A Multidimensional Taxonomy and Systematic Review of Security Threats in VANETs

Dana Kareem Hama[1], Foad Salem Mubarek[2] and Firas Abdulhameed Abdullatif[3]
[1]*Department of Computer Science, College of Computer Science and Information Technology, University of Anbar, 46001 Sulemaniya, Iraq*
[2]*Department of Computer Science, College of Computer Science and Information Technology, University of Anbar, 31001 Ramadi, Iraq*
[3]*Department of Computer Science, College of Education for Pure Sciences (Ibn Al-Haitham), University of Baghdad, 10053 Baghdad, Iraq*
{dan22c1003, Co.foad.salem}@uoanbar.edu.iq, firas.alobaedy@ihcoedu.uobaghdad.edu.iq

Keywords: Intelligent Transportation Systems (ITS), VANET Security, Attacks on VANET, Sybil Attack, DoS Attack.

Abstract: Vehicular Ad hoc Networks (VANETs) are essential in modern Intelligent Transportation Systems (ITS) by facilitating real-time communication between vehicles and roadside infrastructure to enhance road safety, traffic management, and passenger comfort. But several security issues can arise due to its decentralised and wireless nature. This work comprehensively reviews security attacks and mitigation solutions in VANETs. Research articles were sorted according to communication level, security service, and attack type using a systematic literature review. In contrast to previous assessments that mostly focused on descriptive classifications, this work introduces an integrated multidimensional taxonomy that evaluates attacks via three criteria: impact degree, detectability, and target scope. In addition, the article lays out a model for prioritising security services based on the correlation between attack categories and VANET's five core security principles: non-repudiation, authenticity, availability, integrity, and secrecy. Although VANET security has come a long way, current techniques aren't always scalable, flexible, or compatible with emerging technologies such as edge computing and AI-driven detection systems, according to key findings. Future studies and the creation of VANET systems that are safe, scalable, and robust can be organised around the proposed paradigm.

1 INTRODUCTION

Mobile networks that include automobiles and feature both static and dynamic network topologies, as well as intermittent connectivity, are known as vehicular ad hoc networks (VANETs). Because information in VANETs is accessible to the public, protecting user privacy and security is paramount. Virtual area networks (VANETs) rely on security protocols to prevent unauthorized modification of message transmissions, ensuring their effectiveness and reliability [1]. The goal of VANET is to reduce the number of car accidents and improve traffic flow in order to encourage safe driving. Driver safety is at risk if this real-time data is altered in any way. Security professionals place a premium on protecting this data because of its importance to the system's smooth operation [2]. When cars work together as mobile nodes, they form a mobile network that can withstand communication disruptions. This setup is called a VANET. Here are the main parts of VANETs, as described in [3]:

1) Onboard units (OBUs) allow vehicles to communicate with other vehicles and infrastructure; these vehicles are the basic building blocks of VANETs.
2) Secondly, there are infrastructure units known as roadside units (RSUs), which are permanently installed along roads or at locations such as crossroads. To provide essential services such as internet access, traffic reports, and safety warnings, RSUs communicate with OBUs in vehicles. Additionally, they can collect information from moving cars to evaluate environmental or traffic variables.
3) OBUs. These devices are affixed to cars and communicate with RSUs and other OBUs.

They often comprise elements such as a processor, memory, a GPS receiver, and various transceivers for distinct communication standards (e.g., dedicated short-range communication (DSRC), Wi-Fi, and long-term evolution (LTE)) [4]. OBUs process and retain data to facilitate navigation, enhance safety features, and provide entertainment services.

Communication via the DSRC (Dedicated Short-Range Communication) protocol can be V2V (Vehicle-to-Vehicle), V2I (Vehicle-to-Infrastructure), or a hybrid combination. As seen in Figure 2, Users of VANETs benefit from a wide range of applications that fall under entertainment, traffic efficiency, active road safety, and management, the latter of which refers to cooperative navigation and speed management [5], [6]. The absence of threat or danger is the condition of security. Safety and the precautions to keep oneself safe or protected are closely related to security. Due to the inherent challenges of securing VANET as a wireless communication system, it is essential to safeguard against malicious behaviors and meticulously define the security architecture. Security and the level of implementation promised both impact people's safety. We focus on a unique categorization of the numerous attacks and defenses against them documented in the literature on VANET security [7]. Safeguarding VANET connectivity is crucial for enhancing the functionality and communication among vehicle devices. Consequently, formulating security patterns to optimize communication efficacy in VANET has emerged as a challenge for novice researchers[8].

The deficiency in existing research. Recent studies indicate persistent difficulties in categorizing and evaluating risks in actual vehicle contexts, although significant advancements in VANET security research. Several recent studies, including [9] and [10], examine taxonomies that focus solely on a specific layer or danger (e.g., routing or jammer attacks) while overlooking other critical factors, such as the attack's impact on the target, its detectability, and its range of influence. Research conducted by [11] and [12] illustrates progress in AI-based intrusion detection; yet they highlight that the majority of existing frameworks are predominantly descriptive and fail to provide a unified analytical model that associates various attack types with certain security services. The integration of edge and AI-enhanced VANETs inside smart mobility ecosystems has introduced novel vulnerabilities, particularly as vehicles interact dynamically within 5G/6G-enabled intelligent transportation systems (ITS). The current categories are inadequate to capture these complex, cross-layer interconnections and their implications for system scalability and resilience. This study offers a comprehensive attack taxonomy that methodically links VANET threats to security objectives—confidentiality, integrity, availability, authentication, and non-repudiation—and situates these findings within the larger context of smart city infrastructure. This study introduces a framework that enhances both theoretical understanding and practical implementation of secure vehicular networks by merging theoretical classifications with real-world smart mobility applications, including connected autonomous vehicles, cooperative traffic management, and safety-critical communication. This study seeks to conduct a comprehensive analysis of security threats and attack typologies in VANETs, highlighting the utilization of multidimensional categorization frameworks that reflect the dynamic characteristics of VANETs. Unlike traditional research, which provides descriptive categories.

1) This study examines the security threats and assaults in VANET, specifically addressing Confidentiality, Non-repudiation, Data Integrity, Authentication, and Availability within this network.
2) We have performed an extensive study to classify different security threats in VANETs.
3) Vulnerabilities in automotive networks and the deficiencies of existing VANET security standards.

The motivation behind this survey is to identify the security threats in VANET networks. What conditions render the use of the VANET advantageous? What security problems might potentially restrict VANET services? What VANET services may be offered, and what are the immediate implications of those services?

This paper makes several original contributions to the field of VANET security as follows:

1) Integrated Taxonomy Framework, we amalgamate conventional attack classifications (predicated on protocol stack, communication type, and security services) and present an innovative multidimensional classification model that assesses attacks across three dimensions: impact level, detectability, and target scope.
2) Security Service Prioritization classification. A distinctive correlation between VANET assaults and the five essential security services: Confidentiality, Integrity, Availability,

Authentication, and Non-repudiation. This has been suggested to facilitate a systematic assessment of how assaults undermine certain security objectives.

3) Addressing Literature Deficiencies, in contrast to current surveys that are predominantly descriptive, this study offers a decision-focused framework by correlating attack taxonomies.

1.1 Review Methodology

This section comprises a compilation of the sources that constituted the basis for our research, the keywords included in the search phrases, and the search process strategy and filtering methods employed.

1.1.1 Sources of Data

Prior to initiating the search technique, an appropriate selection of electronic resources was identified to locate research papers pertinent to our enquiries. Table 1 presents the research effort allocated to the study before and after filtering (for publications published between 2018 and 2025).

1.1.2 Screening Procedure

Before initiating the search procedure, an appropriate selection of electronic databases was identified to locate research publications relevant to our study. The primary electronic databases utilized in this study were IEEE Xplore, Springer, ScienceDirect, and Google Scholar. Table 2 presents the keywords utilized for the search phrases in the internet databases.

Considering that direct filtering is a characteristic of surfing sites, a total of 18,898 items were acquired following direct exclusion (from 2015 to 2025). This literature review did not encompass all these articles. Papers were chosen according to the following four criteria:

1) Exclusion of publications prior to 2015 (Table 2).
2) Exclusion of books, chapters, master's theses, and doctoral dissertations.
3) Presence of VAENT Attacks in the title or abstract.
4) Presence of ITS, VANET Security Services in the title or abstract.

In total, 72 articles were retrieved according to the requirements mentioned above. We read each article in its entirety and analyzed it. Data and methodology from research papers were extracted, and preliminary study results were reviewed and combined. Figure 1 provides a concise overview and explanation of the sorting and selecting process.

1.2 VANET System Overview

Wireless Ad Hoc Networks (WANET) are the theoretical foundations upon which all ad hoc networks rest. Among the wide varieties of MANETs, one subset is the vehicle ad hoc network. Without a central network, mobile nodes in a MANET can connect. The network's nodes can repair themselves automatically. The intermittent relocation of nodes causes the topology of a Mobile Ad hoc Network (MANET) to change dramatically over time. Every node functions as a router and exhibits independent behaviours [10], [11], [13]. VANETs, comprising high-velocity vehicles and stationary entities, are infrastructure-independent, distributed, and heterogeneous wireless networks [14].

Table 1: Sources were evaluated throughout the search process.

Database	URL
IEEE Xplore	https://ieeexplore.ieee.org/Xplore/home.jsp
Springer	https://www.springer.com/gp/computer-science
ScienceDirect	https://www.sciencedirect.com/
Google scholar	https://scholar.google.com/

Table 2: Keywords for the search queries.

