Cybersecurity Simulator for Connected and Autonomous Vehicles

Sean Folan
University of Massachusetts Amherst
Amherst, Massachusetts, USA
sffolan@umass.edu

Yunsheng Wang
California State Polytechnic University, Pomona
Pomona, California, USA
yunshengwang@cpp.edu

ABSTRACT

In recent years, we have witnessed a significant rise in both the popularity and capability of Connected and Autonomous Vehicles (CAVs). This progress has been facilitated, in part, by advancements in CAV simulators that enable researchers to efficiently, safely, and cost-effectively test their vehicles. However, many current simulators do not directly address one of the most pressing challenges that CAVs encounter: cybersecurity. In this paper, we present a step towards resolving this issue. We have developed a simulator with the ability to simulate various Vehicle-to-Everything (V2X) attacks in real time. Our approach involves co-simulation of three simulators: CARLA, SUMO, and Artery. Utilizing the V2X communication capabilities of these simulators, our attacks involve injecting malicious Cooperative Awareness Messages (CAMs) and Decentralized Environmental Notification Messages (DENMs) into the simulation.

CCS CONCEPTS

• **Security and privacy** → *Mobile and wireless security*; • **Computer systems organization** → **Embedded and cyber-physical systems**; • **Networks** → **Error detection and error correction**.

KEYWORDS

Connected and Autonomous Vehicles (CAVs), Cybersecurity, Simulator

ACM Reference Format:
Sean Folan and Yunsheng Wang. 2023. Cybersecurity Simulator for Connected and Autonomous Vehicles. In *The Twenty-fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (MobiHoc '23), October 23–26, 2023, Washington, DC, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3565287.3617616

1 INTRODUCTION

The increasing adoption of Connected and Autonomous Vehicles (CAVs) has revolutionized the automotive industry, promising safer, more efficient, and convenient transportation. By leveraging cutting-edge technologies such as artificial intelligence, machine learning, and advanced sensor systems, CAVs have the potential to reshape urban mobility, reduce traffic accidents, and enhance overall transportation experiences. However, as with any technology-driven advancement, the integration of CAVs into our daily lives also brings forth significant cybersecurity challenges.

As vehicle technology advances, we have to acknowledge that vehicles are no longer purely mechanical. In fact, it would be more accurate to call recently developed Connected and Autonomous Vehicles complex computers given that the amount of code in a CAV is expected to reach 300 million lines by 2030 [8], which is ten times more than the entire Linux kernel [10]. One major part of this is the capability of a CAV to communicate to the world around it using Vehicle-to-Everything (V2X) communication. While these innovations have the potential to save lives and improve the cost, efficiency, and accessibility of transportation, as anything becomes more connected, it also becomes more vulnerable.

The consequences of cybersecurity breaches in CAVs can be catastrophic, as they can lead to loss of vehicle control, endanger passengers and pedestrians, and disrupt traffic flow. Moreover, a single successful attack on a CAV could have far-reaching consequences, eroding public trust in the technology and hampering its widespread adoption, potentially delaying the realization of its numerous benefits.

To address the critical cybersecurity challenges faced by the CAV industry, researchers and industry professionals are working tirelessly to develop robust and resilient security solutions. Among these efforts, simulation-based approaches have emerged as invaluable tools for comprehending and mitigating cybersecurity risks in CAVs. Cybersecurity simulators offer a controlled environment for testing and analyzing various attack scenarios, evaluating the effectiveness of defensive measures, and honing incident response strategies.

However, the most popular CAV simulators such as CARLA [3], LGSVL [12], and AirSim [13] are mostly built to test the function of various elements of CAVs including perception and V2X communication with little thought given to cybersecurity [6].

In this paper, we present a state-of-the-art cybersecurity simulator specifically designed for the evaluation of Connected and Autonomous Vehicles. The simulator integrates realistic vehicular communication models, sophisticated attack vectors, and cutting-edge security measures to recreate dynamic real-world scenarios. By simulating cyber threats in a controlled environment, researchers and engineers can gain valuable insights into potential vulnerabilities and devise effective countermeasures to bolster the security of CAVs. Our method uses the co-simulation of three Open Source simulators. CARLA [3] provides visualization through Unreal Engine 4, SUMO [7] allows us to efficiently manage traffic and Artery [11] allows us to simulate V2X communication. This trio of simulators is synced up and we are able to handle the real V2X messages, as well as inject fake ones in the form of Cooperative Awareness Messages (CAMs) and Decentralized Environmental Notification Messages (DENMs).

