Simuhack : A Realistic Attack Simulation Framework for Enhancing Cybersecurity in Autonomous Vehicles

D.Kiruthika
Department of Electronics and Communication Engineering
Thiagarajar College of Engineering
Madurai,India
kiruthikadhibakaran123@gmail.com

K.A.Kameshwari
Department of Electronics and Communication Engineering
Thiagarajar College of Engineering
Madurai,India
kameshwari@student.tce.edu

K.S.Sanjay Kumar
Department of Electronics and Communication Engineering
Thiagarajar College of Engineering
Madurai,India
kuduvasanjaykumar@gmail.com

G.Ananthi
Department of Electronics and Communication Engineering
Thiagarajar College of Engineering
Madurai,India
gananthi@tce.edu

***Abstract*—As autonomous driving technology advances, modern vehicles are evolving into sophisticated digital systems. This evolution introduces new challenges for ensuring safety and security in vehicle design, particularly concerning smart sensors, Electronic Control Units (ECUs), and in-vehicle communications. Addressing these challenges requires robust security measures to mitigate potential attacks. However, real-world testing of these systems is both complex and costly. To overcome this hurdle, proposed the Simuhack framework within the CARLA software, which simulates attack datasets for comprehensive security analysis in vehicle design. Simuhack facilitates the creation of realistic attack scenarios, including GPS spoofing, V2X attacks, ECU attacks, and Replay and Bogus Information attacks commonly encountered in modern vehicles. We demonstrate the utility and effectiveness of our framework by evaluating five cyber attack scenarios using the LGSVL simulation software. Our findings underscore the critical importance of proactive security measures in safeguarding autonomous driving systems against potential cyber threats.**

Keywords— Autonomous Driving, Cyber Attacks, ECU, GPS Spoofing, V2X Attacks.

I. INTRODUCTION

The evolution of transportation has led to the development of sophisticated vehicles equipped with intelligent IT systems that leverage artificial intelligence (AI). Autonomous vehicles, capable of independent navigation, represent a significant advancement in intelligent transportation systems and underscore the importance of secure communication [1]. These innovations enhance traffic safety and efficiency while meeting the evolving demands of modern logistics for transporting goods and passengers [2]. However, the security of autonomous vehicles against cyber-attacks presents a formidable challenge. Existing automobile simulators, such as LGSVL [3] and CARLA [4], provide robust sensor support but were not primarily designed to simulate hostile assaults on self-driving cars. The complexity of self-driving vehicles, incorporating diverse components like sensors and control units, necessitates secure testing environments where simulated attacks can validate their functionality. This paper introduces Simuhack, a simulation framework specifically designed to establish a secure and comprehensive environment for assessing cyber attacks on autonomous vehicles. Unlike LGSVL and CARLA, Simuhack focuses on addressing inherent vulnerabilities in automotive systems by simulating various attack scenarios, including GPS Spoofing/Jamming, Vehicle Networking Attacks, Attacks on ECUs, Replay Attacks, and Bogus Information Attacks.

The contributions of the paper are as follows:

- **Development of Simuhack Framework:** Simuhack is introduced as an open-source framework tailored for security testing in autonomous vehicle systems is shown in figure 1.
- **Simulation of Diverse Attack Scenarios:** Simuhack facilitates the generation of realistic attack data, providing researchers and developers with a robust tool for testing and improving AV security.
- **Comprehensive Evaluation:** An exhaustive study assesses the efficacy of Simuhack across various scenarios, rigorously testing the accuracy of simulation data in five critical real-life situations.
- **Advantages and Comparative Analysis:** A comparative analysis illustrates the benefits of Simuhack's attack capabilities against established simulators, highlighting its unique strengths in cyber-attack testing for AVs.
- **Contribution to Cybersecurity Research:** This research advances cybersecurity measures in the automotive industry by addressing critical vulnerabilities, particularly in GPS spoofing attacks on AVs.

