Misbehavior Detection System for Cellular Vehicle to Everything Technologies

Michael Aliberti, Max Ellsworth, Jason Inirio, Sam Krasnoff, Julia Zeng, Yixiu Zhu

Executive Summary— Vehicle to Everything Technology enables cars and IOT devices with an LTE connection to broadcast positional information such that vehicles can perceive their surroundings without line of sight. Before it is widely adopted, however, its reliability and security must be verified. To this end, we are developing a monitoring system that listens on Vehicle to Everything frequency blocks, verifies message integrity, and leverages machine learning to detect denial of service attacks. This system will consist of a dedicated radio and a web application to display information about frequency block resource usage. We will also be modeling examples of ordinary communication and denial of service attacks to provide data to the monitor. The goal of this project is to provide insight into the strengths and vulnerabilities of the Vehicle to Everything protocol.

Index Terms— Distributed Networks, Machine Learning, Network Protocols, Vehicle Operation

- *Michael Aliberti is with the Department of Computer and Electrical Engineering, Boston University, Boston, MA 02215. E-mail: mjali@bu.edu.*
- *Max Ellsworth is with the Department of Computer and Electrical Engineering, Boston University, Boston, MA 02215. E-mail: maxell@bu.edu.*
- *Jason Inirio is with the Department of Computer and Electrical Engineering, Boston University, Boston, MA 02215. E-mail: jasonini@bu.edu.*
- *Sam Krasnoff is with the Department of Computer and Electrical Engineering, Boston University, Boston, MA 02215. E-mail: krasnoff@bu.edu.*
- *Julia Zeng is with the Department of Computer and Electrical Engineering, Boston University, Boston, MA 02215. E-mail: zjulia@bu.edu.*
- *Yixiu Zhu is with the Department of Computer and Electrical Engineering, Boston University, Boston, MA 02215. E-mail: zhuyixiu@bu.edu.*

1 Need For This Project

As the information age continues to push the boundaries of interconnectivity, vehicular communication is beginning to catch up to modern standards. Vehicle-to-Everything, or V2X, technology is poised to revolutionize the way that cars interact with their surroundings. By leveraging LTE signals, the V2X protocol allows for information to be exchanged between cars and any wirelessly connectable device, which includes civilian smartphones, bikes and even other cars. By creating this network of devices, vehicles will be notified of road conditions, accidents, and other unexpected events with unprecedented speed and accuracy. Estimates predict that just signals pertaining to left-turn warnings and blind-spot detection alone could prevent upwards of 600 thousand crashes and save over 1,000 lives each year.

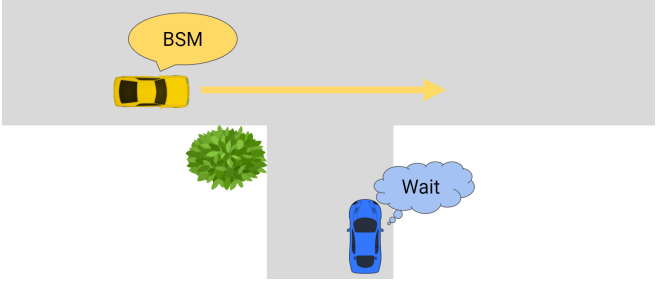

Fig. 1. Within the V2X protocol, cars broadcast Basic Safety Messages (BSMs) which convey location and velocity. This information facilitates inter-vehicle awareness without line of sight.

However, with the arrival of this new technology comes new challenges and malicious actors. In normal use, V2X-capable devices will be transmitting and receiving vital data, like GPS position and velocity. If the transmissibility of messages is poor or if an attacker is able to jam the network through a Denial of Service (DoS) attack, then vehicles will be rendered unable to properly assess their surroundings. This compromises the integrity of the mesh network, and the likelihood of collisions skyrockets.

