Title of Proposed PhD Research:

An Evaluation, Simulation and Improvement of an Autonomous Vehicles Communications Security over 5G Technology.

PhD Principal Supervisor and Second Supervior:

Principal Supervior: Dr. Myasar Tabany.

Second Supervior: TBA.

Contact: Please email: m.tabany@herts.ac.uk for more information.

Introduction:

Traffic accidents are often caused by human error, including driver inattention, distraction, reckless driving, and poor driving ability, as well as road user errors like traffic violations. Road safety can also be impacted by vehicle failures (e.g., brake failure) and environmental conditions (e.g., lack of traffic information). Connected and Autonomous Vehicles (AV) are a new type of vehicle introduced to improve traffic efficiency, reduce congestion, and promote sustainable transportation development, CAVs's reference architecture shown in fig.1. Fully autonomous vehicles use automated driving systems. It can travel with passengers on any type of road without human assistance [1]. Autonomous vehicles provide safe transportation for passengers while also protecting other road users.

The development of this vehicle requires a staged approach from administrations and car manufacturers. They create cars with varying levels of autonomy, ranging from zero (no self-driving) to five (full self-driving). The Internet of Things, cloud computing, wireless technologies, artificial intelligence, and other cutting-edge information technologies are all applied to a new concept and model brought about by autonomous vehicles. AV uses a variety of sensors in addition to those

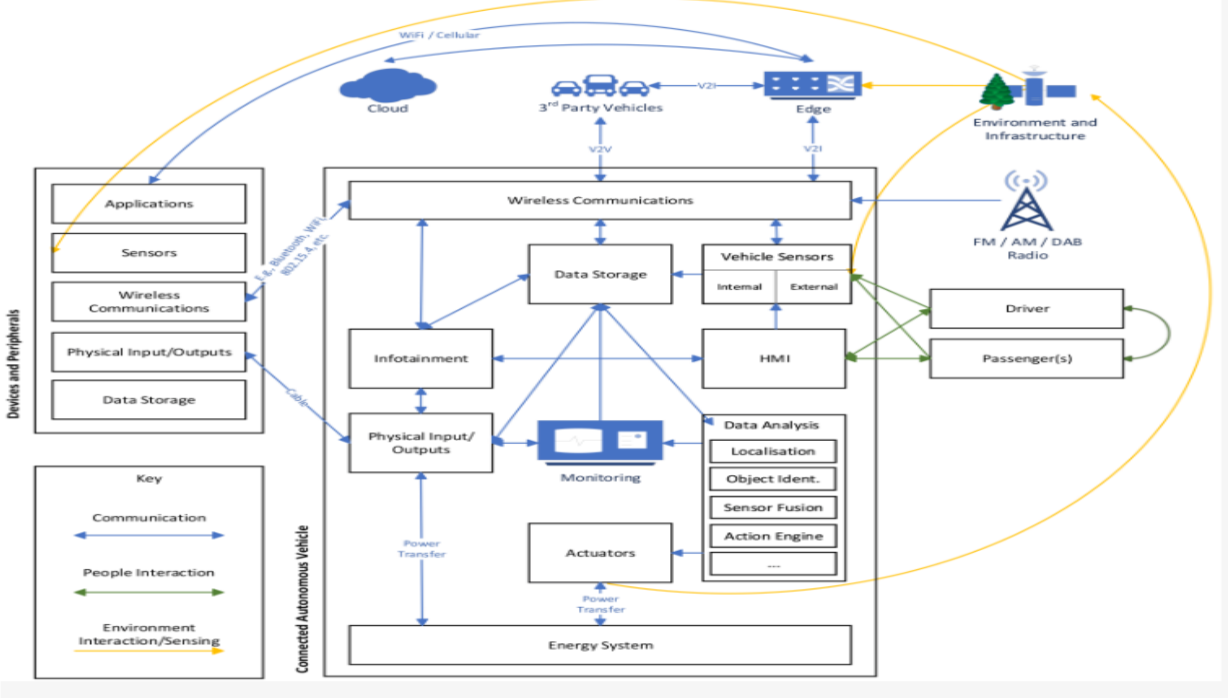

Fig1. Connected and Autonomous Vehicles (CAVs) Technology Reference Architecture [2]

The fifth generation (5G) is an emerging solution for addressing the current vehicular network challenges because it can provide efficient, reliable, and timely communications to all vehicles and their embedded sensors. Fig. 1 overview a general 5G cellular network architecture [4]. The Internet of Vehicles has high requirements, including high data rate, low latency, and high reliability. The Internet of Vehicles (IoV) will facilitate various forms of communication, including Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), Vehicle to Cloud (V2N), and Vehicle to Pedestrian (V2P), owing to the emergence of new technologies in the fifth generation. But with all of these technologies and communication channels in place, the 5G IoV environment open to different attacks such as man in the middle, Sybil, and Denial of Service (DoS) attacks [5].