Keywords	URL	Number of papers	Number of papers after filtering (2015-2025)
("Intelligent Transportation Systems (ITS)" or "VANET Security" ANd "Attacks on VANET")	IEEE Xplore	100	58
	Springer	717	283
	ScienceDirect	1,081	160
	Google Scholar	17,000	398

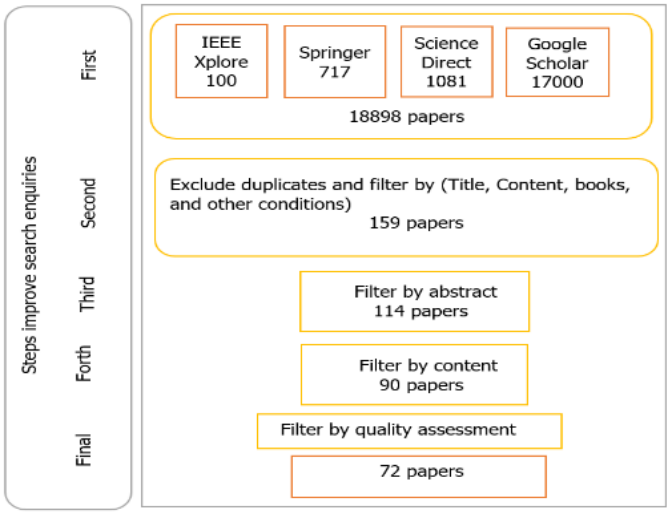

Figure 1: Approach and filtering for search processes in VANET attacks.

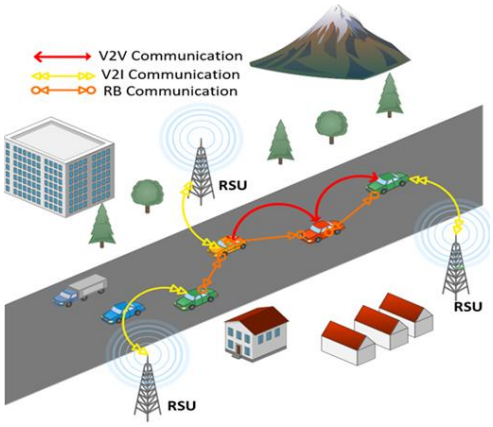

Figure 2: Hybrid vehicle communication in the VANET.

Communication in VANET can occur as V2V, where two vehicles communicate directly or via multi-hop communication, or as V2I, where vehicles interact with fixed infrastructure, referred to as roadside units (RSUs), including base stations, mobile routers (MRs), and access points (APs) [15].

On the other hand, VANET has evolved into a more reliable and stringent alternative to MANET. Different routing protocols are required in VANET compared to MANET, since nodes in VANET can join and leave the network at will. The building blocks of a VANET are RSUs and mobile nodes. An OBU is a component of every vehicle that processes incoming and outgoing data and contains various sensing devices. RSUs are located along highways and act as intermediaries between mobile nodes and the trusted authority. VANET's capacity to enable people to share data over the internet can help make driving safer and more reliable [13], [16]. Figure 3 shows the VANET environment.

The main benefit of VANETs is that they make roads safer by letting vehicles and infrastructure talk to each other. This gives drivers up-to-date information about road conditions, risks, and accidents, which helps them make smart choices and stay safe. VANETs make transport systems work better by making vehicles and infrastructure work together better. Traffic lights that can talk to each other help traffic move faster and cut down on wait times at intersections [15], [17], [18].

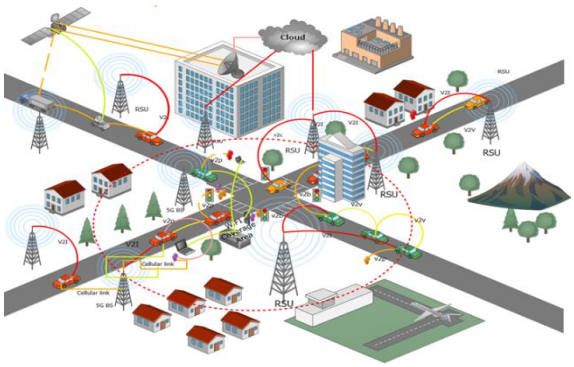

Figure 3: Vehicle Ad Hoc networking environment.

2 VANET SECURITY STANDARDS

Ensuring security is of utmost importance for the successful implementation of VANETs and the overall well-being of society. There are two primary

categories of standards: IEEE 1609 and ETSI standards. The IEEE 1609 family establishes security protocols for vehicle networks at higher levels; however, ETSI standards are predominantly employed in most European countries [19].

Both standard groups have made significant efforts to ensure robust security services in VANET. IEEE 1609.2 offers three fundamental security services: message formats for security-related communications, security for management messages, and security for application messages. This system considers the safety application needs and offers security measures at the lower and upper layers. WAVE Internet Security Services (WISS) offers lower-level security measures, whereas WHLSS provides a revocation service using a Certificate Revocation List (CRL). IEEE 1609.2 establishes the overall structure for security-related messages and techniques; IEEE 1609.3 is a standard that explicitly addresses networking services[15], [17].

ISO/SAE 21434 (Road Vehicles - Cybersecurity Engineering) establishes a framework for cybersecurity engineering throughout the complete vehicle lifecycle. VANET facilitates threat analysis and risk assessment for vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-facility (V2F) communication. Mandates security by design in communication protocols (e.g., authentication, encryption, intrusion detection). Additionally, ensure the security validation of VANET systems [20], [21].

IEEE 1609.4 focuses on facilitating multi-channel operations in VANETs, enabling efficient communication management across multiple safety and non-safety communication channels, as illustrated in Figure 4. All security standards used in VANET will be summarized [2], [20]. These guidelines establish the foundation for safeguarding vehicular communications; yet they are inadequate to confront the diverse array of practical risks.

Security Standard's in VANET	IEEE 1609 Family (WAVE Standards)	1609.1	IEEE 1609 outlines conventional cryptographic primitives including encryption, hashing, and digital signatures. Additionally, it delineates the certificate revocation list (CRL) and the technique for privacy protection through the modification of certificates.
		1609.2	This is a pivotal standard for VANET security. It delineates security services for applications and management messages, encompassing methods for securing communication via the Dedicated Short-Range Communications (DSRC) protocol. It offers mechanisms for authentication, confidentiality, and message integrity.
		1609.3	This standard emphasises networking services and delineates the protocols and services of the network and transport layers, encompassing addressing, routing, and Quality of Service (QoS).
		1609.4	It pertains to multi-channel operations, guaranteeing that VANETs can proficiently oversee communication across various channels, including both safety and non-safety communications.
	ETSI ITS (European Telecommunications Standards Institute Intelligent Transport Systems)	ETSI EN 302 636	This set of standards pertains to networking and transport protocols for Intelligent Transportation Systems communications. It encompasses requirements for GeoNetworking, essential for message transmission in VANETs.
		ETSI TS 103 097	This standard, akin to IEEE 1609.2, delineates security procedures for VANETs within the European framework, encompassing secure message exchange and the implementation of Public Key Infrastructure (PKI) for authentication.
	IEEE 802.11p	IEEE 802.11p is an amendment to the IEEE 802.11 standard that facilitates wireless access in vehicular environments. Although it primarily serves as a communication standard, its significance for security is rooted in its foundational role in Vehicle Ad Hoc Networks (VANET) communication. It encompasses secure communication, as well as media access control (MAC) and physical layer services, specifically pertaining to vehicular networks.	
	C2C-CC (Car-to-Car Communication Consortium) Standards	Protocols and standards for vehicle-to-vehicle (V2V) communication are developed by the C2C-CC. Its primary goals include the development of secure communication protocols and the enhancement of privacy protections in VANETs, as well as the promotion of interoperability across various systems and manufacturers.	
	LTE (TS 33.185)	Security assistance in vehicle-to-everything (V2X) communication, security specifications for V2X, and signaling	
	LTE-A (TS 23.285 v14)	Security support and architecture in V2X, security needs for V2X, authentication, data integrity, secrecy, protection against replay attacks, and signaling.	
	NIST SP 800-53	The NIST Special Publication 800-53 offers a thorough collection of rules for information system security and privacy. The controls described in NIST SP 800-53 can be used to secure VANET infrastructure and components, even though they aren't designed for VANETs specifically.	
	SAE J3061	SAE J3061 delineates protocols for cybersecurity in automotive systems, encompassing VANETs. It provides a procedural framework for managing cybersecurity risks over the lifespan of automotive systems, guaranteeing that cars are developed and maintained with security considerations.	
	SAE J2735	Specifies the collection of transmitted messages between communicating nodes, encompassing the basic safety message (BSM).	
	PKI (Public Key Infrastructure)	PKI is essential in VANET security standards, offering a framework for the issuance, management, and revocation of digital certificates utilised for vehicle authentication and communication security. The incorporation of PKI in standards such as IEEE 1609.2 and ETSI TS 103 097 underscores its significance.	
	5G (TS 23.285 v15)	Verify the V2X security architecture and support, signalling, authentication, data integrity, confidentiality, and protection against replay attacks. Also review the V2X security criteria.	
	ISO 26262	Although largely concentrated on functional safety in road cars, ISO 26262 also impacts VANET security by addressing the safety of electrical and electronic systems within vehicles. The security of these systems is frequently interconnected with their safety, especially with autonomous cars and VANETs.	

Figure 4: Security standards used in vehicular ad-hoc networks.

3 SYNTHESIS AND RESEARCH GAPS FROM RELATED WORKS

Recent research has improved VANET security by creating taxonomies, intrusion detection system models, authentication systems, and frameworks that include fog technology. However, these approaches are either overly narrow and fail to leverage active prioritization or overly rigorous and fail to focus on specific issues. To address this limitation, our study presents a comprehensive framework that combines traditional and multidimensional taxonomies, uses statistical methods to rank assaults by impact, detectability, and scope, and links risks to critical security services. Researchers and practitioners in the field of VANET can benefit more from this systematic approach than from descriptive surveys, as it allows them to make judgments. An attack tree model was published by Houmer and Hasnaoui (2020) in [22]. To evaluate potential attack methods and gauge the danger to network accessibility.

Naqvi and Chaudhary (2021) in [23]. Highlight the significance of Intrusion Detection Systems (IDSs) in protecting against various types of assaults, such as Sybil and Denial-of-Service attacks. One approach to strengthen VANET security proposed by Mengting Yao and Xiaoming Wang [24] is to provide mutual authentication utilizing forward secrecy. In addition, a thorough fine-grained taxonomy is provided by Aldweesh, Derhab, and Emam (2020) that classifies existing intrusion detection system solutions based on deep learning in terms of input data, detection procedures, deployment tactics, and assessment methods [25]. Naqvi, Chaudhary, and Kumar (2022) presented a security-sensitive authentication framework for the VANET system in [26]. The emphasis on VANET security acknowledges the potentially catastrophic consequences of even small security flaws. Implementing Intrusion Detection Systems to protect against malicious nodes is essential. El-Shafai, Azar, & Ahmed, 2025. introduced in [17] An approach that integrates various machine learning and deep learning classifiers to achieve detection accuracy [27]. Their research addresses the significant issue of jamming attacks that threaten the reliability of communication in VANETs.