979-8-3503-6501-6/24/$31.00 ©2024 IEEE

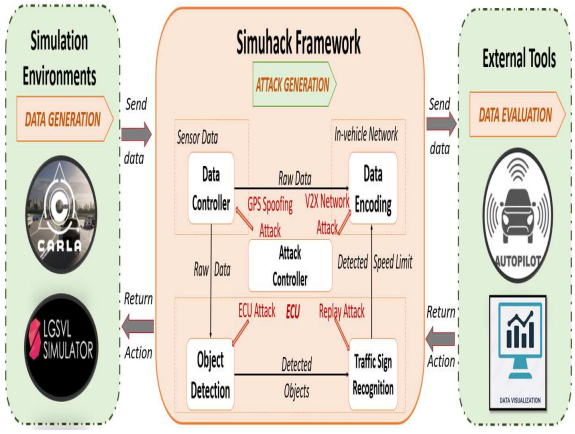

Fig.1. A summary of our Simuhack framework

By addressing these unique security challenges through specialized simulation, Simuhack enhances security testing during the development and deployment of autonomous driving systems.

II. Proposed Simuhack Framework

In the upcoming sections, we will delve into the system architecture and provide a comprehensive exploration of the key elements comprising Simuhack, as illustrated in Figure 2. The Simuhack framework workflow begins with data generation in simulation environments like CARLA and LGSVL, where sensors such as cameras, GPS, and IMUs collect vehicle state information. This data is then sent to the Data Controller, which models the sensors and forwards the data to the Attack Controller to simulate various cyber attacks. The attacked data is encoded using schemes like Ethernet or CAN and processed by ECUs for functions like traffic sign recognition and vehicle control. Finally, the processed data is sent to external tools for data evaluation and visualization, aiding in the analysis of the impact of the attacks.

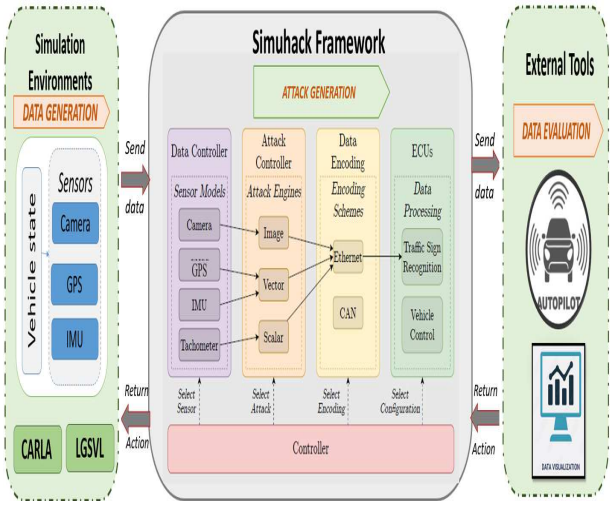

Fig.2. Analysis of Simuhack's System Architecture

A. Data Generation

The Data Generation module integrates with simulation environments such as CARLA and LGSVL to produce realistic vehicle state data. This module employs various sensors, including cameras, GPS, and IMU (Inertial Measurement Unit), to capture detailed information about the vehicle's surroundings and internal states. These sensors model real-world conditions and provide essential input data for the Simuhack framework. By leveraging the robust sensor support from CARLA and LGSVL, this module ensures that the data generated is accurate and representative of real-world scenarios. The generated data is then sent to the Simuhack framework for further processing, forming the basis for subsequent attack simulations.

B. Attack Generation Module

The Attack Generation module is the core component of the Simuhack framework, responsible for creating and simulating various cyber-attack scenarios on autonomous vehicles. This module includes a Data Controller that manages sensor models and an Attack Controller that orchestrates different attack engines. The attacks are categorized into three main types: Image attacks (e.g., camera spoofing), Vector attacks (e.g., GPS spoofing/jamming), and Scalar attacks (e.g., ECU manipulation). These attack engines simulate scenarios such as GPS Spoofing/Jamming, Vehicle Networking Attacks, ECU Attacks, Replay Attacks, and Bogus Information Attacks. The data encoding schemes, such as Ethernet and CAN (Controller Area Network), ensure that the simulated attacks mimic real-world communication protocols. This module allows researchers to select specific attacks and configurations, providing a robust environment for testing the security of autonomous vehicle systems.

