A Comprehensive Threat Model for Autonomous Vehicle Communication Security

1st Niranjan W. Meegammana
Cyber Security Research Lab
Shilpa Sayura Foundation
Kandy, Sri Lanka
niranjan.meegammana@gmail.com

2nd Harinda Fernando
Dept. of Computer Systems Engineering, Faculty of Computing
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
harinda.f@sliit.lk

***Abstract*—The rapid advancement of autonomous vehicles (AVs) promises to enhance transportation efficiency, reliability, and safety. However, these systems, particularly their vehicular communications, are vulnerable to cyber attacks that threaten confidentiality, integrity, and availability. The 2014 Chrysler Jeep hack highlights the urgent need for robust security measures in vehicular communications. This study utilizes the STRIDE, DREAD, and MITRE ATT&CK security frameworks to develop a comprehensive threat model that identifies and assesses critical threats and risks to AV communications. By detailing specific attack vectors and their multidimensional impacts and criticality, the study aims to guide the development of effective cyber security measures to protect AV communications. The insights provided are intended to assist stakeholders in designing innovative security solutions, thereby improving the reliability and safety of AV navigation and fostering growth in the AV industry.**

***Index Terms*—Autonomous Vehicles, Cyber security, Vehicular Communications, Threat Modeling**

I. Introduction

Autonomous vehicles (AVs) operate and navigate without human intervention by using advanced sensors, communications, and artificial intelligence (AI) to provide situational awareness and make real-time decisions for safe navigation [1]. AVs use a myriad of sensors, as described in Table I, to perceive, understand, localize, and safely interact with their environment, ensuring reliable and safe navigation.

TABLE I
Sensors and their purposes in AVs

Sensor	Purpose
LiDAR (Light Detection and Ranging)	Detects and creates 3D maps of AV surroundings.
Radar (Radio Detection and Ranging)	Detects the speed, range, and movement of objects.
Cameras	Captures visuals for object recognition.
Ultrasonic Sensors	Detect nearby objects for low-speed maneuvers.
GPS (Global Positioning System)	Provides geographic location and AV velocity.
Inertial Measurement Unit (IMU)	Measures the AV acceleration and angular velocity.
Infrared Sensors	Detects heat signatures for pedestrian detection.
Odometry Sensors	Track the distance traveled by the vehicle.

A. Vehicular Communications

Vehicular networks are of two types: external and in-vehicle. External networks are decentralized and dynamic, needing no centralized infrastructure. In-vehicle networks connect sensors, electronic modules, software, and vehicle mechanics. In external networks, AVs function as nodes. They act as both clients and routers, enabling direct communication with each other and forwarding data to extend the network. [2]. Vehicular networks use Vehicle-to-Everything (V2X) wireless communications. Vehicles communicate with each other using Vehicle-to-Vehicle (V2V) channels and with infrastructure using Vehicle-to-Infrastructure (V2I) channels, utilizing both single-hop and multi-hop messages. Infrastructure-to-infrastructure (I2I) and Vehicle-to-Pedestrian (V2P) communications provide additional links between infrastructure elements and pedestrians. As shown in Figure 2, these communications enhance road safety by preventing vehicle collisions and reducing human errors [3].

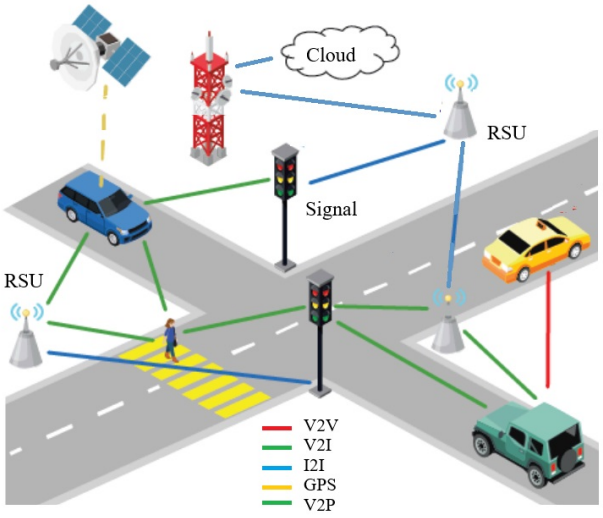

Fig. 1. An Autonomous Vehicle environment [3]

On-board units (OBUs) embedded in vehicles assist in tracking vehicle movements, while Roadside Units (RSUs) manage traffic signals and authenticate vehicles. OBUs and RSUs broadcast safety information using Basic Safety Messages (BSMs) within a single WSMP frame over a single hop. Each BSM consists of a header, payload, and security extension. Vehicles broadcast BSMs every 100–300 milliseconds, including details about the vehicle's position, speed, direction, acceleration, brake condition, and size as shown in Figure 2 [4]. Basic Safety Messages (BSMs) are crucial for Vehicle-to-Everything (V2X) communication systems, enhancing safety, efficiency, and the overall driving experience.