Although current surveys [11]-[47] have analysed VANET security through several lenses, including attack trees, intrusion detection, and protocol-specific vulnerabilities, none have integrated both traditional and multidimensional taxonomies of attacks into a cohesive framework. Critical Analysis Reasons for the inadequacy of prior works Descriptive, compartmentalised taxonomies: Most surveys categorise attacks from a singular perspective, such as protocol layer, attack family, or tool type, without linking them to operational impact, detectability, and target scope. This constrains decision-making for practitioners who must prioritise defences within the limitations of latency and resource availability. Insufficient connection to security objectives: Limited research directly correlates attacks with CIAAN services, facilitating the selection of defences for secrecy versus availability trade-offs in V2V, V2I, and V2X contexts. Deficiencies in scalability and adaptability: Reputation-based or scheme-specific defences are challenged by adaptive adversaries (e.g., sybil and replay combinations) and by city-scale fleets, where certificate verification, revocation, and real-time inference impose significant demands on OBUs and RSUs. Disjointed standards integration: Analyses frequently reference IEEE 1609.x / ETSI-ITS yet fail to correlate how attack classifications impair particular services or applications (such as collision avoidance and cooperative perception) within those standards, the necessity of the proposed classification.

Multidimensional prioritisation: our taxonomy evaluates each attack based on impact intensity, detectability, and target scope, linking it to CIAAN to transform a static list into a decision-making framework for control selection (e.g., determining when to prioritise speedy availability safeguards over stringent authentication measures).

Multilayered, interdisciplinary perspective: It incorporates edge/fog computing, network slicing, and SDN-VANET factors, enabling practitioners to analyse attack vectors that span several layers and slices, rather than merely isolated weaknesses.

We unify attack classification across communication layers, security services, and adversarial viewpoints, and introduce a multidimensional prioritization model that assesses attacks based on impact, detectability, and scope. Table 3 contrasts several aspects of the preceding surveys concerning (1) attack type and scope, (2) the technique used, (3) the strengths, and (4) the limits of the literature.

Table 3: Related works, contributions, and limitations.

Researcher	Year	Attack Type / Scope	Technique Used	Strengths	Limitations
El-Shafai et al.[11]	2025	Jamming (availability)	AI-driven ensemble classifier	High detection accuracy	Limited generalizability for mixed traffic conditions
Abdelmaguid et al.[12]	2025	Mixed/unknown attacks	Dynamic honeypots with attack-rate analysis	Detects unforeseen behaviors	High operational overhead; difficult real-time tuning
Ghaleb Al-Mekhlafi et al.[32]	2024	Security threats in Fog-enabled VANETs	Systematic review with fog-layer taxonomy	Integrates fog computing with VANET security	Descriptive only; lacks empirical validation and AI/5G scope
Goyal et al.[33]	2022	General VANET Threats	Systematic review of attacks and schemes	Broad coverage of applications and issues	Limited analytical depth; lacks cross-domain insights.
Vamshi Krishna & Ganesh Reddy.[34]	2023	DDoS (Layer-wise)	OSI-layer taxonomy with ML/DL survey	Detailed per-layer classification of DDoS attacks	Focused only on DDoS; lacks quantitative evaluation
Hezam Al Junaid et al.[35]	2018	Security design & attack types.	Security classification framework	Early comprehensive taxonomy defines attacker models	Outdated; no multidimensional or AI-driven analysis.
B. K.[36]	2024	Security & Privacy Attacks	Systematic review	Links privacy and cryptographic approaches	Omits conditional privacy models and simulation tools.
Hasan et al.[37]	2020	Platform vulnerabilities	Analytical study of V2X standards	Highlights IEEE/ETSI protocol risks	Pre-AI perspective; no quantitative or empirical validation
Gyawali, Qian & Hu.[38]	2020	Insider / False Data Attacks	ML and Reputation-based Misbehavior Detection	Integrates trust and ML; low detection latency	Heavy reliance on simulation data, limited real-world validation
Velayudhan, Anitha & Madanan.[39]	2022	Sybil & Location Privacy	EPORP protocol for Sybil detection in cities.	High accuracy, low delay, enhanced privacy	Computationally complex due to multi-stage optimization
Hostak & Baronak.[40]	2023	Delay, Drop & Sinkhole	OMNeT++ / IEEE 802.11p simulations	Quantifies QoS impact; realistic VANET modeling	Lacks defense mechanisms or ML integration
Khayati & Mazri.[41]	2020	Routing (DDoS, Wormhole, Blackhole)	Comparative analysis of detection models	Covers major routing-layer threats	no multidimensional classification or real-world validation
Anwar et al.[42]	2023	In-vehicle Protocols	Comparative security analysis	Reviews CAN, LIN, and Ethernet vulnerabilities	Focused on intra-vehicle systems; not VANET-oriented
Baee et al.[43]	2023	Authentication Scheme Flaws	Cryptanalysis and rectification (2FLIP)	Identifies replay and impersonation issues; proposes fixes	Focused on a single scheme; lacks generalization
Pavithra & Nagabhushana.[44]	2020	VANET threats.	Layer & activity-based classification	Links attacks to QoS parameters	No defense or multidimensional evaluation
Quyoom, Mir & Sarwar.[45]	2020	General VANET security.	Service-based classification	Maps attack to CIAAN security services	Descriptive; lacks empirical assessment
Krishna & Reddy.[46]	2022	VANET Vulnerabilities	OSI-layer taxonomy	Clear hierarchical attack mapping	Purely descriptive; no impact/detectability analysis
Setia et al.[47]	2024	DDoS in VANET-Cloud	Hybrid ML-based detection framework	High accuracy; integrates cloud simulation	ML methods may limit adaptability to varied attacks

4 SECURITY REQUIREMENTS IN VANET

Efficient and dependable security procedures are essential for the safety-related applications of VANET to mitigate upcoming attacks. The communications transmitted through these apps must remain unaltered, counterfeited, and unexploited by potential attackers, as any breach of these messages could have life-threatening consequences for drivers and passengers. The main security requirements for VANET and their impact on the network are summarized in Table 4 [19].

Autos connect to roadside infrastructure and each other through public networks. Data transmissions within VANETs are susceptible to unauthorized access. Therefore, guaranteeing the security of sent data is of the utmost importance [16]. As shown below, the literature outlines the primary security requirements for vehicle communication. Here are a few things that VANET security must have:

1) Availability: The primary problem of VANETs is the availability of the wireless channel for receiving vital communications from vehicles. If an intruder executes a Denial-of-Service Attack (DoS) to disrupt traffic, it will prevent the transmission of essential information between vehicles, rendering them ineffective. Therefore, it is necessary to have a high level of accessibility for the wireless channel [13]. Providing real-time network services is the primary goal of VANET. It appears that the majority of attacks are aimed at disrupting the availability of resources[44,45].
2) Data Integrity: Prior to moving on, make sure the messages arrive at their intended recipients. Unauthorized changes to the network are one example of a security breach that requires a rapid reaction mechanism [44]. Regarding VANET security, integrity is paramount. There is zero chance of data corruption or loss when a gearbox is operational or when a vehicle comes into contact with roadside infrastructure [10], [48], [49].
3) Authentication: Authentication is the crucial element in ensuring a secure connection. Authentication is a critical requirement for VANETs to provide secure communication between vehicles. Lack of a secure authentication method between VANET components can result in unauthorized individuals intercepting sent information, leading to potential damage[2], [5],[10], [48].
4) Confidentiality: Confidentiality is the fourth most significant aspect of security. Encrypting sensitive information is essential in some circumstances to safeguard it against unauthorized access. In VANETs, cars occasionally exchange confidential data, as they do in military convoys. To ensure the confidentiality of the sensitive information, it must be transferred in an encrypted manner, preventing unauthorized individuals from comprehending the contents of the communications[2], [10].
5) Non-repudiation: Non-repudiation is a crucial element of secure communication that offers proof of conversation between two parties. Two cars engage in communication and thereafter cannot refute the message that was conveyed between them [2], [4],[16].
6) Verification of data: It is necessary to authenticate data sent between V2V, V2I, and I2V. Therefore, Roadside Access Points (RSAP) and cars need to be alerted ahead of time, hence their identities can be randomly confirmed according to the standards [47], [48].

Table 4: Security requirements and criticality in VANET.

Security requirement	Communication Paradigm	Criticality	Impact
Authentication	V2X	High	Operational, Privacy
Data Confidentiality	In-vehicle, V2X	Medium	Financial, Privacy
Responsibility	V2V	High	Safety, Privacy
Key distribution	V2I	High	Operational, Safety, Privacy
Trust management	V2V	High	Safety, Privacy
Misbehavior	V2V, V2I	High	Safety, Financial
Availability	V2X	High	Operational, Financial, Safety
Integrity	V2X	High	Operational, Financial, Safety
Access control	V2I, V2V	Medium	Financial, Safety, Operational
Privacy	V2V, V2P, V2C	Medium	Financial, Safety
Location privacy	V2V, V2C	Medium	Financial, Safety
Flexibility	V2I, V2C	Low to Medium	Operational, Safety

4.1 Classification of VANET Attacks Based on Security Objectives (CIAAN)

In VANETs, cars travel at high speeds and often experience disconnections, making them more susceptible to attacks. The network topology undergoes rapid modifications every second due to the high-speed mobility of vehicles. Consequently, there was a regular occurrence of link disconnection between cars. Moreover, cars travelling in opposing directions have limited interaction and communicate for only a short time. And perhaps they never saw each other again. Hence, VANETs are susceptible to attacks, and identifying malicious vehicles proves challenging. Secure vehicle communication is possible with a thorough understanding of threats and attacks. Researchers have detected numerous attacks in VANETs [16]. VANETs were mainly developed for vehicle management to lessen traffic jams and accidents. However, VANETs can be compromised, leading to network outages and substantial monetary, time, and even life losses. Attacks such as Sybil and Bogus Information, which involve deceitful data and impersonation, are more prevalent in VANETs. Spoofing the Global Positioning System (GPS), DoS attacks, and DDoS attacks are other harmful cyberattacks [50].