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
MobiHoc '23, October 23–26, 2023, Washington, DC, USA
© 2023 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-9926-5/23/10…$15.00
https://doi.org/10.1145/3565287.3617616

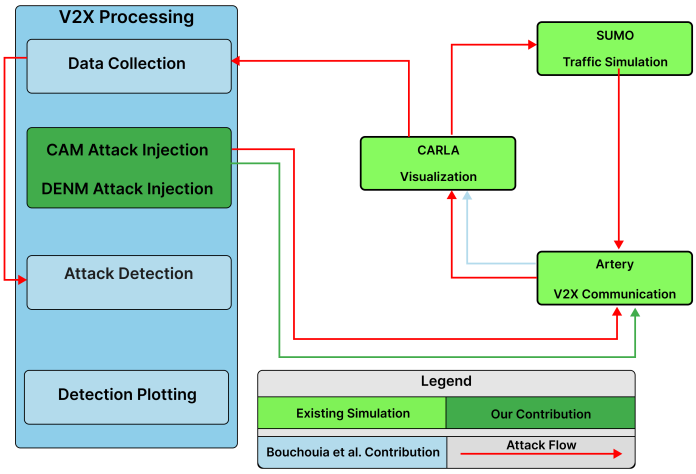

Figure 1: A diagram of the system model and attack flow

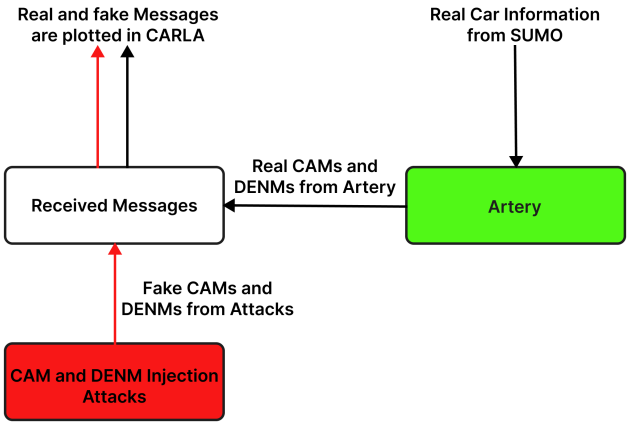

Figure 2: A diagram of the CAM and DENM injection Attacks

The major contributions of our work are as follows:

- Working from a previous setup using the CARLA [3], SUMO [7], and Artery [11] [2] simulators. This setup allows us to visualize, control traffic and send appropriate V2X messages for all of the vehicles in the simulation.
- Changing the injection method from an injection into CARLA to an injection into Artery, eliminating the attacking "ghost vehicles" presence in the simulation.
- Implementing attacks which inject false V2X messages in the form of Cooperative Awareness Messages (CAM) and Decentralized Environmental Notification Messages (DENM) into this simulation loop.

The remainder of this paper is organized as follows: Section 2 discusses the related work on cybersecurity simulators for CAVs. Section 3 provides an overview of our simulation model and attack injections. Section 4 describes the CAM injection attacks. Section 5 describes the DENM injection attacks and Section 6 concludes the paper.

2 RELATED WORK

Despite a large amount of work towards building simulators for CAVs, few of them deal with the cybersecurity aspect. The most popular simulators such as CARLA [3] and LGSVL [12] are built on top of video game engines (Unreal Engine 4 and Unity respectively) and can provide high-definition graphics for testing perception algorithms such as Lane Detection, Traffic Light Recognition, Object Detection, etc. While these are important to test, neither of these simulators implement cyber-attacks or provides a way to detect these attacks.

Dosovitskiy et al. introduced the CAR Learning to Act (CARLA) simulator [3]. This simulator was built with Autonomous Driving research in mind and provides realistic graphics via Unreal Engine 4. It also supports a wide range of sensors and environments.

