Postgraduate Course
Secure RF Communications
(MSc)

1. Instructor Information

1. **Javier Casajús**

E-mail: javier@gaps.ssr.upm.es
Work Phone: +34 91 3367280

2. **Mariano García**

E-mail: mariano@gaps.ssr.upm.es
Work Phone: +34 91 3367269

2. Course Information

1. Course Description

This course is focused on those elements and techniques, which are susceptible to attack in RF communications systems.

It covers those techniques that can be used in electronic warfare areas such as: electronic measures and countermeasures (ECM and ECCM) in communication systems, signal intelligence (SIGINT) and communication intelligence (COMINT). Topics such as intentional interference-resistant transmission methods and low probability of interception schemes are presented as a basis for subsequent studies. The latter include the analysis and application of communication techniques that are robust when confronted to smart attacks taking advantage of signal structure: synchronism attack and follower jammer.

Additional topics present methodologies for information extraction from secure signals, namely basic transmission parameters o even the message itself. These methodologies are based on artificial intelligence concepts, so it can be used in fully automatic systems.

Finally there is a in-depth description of the theory and use of cryptographic methods for tactical, hostile environment and secure communications.

Theoretical topics will be supplemented by practical exercises and analysis of realistic cases involving numerical evaluations.

2. Prerequisites

Digital Communication fundamentals.

Radio Communications

Probability and Stochastic Processes for Engineers

In addition, a working knowledge of a computation environment (MATLAB, Octave,…) is required.

3. Course Goal

To develop a deep understanding of the concepts that underlie secure RF communications and to attain a working knowledge of systems based on them.

4. Summary of intended course outcomes

The students will understand the fundamentals and theoretical basis of RF communications in hostile environments. With this background they will be able to analyse the performance of a real system at the signal level. The work developed within the course should also enable them to carry out an assessment of communication feasibility in a tactical situation. Lastly the student should acquire a working knowledge of supporting methods for communications intelligence.

By the end of the course, students should be able to:

- Design and analyse a secure RF communication system at the system level.
- Evaluate the performance of that system at the signal and tactical levels.

5. Syllabus

1. Communication electronic warfare
    - 1.1. Electronic support, attack and protect
    - 1.2. System configuration

      Textbook based
2. Electronic attack and support
    - 2.1. Electronic attack
        - 2.1.1. Jamming
        - 2.1.2. Synchronization
        - 2.1.3. Follower jammer
    - 2.2. Support
        - 2.2.1. Low probability of detection, interception, exploitation
        - 2.2.2. Location and identification

      Based on textbook and [2]
3. Communication intelligence
    - 3.1. COMINT architectures

3.2. COMINT technology

3.2.1. Detection

3.2.2. Signal classification

Based on [3]

4. Communication protection

4.1. Cryptography

4.2. Steganography

4.2.1. Emission protection

Based on [4]

Textbook:

2. Richard A.Poisel, *Introduction to Communication Electronic Warfare Systems*, Artech House 2008.

1. Recommended reading material:

- A. Graham, *Communications, Radar and Electronic Warfare*, Wiley 2011.
- David L. Adamy, *Tactical Battlefield Communications Electronic Warfare*, Artech House 2009.
- Zhechen Zhu and Asoke K. Nandi, *Automatic Modulation Classification: Principles, Algorithms and Applications*, Wiley 2015.
- Ross J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley 2008.

Student Assessment Criteria

Test exercises	10 %
Final Exam	60 %
Analysis Project	30 %

Test exercises are assigned in lectures as homework. The analysis project is an additional assignment involving the in-depth analysis of a realistic system from different points of view: performance, robustness, feasibility; involving computational developments.