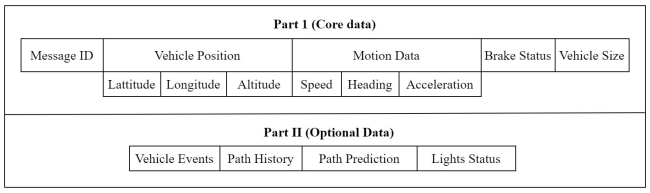

Fig. 2. Basic Service Message [3]

They provide real-time data on a vehicle's speed, position, and heading, helping detect potential collisions and dangerous situations. By sharing this information, BSMs enable nearby vehicles to anticipate and avoid collisions, improving situational awareness. Additionally, they contribute to better traffic management, reduce congestion, support smart infrastructure solutions, and ensure interoperability across different vehicle types. Therefore, protecting BSMs is essential for AV communications security. [3]. AI models used in V2X communication help optimize traffic flow, reduce congestion, manage traffic signals, avoid collisions, provide adaptive cruise control and lane-keeping assistance, facilitate predictive maintenance, and enable vehicle cooperation and platooning [5].

B. Threats to V2X Communication

Attackers can disrupt V2X communications through various methods, such as Denial of Service (DoS) attacks, jamming, spoofing, vehicle impersonation, and message manipulation. These attacks can compromise AV systems' confidentiality, integrity, and availability [3]. Attackers can target AI models through data poisoning during training and by crafting messages to cause unexpected vehicle behaviors during operation. Protecting V2X communications and AI models is essential to ensure reliable and safe navigation [5]. Therefore, implementing robust authentication, strong encryption, real-time monitoring, secure firmware updates, and adversarial training of AI models is essential to safeguard vehicular communications and enable AVs to navigate efficiently and safely [6].

C. Threat modeling

Threat modeling in AVs aims to identify, assess, and prioritize threats and vulnerabilities in software, hardware, and communication interfaces. It helps address vulnerabilities before they can be exploited, design specific security measures, improve incident response, enhance privacy protection, and ensure regulatory compliance [7]. Traditional cyber security frameworks, such as NIST CSF and ISO 27001, are used for threat modeling in organizational environments. They are broad and lack the depth and granularity needed for the real-time and connected nature of AI-driven autonomous vehicles [8].

The study addresses gaps identified in previous research by constructing an optimized threat model for AV communication security. Its novelty lies in the structured approach to identifying threats, assessing risks, creating a threat landscape, and validating results to develop a comprehensive threat model with a unified threat grid. This model offers a clear view of threats to AV communications and informs the development of effective mitigation strategies. Additionally, it provides valuable insights for stakeholders to develop secure AV systems, standards, and regulations, thereby building public trust.

The subsequent sections of this paper include a Literature Review that explores AV threat modeling and relevant research. The Methodology section outlines the steps taken to conduct the research. The Threat Model section presents the developed threat model, including risk assessment and the unified threat grid. Finally, the Conclusion summarizes the key insights gained from the research and suggests directions for future investigation.

II. Methodology

The study followed a systematic approach, described below, to develop a threat model for AV communication security.

A. Data Collection

The study searched Google Scholar using the following terms: *autonomous vehicle threat model*, *STRIDE*, *DREAD*, *MITRE ATT&CK*, and *risk assessment*. Publications from the past three years were selected for the literature review and obtained from IEEE Xplore, ACM Digital Library, and ScienceDirect.

B. Data Analysis

The data analysis involved reviewing and categorizing publications on AV communication security and threat modeling. Studies were evaluated for relevance and impact, and their methodologies and results were compared to identify trends and research gaps. This synthesis helped highlight effective approaches and inform future research directions.

