Graduate Internship position

Wiretap codes: analysis and design criteria

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 **non-reproducible randomness** in the communication links (noisy channels, fading channels, ...) in order to create advantage of the legitimate users over the eavesdroppers.

Whilst long regarded as a purely theoretic form of security inspired from information-theoretic analysis, in the last decades, physical layer security has substancially matured and constructions of **secure transmission** schemes based on channel randomness are now provably implementable for some simple communication scenarios. 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.

In this internship, the focus will be on the analysis and implementation of a state-of-the-art **wiretap code** which combines principles from information theoretic security and design criteria from error correction coding. The research assignement consists first in a bibliographic search about the wiretap channel and an analysis of the design criteria of practical wiretap codes (see [3]). Then, the results will be implemented using Matlab (or equivalent), and possibly, a system level implementation on the locally deployed software-defined radio plateform 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 assignement 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 corrrection coding are particularly encouraged.

Applications (CV, cover letter) are to be addressed to {meryem.benammar,damien.roque}@isae-supaero.fr, and tarik.benaddi@imt-atlantique.fr.

Useful information...

- Financial grant and accommodation and food services are available on the campus.
- Dates and duration: between January and September 2018 (5 to 6 months).
- **Application deadline: 17-Jan-2018**.

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.