In the Simuhack architecture, the Attack Generation module is the core component responsible for creating and simulating various cyber-attack scenarios on autonomous vehicles. Here is an explanation of how each of the five specific attacks is created within the Simuhack framework:

GPS Spoofing/Jamming Attack - In the GPS Spoofing/Jamming Attack, the Data Controller first selects the GPS sensor model, providing real-time location data for the vehicle. The Attack Controller then uses the GPS Spoofing/Jamming engine to manipulate these GPS signals by altering the coordinates or creating signal interference. This manipulated GPS data is subsequently encoded using Ethernet or CAN protocols and sent back to the vehicle's navigation system. During simulation execution, the vehicle reacts to the spoofed or jammed GPS data, revealing potential navigational errors or misguidance.

Vehicle Networking Attacks - In the Simuhack framework, Vehicle Networking Attacks are executed through a series of coordinated steps within the Attack Generation module. The Data Controller first uses sensor models to gather communication data from vehicle networking components such as V2X (Vehicle-to-Everything). Next, the Vehicle Networking Attacks engine within the Attack Controller injects malicious messages or disrupts the network traffic between the vehicle and external communication points. These malicious messages are then encoded using appropriate protocols like Ethernet and CAN and sent through the vehicle's network. Finally, the vehicle's response

to the altered or disrupted network data is observed, highlighting vulnerabilities in its communication systems.

ECU Attacks - In the Simuhack framework, ECU attacks are executed through a multi-step process involving several components. First, the Data Controller selects relevant ECUs (Electronic Control Units) involved in vehicle control processes. Next, the Attack Controller's ECU Attacks engine sends false commands or disrupts the normal operation of these selected ECUs. This altered ECU data is then encoded using Ethernet or CAN protocols and sent back to the vehicle's control systems. Finally, during simulation execution, the impact of the compromised ECUs on the vehicle's behavior and control is evaluated, demonstrating how these attacks could affect driving performance.

Replay Attacks - In the Simuhack framework, Replay Attacks are executed by the Data Controller capturing legitimate data from various sensors such as the camera, GPS, and IMU during normal operation. This data is then stored by the Replay Attack engine within the Attack Controller. At a later time, the stored legitimate data is replayed to the vehicle's systems. The replayed data is encoded using the same protocols as the original data and sent back to the vehicle. During the simulation execution, the vehicle's response to this replayed data is closely observed, demonstrating the potential effects and vulnerabilities that arise from using outdated or incorrect information.

Bogus Information Attacks - In a Bogus Information Attack scenario, the Data Controller gathers input from various sensors that feed into the vehicle's systems, such as Traffic Sign Recognition and Vehicle Control. The Attack Controller, equipped with the Bogus Information Attack engine, generates false data, including fabricated traffic signs and inaccurate sensor readings. This bogus data is then encoded and transmitted back to the vehicle's systems using Ethernet or CAN protocols [6]. During the simulation execution, the vehicle's response to the erroneous data is observed, demonstrating how misleading information can adversely affect its decision-making processes.