Another Open Source simulator, the Simulation of Urban MObility (SUMO) was introduced by Krajzewicz et al. [7]. This simulator interfaces well with CARLA and provides a way to model traffic effectively and realistically.

A third important simulator called Artery was introduced by Riebl et al. [11]. This simulator interfaces with SUMO and provides a way to simulate Vehicular Ad Hoc Networks (VANETs) with ETSI ITS-G5 protocol stack.

Finally, research done by Bouchouia et al. [2] combined the previous three simulators to develop "the first simulator that simultaneously supports, communication, sensor, and security aspects (attacks and attack detectors)."

Our work improves upon these simulators by modifying the model proposed in Bouchouia et al. [2]. We reimplement the injection of malicious CAMs so that they do not manifest themselves as physical vehicles in the simulation and we also add in DENM injections.

3 SYSTEM MODEL

Our simulator builds on top of Bouchouia et al. who in turn built off of CARLA [3], SUMO [7], and Artery [11] [2]. As seen in Figure 1, the simulator synchronizes CARLA, SUMO, and Artery such that each step of the simulation allows CARLA to process the graphics, SUMO to process the traffic and movement, and Artery to process all of the V2X communication. Specifically, Artery will send off CAMs for each vehicle as well as DENMs if events mandate it to do so.

While Bouchouia et al. implemented their attacks by introducing them as cars within CARLA, we believe that a more precise and realistic approach involves injecting our attacks without manifesting them as vehicles. In our methodology, Artery sends all real V2X messages to our Python program through a socket. Subsequently, we combine these real messages with fake ones in an identical format. This integration enables us to visualize both the real and fake messages within the CARLA environment.

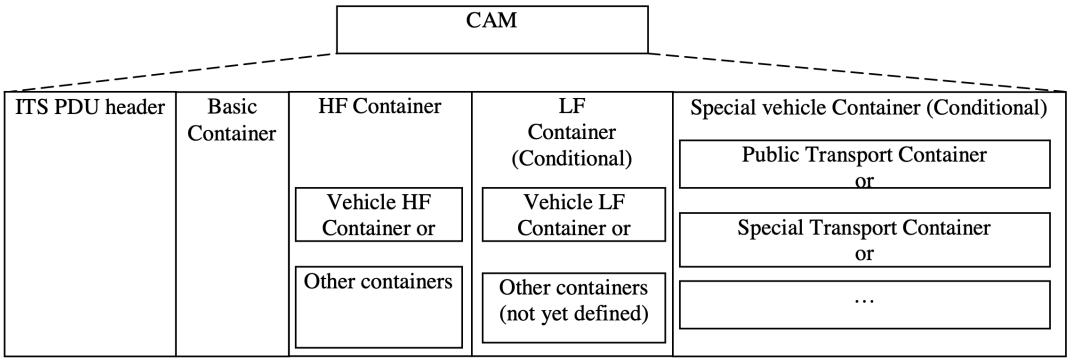

Figure 3: General Structure of a CAM [4]

Figure 2 shows a close-up of the injection attack. The attack occurs between Artery and CARLA. Artery generates real CAMs and DENMs based on the data passed from SUMO. Our attack injection generates fake CAMs and DENMs, which are then inserted into the same message list received by our Data Collection module. Both real and fake messages can subsequently be plotted in CARLA. This process recurs at every time step within the simulation.

4 CAM INJECTION ATTACKS

As defined by the European Telecommunications Standards Institute, a Cooperative Awareness Message (CAM) allows cars to send and receive information such as "time, position, motion state, activated systems, etc" to and from other cars [4]. These messages allow cars to perceive each other even when sensors such as cameras and LiDAR are obstructed. The general structure of a CAM is found in Figure 3.

When working correctly, these messages can be an enormous benefit to CAVs. However, potential attacks such as the injection of altered or false messages have been theorized [1]. We broke up the injection of fake CAMs into two different attacks: ***Position Attack*** and ***Offset Attack***.

4.1 Position Attack

For our Position Attack as shown in Figure 4, we took the standard CAM format and repeatedly injected a CAM which asserted that there was a vehicle at a specific x and y coordinate. This results in signals being sent out at every time step indicating there is a car at that x and y location. Sending out fake CAMs such as this could interfere with a vehicle's ability to make an accurate model of the world around it.