C. Threat modeling

The study utilized the STRIDE framework to systematically identify and categorize potential security threats by focusing on various types of attacks. The DREAD framework was used to assess and prioritize the identified security threats by evaluating their potential impact. The MITRE ATT&CK framework provided detailed insights into how attacks may be carried out and how to mitigate them effectively, as well as to validate the threat model [8].

The STRIDE framework categorizes cyber security threats into six categories: **S**poofing affecting authenticity, **T**ampering affecting integrity, **R**epudiation affecting non-repudiation, **I**nformation disclosure affecting confidentiality, **D**enial of Service, and **E**levation of privilege affecting authorization [9]. The DREAD methodology assesses risks for **D**amage, **R**eproducibility, **E**xploitability, **A**ffected users, and **D**iscoverability [10].

The MITRE ATT&CK Framework provides adversary tactics and techniques, offering a granular analysis of attacks that helps in planning effective defense mechanisms. It supports the validation of threat modeling results by mapping similar incidents to the Common Vulnerability Scoring System

(CVSS), which is derived from real-world observations. The study identifies attacks on AVs using the STRIDE,determines the risk level of each attack using the DREAD and validate the threat model using MITRE ATT&CK. This integration helps ensure that threat models are grounded in practical, observable vulnerabilities and attack patterns.

D. Risk Score Calculation

The study assesses the impact of an attack in three CIA triad dimensions to calculate the average impact. Confidentiality refers to how well the system protects sensitive information. Integrity pertains to the accuracy and reliability of the data and systems. Availability relates to how accessible the system and its data are. likelihood refers to the probability that a specific attack will occur.

The attack likelihood is assigned as follows: Unlikely (0), Low (1), Likely (2), Moderate (3), and High (4). Impact levels are assigned as Low (1), Moderate (2), Significant (3), High (4), and Critical (5) for Confidentiality, Integrity, and Availability. The Risk Score [10] of an attack is given by:

$$\text{Risk Score} = \text{Impact} \times \text{Likelihood}$$

The risk classification thresholds were calculated using percentile values from the distribution of risk scores. The risk level classification thresholds are as follows:

$$\text{Risk Level} = \begin{cases} \text{Critical} & \text{if Rs} > 16.0 \\ \text{High} & \text{if } 13.3 < \text{Rs} \leq 16.0 \\ \text{Medium} & \text{if } 10.7 < \text{Rs} \leq 13.3 \\ \text{Low} & \text{if } 10 < \text{Rs} \leq 10.7 \\ \text{Very Low} & \text{if Rs} \leq 10 \end{cases}$$

III. Literature Review

The literature listed in Table II was reviewed to examine threat modeling in AV communications.

TABLE II
LITERATURE ANALYSIS ON THREAT MODELING

Study	Focus	Contribution	Gaps
[11]	Attacks and defenses.	V2X vulnerabilities.	Adversarial attacks.
[12]	Attacks and defenses.	Common taxonomy.	AI and privacy.
[7]	Threat assessment.	ADAS vulnerability.	Lack expert review.
[10]	Threat modeling.	ADAS attack map.	GPS and AI attacks.
[13]	Attack analysis.	Forensic investigation.	Repudiation attacks.
[14]	Threat Modeling.	Attack tree analysis.	Adversarial attacks.
[15]	Threat Intelligence.	Examples and use cases.	AI integration.
[16]	Threat Modeling.	Nature-inspired algorithms	Limits generalization

A. Similar Work

[11] highlight increasing attacks on V2X communications, emphasizing the potential of AI-enabled defenses. However, the study leaves out adversarial attacks on AI models. [12] explore security threats using a reference architecture based on cloud, edge, and AVs, and present a common attack taxonomy, However, they overlook blockchain defense approaches and adversarial and physical attacks.

[7] perform threat modeling based on ISO/SAE 21434:2021, using the STRIDE methodology to produce an Attack Tree Analysis (ATA). However, it requires complementing the framework with manual expert review. [10] investigated the security of ADAS, using STRIDE and DREAD frameworks to create a threat model based on ISO/SAE 21434 guidelines. The study overlooks GPS location and adversarial attacks on ADAS AI models.

[13] using the STRIDE framework creates a threat model to detect anomalies and suspicious activities in AVs to assist in post-crash analysis and forensic investigations. The study does not consider repudiation attacks that can erase logs, adversarial attacks deceiving AI models, or the use of AI for attack analysis. [14] creates an attack tree using STRIDE and DREAD frameworks and provides defense taxonomy for cloud-assisted AVs. Their threat model leaves out adversarial attacks and defense strategies.