C. Data Visuvalization Module

The "Data Visualization" module in the Simuhack Framework, located in the "External Tools" section, serves as a critical component for evaluating and interpreting data generated by the simulation environments. Its primary purpose is to provide graphical and analytical insights into the processed data, facilitating a comprehensive understanding of the simulation results. After data is collected from sensors such as cameras, GPS, and IMUs within the CARLA or LGSVL simulation environments, and subsequently manipulated through the various attack engines and encoding schemes, it is fed into this module. The Data Visualization module then translates this complex data into accessible and interactive visual formats, such as graphs, charts, and dashboards. This allows users to easily identify patterns, trends, and anomalies related to cyber attacks and their impacts on autonomous vehicle systems. By presenting data in a visually intuitive manner, the module aids in the thorough evaluation and validation of the attack scenarios and the effectiveness of the applied security measures, ultimately enhancing the decision-making process for researchers and engineers. Additionally, the framework integrates an autopilot system to simulate real-world driving conditions and responses, which helps in assessing the robustness of autonomous vehicle control systems under various cyber attack scenarios. For data visualization, tools such as MATLAB [5] or Google Colab can be used, providing powerful platforms for creating detailed and interactive visualizations. MATLAB offers extensive capabilities for data analysis and visualization, while Google Colab provides a flexible, cloud-based environment that supports collaborative work and easy sharing of results.

III. Attack Execution

Following an overview of the attack generation process in Section II, we will delve deeper into various attack vectors and simulate corresponding realistic attacks. The highlighted assaults represent relevant and widely acknowledged examples from existing literature, demonstrating Simuhack's expertise in the field. However, it is essential to emphasize that the presented selection does not encompass all potential attacks that can be conducted using our framework.

A. GPS Spoofing Attack

A GPS spoofing attack in autonomous vehicles involves sending fake GPS signals to mislead the vehicle's navigation system, causing it to think it is in a different location, which can lead to dangerous situations [7]. In the LGSVL simulator, such attacks are simulated by injecting false GPS data. Sensor attacks, like jamming and spoofing, disrupt a sensor's perception: jamming blocks sensor awareness, while spoofing creates false inputs [8]. Although these attacks are complex and costly to perform in reality, analyzing their effects on data output is straightforward once detected. By examining the relationship between known GPS sensor attacks and changes in output data, and classifying attacks by the type of data they affect, information can be shared across multiple sensors. This approach helps in understanding the impact of sensor attacks on autonomous vehicle systems, highlighting the importance of robust defenses to mitigate these threats.

B. Vehicle Networking Attacks

Sensors are vital for collecting and sending data to Electronic Control Units (ECUs) via dedicated bus systems. From an attacker's viewpoint, this data transmission is akin to basic network packet transmission. Typical network threats include denial of service attacks, message manipulation, and signal spoofing. Denial of service attacks can interrupt sensor communication by causing packet drops, hindering crucial data delivery. Message manipulation involves altering messages, leading to transmission errors [9]. These threats affect both in-vehicle networks and external Vehicle-to-Everything (V2X) connections. Due to their similar impacts, sensor and network attacks are often assessed together when evaluating ECUs and related algorithms. Understanding and mitigating

these attacks is crucial for maintaining the integrity and security of autonomous vehicle systems.

C. Attacks on ECU

Attacking autonomous vehicles can exploit software vulnerabilities in Electronic Control Units (ECUs) to gain control and manipulate functions. Since ECUs are interconnected, compromising one can lead to infiltrating others [10]. Simuhack struggles to model all ECU internals due to their diversity. For example, hacking an ECU for traffic sign recognition could provide incorrect data, jeopardizing dependent systems. This highlights the need for security assessments and safeguards to protect ECUs from cyber threats in autonomous vehicles.

D. Replay Attack

Replay attacks involve intercepting and retransmitting pre-recorded valid messages across a V2X communication protocol. For instance, during an emergency braking situation, beacons are sent to nearby cars to alert drivers and automatically apply brakes, enhancing safety [11]. An attacker can intercept these messages and retransmit them in scenarios like synchronized platoon systems or high-speed traffic, potentially causing crashes.

E. Bogus Information Attack

A bogus information attack on self-driving vehicles involves sending false data to the vehicle's networks, leading to incorrect decisions [12]. For example, falsifying traffic light information could cause the vehicle to proceed through a red light, risking collisions and other hazards. These attacks exploit vulnerabilities in V2X communication systems, highlighting the need for improved security measures to ensure the integrity and authenticity of information crucial for the safe operation of autonomous vehicles.