4.2 Offset Attack

Another type of CAM injection attack in our simulation is the Offset Attack. The offset attack targets a specific vehicle. It receives the CAM for that vehicle and then sends out its own CAM asserting that it is a vehicle heading in the same direction and same speed as that vehicle but at a different position. The Constant Offset Attack asserts that it is always 10 meters ahead of the target vehicle, as shown in Figure 5; while the Random Offset Attack asserts that it is

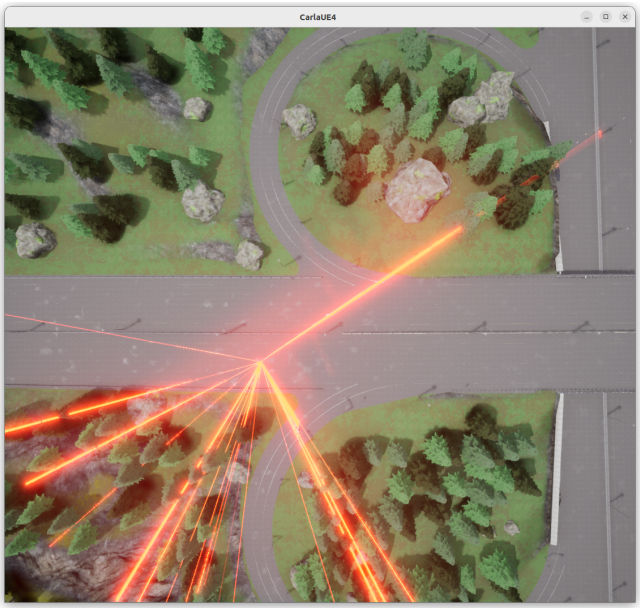

Figure 4: A picture displaying CAMs radiating out from a non-existent car as the result of a Position Attack

a random distance sampled from the Normal distribution $\mathcal{N}(10, 5)$ meters ahead of the target vehicle, as shown in Figure 6. This attack affects all vehicles within the range of the signal. Similar to the Position Attacks, this could be detrimental to vehicles as they trust CAMs as a way to perceive the world and fake messages could interfere with this perception.

5 DENM INJECTION ATTACKS

Another critical form of Vehicle-to-Vehicle (V2V) communication defined by ETSI is Decentralized Environmental Notification Messages (DENMs) [5]. These messages are sent out aperiodically and in response to events that other drivers should know about or conditions, which make driving potentially dangerous. These messages

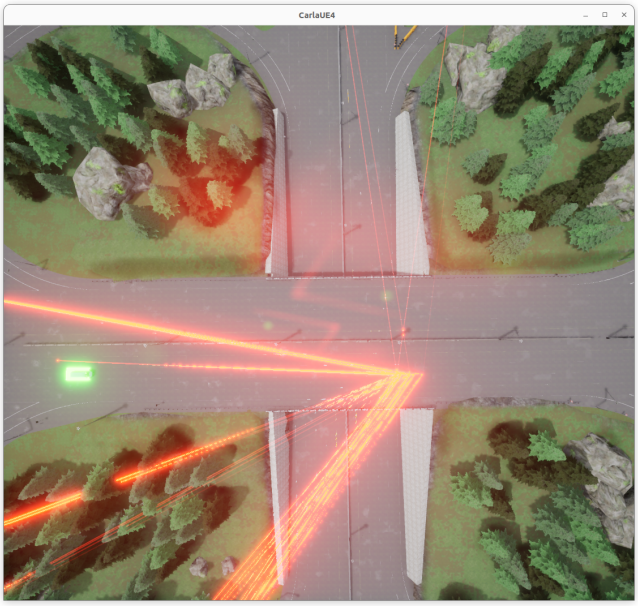

Figure 5: Constant Offset Attack: A CAM is projected 10 meters ahead of the vehicle shown in green