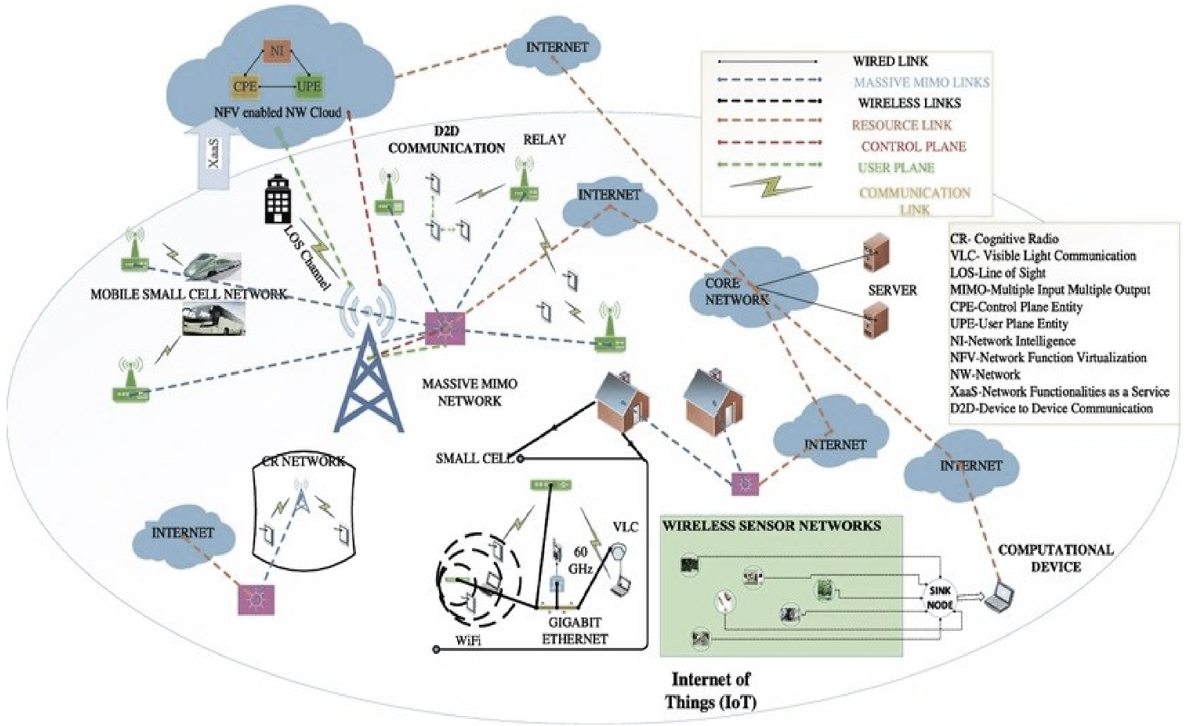

Fig. 2 An overview of the general 5G cellular network architecture [4]

Research Questions:

1. How can 5G technology support real-time communications for autonomous vehicles in a cyber security environment, as well as analyse and assess potential cyber threats.
2. Propose and implement/ simulate a novel communications platform that makes use of 5G technology capabilities to enhance real-time communication security while maintaining the highest standards of the system capacity, mobility, and reliability.

Aims and Objectives:

1. Simulate an autonomous vehicles network scenario that used 5G for real time communications and evaluate the security features against standard cybersecurity attacks.
2. Propose, design, and simulate a novel end to end security communications platform over autonomous vehicles that can helps overcome several 5G security limitations.

Proposed Work:

Due to the interference form so many other networks with the autonomous vehicles, which mean increasing the attack surface, a solid and more reliable security platform is vital for this human life-threating application. The 5G networks are still in the early phases of development, security protocols and best practices are still not standardised, and since various vendors and operators are using different versions of the technology, it can be challenging to guarantee that all systems and devices are completely compatible with one another. This may result in disparities in security between various networks, opening doors for hackers to take advantage of.

The novel proposed platform must focus on the increased number of networks involved on the autonomous and connected vehicles as well as the main limitations of the 5G security communication protocols. The proposed security end to end platform should consider the outcome of the critical analysis and evaluations to the state of the art of the Autonomous vehicles 5G communications and hence update the proposed platform based on addressing those critical vulnerabilities.

References:

[1] Lu, R., Zhang, L., Ni, J., & Fang, Y. (2020). 5G Vehicle to Everything Services: Gearing Up for Security and Privacy. Proceedings of the IEEE, 108(2), 373-389.

[2] Carsten M., Matthew B., Anh L. and Kevin G. (2019), A Connected and Autonomous Vehicle Reference Architecture for Attack Surface Analysis,
Applied Sciences, V9, 5101; doi:10.3390/app9235101.

[3] Ahangar, M. N., Ahmed, Q. Z., Khan, F. A., & Hafeez, M. (2021). A Survey of Autonomous Vehicles: Enabling Communication Technologies and Challenges. Sensors, 21(3), Art. 3.

[4] Gupta A. and Jha R. K. (2015), A Survey of 5G Network: Architecture and Emerging Technologies, IEEE Access, Volume: 3.

[5] Wu, Xu and Bilal (2022), Security and Privacy on the Internet of Vehicles (IoV): Toward Privacy Protection Composition Framework on Internet of Vehicles, IEEE Consumer Electronics Magazine, Volume: 11, Issue: 6.