This study examined several security threats and attacks that impact VANET security services. Attacks from within an organization are committed by authenticated users within the VANET. Even more damage can come from authorized users abusing their privileges and accessing network resources than from untrusted outsiders. Their motives can range from financial gain to malign intent. Outside Invasion: Without adequate authorisation to access the network, these acts are carried out by unauthenticated entities [19]. They may not have as much access as insiders, but they remain a substantial danger to the network's security and integrity. Many security vulnerabilities may occur in VANETs during communication between cars (V2V) and between vehicles and roadside equipment (V2R). Because they are ad hoc networks that continually evolve, VANETs are exposed to a variety of security vulnerabilities that could jeopardise their operation. The literature discusses several securities concerns [16].

The classification of the attacks and the VANET communication types they target (V2V, V2I, or both). This classification helps to identify specific attacks on these entities (hardware or software, members or authorities) as well as the VANET communication mode they influence. Identifying these assaults facilitates mitigating their impact, thereby enhancing VANET security [48]. It is essential to categorize the risks and dangers associated with VANET security requirements appropriately.

VANET encompasses twenty-six distinct risk categories, in addition to several assaults and security protocols. Figure 5 illustrates the categorization of security attacks within VANET. Each assault is governed by a security protocol [6], [51].

We correlated the identified attacks with the five VANET security services to establish a decision-making framework. This approach identifies the services most susceptible to specific attack vectors and assists in selecting optimal protective measures.

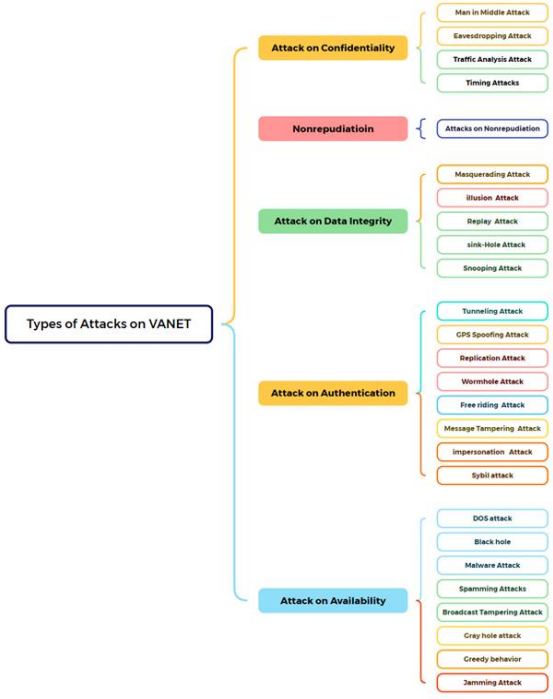

Figure 5: Taxonomy of VANET attacks based on the CIAAN framework.

4.2 Taxonomy of VANET Attacks: CIAAN Perspectives

This section examines various types of attacks in VANETs related to their security services. Subsequently, we conduct a comparative study of all potential attacks by varying factors. Network attacks can be classified into two categories: data traffic attacks and Control Traffic attacks. These attacks can be categorized as active or passive, based on whether the attacker modifies the data packet or observes its contents. Network attacks can be classified according

to the Protocol Stack, based on the particular layer at which the attack originates [29], [49].

4.2.1 Attacks on Confidentiality

Due to the highly confidential nature of data, networks must maintain data confidentiality, particularly in the context of two vehicles' communications and movement patterns. This may be further impeded or verified through malignant intent [46]. The confidentiality of the transmitted communication is guaranteed by using public-key and certificate-based encryption, which restricts access to only authorized vehicles. As a result, malevolent cars cannot access sensitive and personal information shared between vehicles. The following are many prevalent attacks that compromise confidentiality [9], [10],[19].

1) Man-in-the-middle attack: This attack occurs within the midst of V2V transmission to modify and analyse the messages in detail. The attacker has complete access and control over the whole V2V conversation, as seen in the Figure 6 scenario [50], [52].
2) Eavesdropping attack: An eavesdropping attack (EA) aims to gain unauthorized access to a communication channel by stealing its parameters or session key. Figure 7 shows that an attack impacts the network layer, enabling unauthorized access to sensitive data. It breaches confidentiality and is prevalent on VANETs [1], [53].
3) Traffic analysis attack: The attacker focuses on getting the most valuable information by eavesdropping on the message transmission and scrutinizing its frequency. This attack poses a significant threat to the privacy and security of VANETs [54]. In this case, bad people listen in on the network to get information about the cars. As shown in Figure 8, this attack looks at the flow of network packets, sorts the nodes into groups based on how important they are, and then only attacks some of them [47], [53].
4) Timing Attacks: In a timing attack, enemies purposefully slow down the transfer of important signals and data, which causes bad timing. This attack is very hard to deal with, especially for apps that need to work quickly [55]. By adding a delay to this attack, the timing of the communication is changed [16].

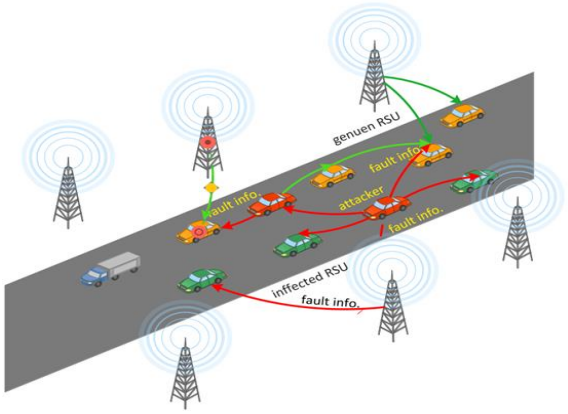

Figure 6: Attack scenario with a man-in-the-middle.

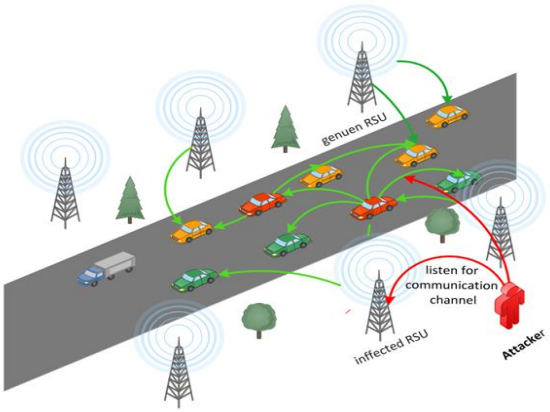

Figure 7: Eavesdropping attacks scenario.

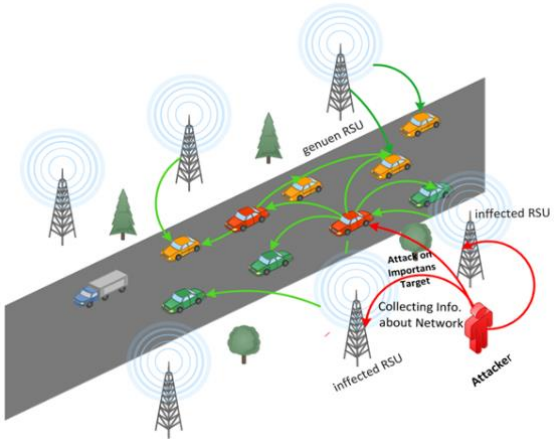

Figure 8: Traffic analysis attack scenario.

4.2.2 Attacks on Nonrepudiation

Repudiation attacks (RUA) happen when a vehicle purposely says it didn't send or receive a message, depending on whether it was the sender or the receiver. When senders retransmit, they use up

VANET resources and slow down the network. Figure 9 shows that it ends up using too much network bandwidth [9], [47].

This kind of attack occurs when someone sends a message but refuses to admit it or take responsibility for it, especially during a disagreement or argument [10], [53].

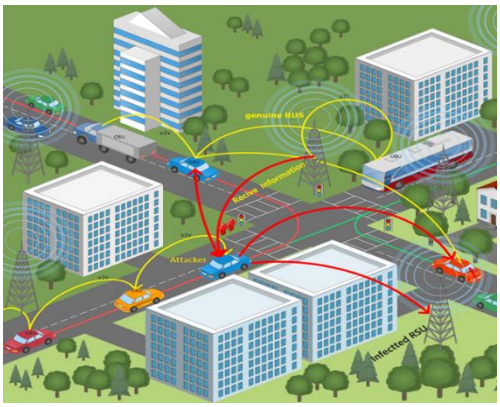

Figure 9: Nonrepudiation attacks scenario.

4.2.3 Attacks on Data Integrity

Data integrity is a crucial security objective for the vehicle network and must be maintained throughout V2V and V2R transmissions. The message remains unaltered from sender to receiver. If the source is a legitimate network user but the message quality has been altered, the original user's authenticity does not need to be confirmed. The accuracy and integrity of the data must be ensured [16]. The integrity of the shared data guarantees its authenticity [10]. These may lead to multi-vehicle risks and misleading safety signals. Attacks that compromise the authenticity of the data being communicated are known as data integrity attacks. Here are some potential attacks that may be employed in this situation [9], [47].

1) Masquerading attack. A masquerading attack occurs when malicious actors pose as a vehicle to inject other cars with false or worthless information about that vehicle. Even at great distances, this causes communication issues between vehicles. If a car pretends to be an ambulance, for instance, it might be given priority in the lane instead of other vehicles, as seen in Figure 10 [1], [56].

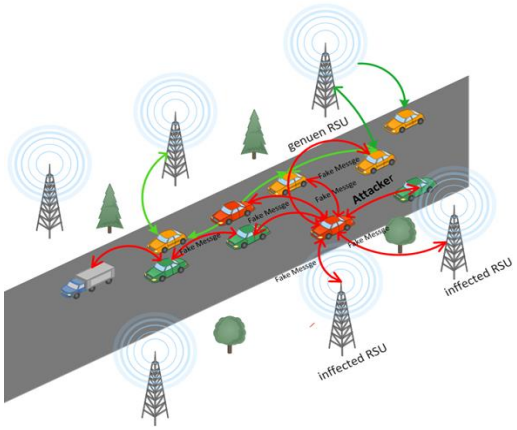

Figure 10: Masquerading attack.