[15] provides a comprehensive overview of threat intelligence in his book by breaking down complex concepts into practical examples and case studies. The author illustrates how threat intelligence can be applied in real-world scenarios. Threat intelligence is invaluable for threat modeling to protect assets from potential attacks with informed decision-making. The book covers the collection, analysis, and integration of threat intelligence with threat models. Threat intelligence helps threat modeling by providing detailed information about potential threats and vulnerabilities. This includes identifying threat actors who might attack, understanding attack patterns they might use, defining indicators of compromise for monitoring, contextualizing vulnerabilities within the threat model, and improving incident response.

[16] examines autonomous vehicle (AV) security, highlighting the importance of understanding attacker models in threat analysis. They use nature-inspired algorithms to optimize threat models and demonstrate their superior convergence rates and effectiveness in developing security measures. However, the study's focus on nature-inspired algorithms limits its generalizability and does not cover all real-world scenarios, which may reduce the robustness of the proposed solutions. Traditional frameworks lack the scope, and scalability required to address the evolving threats to AV communications.

B. Gaps

References [7], [10], and [14] do not address adversarial attacks against AI models in AVs. Most studies also overlook blockchain approaches and the importance of expert reviews. Additionally, their defense strategies often exclude novel AI approaches such as autoencoders and hybrid models. Therefore, there is a need for comprehensive threat modeling that is cross-validated with threat intelligence and expert reviews. Reference [15] requires the inclusion of integrating AI into threat intelligence.

Reference [16] limits threat modeling to nature-inspired algorithms, which restricts the generalization of the solution and

its applicability in real-world scenarios. Overall, cyber security frameworks focused on static environments lack the diverse threat taxonomies, scope and scalability needed to address the evolving risks associated with the real-time and connected nature of AI-driven AVs. This study extends existing frameworks by employing an integrated threat modeling process that uses color coded threat maps and multidimensional risk assessment to develop a detailed threat model to understand the threat landscape in AV communications for developing robust security measures to ensure reliability and safety of AVs.

IV. THREAT MODELING

A. *Threat Maps*

Threat maps visualize threats, attacks, and assets under STRIDE categories. Figure 3 illustrates spoofing attacks that can compromise the integrity of AV communications.

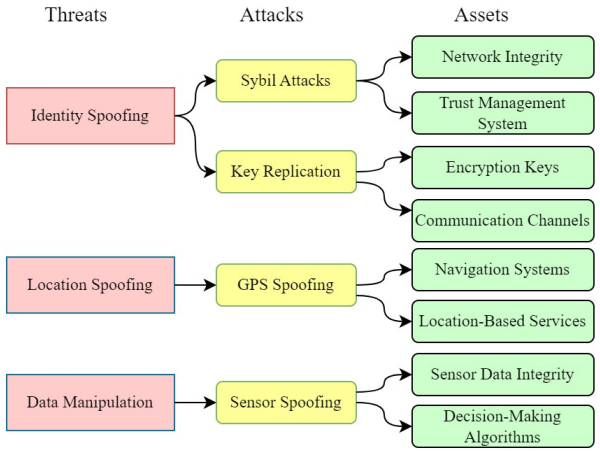

Fig. 3. Spoofing threat map

Identity spoofing includes Sybil attacks and key replication. They undermines the authenticity and reliability of networks. GPS spoofing threatens navigation systems. Data manipulation with sensor spoofing further jeopardizes the system's reliability.

Tampering threats shown in Figure 4 target the integrity of messages, code, and AI systems in AV communications.

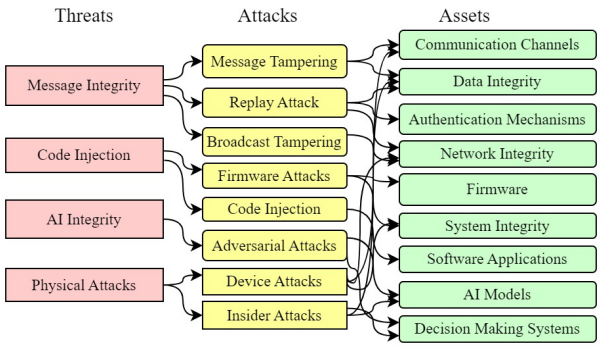

Fig. 4. Tampering threat map

Message tampering, replay attacks, and broadcast tampering aim to jeopardize communication channels, data integrity, authentication mechanisms, and network integrity. Code injection threats target firmware through attacks and direct code injections, threatening firmware, system integrity, and software. Adversarial attacks can compromise AI models and decision-making systems. Physical attacks can impact many assets.