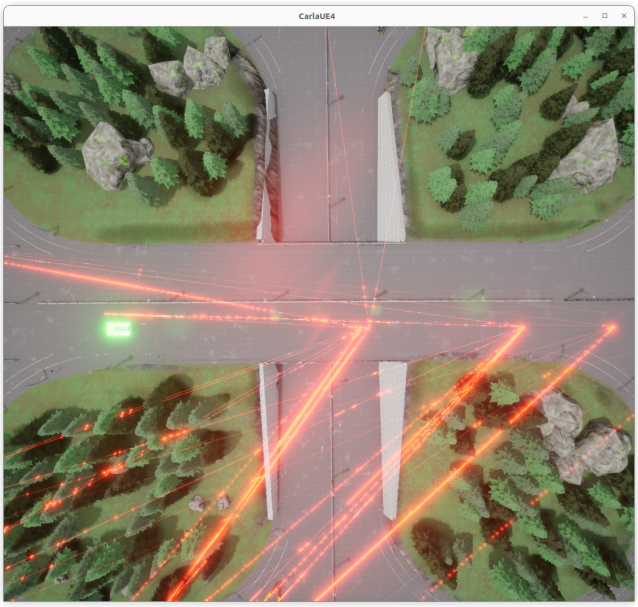

Figure 6: Random Offset Attack: A CAM is projected at a number sampled from $\mathcal{N}(10, 5)$ meter away

are highly customizable, which allows them to represent a myriad of events. The general structure of a DENM is found below 7

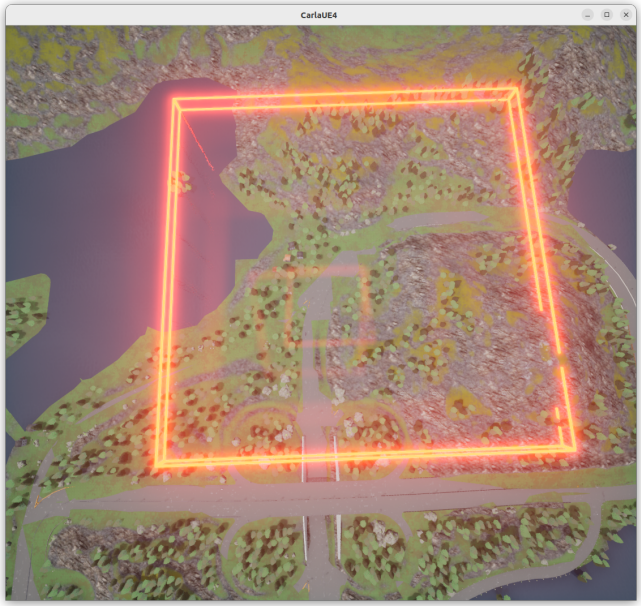

Figure 8: The area affected by the Emergency Braking Attack enclosed in a red box

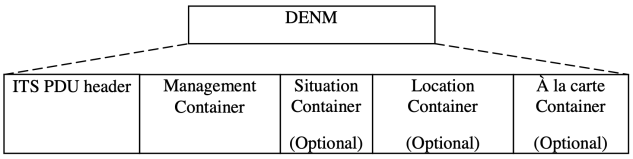

Figure 7: General Structure of a DENM [5]

Similar to the injection of CAMs, the injection of DENMs can pose a risk to CAVs if they give fake information. In our simulator, we make use of three different types of DENMs: ***Emergency Braking Attack***, ***Traffic Jam Attack***, and ***Traction Loss Attack***.

5.1 Emergency Braking Attack

The Emergency Braking Attack sends out a fake DENM indicating that a car has suddenly braked. As shown in Figure 8, the Emergency Braking Attack sends out signals to a wider area than for example the Traction Loss attack in Figure 10. This is one of the many things that can be customized in the DENM format. Each signal has a specific area that it affects, with an Emergency Braking DENM affecting cars within 500 meters of the original sender. Sending out this attack could have obvious repercussions for other vehicles including could potentially cause other cars to suddenly brake or slow down.

