Securing Automotive Networks with Vehicle-Agnostic Technologies

Samuel C. Hollifield, Robert A. Bridges, Miki E. Verma, Michael Iannacone, Sheikh Ghafoor

Controller Area Networks (CANs)

The CAN Bus exists as the primary network in modern automobiles. It accounts for communication between electronic control units.

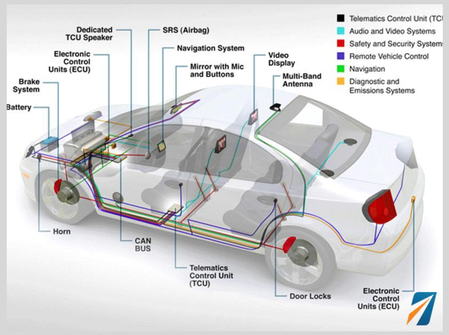


Photo credit: www.fleetistics.com/wp-content/uploads/2016/11/Telematics-Vehicle-Network-System.png

Problem

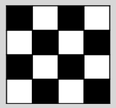
- Despite being used for critical communications, the CAN is vulnerable to exploitation.
- Previous research has shown vulnerabilities in receiving, injecting, and even remotely accessing vehicles via CANs.
- Cybersecurity solutions that can accomodate all vehicles with CAN are needed.
- Translation of CAN data to encoded signals is proprietary, secret, and unique per make, model, year, and trim.

Approach

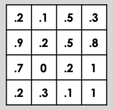
- Develop a vehicle-agnostic CAN intrusion detection system.
  - Use off-the-shelf supplies to build low cost units
  - Understand the signals hidden within obfuscated networks.
  - Use this understanding to inform Intrusion Detection Systems (IDS) for anomalous signal content
- Prototype IDS on a lightweight OBD-II plugin device.
  - Signal-based vs. Payload-based
  - Supervised learning vs. Unsupervised learning
  - Content-based vs. Timing-based

Understanding Signals in Obfuscated CANs

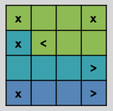
To understand signals in an obfuscated CAN, we present ACTT: Automotive CAN Tokenization and Translation



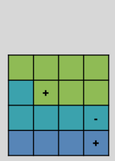
1. Learn Signal Boundaries — Get probability of cut between each bit in network trace using various classification methods



2. Pack Big/Little Endian Tokens — Run Token Packing Optimization to identify endianness of the message.



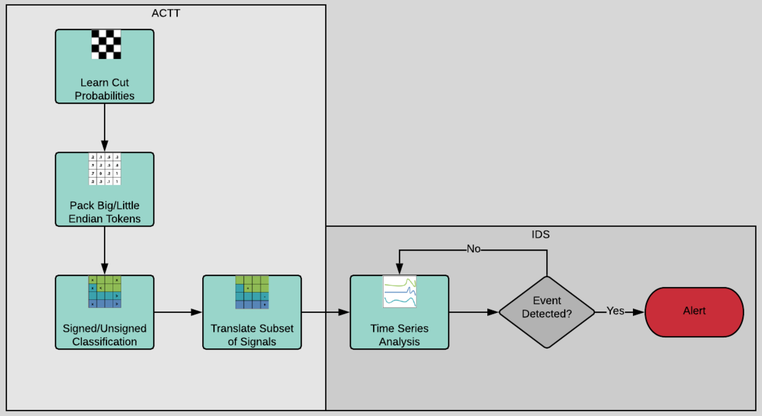
3. Signed/Unsigned Classification — Classify each token as signed/unsigned using various classification methods



4. Diagnostic Matching — Determine if any token signal is linearly related to any available diagnostic signal

Using ACTT to Test and Develop Vehicle-Agnostic IDS

Step 1. Extract encoded signals using ACTT2.0 to time series.
Step 2. Perform time series anomaly detection.



Acknowledgements

Special thanks to B. Kay for guidance and thoughtful conversation.
Research sponsored by the Laboratory Directed Research and Development Program of Oak Ridge National Laboratory, managed by UT-Battelle, LLC, for the U. S. Department of Energy.

OAK RIDGE NATIONAL LABORATORY
MANAGED BY UT-BATTELLE FOR THE DEPARTMENT OF ENERGY

Future Work

- Test different methods for intrusion detection. Once we compare these technologies, we can better inform our detector as to which system is best for a given intrusion.
- Implement hardware prototype:
  - Automatically collect CAN data from vehicle.
  - Use ACTT2.0 to build a translation dictionary for the given vehicle.
  - Implement a suite of complementary time-series anomaly detectors.
  - Create a UI for alerting and visualizing translated CAN data.

Conclusions

Signal Extractions

- Our methods to extract signals from obfuscated CANs exceeds current state-of-the-art methods
- The availability of this tool will accelerate signal-based approaches to secure in-vehicle networks.
- We are using ACTT2.0 for intrusion detection on automobiles, but it can be useful for any system which operates with a CAN.

Intrusion Detection System

- With an ACTT-informed IDS, we can use signal-based detectors with high fidelity to pinpoint intrusions.
- We believe signal-based detectors will perform better than payload-based detectors and our comparative study will allow us to test this hypothesis.

Contact Information

- Samuel C. Hollifield[1,2], schollifie42@students.tntech.edu, hollifieldsc@ornl.gov
- Robert A. Bridges[1], bridgesra@ornl.gov
- Miki E. Verma[1], vermake@ornl.gov
- Michael Iannacone[1], iannaconemd@ornl.gov
- Sheikh Ghafoor[2], sghafoor@tntech.edu

[1] Cyber and Applied Data Analytics Division.
Oak Ridge National Laboratory

[2] Tennessee Technological University