Repudiation threats are shown in Figure 5, aimed at modifying logs to compromise the integrity of accountability systems, audit logs, and forensic data used in AV communications.

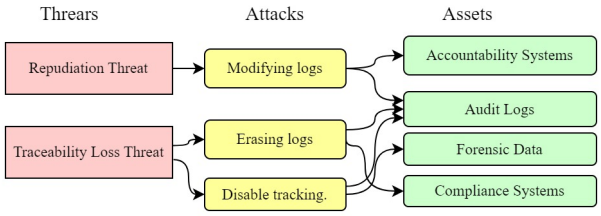

Fig. 5. Repudiation threat map

Traceability loss involves erasing logs or disabling tracking mechanisms, can severely hinder the ability to trace activities, undermining both compliance and forensic investigations.

The information disclosure threats shown in Figure 6 significantly impact confidentiality in AV communications.

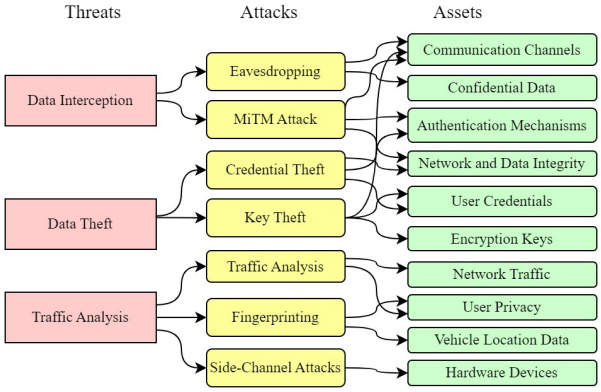

Fig. 6. Information Disclosure threat map

Data interception enables eavesdropping and man-in-the-middle (MiTM) attacks, compromising communication channels, confidential data, and authentication mechanisms. Data theft, through credential and key theft, threatens network and data integrity, compromises user credentials, and undermines encryption keys, and jeopardizes the confidentiality and integrity of the system. Traffic analysis, including fingerprinting, targets network traffic, user privacy, and vehicle location data. Side-channel attacks on hardware devices can reveal critical information about the system.

Denial of Service (DoS) attacks shown in Figure 7, target the Network Bandwidth by overwhelming the AV network with an excessive number of messages. This causes significant degradation in network performance and disrupts vehicle operations.

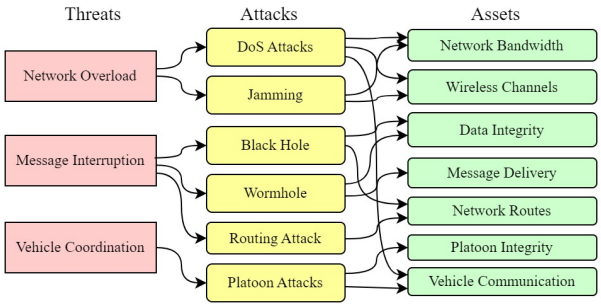

Fig. 7. DoS Attacks threat map

Jamming attacks can compromise essential communication channels through interference. Platoon attacks can disrupt vehicle coordination and formations.

Elevation of privileges attacks shown in Figure 8, involves credential theft, key theft, and privilege escalation, each targeting the AV access control system and allowing unauthorized access to higher privilege levels in the AV system.

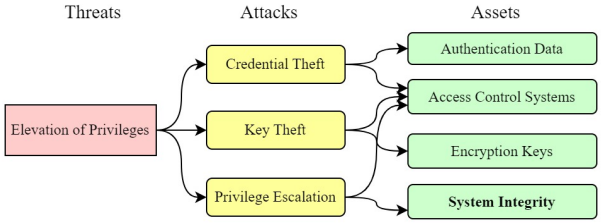

Fig. 8. Tampering threat map

Key theft undermines the security of encryption keys, jeopardizing access control and the confidentiality of communications. Privilege escalation threatens system integrity by enabling attackers to abuse higher access levels.