5.2 Traffic Jam Attack

The Traffic Jam Attack as seen in Figure 9 has two types of DENMs associated with it. First, we send out a fake *TrafficJamAhead* DENM. This sends out a signal telling other cars to expect a traffic jam unless they receive a *TrafficJamEndOfQueue* message which indicates they

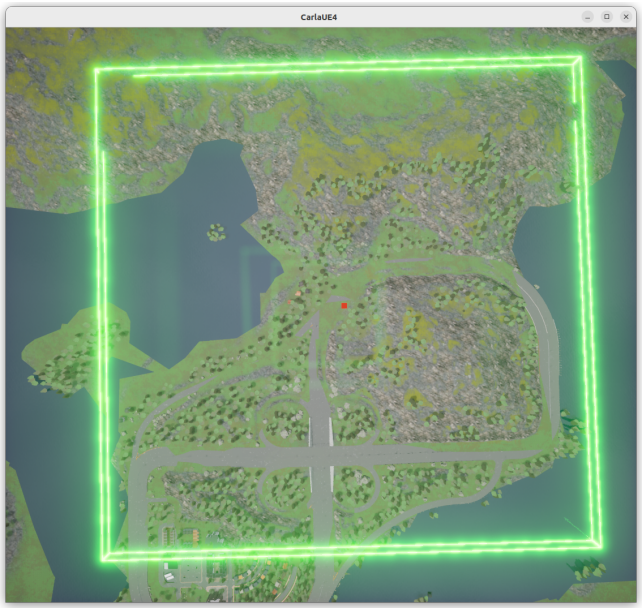

Figure 9: The area affected by the Traffic Jam Attack enclosed in a green box

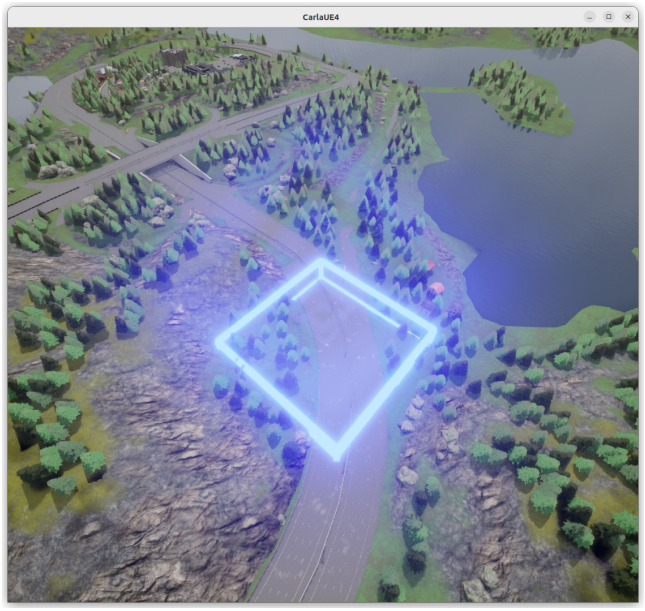

Figure 10: A box is plotted over the area which receives a fake DENM indicating Traction Loss

are either at the end or behind the traffic jam. These signals affect the widest area of the three attacks shown, with each signal affecting cars within 1000 meters of the original sender. When a car receives these messages, it will try to slow down in anticipation of a traffic jam. If this sort of attack was implemented on a busy highway, it could cause 1 km to come to a crawl which would in turn create a traffic jam behind it, perhaps snowballing into a much larger traffic jam.

5.3 Traction Loss Attack

The Traction Loss Attack, shown in Figure 10, sends a fake DENM at a selected spot on the map indicating that there are adverse conditions on the road which led a car to lose traction or hydroplane. The area affected by this attack is the smallest of the three, at only 100 meters, but it would cause cars to slow down and be extra cautious within that area. Again, this could cause cars to slow down and drive much more cautiously within this area, causing a needless traffic jam.

6 CONCLUSION

In this paper, we underscore the critical need for a dedicated cybersecurity simulator tailored to Connected and Autonomous Vehicles (CAVs). By examining the vulnerabilities within the V2X communication framework, we have highlighted the significance of safeguarding Cooperative Awareness Messages (CAMs) and Decentralized Environmental Notification Messages (DENMs) – two pivotal elements as defined by the ETSI standards.

Our contributions thus far have illuminated the potential risks by implementing various attack scenarios on CAMs and DENMs.With our newly implemented attacks, researchers can test the effectiveness of defense strategies in a cost-effective and low risk environment. This will allow testing cybersecurity strategies in CAVs to be more accessible, even if the researcher does not have access to a physical vehicle and thus may help the field evaluate attacks and defenses more efficiently. However, the primary focus continues to be on the defensive aspect. While we have simulated attacks, the absence of detection methods is an explicit limitation. Our future endeavors will center on developing robust detection mechanisms to effectively fortify CAVs against these threats.