2) Illusion attack. In an illusion attack (ILA), hostile attackers disseminate false warnings about road conditions, such as traffic congestion, accidents, and system deterioration, to mislead other drivers [57].
3) Sink-Hole attack. A sinkhole attack occurs when a malicious entity broadcasts bogus route information to divert all network traffic towards it. The network experiences complexity and performance degradation because of a sinkhole attack, which can occur through data packet manipulation or dropping [58], [59].
4) Snooping attack. Snooping is a form of attack that occurs in isolation, when a malicious entity has access to the content and information that passes through it, to exploit it for its benefit without making any changes [58].

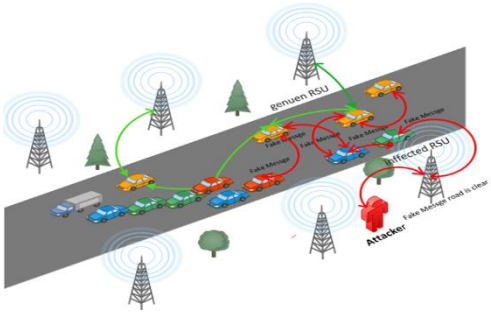

Figure 11: Replay attack scenario.

5) Replay attack. The attacker creates a hidden conversation and connects two parts of the network using a tunnel, an external communication conduit, as shown in Figure 11. This means that nodes in different parts of the network can talk to each other as if they were next door, which could cause all sorts of problems [5], [52].

4.2.4 Attacks on Authentication

Authentication is crucial for safeguarding a VANET network. It ensures that messages remain immutable. This approach necessitates safeguarding actual nodes against malicious entities that infiltrate the network using counterfeit identities, transmit fraudulent GPS signals, alter or fabricate messages, inject misleading information, and disrupt communication among linked vehicles [9], [47].

1) Tunneling attack. The hacker establishes a secret conversation and links two nodes in the network using a tunnel, as shown in Figure 12. Consequently, faraway nodes can communicate with each other as though they were physically nearby, which could lead to serious issues for the network [1], [10], [59].
2) Wormhole attack. In a wormhole attack, two or more malicious vehicles work together to set up a connection so they can send and receive data packets. Therefore, hostile vehicles attract nearby cars to launch an assault, exploiting the link between them as a more effective means of obtaining information than the original, trustworthy method. Once malignant cars receive parcels from unlucky victim vehicles, as seen in Figure 13, they encapsulate and transmit them to another pernicious vehicle, where the last vehicle opens the parcels and disperses their contents throughout the system [60].
3) GPS spoofing attack. The integrity of GPS signals in VANET is crucial for the proper functioning of nodes. The position and placement of nodes must be accurate. The objective of this assault is to overwhelm the GPS signal and manipulate it to modify the position data stored in the GPS satellite. This altered information is then transmitted to automobiles, which are deceived into accepting it as legitimate. As illustrated in Figure 14. There is much weight on the reliability of the GPS signals transmitted by vehicle nodes in the VANET. Attacks like this work by making it harder for receivers to obtain data, such as the whereabouts and timing of the vehicle nodes. By overwhelming the GPS signal as it comes, malicious attackers can modify the reading from the signal and change the information arbitrarily [53], [56].

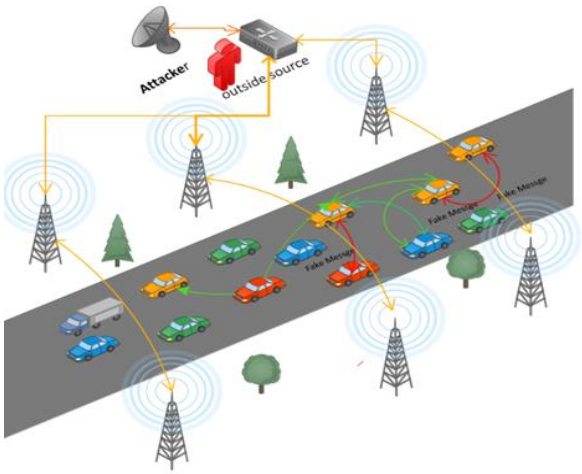

Figure 12: Tunneling attack.

4) Replication attack. A replication attack occurs when an intruding node tries to join the network. To send misleading signals over the network, these attacks assume the identity of another authorized node [57]. Also, in this assault, the malevolent node is tasked with incorporating other nodes into the network. It utilizes the identity of another node that is legitimately present in the network to send deceptive messages to the network. The attacker seeks to undermine the system by obtaining evidence of authentication [10], [56].
5) Free riding attack. A free riding attack occurs when a vehicle node uses the network's resources without giving anything back. Using a TCP header, a bogus header is employed to masquerade a transmission, encapsulating the actual content [1], [53].
6) Message tampering attack. a vehicle functioning as a transfer can disrupt the communications of other cars, resulting in movement changes. The vehicle can terminate, modify, or deteriorate communication from now on. The OBU modification utilizes the information layer level of established designs developed by various vehicles. The perpetrator might manipulate data, potentially disrupting the onboard detection system [50]. When traffic is heavy and the attacker needs to clear the path, they employ this

tactic. Consequently, it compromises message integrity and causes network difficulty, as any node in the vicinity may intercept it; the malicious node then sends the modified message to the destination as if it were a valid one [10], [29].

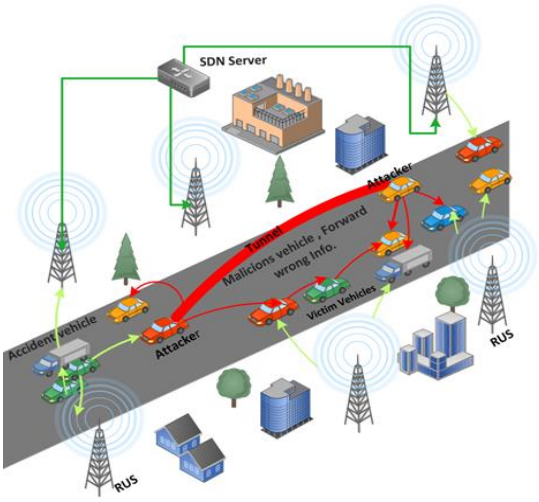

Figure 13: Wormhole attack scenario.

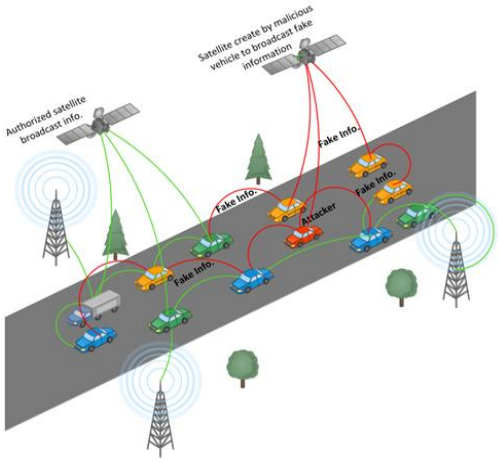

Figure 14: GPS spoofing attack.

7) Impersonation attack. In this type of attack, a malicious individual can impersonate law enforcement to trick various vehicles into retreating or changing their route. An assailant can mimic favorable words or government advertisements and similarly replicate RSU controls. Furthermore, an assailant can influence the behavior of nearby vehicles in the network by disseminating erroneous data about the road's state. Several approaches have been developed to detect pantomime attacks in vehicle networks. The impersonation assault is depicted in Figure 15 [1], [50]. Moreover, an impersonation attack occurs when a malicious actor pretends to be an authorized node, which in turn impersonates the real node [5], [43].

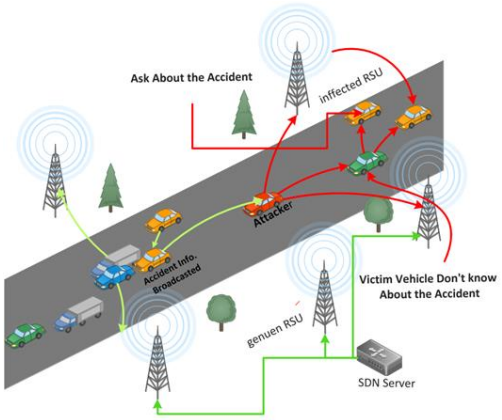

Figure 15: Impersonation attack.

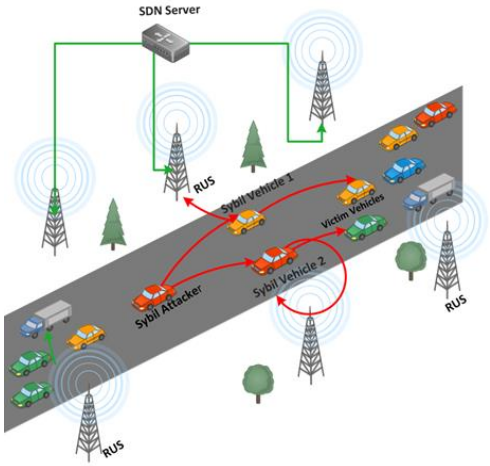

Figure 16: Sybil attacks.

8) Sybil attack. A Sybil Attack (SA) allows a malicious actor to take over a VANET system by sending false information over the network. This might lead vehicle nodes to make the wrong judgments, as illustrated in Figure 16. It also disrupts the system's consistency and efficiency. The produced report could differ from the actual ground situation due to the injection of false information if SAs impact nodes [57]. Moreover, the objective of this assault is to introduce false information into the system to gain control over the network through a malicious node. This directly impacts the accuracy of the reports provided by various nodes. Consequently, vehicle nodes that are affected may make

incorrect judgments that deviate from the actual reality, thus compromising the efficiency of the system [49], [56].

4.2.5 Attacks on Availability

The availability of information is crucial in VANETs. The lack of timely information availability negatively impacts the efficiency of VANETs. AI-orchestrated DDoS and jamming can dynamically choose channels and timings to optimize congestion, surpassing static defences [61]; your synthesis of similar works already emphasizes ML-driven DDoS perspectives and the importance of jamming in safety applications. The availability of VANETs is susceptible to the following assaults [10], [53].

