are studied.

STUDY LOAD

<table>
<thead>
<tr>
<th>Type</th>
<th>Hours</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self study</td>
<td>86,0</td>
<td>68.80</td>
</tr>
<tr>
<td>Hours large group</td>
<td>33,0</td>
<td>26.40</td>
</tr>
<tr>
<td>Hours small group</td>
<td>6,0</td>
<td>4.80</td>
</tr>
</tbody>
</table>

Total learning time: 125 h
## 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: