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

PHD STUDENT PROJECT

Funding and application details

Funding status: Self funded students only

Application instructions:
Detailed instructions are available at https://blogs.napier.ac.uk/scebe-research/available-phd-student-projects/

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: Petros Karadimas (Email: P.Karadimas@napier.ac.uk)
- 2ND SUPERVISOR:

Subject Group: Cyber-security and system engineering

Research Areas: Cyber Security, Networks, Software Engineering, Communications Engineering, Electrical Engineering, Electronic Engineering, Applied Mathematics, Engineering Mathematics, Mathematical Modelling, Probability, Pure Mathematics, Statistics, Stochastic Processes

Project Title: Physical layer security for connected autonomous vehicles

Project description:

Secure data exchange between communicating 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 and authentication enhancement 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 in PLS and how this can be implemented in CAVs. Accordingly, the PhD candidate will have to understand the algorithmic solutions and steps involved in the key establishment and authentication enhancement processes, including vehicular channel modeling, estimation, and simulation, received signal quantization, information reconciliation and privacy amplification. The final goal is to develop a symmetric cryptographic key establishment algorithm and evaluate its performance according to certain key performance indicators such as the key generation rate and key entropy. The symmetric key 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:

A first-class honours degree, or a distinction at master level, or equivalent achievements in Electrical/Electronic Engineering, Computer Science, or Mathematics

Subject knowledge:

- Communication Principles
- Digital Communications
- Wireless Security
- Cryptography
- Algorithms
- Programming

Essential attributes:

- Good written and oral communication skills
- Strong motivation with evidence of independent research skills relevant to the project
- Good time management

Desirable attributes:

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