1) DoS attack. The purpose of a Denial of Service (DoS) attack is to disrupt the data flow between cars and the system, such as road status updates, by preventing the transmission or reception of data, as illustrated in Figure 17. A primary DoS assault might use interest flooding. An attacker sends many interest requests for content that may not be available in the cache. This condition is linked to automobiles, RSUs, and other foundational components of the system failing [58]. Moreover, this is the most notable assault. The attackers block access to a specific node's services. It can be initiated by either an internal or an external vehicle to render network resources and services unavailable to users [1], [20], [62].

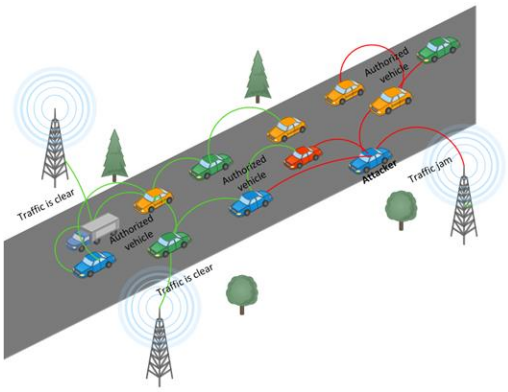

Figure 17: Denial of service attack.

2) Black hole attack. The black hole attack, depicted in Figure 18, is another dangerous assault that specifically impacts security applications. In this attack, malicious vehicles deceive other vehicles by falsely claiming the optimal route to the destination or the optimum location to forward the packet[57]. Moreover, a black hole is a malicious node that falsely claims to have the shortest path, intercepts data from a registered user, and refuses to contribute to the system. Indeed, the receiver can discard all received packets, which may lead to a disturbance in the routing table. This assault aims explicitly to disrupt the availability of the VANET [53], [56], [62].

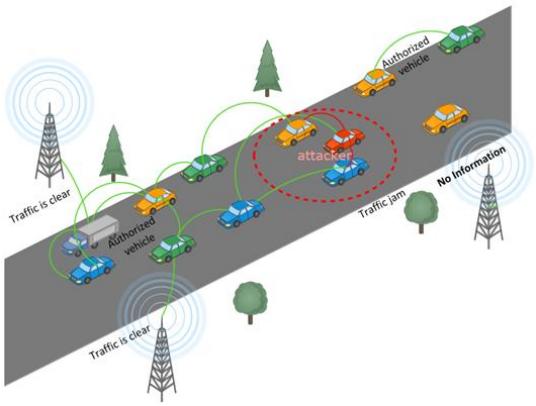

Figure 18: Black hole attack.

3) Malware Attack. This attack employs software components to manipulate and gain control over the OBUs and RSUs. As a result of this attack, the components of VANETs begin to experience malfunctions [10], [29].
4) Spamming attack. A malevolent node's spamming of other nodes in a VANET significantly increases the transmission delay. This attack may result in inefficient use of bandwidth and other vital resources. The absence of appropriate design, infrastructure, and centralized management makes it very difficult to control it [47], [53].
5) Broadcast Tampering Attack. In this attack, the attacker engages in inter-vehicle communication by acting as a transmitting node and replicating the same message by introducing a new message into VANETs. The safety notice message is obscured, leading to hazardous road accidents [10], [53].
6) Gray hole attack. Gray hole attacks (GHAs) aim at the VANET's network layer, causing vehicle nodes to discard all or part of the packets they receive. Overhead increases during a gray attack, and packet delivery rates become an issue for some networks. The fact that both benign and malevolent networks can transmit all packets to a specific node makes GHAs hard to identify [16], [47], [49].

7) Greedy behavior attacks. Attacks on VANETs can also be motivated by selfish drivers who want to exploit the network's resources by tricking other nodes into taking different routes and obstructing their way to their goal. This causes other nodes to divert through alternate routes, resulting in congestion, collisions on the transmission channel, and delays in providing legitimate services to registeredusers [1], [10], [47].
8) Jamming attack. This attack aims to disrupt the communication channel in VANETs by transmitting a highly amplified signal at the same frequency, hence reducing the signal-to-noise ratio for the receiver, as illustrated in Figure 19. As this assault did not adhere to the legitimate safety alert, it is deemed the most perilous attack for safety applications [54]. This sort of attack can trigger a response by collecting observed information in the event of an intelligent blocking program [43], [49].

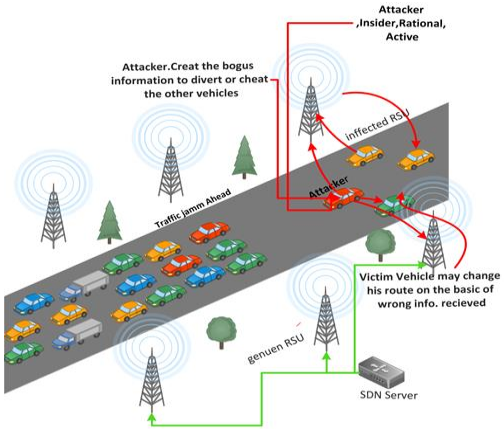

Figure 19: Jamming attack.

4.2.6 Vehicle Ad-Hoc Network Categorization Attacks

VANET attacks can be initiated by internal or external attackers, depending on the roles they assume and their level of access to the system. Inside attackers are those who possess permitted access or knowledge of the system, whereas outside attackers are individuals who do not have authorized access [28]. Depending on whether the attack targets a data or control packet, it can be categorized as either a Data Traffic attack or a Control Traffic attack. Depending on whether the attacker changes the data packet or just watches its contents, these attacks can be called active or passive. Network attacks are classified according to the Protocol Stack, depending on the layer where the attack starts. These attacks target different types of communications in the VANET environment. Attacks in VANETs; furthermore, classifying these attacks is advantageous due to the intrinsic vulnerabilities and constraints of VANETs that require solutions. Division makes it easier to control. There are four main types of attacks: (1) those that threaten wireless interfaces, (2) those that threaten hardware and software, (3) those that compromise sensor inputs in vehicles, and (4) those that threaten infrastructure, such as Certificate Authorities or vehicle manufacturers. Table 5 shows a summary of how the six factors above were used to group network attacks [2], [29], [49], [50].

5 MULTI-DIMENSIONAL CLASSIFICATION MODEL FOR VANET SECURITY THREATS

Traditional ways of classifying VANET attacks are useful, but they don't always show how complicated and real-time threats are these days. The authors aim to improve the reliability and speed of VANET connections, which will make transportation systems safer and more secure [26]. It looks at a lot of different uses for cryptography, like Blockchain and hybrid methods, and it talks about important security issues like authentication. The paper sorts of authentication methods into groups, looks at how well they can stand up to attacks, and talks about the privacy issues that come with them. Multifaceted attacks in VANETs take advantage of the networks' dynamic and decentralized nature to create a wide range of security problems. These attacks could compromise vehicle safety, data privacy, and communication integrity [60].

A multi-dimensional classification system that evaluates attacks according to three crucial criteria: impact level, detectability, and extent of attack. Multiple factors, including CIAAN, high impact, and low detectability, are often present in practical VANET attacks. The classification of network attacks according to the three criteria above is summarised in Table 6. Several security properties, such as availability, secrecy, authenticity, data integrity, and non-repudiation, may be compromised in multidimensional attacks on VANETs. These attacks can cause service slowness, flood the network with incorrect data, intercept and reroute data, or both [54], [63].

Table 5: VANET attack classification.

Type of Attack	Attackers from both inside and outside	Categorize based on the Packet	Categorize based on interfaces	Categorize based on Protocol Stack	Attacks based on different types of communications	Impact of the Attack
Man-in-middle Attack	Outside/Inside Attack	Control Traffic Attack	Attacks on wireless interface	Multilayer attack/Network	(V2V), (V2N) communication attacks	Passive
Eavesdropping Attack	Outside Attack	Data Traffic Attack	Attacks on wireless interface	Physical Layer	(V2I), (V2V) communication attacks	Passive
Traffic analysis attack	Outside Attack	Data Traffic Attack	Attacks on wireless interface	Data Link/Physical	(V2I), (V2N) communication attacks	Passive
Timing Attacks	Outside Attack	Control Traffic attack	Attacks on hardware and software	Network Layer	(V2I), (V2V) communication attacks	Active
Repudiation Attack	Inside Attack	Control Traffic Attack	Attacks on Infrastructure	Network Layer	(V2I), (V2V) communication attacks	Passive
Masquerading Attack	Inside Attack	Data Traffic Attack	Attacks on hardware and software	Application Layer	(V2I), (V2V), (V2N) communication attacks	Active
Illusion Attack	Inside Attack	Data Traffic Attack	Attacks on Sensors input in vehicle	Network Layer	(V2I), (V2V) communication attacks	Active
Sink-Hole Attack	Outside/Inside Attack	Data Traffic Attack	Attacks on Infrastructure	Network Layer	V2I),(V2V), (V2N) communication attacks	Active
Replay Attack	Outside / Inside Attack	Data Traffic Attack	Attacks on Infrastructure	Network Layer	(V2V) (V2P) (V2I) communication attacks	Active
Tunneling Attack	Inside Attack	Control Traffic Attack	Attacks on hardware and software	Network Layer	(V2I), (V2N) communication attacks	Active
GPS Spoofing Attack	Outside Attack	Control Traffic Attack	Attacks on Sensors input in vehicle	Physical Layer	(V2N),(V2S) communication attacks	Active
Replication Attack	Inside Attack	Data and Control Traffic	Attacks on Sensors input in vehicle	Network Layer	(V2I), (V2N) communication attacks	Active
Free riding Attack	Inside Attack	Data Traffic Attack	Attacks on Sensors input in vehicle	Transport Layer	(V2N) communication attacks	Passive
Message tampering Attack	Inside Attack	Data Traffic Attack	Attacks on hardware and software	Network Layer	(V2I) (V2V) communication attacks	Active
Impersonation Attack	Outside / Inside Attack	Data Traffic Attack	Attacks on Infrastructure	Network Layer	(V2I),(V2V) communication attacks	Active
Sybil Attack	Inside Attack	Control Traffic Attack	Attacks on wireless interface	Network Layer	(V2V) communication attacks	Active
DoS Attack	Inside Attack	Data and Control Traffic	Attacks on wireless interface	Multilayer attack/Network	(V2N), (V2S), (V2V),(V2I) communication attacks	Active
Black hole Attack	Outside Attack	Data Traffic Attack	Attacks on hardware and software	Network Layer	(V2V),(V2I) communication attacks	Active
Malware Attack	Outside Attack	Control Traffic Attack	Attacks on wireless interface	Network Layer	(V2I),(V2V) communication attacks	Active
Spamming Attack	Outside Attack	Control Traffic Attack	Attacks on wireless interface	Transport Layer	(V2I), (V2N) communication attacks	Active
Broadcast Tampering Attack	Inside Attack	Data and Control Traffic	Attacks on hardware and software	Network Layer	(V2I), (V2V) communication attacks	Active
Gray hole attack	Inside Attack	Data Traffic Attack	Attacks on hardware and software	Network Layer	(V2V) communication attacks	Active
Greedy behavior Attacks	Inside Attack	Control Traffic Attack	Attacks on hardware and software	Network Layer	(V2I), (V2V), (V2N) communication attacks	Active
Jamming Attack	Outside Attack	Data Traffic Attack	Attacks on Sensors input in vehicle	Physical Layer	(V2I) (V2S) (V2P communication attacks	Active

