# Performance and security in VANETs

**Contact**
Dr Nigel Thomas, nigel.thomas@newcastle.ac.uk

**Research project**
Wireless networks are used for a wide range of applications in a wide range of operating scenarios. Clearly, it is infeasible to expect that a given network protocol will perform well in all situations, as protocol are typically designed to perform well in respect to a limited set of performance metrics under a limited set of operating conditions. It is therefore necessary to understand the limitations of such protocols in terms of factors such as fairness and energy, when the network topology is sub-optimal or where nodes are misbehaving, for example when compromised due to infection by a virus or a fault, or subject to a denial-of-service attack.

VANETs are a specific form of wireless network used for vehicle-to-vehicle communications. VANET services may be delivered by traditional wireless protocols, such as 802.11p, or cellular networks. They may also involve roadside communication infrastructure and might be augmented by the use of drones. VANETs are used for numerous applications, including platooning (vehicle convoys) and safety (road traffic) information, as well as other network services. Attacks against these applications have safety implications for the vehicles involved and so maintaining performance in the presence of attack and misbehaviour is of critical importance [1].

Security measures impose a performance overhead, as more work needs to be done in order to perform operations such as authentication, encryption and recording transactions. Understanding this overhead is vital in order to make intelligent choices in the design of secure systems. Of particular interest is the performance effect of attacks against the system. Choosing the right security measures and a good protocol enables the system to maintain an acceptable performance even when under attack [2].

The aim of this project is to study network applications in VANETs under different forms of attack and to investigate the overheads of different defensive measures. There is considerable scope to vary the project according to specific interests of the candidate.

**Applicant skills/background**
Knowledge of computer networks, alongside good numerical and programming skills are essential. Experience using network simulation tools such as OMNET++, NS3 and SUMO would be a distinct advantage.

**References**
[1] H. Laghbi, S. Alateef, N. Thomas, The Impact of Resource DoS and Propagation Loss on VANET Routing, 39th Annual UK Performance Engineering Workshop, 2023.
[2] H. Jari, A. Alzahrani, N. Thomas, A novel indirect trust mechanism for addressing black hole attacks in MANET, Proceedings of the 11th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, 2021.