An Experiment to Investigate the effects of QoS-Like property tampering on Autonomous System Behavior

Xavier Hickman & Daniel Prince

Experiment overview

Research Motivation –

- Autonomous Systems (AS) are emerging technologies which require reliable vulnerability models. Examples of these include Vehicular Ad-Hoc Networks (VANETS).
- Much of the existing research in this area accumulates around targeting AS decision centres with explicit data manipulation rather than the implications of manipulating the QoS-like properties (Jitter, Delay, etc) for the underlying networks supporting the AS.

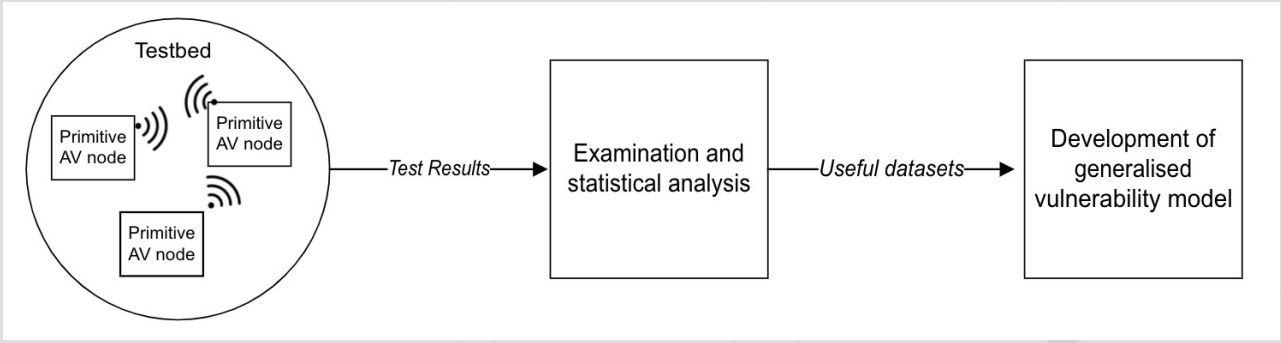
Research Objectives –

- Expose the hidden vulnerabilities in autonomous systems specifically in DSRC enabled AVs, VANETs, V2X.
- Identify a generalized vulnerability model for autonomous systems with a focus on V2X communication.

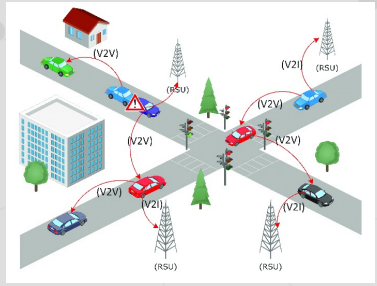
Key Points –

- Many advancements in autonomous systems over the past 20 years; AVs VANETs, DSRC, V2X [V2V, V2I, V2P..].
- The VANET's unique topological properties present novel opportunities for attack.

General Methodology Flow Diagram



Vehicular Ad-Hoc Network (VANET)



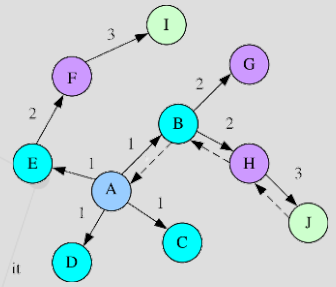
Topologically volatile network made up of AVs supporting the DSRC protocol.

The dedicated short range communication protocol (DSRC)

Short range comms protocol for AVs to communicate in real time while in motion. Radius is 1000m.

The Testbed

Test ground is a platform developed at protocol labs designed for testing, benchmarking and simulating distributed systems and peer to peer networks at scale. The platform can virtualize up to 10,000 nodes and allows the experimenter to examine the system in many dimensions and extract a variety of datasets. We intend to use this platform to simulate a VANET and virtualize primitive AVs for testing. The testing will involve attack simulation that targets VANET QoS-like properties.



This work is supported, in part, by the Engineering and Physical Sciences Research Council [grant number EP/V026763/1]