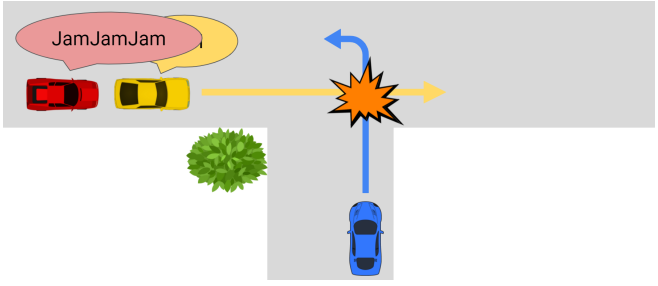

Fig. 2. When an attacker disrupts the transmission of basic safety messages, V2X provides limited information and collisions are far more likely to occur.

This project aims to not only examine the speed and efficacy of a cellular V2X network, but also to explore the detection and possible avoidance of malicious signals sent by attackers. Through machine learning and cyber security principles, a monitoring system will be set up to detect and warn users in real-time about ongoing DoS attacks. By verifying the reliability and security of V2X technology, we can hopefully reap its benefits while avoiding its pitfalls.

2 Problem Statement and Deliverables

2.1 Problem Statement

To gauge reliability and end-user safety in cellular Vehicle-to-Everything communication, a functional model must be created. This model will include two radios functioning as ordinary vehicles. Normal basic safety messages will be sent on multiple orthogonal frequency bands in the V2X range between these two radios, serving as a source of control data and as a testbed for attack

models. A third radio will act as an attacker or team of attackers, attempting to prevent normal operation and cause instability through denial of service attacks. A fourth radio will monitor the entire V2X frequency spectrum and pass the data it receives to a connected device, which will in turn store the data in a database. This data can then be visualized and used to train a machine learning algorithm in order to provide insights into V2X resource utilization and attack patterns.

2.2 Deliverables

Before implementing anything in hardware, this project demands two literature reviews. The first is intended to investigate the nature of V2X communication and its execution on software defined radios.. The other review will focus on the nature of possible attacks on V2X and how they have been detected in the past, thus informing the design of our monitoring system.

The functional hardware implementation of V2X behavior detailed above serves as a deliverable in-and-of-itself, as it may be used independently to explore other practical dimensions of the protocol. Three distinct DoS attack scenarios - oblivious, smart, and coordinated attacks [2] - must also be modeled in hardware, with documentation of all code changed in the V2X library for ease of replication. The final hardware-adjacent deliverable is a monitoring system to record data across all V2X frequency bands and store said data in a web-accessible API. There must also be a simple GUI for visualization of the monitored data and the overall resource usage of the V2X frequency band.

At the very core of the project is the misbehavior detection system itself. This must be a piece of software running on the monitor which uses data generated by the model to ascertain whether or not a specific snapshot of V2X traffic represents an attack. This will likely take the form of a machine learning algorithm which uses classification techniques to identify normal behavior as well as the three different avenues of attack.

3 Visualization

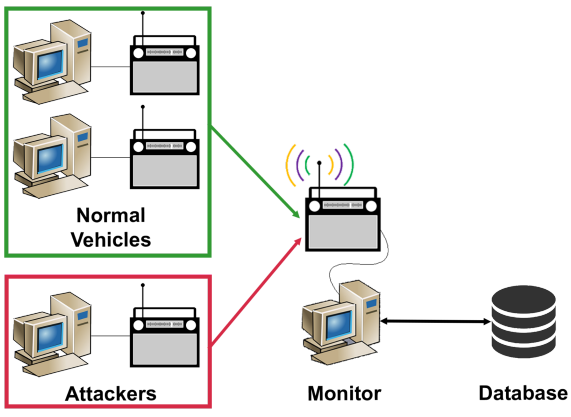

Fig. 3. The hardware setup that will be used to model V2X behavior and attacks. The monitor will listen in on all V2X frequency blocks and save collected data to a web-accessible API. This data can then be visualized and fed into a machine learning algorithm to find attacks.

Of note is the fact that only three radios are available to model V2X communications. Thankfully, the way in which vehicles divide up the frequency band in V2X allows one radio to simulate multiple vehicles at a time.