IV. Results And Discussion

To validate our methodology and simulated intrusion data, we conducted a scenario-based study using three hypothetical attack vectors targeting autonomous vehicles. We developed a basic autopilot program with publicly available sensor data to generate vehicle control commands and evaluate the impact of simulated attacks in real-time. The system includes two PID controllers for longitudinal and lateral motion, operating solely on real-time sensor and ECU data. The autopilot functions as an external application, assigning predefined vehicle paths and integrating steering and throttle commands into the simulation for closed-loop control.

A. Case 1: GPS Spoofing Attack

In this case, we simulate a GPS spoofing attack on an autonomous vehicle using the LGSVL simulation software. The vehicle's autopilot program relies on the GPS sensor to determine its current location. This location data, combined with the desired destination, allows the controller to generate a target vector representing the optimal driving route. The difference between this target position and the vehicle's current orientation, as measured by the Inertial Measurement Unit (IMU) sensor, is used as an error term that controls the steering behavior via the horizontal PID controller. Under normal conditions, the target direction is accurately calculated, enabling the vehicle to navigate curves and follow the desired path seamlessly (illustrated by the green line in the figure). However, during the GPS spoofing attack, the GPS sensor updates are manipulated, resulting in incorrect position data. This manipulation disrupts the calculation of the target direction, making it impossible to accurately steer the vehicle. As a result, the steering behavior becomes erratic, causing the vehicle to deviate from the intended path (represented by the red line in the figure). The graph also illustrates the vehicle's orientation over time, as obtained by the Global Positioning System (GPS) sensor, demonstrating the effect of the spoofing attack on regular operation. The attack induces significant variations, emphasizing the vulnerability of autonomous systems to GPS spoofing and the critical need for robust security measures to mitigate such attacks.

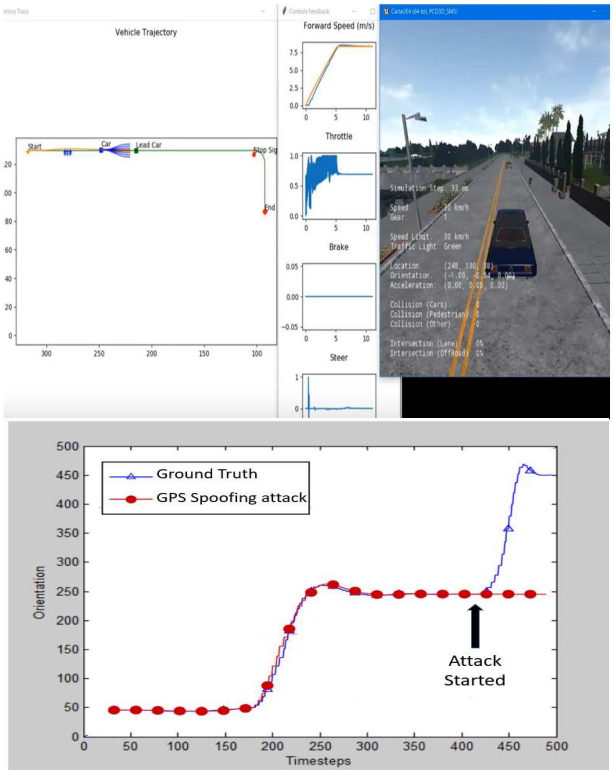

Fig.3. Simulating and testing GPS spoofing attack on AV

Figure 3 illustrates a GPS Spoofing Attack Scenario, showing how inaccurate position updates can severely impact the autopilot's ability to maintain control. The vehicle deviates from its intended path (blue) and collides with a wall (red). This highlights the importance of accurate GPS data for the safe operation of autonomous vehicles. Simulations using LGSVL demonstrate how compromised GPS signals lead to erroneous navigation decisions, causing incorrect steering and path deviation. The scenario emphasizes the vulnerability of autonomous systems to cyber attacks and the need for robust security measures. It also aids researchers and engineers in improving the resilience of autonomous driving technologies.

