Secure aerospace communication systems at the physical layer

ISAE-SUPAERO

NICOLAS BAUDIN
INTERNSHIPS IN FRANCE INITIATIVE

Name of the hosting institution in France	ISAE Supaéro
Name of the host laboratory / research team	Department of Electronics, Optronics and Signal processing (DEOS)
Address	10, avenue Edouard Belin, 31055, Toulouse, France
Website	https://personnel.isae-supaero.fr/meryem-benammar/?lang=fr
Name of the supervisor	Meryem Benammar
Function	Associate Professor
Email	meryem.benammar@isae-supaero.fr
Phone number	0033561338320

Internship offer

Topic of the internship (title)	Secure aerospace communication systems at the physical layer			
Proposed dates of the internship*	Start:	02-2021	End	07-2021

* The supervisors have indicated the dates proposed are flexible and are able to be postponed subject to COVID-19 border closures

Scientific and academic objectives of the internship (detailed description of the internship content, work expected from the intern and expected outcomes):

In this internship, the focus will be on the analysis and implementation of a state-of-the-art based on a block linear code (Polar codes) which combines principles from information theoretic security and design criteria from error correction coding. The design will account for a variety of satellite and aeronautical communication channel models, including Gaussian channels, fading channels, and a possible generalization to multi-terminal communication settings.

The research assignment will consist first in a bibliographic study of the wiretap channel and an analysis of the design criteria of theoretical and practical wiretap codes. Then, a security analysis will be carried out through computation of the information leakage for a specific communication scheme. The results will then be implemented using Matlab (or equivalent), and possibly, a system level implementation on the locally deployed software-defined radio platform RALF.

Expected profile of applicant

Level of study	Bachelor, Master, PhD students
Discipline	Electrical engineering, Telecommunications
Required qualities, knowledge and skills	Strong background in electrical engineering and applied mathematics: -Digital communications -Information theory -Error correction coding Good implementation skills: Matlab or Python

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
AMBASSADE DE FRANCE
EN AUSTRALIE

Isae
Institut Supérieur de l'Aéronautique et de l'Espace
SUPAERO

Graduate Internship position

Secure aerospace communication systems at the physical layer

Context and research statement

Since its introduction in one of Shannon's most celebrated papers, physical layer security has proved to be a promising means of **securing communications** by exploiting the inherent **nonreproducible randomness and asymmetry** in the communication links (noisy channels, fading channels, ...) in order to create advantage of the legitimate users over the eavesdroppers. Unlike cryptographic based methods, which are applied at the upper layers of the communication protocols stack, security at the physical layer is resilient to any computational power of the eavesdropping nodes, since it does not rely on the algebraic hardness of key reproduction, e.g, prime numbers based factorization.

Whilst long regarded as a purely theoretic form of security inspired from information-theoretic analysis, in the last decades, physical layer security has substantially matured, and constructions of **secure transmission** schemes based on channel randomness and asymmetry are now provably implementable for some simple communication scenarios, e.g., Point-to- Point Binary Erasure Channels (BEC) or Binary Symmetric Channels (BSC). These constructions consist in the so-called wiretap codes, [1, 2], which are error correction codes judiciously designed to create advantage of the legitimate receivers over the eavesdroppers and thus, secure the communication.

Yet, wiretap codes constructions for more complex scenarios (multiple users, fading channel, distributed key generation,...) remain, to date, not fully explored and understood. Applications of such schemes would range from wireless communications, to more specific scenarios such as satellite and aeronautical communications.

In this internship, the focus will be on the analysis and implementation of a state-of-the-art **wiretap code** based on a block linear code (Polar codes) which combines principles from information theoretic security and design criteria from error correction coding. The design will account for a variety of satellite and aeronautical communication channel models, including Gaussian channels, fading channels, and a possible generalization to multi-terminal communication settings. The research assignment will consist first in a bibliographic search about the wiretap channel and an analysis of the design criteria of theoretical and practical wiretap codes (see [3]). Then, a security analysis will be carried out through computation of the information leakage. The results will then be implemented using Matlab (or equivalent), and possibly, a system level implementation on the locally deployed software-defined radio platform RALF.

Candidate profile and application

Applicants should be last-year research master (or/and engineer) students. A strong background in digital communications, signal processing, and applied mathematics is required since the research assignment requires tools from information theory and error correction coding. Good communication skills in English are necessary (written and oral), as well as good development skills (Matlab, C++). Applications from candidates familiar with digital communications, information theory or error correction coding are particularly encouraged.

About

ISAE-Supaero is a leading European institute in system designs for aeronautical and space applications. The internship will take place in the Department of Electronics, Optronics and Signal processing (DEOS) of ISAE-Supaero. Among the department's main research interests lies the design of "satellite communication systems with high spectral efficiency and enhanced security", and this internship is directly related to this research activity.

- Financial grant, accommodation and food services are available on the campus of ISAE.
- Dates and duration: between February and October 2021 (5 to 6 months).

References

[1] M. Hayashi and R. Matsumoto, "Construction of wiretap codes from ordinary channel codes," in *2010 IEEE International Symposium on Information Theory*, 13-18 June 2010, pp. 2538– 2542.

[2] O. O. Koyluoglu and H. El Gamal, "Polar coding for secure transmission and key agreement," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1472–1483, 2012.

[3] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.