4 Competing Technologies

The purpose of this project is to further the efficacy and security of the V2X standard, which is still in the earlier stages of development. Due to this, research has mainly consisted of related products and technologies, rather than those competing directly against what this project aims to accomplish. One piece of technology that was found was the SA8700A C-V2X Test Solution from Keysight Technologies. This machine has a built-in high-power RF signal generator that allows it to accurately send messages in the V2X frequency band. It also possesses a large amount of high-quality signal monitoring solutions that measure values such as frequency accuracy, in-band emissions, and adjacent channel leakage ratio. However, Keysight's device lacks the post-processing of data that this project will provide.

Another related product is the Qualcomm 9150 C-V2X ASIC, which is mainly used for preliminary automotive applications, but again does not have any ability to detect an attack, much less differentiate from normal operating procedures. Next was the CV2XinFIRE experiment, from the 5GinFIRE project. The experiment focused on comparing another high-frequency standard called ITS-G5 to CV2X in a variety of real-world scenarios. A large amount of transmission data was collected and statistically analyzed, but the experiment did not focus on security, nor did it use machine learning in its results.

There have been a handful of academic studies focused on security within C-V2X, such as An MEC-based DoS Attack Detection Mechanism for C-V2X Networks from Li et al. [1]. Their paper and experiment theorized a statistical approach to monitor malicious actors on a V2X network. Our project differs in that it will utilize classification-based machine learning from both normal and DoS corrupted data streams to warn of attacks. By using various machine learning approaches, we aim to streamline the process of detecting malicious attacks in real-time.

5 Engineering Requirements

The model of C-V2X communication must be implemented, attacked, and monitored using only four National Instruments USRP-2901 software-defined radios (SDRs) operating in the 5.9 GHz band. These SDRs must be capable of regular C-V2X communication with a packet delivery success rate of 90% up to 30 ft. The C-V2X protocol must be simulated faithfully on the SDRs using an existing implementation like the SrsRAN radio suite [3]. There must be a visualization of channel resource usage via a web-accessible API populated by the monitor SDR and accessible 24/7.

There must be three classes of DoS attacks analyzed with samples labelled appropriately to distinguish them. To ensure that our ML algorithm is invariant to any class

disproportionality in the dataset, we are aiming for 95% classification accuracy within each denial-of-service attack type – oblivious, smart, and cooperative. These attacks are outlined in Denial-of-Service Attacks on C-V2X Networks [2]. We aim for 90% accuracy of classification in smart and cooperative attacks for low-vehicle density settings, since this is the most effective attack type in this environment. An AUC value of 0.9 or higher and an F1-score of 0.95 or higher is desirable to favor false positives and minimize false negative detections of malicious attacks.

The misbehavior detection system is to be supported by a batch offline learning model when the live dataset is small and by an online learning model with progression validation when the live dataset becomes larger than the batch model's. Online learning is necessary to account for the temporal aspect of our data.

Acknowledgment

The authors wish to thank Professor David Starobinsky, Stefan Gvozdenovic, and Tony Lizza (Air Force Research Laboratory) for their continued support of this project.

References

[1] iL, Yang & Hou, Ronghui & Lui, King-Shan & Li, Hui. (2018), "An MEC-Based DoS Attack Detection Mechanism for C-V2X Networks," 1-6. 10.1109/GLOCOM.2018.8647323.

[2] Nataša Trkulja, David Starobinski, and Randall Berry, "Denial-of-Service Attacks on C-V2X Networks," AutoSec 2021, February 2021.

[3] R. Lindstedt, M. Kasparick, J. Pilz and S. Jaeckel, "An Open Software-Defined-Radio Platform for LTE-V2X And Beyond," 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), 2020, pp. 1-5, doi: 10.1109/VTC2020-Fall49728.2020.9348771.

[4] G. Twardokus, and H. Rahbari, "Evaluating V2V Security on an SDR Testbed"

[5] *Wireless Access in Vehicular Environments–Security Services for Appli- cations and Management Messages*, IEEE Standard 1609.2-2016, 2016.

[6] Twardokus, Geoff, "Intelligent Lower-Layer Denial-of-Service Attacks Against Cellular Vehicle-to- Everything" (2021). Thesis. Rochester Institute of Technology.

[1] a
[2] b
[3] 4