B. Threat Landscape

Figure 9 represents the threat landscape of AV communications derived from STRIDE threat modeling. It maps the identified attack vectors to targeted assets and is color-coded for criticality based on the risk assessment.

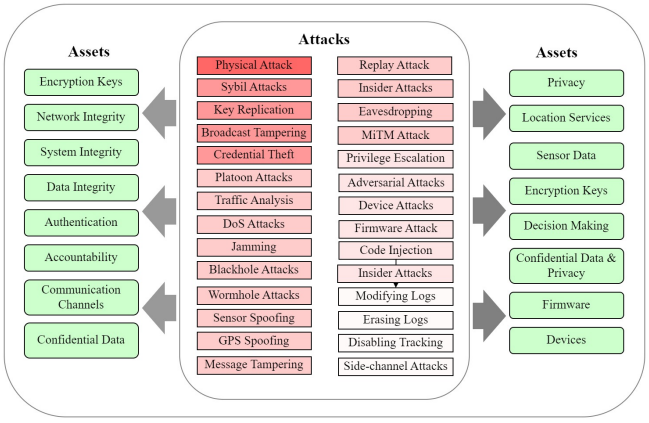

Fig. 9. Threat Landscape

This mapping, along with the risk assessment in Table III, is highly valuable for identifying both individual and multilateral attack vectors that can exploit vulnerabilities in AV communications. By clearly illustrating the relationships between attacks, assets, and their criticality, they help in the development of targeted mitigation strategies to address threats to AV communications.

C. Risk Assessment

Table III highlights the likelihood (Lh), impact on confidentiality (Cn), integrity (In), availability (Av), risk score (Rs), risk and criticality of identified attacks, ordered by risk score.

TABLE III
RISK ANALYSIS OF ATTACKS ON AV COMMUNICATIONS

Attack	Lh	Cn	In	Av	Rs	Risk	Criticality
Physical Attack	H(4)	C(5)	C(5)	C(5)	20.0	Attacks on communication devices.	Critical
GPS Spoofing	H(4)	S(3)	H(4)	C(5)	16.0	Transmit incorrect GPS signals.	High
MiTM Attack	H(4)	C(5)	H(4)	S(3)	16.0	Intercept and alter messages.	High
Key Theft	H(4)	C(5)	H(4)	S(3)	16.0	Stealing encryption keys.	High
Code Injection	H(4)	S(3)	C(5)	H(4)	16.0	Inserting harmful code to software.	High
Credential Theft	H(4)	H(4)	H(4)	S(3)	14.7	Stealing authentication data.	Medium
Firmware Attack	H(4)	M(2)	C(5)	H(4)	14.7	Manipulating the low-level software.	Medium
Message Tampering	H(4)	H(4)	H(4)	S(3)	14.7	Intercept and modify messages.	Medium
Replay Attack	M(3)	M(2)	S(3)	H(4)	14.7	Replay captured messages.	Medium
Sybil Attacks	H(4)	S(3)	H(4)	S(3)	13.3	Create multiple fake nodes.	Medium
Fingerprinting	M(3)	C(5)	S(3)	M(2)	13.3	Tracking vehicle movements.	Medium
Sensor Spoofing	M(3)	S(3)	C(5)	H(4)	12.0	Feeding incorrect data to sensors.	Medium
Privilege Escalation	M(3)	H(4)	C(5)	S(3)	12.0	Gains a higher level of access.	Medium
Adversarial Attacks	M(3)	S(3)	C(5)	H(4)	12.0	Send malicious inputs to AI.	Medium
Device Attacks	M(3)	H(4)	C(5)	S(3)	12.0	Compromise device functionality and security.	Medium
Eavesdropping	M(3)	H(4)	M(2)	M(2)	12.0	Intercepting communications.	Medium
Key Replication	M(3)	H(4)	H(4)	S(3)	11.0	Steal and use encryption keys.	Medium
Insider Attacks	M(3)	M(2)	H(4)	C(5)	11.0	Compromise system and data security.	Medium
Traffic Analysis	H(4)	H(4)	M(2)	M(2)	10.7	Monitoring network traffic.	Low
Jamming	H(4)	L(1)	M(2)	C(5)	10.7	Overloading wireless frequencies.	Low
Blackhole Attacks	H(4)	L(1)	M(2)	C(5)	10.7	Drop messages without forwarding.	Low
Platoon Attacks	M(3)	M(2)	S(3)	C(5)	10.0	Disrupt vehicle movement.	Low
Wormhole Attacks	M(3)	M(2)	H(4)	H(4)	10.0	Capture and replay messages.	Low
Modifying Logs	M(3)	S(3)	H(4)	S(3)	10.0	Deny action by modifying logs.	Low
Erasing Logs	M(3)	S(3)	H(4)	S(3)	10.0	Erasing logs to disable tracking.	Low
Disabling Tracking	M(3)	S(3)	H(4)	S(3)	10.0	Compromise safety in navigation.	Low
DoS Attacks	H(4)	L(1)	L(1)	C(5)	9.3	Flooding systems with messages.	Very Low
Broadcast Tampering	M(3)	M(2)	H(4)	S(3)	9.0	Broadcast unauthorized messages.	Very Low
Side-channel Attacks	L(2)	C(5)	S(3)	M(2)	6.7	Low-level signal monitoring.	Very Low