B. Case 2: V2X Attacks

In a platooning scenario with three networked vehicles using Vehicle-to-Everything (V2X) communication, a

message falsification attack can have severe consequences. In this example, an attacker gains access to the second vehicle in the convoy and manipulates V2X data to falsely maintain the original lane information, despite the lead vehicle's lane change due to a roadblock warning. As a result, the trailing vehicle, unaware of the altered data, continues on the same path and crashes into the barrier. This attack disrupts vehicle coordination and safety, highlighting the urgent need for robust security measures to protect V2X communications and ensure the safety of autonomous vehicle platoons. Figure 4 shows a V2X attack scenario where a victim vehicle receives tampered V2X communications instructing it to switch lanes. Despite the instruction (indicated by a ring), the vehicle does not change lanes and instead crashes into an obstacle in its original lane (shown by a triangle). This demonstrates the critical need for secure V2X communication protocols, as malicious alterations can lead to dangerous outcomes, such as collisions. The incident highlights the severe consequences of compromised V2X communications and the necessity for strong security measures to safeguard autonomous vehicle systems from such attacks.

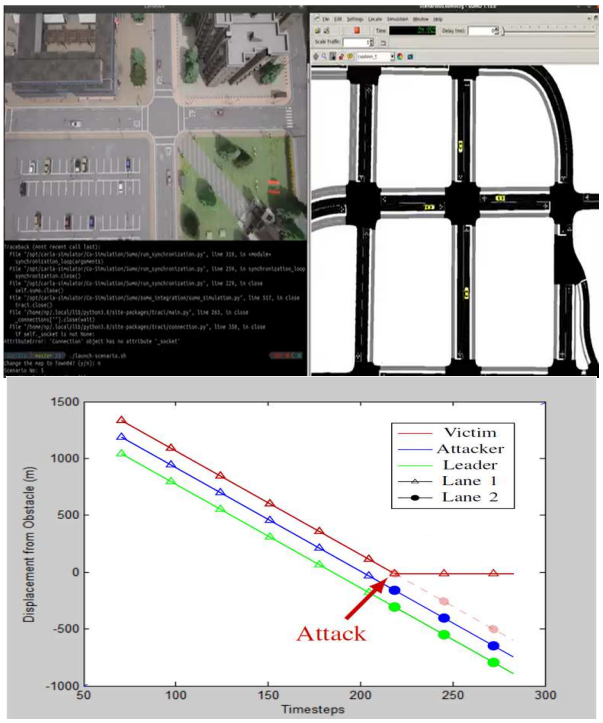

Fig .4. Simulating and testing V2X attacks on AV

C. Case 3 : Replay Attack

In figure 5 , a replay attack scenario is simulated, the study investigates changes in a vehicle's speed profile under normal and manipulated conditions. Initially, normal driving speed data is recorded, followed by a simulated attack where altered speed data is replayed to the vehicle's control system. This manipulation causes a significant, artificial increase in speed, mimicking unsafe driving conditions. The attack lasts from the 200-second to the 400-second mark, demonstrating prolonged injection of erroneous data. Figure 5 contrasts the normal speed profile (black line) with the attacked profile (red line), showing a 50% increase starting at the 200-second mark. Vertical dashed lines and a shaded area denote the attack duration, with annotations highlighting its start and end, underscoring the deviation from normalcy and potential safety risks posed by falsified speed data.

