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 Leandros Maglaras (Email: l.maglaras@napier.ac.uk)
- 2ND SUPERVISOR: Prof Bill Buchanan

Subject Group: Cyber-Security and System Engineering

Research Areas: Cyber Security

Project Title: Secure V2V Communication for self-driving NETworks

Project description:

The project aims at designing an integrated end-to-end VANET (+ UAV) Simulation Framework which gets feedback from relevant traffic applications that actually simulate a realistic VANET environment. The proposed framework is designed to emulate complex V2X scenarios by incorporating real hardware. Physical On-Board Units (OBUs) and RSUs are connected to a computer that is running the proposed simulation framework. For each physical device connected to the computer, there is a corresponding virtual OBU or RSU in the simulation.

The project objectives are:

- Simulation of a hybridic network with the integration of Dedicated Short Range Communication (DSRC) with the V2X-LTE technology.
- Reproduction of Denial of Service (Dos) and Distributed Denial of Service (DDoS) attacks in the proposed simulator.
- Utilize a probabilistic cross-layer IDSs for DoS/DDoS attack detection in the overall simulation framework stack.
- Create novel anti-jamming techniques.

References:

[1] D. Kosmanos et al., "Intrusion Detection System for Platooning Connected Autonomous Vehicles," 2019 4th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Piraeus, Greece, 2019, pp. 1-9

[2] Iman Almomani, Mohanned Ahmad, Dimitrios Kosmanos, Aala Alkhayer, Leandros Maglaras, "An Efficient Localization and Avoidance Method of Jammers in Vehicular Ad hoc Networks", IEEE Access, December 2022, DOI: 10.1109/ACCESS.2022.3229623

[3] Dimitrios Kosmanos, Dimitrios Karagiannis, Antonios Argyriou, Spyros Lalis, Leandros Maglaras, "RF Jamming Classification using Relative Speed Estimation in Vehicular Wireless Networks", Security and Communication Networks (Hindawi, Wiley), August 2021, DOI: 10.1155/2021/9959310

[4] Dimitrios Kosmanos, Apostolos Pappas, Leandros Maglaras, Sotiris Moschoyiannis, Francisco J. Navarro, Antonios Argyriou and Helge Janicke, "A Novel Intrusion Detection System Against Spoofing Attacks in Connected Electric Vehicles", Elsevier Array, Vol. 5, March 2020, DOI: 10.1016/j.array.2019.100013

Candidate characteristics

Education:

A second class honour degree or equivalent qualification in Electrical / Electronic / Communications Engineering, Computer Science/Engineering, Mathematics with a good fundamental knowledge of Network Communication Principles, Digital Communications, software engineering

Subject knowledge:

- Wireless communications, OMNET++, communication protocols, Jamming and DDOS attacks

Essential attributes:

- Experience of cybersecurity attacks and defenses
- Competent in software development
- Knowledge of wireless communication principles, protocols, algorithms
- Good written and oral communication skills
- Strong motivation, with evidence of independent research skills relevant to the project
- Good time management

Desirable attributes:

- Team player, eager to learn new technologies, flexible and knowledge of Python, R or Matlab.