6 AI AND QUANTUM COMPUTING-BASED VANET ATTACKS

Ensuring the confidentiality, authenticity, privacy, and integrity of communications transmitted between cars and infrastructures along roadways is the primary goal of security in VANETs. Data consistency, signal reliability from other vehicles, and the need for safety-critical applications to function in real time are important factors to consider. While AI improves VANET speed, it also opens the door to vulnerabilities that could compromise the network's CIAAN properties; attacks that target AI generally aim to undermine data dependence and learning procedures used by AI models [58], [63], [64].

Due to its wireless nature and the complexity of its operational environment, a VANET is susceptible to a wide range of attacks. Although most intrusion detection systems (IDSs) only detect known attacks, one way to detect new ones is with an IDS that uses statistical machine learning. One alternative defensive strategy uses honeypots and Machine Learning (ML) to better detect known and unknown threats by analysing attack rates. This approach assesses the network's defences by examining how well they can identify known or anticipated threats [64].

Table 7 summarises the results of an analysis of the suitability and limitations of several AI approaches for tackling various VANET-related difficulties. The exceptional problem-solving capabilities of AI approaches are the reason for their utilisation. Improvements in computationally efficient algorithms and the availability of big data have been the driving forces behind the current success of AI technique [63], [66].

7 CHALLENGES OF DATA SECURITY IN VANET

Vehicular Ad-Hoc Network (VANET) security requires meeting specific prerequisites. Vehicles must only respond to packets sent by authorized network members. Therefore, it is essential to authenticate the sender of the communication. In addition, the recipient should perform data integrity checks to identify any inaccurate data that an authenticated sender may have transmitted. Nevertheless, it is essential to thoroughly examine and successfully tackle the following significant obstacles to create scalable solutions for resolving them [58], [59], [67].

Table 6: Multidimensional VANET attack classification.

Type of Attack	Impact Level	Detectability	Target Scope
Man-in-middle Attack	High	Hard to detect	Single Vehicle, RSU
Eavesdropping Attack	Medium	Hard to detect	Single Vehicle
Traffic analysis attack	Medium	Hard to detect	Cluster, Whole Network
Timing Attacks	Medium	Hard to detect	Cluster
Repudiation Attack	Medium	Hard to detect	Single Vehicle
Masquerading Attack	High	Hard to detect	Single Vehicle, RSU
Illusion Attack	High	Hard to detect	Single Vehicle
Sink-Hole Attack	High	Hard to detect	Cluster, RSU
Replay Attack	High	Medium	Cluster
Tunneling Attack	High	Hard to detect	Whole Network
GPS Spoofing Attack	High	Hard to detect	Single Vehicle
Replication Attack	High	Hard to detect	Cluster
Free riding Attack	Medium	Medium	Cluster
Message tampering Attack	High	Medium	Cluster
Impersonation Attack	High	Hard to detect	Cluster
Sybil Attack	High	Hard to detect	Whole Network
DoS Attack	High	Easily detectable	Whole Network
Black Hole Attack	High	Medium	Cluster
Malware Attack	High	Medium	Cluster, RSU
Spamming Attack	Low	Easily detectable	Single Vehicle
Broadcast Tampering Attack	High	Medium	Cluster
Gray hole attack	High	Hard to detect	Cluster
Greedy behavior Attacks	Medium	Medium	Cluster
Jamming Attack	High	Easily detectable	Whole Network

Table 7: VANET attacks based on ML techniques and CIAAN targets.

Type of Attack	ML Technique	Advantage	Limitation
Man-in-middle Attack	Random Forest, Deep Neural Networks (DNN)	Detects abnormal communication patterns	Needs large training data; high computation
Eavesdropping Attack	SVM, Naive Bayes	Works with small data; effective on classified traffic	Misclassifies encrypted traffic
Traffic analysis attack	Decision Trees, K-Means	Detects flow anomalies without labels	High false positives in dynamic networks
Timing Attacks	Hidden Markov Model, RNN	Captures temporal/sequence anomalies	Sensitive to noise; large data required
Repudiation Attack	Logistic Regression, Rule-based ML	Simple, interpretable	Weak in complex scenarios
Masquerading Attack	SVM, Random Forest	Good identity verification	May fail against adaptive mimicry
Illusion Attack	CNN, Autoencoders	Detects falsified sensor data	High computational cost
Sink-Hole Attack	K-Means, Random Forest, ISVM	Detects routing manipulation	Requires diverse features
Replay Attack	Long Short-Term Memor, RNN	Detects repeated patterns	Sensitive to synchronization issues
Tunneling Attack	Ensemble Learning, SVM	Detects suspicious multi-hop routing	False alarms in mobility
GPS Spoofing Attack	CNN, RNN, Hybrid DNN	Strong detection of fake GPS/location	Sensor/data dependency
Replication Attack	K-Means, DBSCAN	Spots cloned nodes	Confuses with redundancy
Free riding Attack	Reinforcement Learning	Learns selfish vs cooperative nodes	Requires ongoing learning
Message tampering Attack	Random Forest, Naive Bayes	Identifies altered packet contents	Limited vs subtle manipulations
Impersonation Attack	SVM, DNN	Detects spoofed identities	Needs robust identity data
Sybil Attack	graph neural network, SVM, ISVM	Detects multiple fake IDs	High computational cost
DoS Attack	Random Forest, ANN, ISVM	Accurate anomaly detection	May fail with new DoS variants
Black Hole Attack	Decision Trees, Ensembles, ISVM	Detects packet drops	Hard against large-scale collusion
Malware Attack	CNN, Autoencoders	Detects malicious binaries	Needs large labeled datasets
Spamming Attack	Naive Bayes, Logistic Regression	Lightweight; effective on text/traffic	Weak vs adaptive spam
Broadcast Tampering Attack	Random Forest, SVM	Detects altered broadcasts	Less reliable in high mobility
Gray hole attack	Hybrid ML (SVM + K-Means)	Detects selective forwarding	False negatives if low intensity
Greedy behavior Attacks	Reinforcement Learning	Learns selfish node behavior	Slow convergence
Jamming Attack	SVM, CNN (spectrum data)	Detects abnormal PHY/MAC patterns	Confuses with natural interference

Several important challenges and security requirements associated with VANET environments are summarized as follows:

1) Scalability. A wide variety of entertainment and security applications can be supported by VANETs, which are very scalable. Nevertheless, worries over data security and possible assaults are heightened by the proliferation of automobiles and VANET applications [63], [58].
2) Message Authentication. Is an approach where digital signatures are used to ensure the authenticity, non-repudiation, and integrity of every communication sent by vehicles. For the automobile to authenticate incoming messages, it must use computationally costly ways to verify the digital signature [58], [63], [68].

3) Roadside Infrastructure Accessibility. Roadside Units have been proven by a plethora of security-conscious methods. The major uses of RSUs are cryptographic key maintenance and privacy assurance [63], [58].
4) Anti-malware and Intrusion Detection System (IDS). When it comes to finding harmful actions on a network, intrusion detection systems are vital. Every single vehicle must have an intrusion detection system (IDS). There are many benefits to using intrusion detection systems (IDS) in VANETs. However, a major problem is ensuring that IDS can handle damaging and erroneous information in VANETs [69].
5) QoE. The Quality of Experience (QoE) in immersive media consumption in autonomous vehicles is challenged by cybersickness and motion sickness, which detract from user enjoyment. Additionally, variable network conditions in high-speed 5G/6G environments affect the delivery of high-quality content [67].
6) Attack sophistication scales. Medium-sophistication attacks necessitate more complicated and costly solutions like certificate verification, although basic assaults can frequently be mitigated using simple approaches like rate restrictions and timestamp verifications. Defenses that are resource-intensive, such as adversarial detectors and ensemble detection systems, are necessary to withstand sophisticated attacks, but they have a major influence on the performance of onboard units when latency is tight [70].

8 IMPACT OF EMERGING NETWORKING TECHNOLOGIES ON VANET SECURITY

8.1 Edge Computing

Offloading resource-intensive defences, such as cryptographic verification, intrusion detection, and federated-learning-based anomaly detection, to edge servers at RSUs and roadside fog nodes enables low-latency offloading. This resolves our issues with OBU resource limitations and time constraints, but it leaves the distributed edge layer vulnerable to resource depletion, poisoning, or compromise. The importance of trustworthy edge management and secure orchestration is highlighted by our multi-dimensional approach, which classifies these as medium-detectability, high-impact attacks [70], [71].

8.2 Network Slicing

Network slicing enables intelligent applications in NFV, SDN, and cloud-RAN to leverage enhanced flexibility and quality of service by creating virtual networks on a common physical infrastructure. This strategy is facilitated by fundamental processes like virtualisation and centralisation, enabling virtualised network services to operate without specific hardware. It enables the segregation of logical resources, distinguishing infotainment streams from safety-critical control traffic that demands strict latency and availability standards. Nonetheless, challenges like as authentication and isolation of slices are crucial to prevent cross-slice leaking. Slice orchestration services are vulnerable to resource-intensive assaults, especially if a slice controller is compromised [70], [71].

