Department	School of Computing
Supervisors	Dr Zhiyuan Tan, Dr Chan Hwang See, Dr Jawad Ahmad
Project Title	Security and Privacy in Vehicular Ad-hoc Networks

PROJECT DESCRIPTION

The great leap forward in wireless communications technology drives the recent advancements of Vehicular Ad hoc NETworks (VANETs). As a key part of the Intelligent Transportation Systems (ITS) framework, VANETs offer active road safety, and traffic efficiency and management. However, they are not free of security and privacy issues by design.

This project aims to address three critical challenges of VANETs. 1) Protecting a vehicle's secret key from being physically stolen: A secret key is required for vehicle authentication and data security. The key is usually stored in Non-Volatile Memory (NVM) but threaten by physical acquisition. 2) Protecting vehicle route information from being leaked to other vehicles, roadside units and even certificate centres: Vehicle's route information is drivers' personal data needing to be protected in compliance with GDPR. 3) Protecting traffic trajectories from being exposed to a route planning server: It is critical to balance the usability and privacy of traffic trajectories as it is an important public resource and personal data of drivers. Therefore, the project seeks to overcome these challenges through PUF-based security authentication, as well as privacy protection in route planning and trajectory publishing.

Based on the vital roles of VANETs in life, economy, smart city, and society, the proposed project will promise to generate significant economic and societal impacts once it is completed and adopted by intelligent transportation infrastructure. Additionally, the research outcomes of this project will provide solid theoretical guidance for the further development of security and privacy in the VANETs.

Academic qualifications

A first degree (at least a 2.1) ideally in Electronic Engineering or Computer Science with a good fundamental knowledge of Cybersecurity.

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 cybersecurity or system security
- Competent in programming and critical analysis
- Knowledge of machine learning
- Good written and oral communication skills
- Strong motivation, with evidence of independent research skills relevant to the project
- Good time management

Desirable attributes:

- Experience in security and privacy research
- Preliminary experience in Generative Adversarial Network (GAN)

Indicative Bibliography	- Cai, Z., Xiong, Z., Xu, H., Wang, P., Li, W., & Pan, Y. (2021). Generative adversarial networks: A survey toward private and secure applications. ACM Computing Surveys (CSUR), 54(6), 1-38. - Shamsoshoara, A., Korenda, A., Afghah, F., & Zeadally, S. (2020). A survey on physical unclonable function (PUF)-based security solutions for Internet of Things. Computer Networks, 183, 107593. - Aloufi, A., Hu, P., Song, Y., & Lauter, K. (2021). Computing Blindfolded on Data Homomorphically Encrypted under Multiple Keys: A Survey. ACM Computing Surveys (CSUR), 54(9), 1-37.
Enquiries	For informal enquiries about this PhD project, please contact Dr Zhiyuan Tan z.tan@napier.ac.uk
Web page	https://www.napier.ac.uk/research-and-innovation/research-degrees/application-process