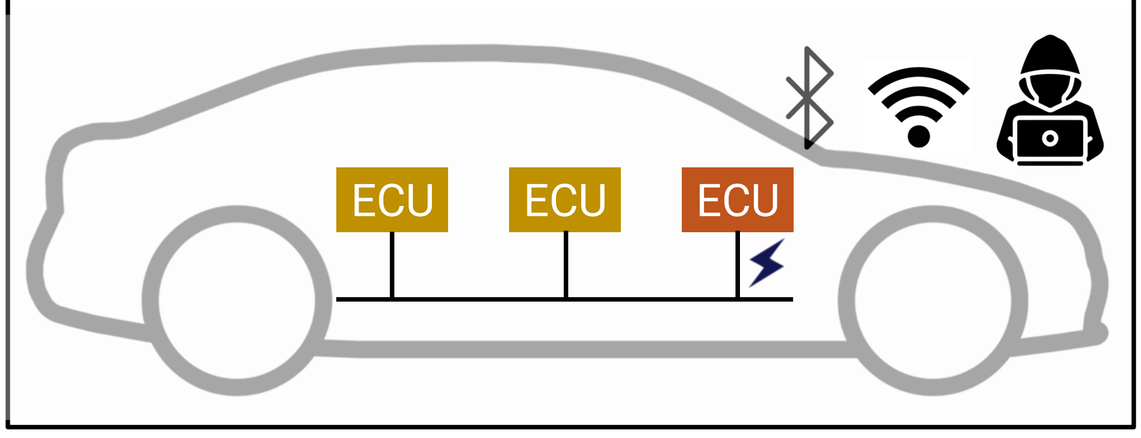
Intrusion Detection and Prevention System for Controller Area Network

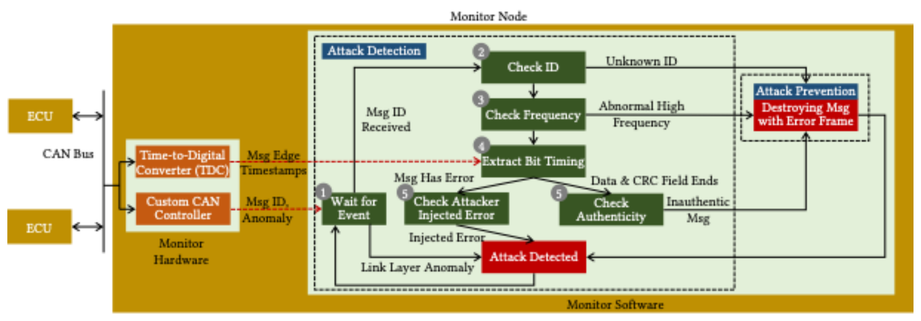
Problem Statement and Goals

- Controller Area Network (CAN) is the most widely-used in-vehicle network protocol
- It allows Electronic Control Units (ECU) to communicate and control vehicle operations
- Increased ECU connectivity makes CAN vulnerable to cyberattacks
- Our goal is to design an Intrusion Detection and Prevention System for CAN against remote attackers controlling in-vehicle ECUs

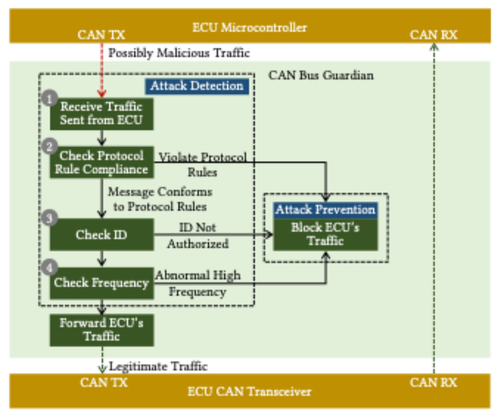


Approach

- CAN bus monitor
  - Single node to monitor bus events



- CAN bus guardian
  - Hardware monitoring each ECU's activity



Results

- Experimented on testbed and real vehicle
- Tested common CAN attacks
  - E.g., Spoofing/replay, fuzzing, flooding, error injection
- CAN bus monitor
  - 99.8+% detection for 10 CAN attacks
  - Guaranteed prevention for 4 attacks
- CAN bus guardian
  - Deterministic detection & prevention for 11 attacks
- Future work
  - Leverage more traffic features to detect other classes of attacks
- Acknowledgements
  - This research is funded by Hyundai America Technical Center, Inc.

