A Framework for Detection of Anomalies in Sensor Data for Prevention of Cyber Attacks in Connected Autonomous Vehicles

Keane Fernandes

University of Bristol

September 6, 2021

Background

- Pollution, congestion, road accidents
- The solution – smart cities
- Enabled by V2X – a communications platform

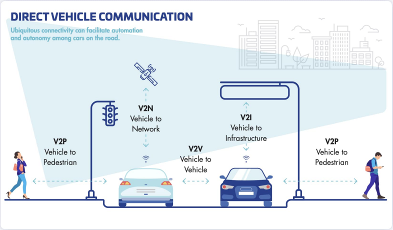

DIRECT VEHICLE COMMUNICATION
Ubiquitous connectivity can facilitate automation and autonomy among cars on the road.
V2N
Vehicle to Network
V2I
Vehicle to Infrastructure
V2P
Vehicle to Pedestrian
V2V
Vehicle to Vehicle
V2P
Vehicle to Pedestrian

Figure 1: A V2X enabled smart city.

Motivation

- Today's car – over 150 ECUs
- Wi-Fi hotspots, bluetooth enabled infotainment systems – increase in attack surfaces
- Cyber security standards – lagging behind
- Incentive now exists to break into car – valuable personal information held

Figure 2: A vehicle of the future.

Project Overview

- Aim - implement an automated knowledge discovery framework – intelligence generation, enhance decision advantage
- Automotive Test Rig – abstraction to a vehicle
- Input - Throttle, brake, cruise control
- Output - Motor

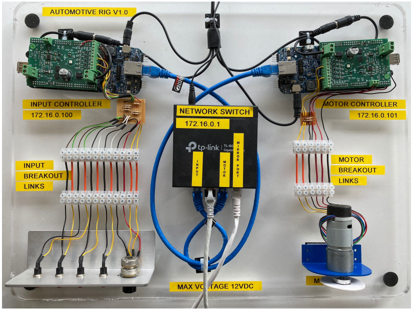


Figure 3: Hardware demonstrator.

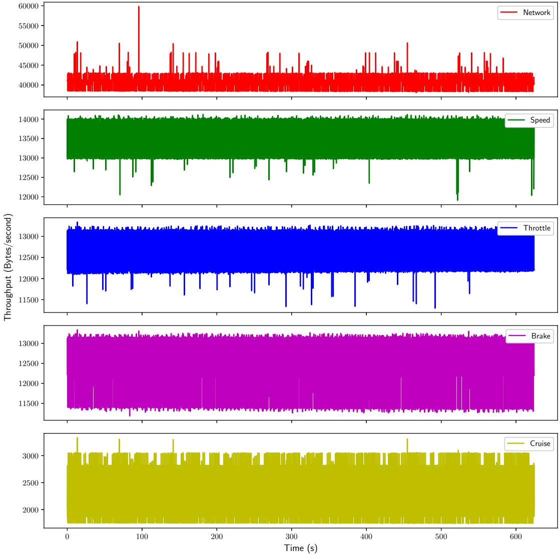
Project Objectives

- Record packets of data being sent across the network
- Extract features and use them as a basis for pattern analysis / ML / anomaly detection
- Attack the board using a DoS attack
- Observe network features and look for patterns that would help prevent them in the future
- Publish the findings of this research with Dr. Kerstin Eder

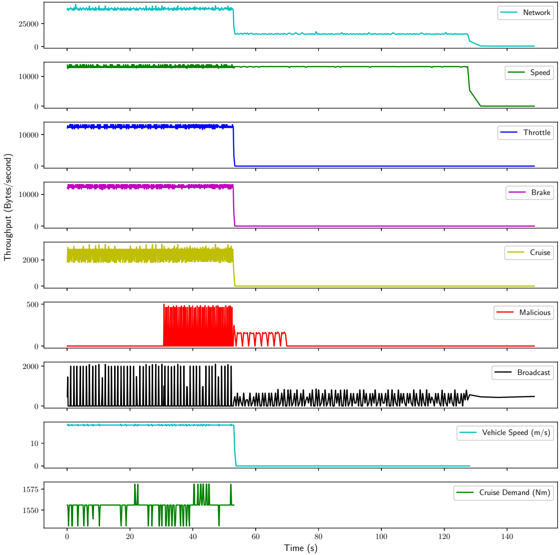
Project Implementation

- Packet information retrieved through command line version of Wireshark (tshark)
- 4 layered application written entirely in Python
- Link to GitHub repository.

Premliminary Results - Baseline Operation



Premliminary Results - DoS Attack



Challenges

- Data collection tool took a lot longer than expected due to the lack of compatibility of the Lua dissectors with Python
- Decision on software toolchain during the initial few weeks of the project
- Lack of support in terms of related literature – early days for an application of this nature in the automotive domain
- Code Quality vs Deliverables

What next?

- Implement an anomaly detection layer that can predict early onset of the attack using the network throughput
- Project carried out in a python virtual environment, *requirements.txt* available for somebody else to take over for layer optimisation, further work
- Large dataset is available for free for people who do not have access to the hardware

The End

Thank you for listening, any questions?