D. Impact of Attacks on AV Communication

Figure 10 illustrates the likelihood and impact of various attacks on confidentiality, integrity, availability, and the overall risk score for AV communications.

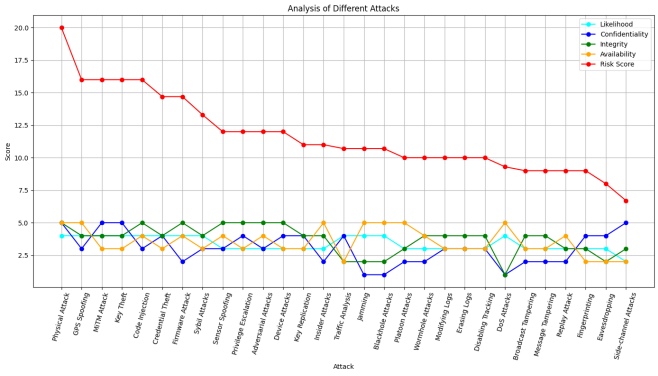

Fig. 10. Impact of various communication attacks

In this threat model, Physical Attacks are the most critical risk. Sybil Attacks, Key Replication, Broadcast Tampering, and Credential Theft are high risks. Risks ranging from Platoon Attacks to Eavesdropping are medium risks. From Key Theft to Insider Attacks are low risks. The remaining threats are very low risks. However, depending on the scenario and the attacker's motivation, even a low-risk attack can escalate to a critical risk [3].

E. Threat Grid

Figure 11 shows a uniform threat grid derived from the threat model. It represents assets, attacks, and their impact on confidentiality, integrity, and availability (CIA), including the criticality of each impact. The color-coded visualization aids in understanding how each attack affects each asset and the CIA triad in AV communications.

	Network Integrity	System Integrity	Data Integrity	Authentication	Accountability	Com. Channels	Location Services	Sensor Data	Encryption Keys	Decision Making	Privacy	Hardware Devices	Firmware	Confidentiality	Integrity	Availability	Criticality
Physical Attack	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	C
Sybil Attacks	1					1									1		H
Key Replication	1					1			1					1	1		H
Broadcast Tampering	1					1									1		H
Credential Theft	1		1	1					1					1	1		H
Platoon Attacks	1					1										1	M
Traffic Analysis	1										1			1			M
DoS Attacks	1														1		M
Jamming	1					1										1	M
Blackhole Attacks	1		1													1	M
Wormhole Attacks	1		1												1	1	M
Sensor Spoofing						1		1		1					1		M
GPS Spoofing							1								1	1	M
Message Tampering			1												1		M
Replay Attack			1	1											1		M
Insider Attacks			1												1	1	M
Eavesdropping						1					1			1			M
MiTM Attack						1					1			1	1		M
Key Theft			1	1					1						1		L
Privilege Escalation		1		1					1						1		L
Fingerprinting							1				1			1			L
Adversarial Attacks								1		1					1		L
Device Attacks		1	1					1		1			1		1		L
Firmware Attack		1											1		1	1	L
Code Injection		1													1		L
Insider Attacks		1	1												1		L
Modifying Logs					1										1		VL
Erasing Logs					1										1		VL
Disabling Tracking					1										1		VL
Side-channel Attacks												1		1			VL

Fig. 11. Threat Grid

The bird's-eye view of the threat grid helps in developing tailored security controls specific to each threat type. For example, stronger encryption can be implemented for attacks affecting confidentiality, integrity checks for attacks impacting integrity, and redundancy and failover strategies for attacks affecting availability. Moreover, the threat grid helps prioritize defense strategies to protect the most vulnerable components in AV communications.