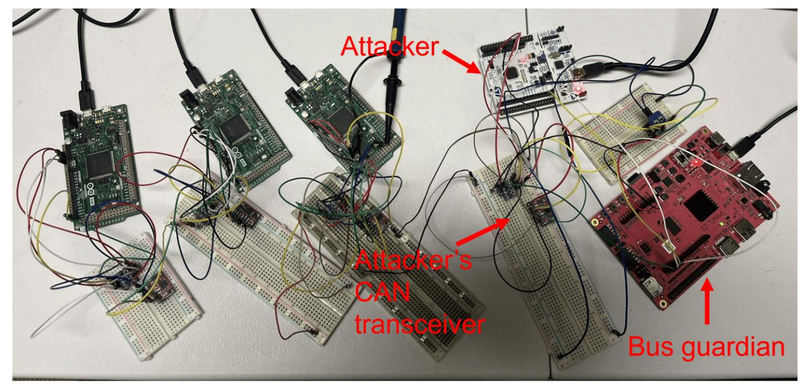


Figure 1. Testbed experiments

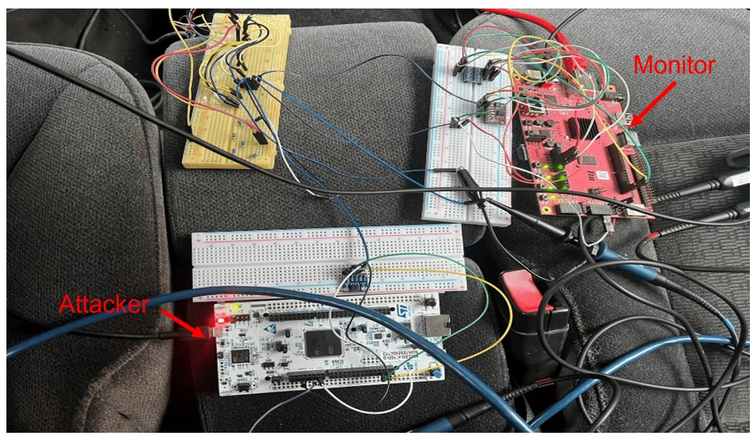


Figure 2. Real vehicle experiments

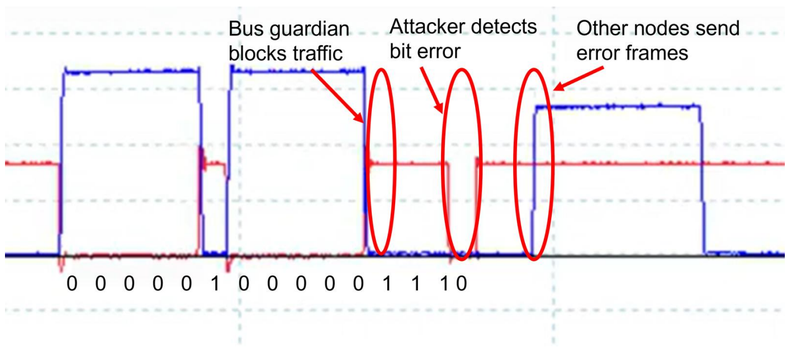


Figure 3. Detecting and preventing spoofing attacks

Zhaozhou Tang
Georgia Institute of Technology

Intrusion Detection and Prevention System for Controller Area Network

Abstract

The Controller Area Network (CAN) is a critical network protocol extensively utilized in vehicles, allowing Electronic Control Units (ECUs) to communicate and control a vehicle's operations. Modern ECUs offer increased external connectivity, such as WiFi, Bluetooth, and Cellular. Researchers have demonstrated that malicious attackers could exploit such connectivity channels to compromise in-vehicle ECUs and gain access to a vehicle's CAN bus. Since CAN does not offer any built-in security mechanism, attackers can launch a wide range of attacks by manipulating CAN traffic, which pose severe dangers to vehicle users.

In this research, we design Intrusion Detection and Prevention Systems (IDPS) for CAN. We propose two IDPS designs. First, we propose the CAN bus monitor. It is a single node attached to a CAN bus in parallel. It offers detection for most common CAN attacks and prevention when possible, by comprehensively monitoring bus traffic patterns and low-level events. Second, we propose the CAN bus guardian. It is a piece of hardware installed between each ECU and the CAN bus. It offers both detection and prevention for common CAN attacks by monitoring each ECU's activity.

We have implemented both designs and evaluated them on a testbed and real vehicle. The CAN bus monitor offers real-time detection for 10 CAN attacks with 99.8+% accuracy and guaranteed prevention for 4 attacks. The CAN bus guardian offers deterministic detection and prevention for 11 CAN attacks.

Zhaozhou Tang
Georgia Institute of Technology