In future work, our research will also diversify its scope by introducing novel types of DENMs for injection, further exploring the vulnerabilities across a broader spectrum of V2X communication modes. Additionally, extending the analysis to encompass services like Maneuver Sharing Coordination Services would provide a more comprehensive understanding of potential vulnerabilities within the CAV ecosystem [9].

ACKNOWLEDGMENTS

Thank you to Dr. Wang for being my mentor and to all involved in the "Big Data Security and Privacy" REU at California Polytechnic State University, Pomona. This material is based upon work supported by the National Science Foundation under Grant No. 2050826.

REFERENCES

[1] Aljawharah Alnasser, Hongjian Sun, and Jing Jiang. 2019. Cyber security challenges and solutions for V2X communications: A survey. *Computer Networks* 151 (2019), 52–67.

[2] Mohammed Lamine Bouchouia, Jean-Philippe Monteuuis, Houda Labiod, Ons Jelassi, Wafa Ben Jaballah, and Jonathan Petit. 2022. A simulator for cooperative and automated driving security. In *Workshop on Automotive and Autonomous Vehicle Security (AutoSec), Ndss-Symposium.*

[3] Alexey Dosovitskiy, Germán Ros, Felipe Codevilla, Antonio M. López, and Vladlen Koltun. 2017. CARLA: An Open Urban Driving Simulator. *CoRR* abs/1711.03938 (2017). arXiv:1711.03938 http://arxiv.org/abs/1711.03938

[4] European Telecommunications Standards Institute. 2019. *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service.* Technical Report. ETSI.

[5] European Telecommunications Standards Institute. 2019. *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service.* Technical Report. ETSI.

[6] Prabhjot Kaur, Samira Taghavi, Zhaofeng Tian, and Weisong Shi. 2021. A Survey on Simulators for Testing Self-Driving Cars. In *2021 Fourth International Conference on Connected and Autonomous Driving (MetroCAD).* 62–70. https://doi.org/10.1109/MetroCAD51599.2021.00018

[7] Daniel Krajzewicz, Georg Hertkorn, Christian Feld, and Peter Wagner. 2002. SUMO (Simulation of Urban MObility); An open-source traffic simulation. *4th Middle East Symposium on Simulation and Modelling (MESM2002)*, 183–187.

[8] Yufeng Li, Qi Liu, Xuehong Chen, and Chenhong Cao. 2023. Integrated safety and security enhancement of connected automated vehicles using DHR architecture. *Security and Safety* 2 (01 2023), 2022009. https://doi.org/10.1051/sands/2022009

[9] Jean-Philippe Monteuuis, Jonathan Petit, Mohammad Raashid Ansari, Cong Chen, and Seung Yang. 2022. V2x misbehavior in maneuver sharing and coordination service: Considerations for standardization. In *2022 IEEE Conference on Standards for Communications and Networking (CSCN).* IEEE, 194–199.

[10] Rajan Patel. 2022. An overview of live kernel patching. https://ubuntu.com/blog/an-overview-of-live-kernel-patching#:~:text=The%20Linux%20kernel%20has%20over,receive%2025%20patches%20every%20day.

[11] Raphael Riebl, Hendrik-Jörn Günther, Christian Facchi, and Lars Wolf. 2015. Artery: Extending Veins for VANET applications. In *2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS).* 450–456. https://doi.org/10.1109/MTITS.2015.7223293

[12] Guodong Rong, Byung Hyun Shin, Hadi Tabatabaee, Qiang Lu, Steve Lemke, Mārtiņš Možeiko, Eric Boise, Geehoon Uhm, Mark Gerow, Shalin Mehta, Eugene Agafonov, Tae Hyung Kim, Eric Sterner, Keunhae Ushiroda, Michael Reyes, Dmitry Zelenkovsky, and Seonman Kim. 2020. LGSVL Simulator: A High Fidelity Simulator for Autonomous Driving. arXiv:2005.03778 [cs.RO]

[13] Shital Shah, Debadeepta Dey, Chris Lovett, and Ashish Kapoor. 2017. AirSim: High-Fidelity Visual and Physical Simulation for Autonomous Vehicles. arXiv:1705.05065 [cs.RO]