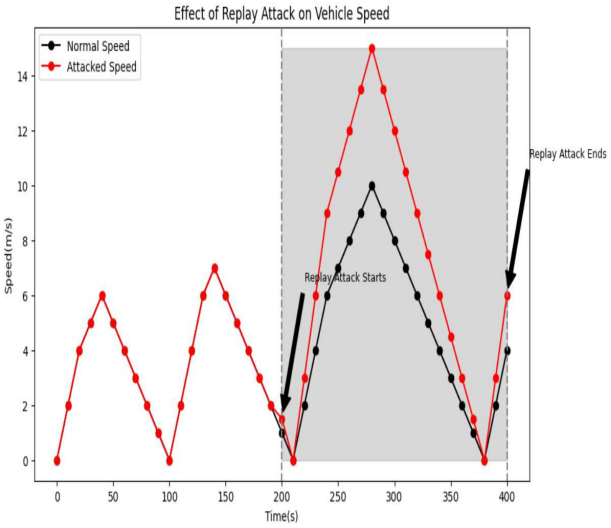

Fig.5. Simulating and testing Replay attacks on AV

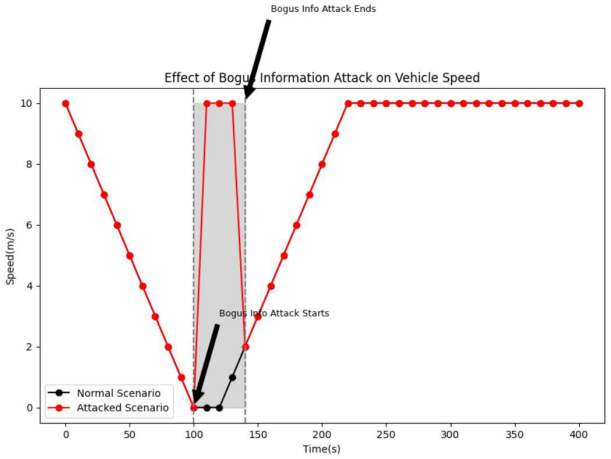

Fig.6. Simulating and testing Bogus Information attacks on AV

D. Case 4 : Bogus Information Attack

In figure 6, a bogus information attack scenario is simulated, the response of an autonomous vehicle to traffic light signals is observed under normal conditions and during an attack. Normally, the vehicle decelerates and stops at a red traffic light. However, during the attack, false information makes the vehicle perceive the red light as green, causing it to continue through the intersection instead of stopping. A plot shows the vehicle's speed over time: the black line indicates normal conditions with deceleration and stopping, while the red line shows the vehicle maintaining speed through the intersection during the attack. Vertical dashed lines and a shaded grey area indicate the attack duration. This visualization highlights the dangers of erroneous information in V2X communication systems and the need for secure communication to prevent such vulnerabilities.

E. Discussion

As stated before, different simulators are used in the creation of self-driving systems to examine various navigation scenarios within a safe yet flexible environment. These simulators can be categorized based on their focus: 1) sensor suites like Lidar, camera, and GNSS (e.g., CARLA, LGSVL), 2) in-vehicle networks (e.g., VEOS), and 3) external communication (e.g., Veins, SUMO, OMNeT++). Integrating multiple tools to simulate various system components is time-consuming and complex. Furthermore, these environments were not originally designed to address adversarial attacks. Recent research has started to bridge this gap by simulating attacks on smart vehicle components. For example, one study extended CARLA to implement GNSS sensor attacks, another used CARLA to evaluate Adversarial Patch Attacks, and Iqbal et al. generated attack data for V2X communication using Eclipse MOSAIC with OMNeT++ and SUMO for 2D visualization. The paper emphasizes Simuhack's effectiveness in generating realistic attack scenarios for autonomous vehicles within a secure testing environment. Simuhack allows for secure examination of each component's security by creating attack data and evaluating system responses. Deviations from expected behavior indicate vulnerabilities. Using LGSVL for sensor data enhances credibility, and Simuhack's advanced attack layer simulates highly relevant assaults, surpassing existing assessment tools. Simuhack's comprehensive security assessment approach helps researchers and developers identify and mitigate vulnerabilities, significantly advancing the safety and security of autonomous driving technologies.

