Cyber Security for Autonomous Vehicle

Security is one of the critical challenges of Autonomous Vehicles (AV) technology. Any failure of AV may result in severe human injuries or even death. An autonomous vehicle consists of a myriad of heterogeneous components, both cyber and physical, which gives to additional security challenges. The complex interactions between these components inside the AV make it difficult to model the system and the adversary. To make the matter worse, autonomous vehicles from different manufacturers are likely to have different architectures and components, which makes the modelling task even more challenging. The inertia of the physical components implies that an AV cannot be easily stopped when under an attack. Therefore, the successful AV system needs to be able to respond and adapt to new security threats (even unknown zero-day threats) while guaranteeing safety of operation in real time. The overarching goal of our research is to provide novel solutions to address the security challenges raised by autonomous vehicles. Hence, we aim to achieve the following research objectives.

1. To develop a modelling approach for assuring security in autonomous vehicles from six aspects: standards, structure, functions, failures, attacks and countermeasures. These aspects will be aligned in a consistent manner and in compliance with international autonomous vehicle standards;

2. To develop resilient and efficient run-time fault detection, estimation and control algorithm that provide performance guarantee and degrade gracefully in the presence of malicious attacks.

3. To develop run-time attack detection, self-adaptation and incremental verification algorithms for continuously protecting autonomous vehicles from faults and attacks while ensuring the trustworthiness and security of autonomous vehicles

4. To integrate all the research results and implement them on the NTU robotics platform to demonstrate the feasibility of the proposed approaches

An AV is composed of a physical system (mainly the mechanical systems), sensing units, control units and actuation units, which are connected via CAN bus. The AV will also include other modules such as the infotainment system, which should not interfere with the autonomous driving. Finally, wireless communication module will be include to enable vehicle to vehicle and vehicle to infrastructure communication to increase the situational awareness of AV. Our proposed secure AV architecture is illustrated in Fig 1. The red modules (monitoring and adaption) are the new modules that will be developed in the proposed project. The blue modules (estimation/navigation) are the existing modules that will be enhanced with security features to ensure that they are resilient to malicious attack.

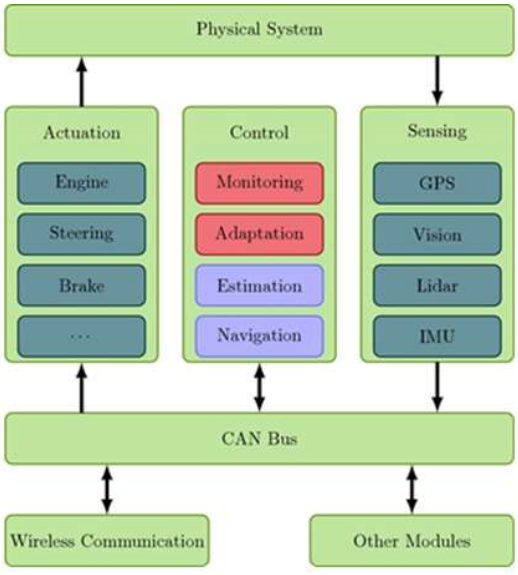

Figure 1. Secure autonomous vehicles architecture.

We will demonstrate that the secure AV platform can withstand and recover from the attack and ensures the performance and safety of the vehicle (collision avoidance) using the following countermeasures:

1. Monitoring: - To provide better security measures, we will implement two monitoring schemes – 'Model-based intrusion detection' and 'Logic-based intrusion detection'.

2. Resilient Estimation and Control: The goal is to ensure that the system is safe before detecting the malicious components. This is done by designing robust estimation and control algorithms.

3. Adaptation: The goal is to make the system to adaptively change its behaviour after the detection of malicious components. This is done by isolating the malicious component and switching the control algorithms to the new system architecture.

In summary, our research is aimed at advancing research in the area of developing safe and secure autonomous vehicles, which will be able to withstand not only accidental failures, but also malicious cyberattacks, while providing required functions and performance. We will also achieve this by jointly addressing and integrating inter-related dimensions of autonomous vehicles, such as international AV standards, functions, structure, safety, security, and other non-functional aspects.

Principal Investigator	Asst. Prof. Mo Yilin *(EEE)* Asst. Prof. Liu Yang *(SCSE)* Prof. Wang Danwei *(EEE)* Dr. Giedre Sabaliauskaite *(SUTD)*
Researcher	Dr. Liu Xinghua Dr. Ren Xiaoqiang Dr. Chen Bihuan
Student	Mr Cheng Kun Mr Mihankhah Ehsan
School / Department	School of Electrical and Electronic Engineering
Collaborator	California Institute of Technology
Source of Funding	Future Systems and Technology Directorate (FSTD), MINDEF