School of Computing, Engineering, and the Built Environment
Edinburgh Napier University

PHD STUDENT PROJECT

Application instructions:
Detailed instructions are available at :
https://www.napier.ac.uk/research-and-innovation/doctoral-college/how-to-apply

Prospective candidates are encouraged to contact the Director of Studies (see details below) to discuss the project and their suitability for it.

Project details

Supervisory Team:

- Director of Study: Prof Petros Karadimas (Email: p.karadimas@napier.ac.uk)
- 2ND SUPERVISOR: tbc

Subject Group: Cyber Security and Systems Engineering

Research Areas: Communications Engineering, Electrical Engineering, Electronic Engineering, Systems Engineering

Project Title: Adaptive physical layer security for connected autonomous vehicles

Project description:

Secure data exchange between vehicles is one of the greatest technical challenges pending to be addressed prior to mass production of fully autonomous vehicles. The security solution has to be energy-efficient and adaptable to any wireless propagation environment in which connected autonomous vehicles (CAVs) operate. The proposed communication security solution relies on symmetric cryptographic key establishment by exploiting the physical layer characteristics of the wireless propagation environment. In the international literature, it has been named as physical layer security (PLS) and proven to be an ideal candidate for secure communications with strict constrains on computational resources and power consumption. Starting from a very thorough literature review, the PhD candidate will have to understand and become familiar with the most recent advances of PLS and how PLS can be applied in CAVs. Accordingly, the PhD candidate will have to understand the state-of-the-art algorithms and steps involved in the key establishment process, including vehicular channel modeling,

estimation, and simulation, received signal quantization, information reconciliation, privacy amplification. The ultimate goal is to devise a symmetric cryptographic key establishment algorithm and adapt it to the state-of-the-art standards of future vehicular communications, that is, the IEEE 80211.bd and NR V2X evolutions. The symmetric keys can then be used for essential security operations in CAVs, such as encryption and authentication.

References

1. M. Bloch and J. Barros, “Physical-layer security: from information theory to security engineering,” Cambridge University Press, 2011.

2. M. Bottarelli, P. Karadimas, G. Epiphaniou, D. K. B. Ismail and C. Maple, “Adaptive and Optimum Secret Key Establishment for Secure Vehicular Communications,” IEEE Transactions on Vehicular Technology, vol. 70, no. 3, pp. 2310-2321, March 2021.

3. M. A. Shawky, M. Bottarelli, G. Epiphaniou and P. Karadimas, “An Efficient Cross-Layer Authentication Scheme for Secure Communication in Vehicular Ad-Hoc Networks,” IEEE Transactions on Vehicular Technology, vol. 72, no. 7, pp. 8738-8754, July 2023.

Candidate characteristics

Education:

Minimum 2:1 degree Electrical/Electronic/Communications Engineering, Computer Science/Engineering, Mathematics

Subject knowledge:

Communication Principles, Digital Communications, Cryptography, Algorithms, Programming

Essential attributes:

- Knowledge of Communication Principles, Digital Communications, Cryptography, Algorithms, Programming
- Competent in Programming and Software Engineering
- Strong motivation with evidence of independent research skills relevant to the project
- Good written and oral communication skills
- Good time management

Desirable attributes:

- Experience with programming environments such as Matlab, C, C++