V. Conclusion

This paper introduces Simuhack, an innovative framework tailored to enhance cybersecurity in autonomous vehicles. Simuhack effectively simulates GPS spoofing and jamming attacks to evaluate detection and mitigation capabilities against GPS vulnerabilities. It also addresses vehicle networking attacks by emulating CAN bus, Ethernet, and V2X channels to assess communication protocol vulnerabilities. The framework systematically targets ECUs with tailored attacks and simulates replay and bogus information attacks, bolstering cybersecurity measures. Our key findings demonstrate Simuhack's ability to replicate a wide array of cyber attack scenarios, providing a comprehensive testing ground for evaluating the resilience of autonomous vehicle systems. The implications of these findings for cybersecurity in autonomous vehicles are significant: Simuhack enables rigorous testing and validation of defensive mechanisms, facilitates the identification of system weaknesses, and aids in the development of robust, proactive cybersecurity strategies. Practically, Simuhack stands out as a critical tool for researchers, developers, and industry stakeholders. It offers a versatile and scalable solution for safeguarding autonomous vehicles against emerging cyber threats, ensuring their safe and secure deployment in real-world environments. By enabling the detailed study and mitigation of potential cyber attacks, Simuhack contributes to the advancement of autonomous driving technologies, promoting safer and more reliable autonomous vehicle operations on our roads.

References

[1] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, “Remote attacks on automated vehicles sensors: Experiments on camera and lidar,” in Black Hat Europe, vol. 11, 2015.

[2] W. Thiel, “The VaMoRs Was the World’s First Real-Deal Autonomous Car,” [Online]. Available: https://www.web2carz.com/autos/car-tech/6396/the-vamors-was-the-worlds-first-real-deal-autonomous-car. [Accessed: 17-October-2022].

[3] G. Rong, B. H. Shin, H. Tabatabaee, Q. Lu, S. Lemke, M. Možeiko, E. Boise, G. Uhm, M. Gerow, S. Mehta, E. Agafonov, T. H. Kim, E. Sterner, K. Ushiroda, M. Reyes, D. Zelenkovsky, and S. Kim, "Lgsvl simulator: A high fidelity simulator for autonomous driving," in 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC). IEEE Press, pp. 1–6,2020.

[4] Dosovitskiy, Alexey, et al. "CARLA: An open urban driving simulator." Conference on robot learning. PMLR, 2017.

[5] Olasupo, O., "An Efficient Vehicle-to-Everything (V2x) Communication Algorithm for the Deployment and Operation of Self-Driving Cars," SSRN Electronic Journal, 2022.

[6] Khemissa, Hamza, and Pascal Urien. "Centralized architecture for ECU security management in connected and autonomous vehicles." 2022 13th International Conference on Information and Communication Technology Convergence (ICTC). IEEE, 2022.

[7] Tippenhauer, Nils Ole, et al. "On the requirements for successful GPS spoofing attacks." Proceedings of the 18th ACM conference on Computer and communications security. 2011.

[8] Kiruthika, D., N. Vinothini, and G. Ananthi. "Probabilistic Analysis of GPS Spoofing Attack Failures Using Poisson Point Process." 2024 Third International Conference on Power, Control and Computing Technologies (ICPC2T). IEEE, 2024.

[9] Sadaf, Memoona, et al. "A novel framework for detection and prevention of denial of service attacks on autonomous vehicles using fuzzy logic." Vehicular Communications 46 ,2024.

[10] K. Kim, J.S. Kim, S. Jeong, J.-H. Park, and H.K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense ," Computers & Security, vol. 103, p. 102150, 2021.

[11] Al-shareeda, Mahmood A., et al. "Review of prevention schemes for replay attack in vehicular ad hoc networks (VANETs)." 2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP).,IEEE, 2020.

[12] Stępień, Krzysztof, and Aneta Poniszewska-Marańda. "Security measures with enhanced behavior processing and footprint algorithm against sybil and bogus attacks in vehicular Ad Hoc network." Sensors, 21(10) ,2021.