Overall, the threat maps, threat landscape, risk assessment, and threat grid of the threat model support the creation of robust security policies, guide risk mitigation strategies, and facilitate compliance with regulatory requirements. Collectively they provide a comprehensive understanding of potential attack vectors risks and criticality for developing effective mitigation strategies and supports the ongoing improvement of security measures to ensure secure communications for AV reliability and safety.

V. Conclusion

This paper identifies various threats to AV communications by building a comprehensive threat model through a structured process. It integrates attack vectors, assets, impact dimensions, and criticality into a unified threat grid for thorough threat analysis. This model aids in developing robust security policies, guiding risk mitigation strategies, and facilitating compliance with regulatory requirements. The insights provided offer a valuable understanding of the threat landscape for AV communications.

We suggest, that future research should incorporate additional impact dimensions and develop targeted mitigation strategies for the identified threats. Areas of focus should include security strategies for sensor fusion, AI, blockchain, lightweight encryption, real-time monitoring, collaborative attack detection, and auditing [3], while addressing the resource constraints inherent in AVs. This paper serves as an essential resource for stakeholders committed to advancing the security of AV communications.

References

[1] M. N. Ahangar, Q. Z. Ahmed, F. A. Khan, and M. Hafeez, "A survey of autonomous vehicles: Enabling communication technologies and challenges," *Sensors*, vol. 21, no. 3, p. 706, January 2021.

[2] E. Hamida, H. Noura, and W. Znaidi, "Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures," *Electronics*, vol. 4, no. 3, pp. 380–423, July 2015.

[3] N. W. Meegammana and H. Fernando, "Ai-enabled communications security and privacy in autonomous vehicles: Comprehensive review of novel approaches," 2024, unpublished.

[4] A. Sharma and A. Jaekel, "Machine learning based misbehaviour detection in vanet using consecutive bsm approach," *IEEE Open Journal of Vehicular Technology*, vol. 3, pp. 1–14, January 2022.

[5] A. Giannaros *et al.*, "Autonomous vehicles: Sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions," *Journal of Cybersecurity and Privacy*, vol. 3, no. 3, pp. 493–543, September 2023.

[6] A. Talpur and M. Gurusamy, "Machine learning for security in vehicular networks: a comprehensive survey," *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2021.

[7] Z. Abuabed, A. Alsadeh, and A. Taweel, "Stride threat model-based framework for assessing the vulnerabilities of modern vehicles," *Computers & Security*, vol. 133, p. 103391, October 2023.

[8] M. Howard and S. Lipner, "Security development lifecycle," *Datenschutz Und Datensicherheit - DuD*, vol. 34, no. 3, pp. 135–137, February 2010.

[9] Microsoft, "Threats - microsoft threat modeling tool - azure," August 2022, available at: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats.

[10] F. Siddiqui *et al.*, "Cybersecurity engineering: Bridging the security gaps in advanced automotive systems and iso/sae 21434," in *IEEE Xplore*, June 2023.

[11] 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, April 2021.

[12] S. Gupta, C. Maple, and R. Passerone, "An investigation of cyber-attacks and security mechanisms for connected and autonomous vehicles," *IEEE Access*, vol. 11, pp. 90 641–90 669, January 2023.

[13] M. Girdhar, Y. You, T.-J. Song, S. Ghosh, and J. Hong, "Post-accident cyberattack event analysis for connected and automated vehicles," *IEEE Access*, vol. 10, pp. 83 176–83 194, 2022.

[14] A. T. Sheik, C. Maple, G. Epiphaniou, and M. Dianati, "Securing cloud-assisted connected and autonomous vehicles: an in-depth threat analysis and risk assessment," *Sensors*, vol. 24, no. 1, p. 241, January 2024.

[15] M. Lee, *Cyber Threat Intelligence*. John Wiley & Sons, 2023.

[16] M. K. Yogi, D. Sreeja, and S. Siva, "Applying nature-inspired algorithms for threat modeling in autonomous vehicles," in *Advances in Cyber Security*, 2022, pp. 253–276.