| | |
|---|---|
| **Department** | School of Computing |
| **Supervisors** | Petros Karadimas |
| | |
| | |
| **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 design 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.

**Academic qualifications**

A first degree (at least a 2.1) ideally in Electrical/Electronic/Communications Engineering, Computer Science/Engineering, Mathematics with a good fundamental knowledge of Communication Principles, Digital Communications, Cryptography, Algorithms, Programming.

**English language requirement**

IELTS score must be at least 6.5 (with not less than 6.0 in each of the four components). Other, equivalent qualifications will be accepted. Full details of the University's policy are available online.

**Essential attributes:**

- Experience of fundamental Wireless Communications and Security
- Competent in Programming and Software Engineering
- Knowledge of Communication Principles, Digital Communications, Cryptography, Algorithms
- 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 tools and environments such as Matlab, C, C++. | |
| **Indicative Bibliography** | 1. Bloch M, Barros J. Physical-layer security: from information theory to security engineering. Cambridge University Press; 2011.<br>2. M. Bottarelli, P. Karadimas, G. Epiphaniou, D. K. B. Ismail and C. Maple, "Adaptive and Optimum Secret Key Establishment for Secure Vehicular Communications," in *IEEE Transactions on Vehicular Technology*, vol. 70, no. 3, pp. 2310-2321, March 2021. |
| | |
| **Enquiries** | For informal enquiries about this PhD project, please contact Dr Petros Karadimas, email: pkaradimas@napier.ac.uk |
| **Web page** | https://www.napier.ac.uk/research-and-innovation/research-degrees/application-process |