Title: Attacks detection and cyber resilience: securing in-vehicle controller area network

Abstract: Nowadays, connected vehicles can communicate through wireless networks through the internet, road infrastructure, and other vehicles. The ECUs that control the behavior of each of these vehicles communicate through the CAN Bus, which is widely used in automotive, aerospace, and many other industries because of its low cost, error detection capability, and reliability. The CAN bus protocol was designed more than 40 years ago and does not include security measures such as authentication, which makes it target to unauthorized access and use.

Researchers proposed two categories of solutions to address this problem: security extension for the CAN bus and IDS solutions. Unlike the first category of solutions, the second category does not need to alter the CAN protocol and could be used for after-market vehicles. Currently, most of existing practical IDS solutions (1) rely on the knowledge of the identities of the ECUs of the given vehicle, which is proprietary information, (2) evaluate their efficacy in terms of accuracy in detecting message injections offline, which limits the confidence in their use for real-time protection scenarios, and (3) do not assess their efficacy to preserve vehicle safety measures.

This thesis proposes an IDS solution for connected vehicles that is independent of the identities of the ECUs, assesses the performance of the IDS for real-time attack detection, and explores its use to avoid accidents through an extension to the adaptive cruise control mechanism as a real-time resilience mechanism to cyber-attacks. First, we represent the sequencing of the messages that the ECUs of a given vehicle exchange in the CAN bus in successive time intervals as direct graphs and use the changes to the similarities of the successive graphs to detect malicious message injections into the CAN bus. Secondly, we simulated four real-time IDS architecture alternatives for connected vehicles and evaluated their efficacy in terms of the percentage of messages lost due to the service/arrival rate of the CAN messages and attack identification time. Third, we showed through simulations that the injection of CAN messages could mislead the ACC system to induce a collision of the simulated vehicle with the near-by vehicle, and the capability of the proposed real-time IDS to avoid that by applying an emergency brake to avoid a crash when it detects CAN Bus message injection.

The assessment of the IDS using datasets collected from a moving vehicle subjected to CAN bus spoofing that changed its behavior and the evaluation of the efficacy of ACC extension to avoid accidents using the proposed IDS demonstrate the possibility of using machine-learning IDS for resilience to cyber-attacks on connected vehicles. The evaluation of the efficacy of the real-time IDS and ACC extension using simulations may not justify their use in practice yet. Further research needs to be performed to assess the efficacy of the proposed solutions for resilience to cyber-attacks in real scenarios.