8.3 Software-Defined Networking (SDN)

Minimised idle time, enhanced energy economy, and augmented throughput are among the advantages provided by systems employing SDN-based VANETs. These advantages stem from decentralisation. Modern automotive sensors provide remote connection, providing numerous benefits such as safety, efficiency, and user-friendliness. Notwithstanding the advantages, SDN-based VANETs have obstacles, especially due to the vulnerability of SDN controllers, which are prime targets for assaults. To bolster network integrity and availability, SDN provides centralized visibility and programmable security measures such as flow monitoring and anomaly detection. Mitigation strategies include controller redundancy, distributed architectures, and secure APIs [56], [72].

9 DISCUSSIONS

The majority of surveyed studies are predominantly descriptive and compartmentalised (by layer or attack family), providing minimal direction for prioritising controls within stringent VANET latency and resource limitations. They infrequently associate threats with CIAAN services or assess impact, detectability, or scope, resulting in ambiguous deployment decisions for city-scale fleets. The five-

dimensional taxonomy addresses this deficiency by transforming classification into a decision-making framework that corresponds with the reality of smart mobility (edge/fog offload, 5G/6G variability) and emphasises low-detectability, high-impact categories (e.g., Sybil, wormhole) that existing IDSs inadequately address.

The results of this review show that there have been significant strides in vehicle network security, but that the existing literature is scattered and often lacks in-depth analysis. Hasan et al. (2020) and Pavithra & Nagabhushana (2020) laid the groundwork for authentication frameworks and taxonomies; however, their descriptive approaches aren't strong enough to grasp the complex, multi-layered dynamics of modern VANET systems. Although adaptive security frameworks that leverage fog and edge computing improve response times and reduce processing burdens, they still face scalability and interoperability challenges in complex, heterogeneous vehicular environments. This has been highlighted in recent studies (e.g., Naqvi et al., 2022; Ghaleb Al-Mekhlafi et al., 2024; Abdelmaguid et al., 2025).

Moreover, AI-driven solutions, shown by El-Shafai et al.'s (2025) ensemble classifier, represent a substantial shift from rule-based intrusion detection to intelligent, self-learning defence systems. The computational expense of real-time deployment on resource-limited OBUs, the inconsistency in training datasets, and the propensity for overfitting to specific attack types are substantial constraints of these models. Trust management and authentication systems are becoming progressively susceptible to new attacks due to our growing dependence on AI and deep learning. These vulnerabilities include malicious manipulation, data contamination, and privacy violations. This highlights the necessity of incorporating AI with secure orchestration frameworks, such as SDN and intrusion detection systems utilizing federated learning, to facilitate continuous adaptation to new threats.

Weaknesses: Established standards framework (IEEE 1609.x, ETSI); strong emphasis on safety; extensive telemetry for anomaly detection; and reduced workload in operational behaviour units (OBUs) due to edge/fog offloading. Problems include a constantly changing topology, datasets that aren't cohesive, and the reliance of many solutions solely on simulations. In earlier research, there was only a weak association between attacks and CIAAN.

Prospects:5G/6G, Software-Defined Networking (SDN) and network slicing for traffic segregation; federated and online learning for adaptive Intrusion Detection Systems (IDS); Post-Quantum Cryptography (PQC) and lightweight cryptography; digital twin testbeds for realistic assessment.

Threats: AI-enabled adversaries (adaptive jamming, data contamination); cross-slice information leakage and controller penetration; significant DDoS assaults on RSU/cloud infrastructures; privacy backlash and regulatory discord.

10 CONCLUSIONS

To build ITS, vehicular ad hoc networks (VANETs) are essential, as they enable vehicles to communicate with each other and with infrastructure in real time. There are many security risks to these networks because they are decentralized, dynamic, and wireless. By combining classic and modern attack taxonomies and systematically comparing them with critical security objectives, CIAAN, this study provides a thorough analysis of VANET security. Scalability, interoperability, and adaptability continue to be major obstacles, according to this paradigm, even though advances in authentication methods, intrusion detection systems, and defensive models, improved with artificial intelligence, have been substantial.

Despite the comprehensive analysis of VANET security this paper offers, it still has significant limitations. To begin with, the majority of the frameworks and attack models evaluated have relied on testbeds that are either too small or too synthetic to accurately represent real-world traffic conditions. Intrusion detection systems that use AI and ML have great potential, but they frequently encounter problems such as limited datasets, overfitting, and insufficient cross-validation across diverse vehicle scenarios. Third, due to its scope, this review could only provide a cursory examination of several issues, including in-vehicle security protocols, cross-domain attacks in 5G/6G networks, and new quantum-resistant encryption methods.

Collectively, these findings suggest three pragmatic goals for research and implementation. Initially, threat-aware system design requires selecting security controls based on multidimensional attack priorities (impact, detectability, scope), ensuring that the protection strategy aligns with the service being protected (e.g., prioritizing availability for safety-critical messages and implementing stronger authentication for privacy-sensitive flows). Secondly, lightweight adaptive detection: IDS architectures must utilize federated and edge learning to maintain privacy and alleviate the burden on OBUs while facilitating ongoing model adaptation to counteract developing adversaries. Third, resilient

orchestration and standards integration: SDN, network slicing, and fog layers must have redundancy, secure APIs, and slice isolation to mitigate systemic failure modes.

We highlight some specific research and validation tasks required to implement the taxonomy and address the observed gaps: (1) Develop and benchmark lightweight, explainable machine learning detectors for hybrid OBU-fog deployments, incorporating adversarial robustness assessments; (2) Establish urban-scale testbeds or digital twin platforms that simulate realistic mobility, traffic compositions, and cross-domain interactions (5G/6G, cloud, edge) to assess real-world performance and false positive/negative behaviors; (3) Explore post-quantum and hybrid authentication mechanisms integrated with scalable revocation systems appropriate for city-scale fleets; and (4) Assess governance, privacy, and regulatory dimensions to foster user trust and societal acceptance.

Future research should focus on developing efficient, lightweight, and adaptable intrusion detection systems that protect users' privacy through federated and edge-based learning. To safeguard future 5G/6G-connected cars from the development of adversarial models, it will be important to integrate blockchain authentication with quantum-resistant encryption. In addition, testbeds on an urban scale and validation frameworks based on digital twins are necessary to evaluate proposed taxonomies and defensive strategies in real-world scenarios with real-world network conditions and movement patterns. To create comprehensive, workable security frameworks for future smart cities, experts from many fields must collaborate, combining machine learning, cybersecurity, vehicular networking, and regulatory policy.

This study's multidimensional taxonomy introduces a novel framework for comprehending and assessing security concerns in VANETs. This paradigm integrates theoretical classification with actual defence prioritisation, providing a scientific reference for future researchers and system designers aiming to develop secure, scalable, and resilient vehicular communication systems.

REFERENCES

[1] H. Amari, Z. A. El Houda, L. Khoukhi, and L. H. Belguith, “Trust Management in Vehicular Ad-Hoc Networks: Extensive Survey,” IEEE Access, vol. 11, no. May, pp. 47659-47680, 2023, [Online]. Available: https://doi.org/10.1109/ACCESS.2023.3268991.

[2] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, “VANet security challenges and solutions: A survey,” Vehicular Communications, vol. 7, pp. 7-20, 2017, [Online]. Available: https://doi.org/10.1016/j.vehcom.2017.01.002.

[3] A. M. Farooqi, M. A. Alam, S. I. Hassan, and S. M. Idrees, “A Fog Computing Model for VANET to Reduce Latency and Delay Using 5G Network in Smart City Transportation,” Applied Sciences (Switzerland), vol. 12, no. 4, 2022, [Online]. Available: https://doi.org/10.3390/app12042083.

[4] Z. Ghaleb Al-Mekhlafi et al., “Coherent Taxonomy of Vehicular Ad Hoc Networks (VANETs) Enabled by Fog Computing: A Review,” IEEE Sensors Journal, vol. 24, no. 19, pp. 29575-29602, 2024, [Online]. Available: https://doi.org/10.1109/JSEN.2024.3436612.

[5] M. A. Al-Shareeda, M. Anbar, S. Manickam, A. Khalil, and I. H. Hasbullah, “Security and Privacy Schemes in Vehicular Ad-Hoc Network with Identity-Based Cryptography Approach: A Survey,” IEEE Access, vol. 9, pp. 121522-121531, 2021, [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3109264.

[6] M. Noman, M. Iqbal, and A. Manzoor, “A survey on detection and prevention of web vulnerabilities,” International Journal of Advanced Computer Science and Applications, vol. 11, no. 6, pp. 521-540, 2020, [Online]. Available: https://doi.org/10.14569/IJACSA.2020.0110665.

[7] S. Babu, I. Ghosh, and B. S. Manoj, “Effort: A New Metric for Roadside Unit Placement in 5G Enabled Vehicular Networks,” 2020 IEEE 3rd 5G World Forum (5GWF), pp. 263-268, 2020, [Online]. Available: https://doi.org/10.1109/5GWF49715.2020.9221228.

[8] M. J. N. Mahi, S. Chaki, E. Humayun, H. Imran, A. Barros, and M. Whaiduzzaman, “A Review on VANET Security: Future Challenges and Open Issues,” Indonesian Journal of Electrical Engineering and Informatics, vol. 11, no. 1, pp. 180-193, 2023, [Online]. Available: https://doi.org/10.52549/IJEEI.V11I1.4295.

[9] Y. Amol Rathod et al., “Energy Meter Tamper Detection and Alert Messaging System,” International Journal of Technology Engineering Arts Mathematics Science, vol. 1, no. 2, pp. 2583-1224, 2022, [Online]. Available: https://doi.org/10.11591/eei.v9i3.xxxx.

[10] S. A. Jan, N. U. Amin, M. Othman, M. Ali, A. I. Umar, and A. Basir, “A Survey on Privacy-Preserving Authentication Schemes in VANETs: Attacks, Challenges and Open Issues,” IEEE Access, vol. 9, pp. 153701-153726, 2021, [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3125521.

[11] S. Ajjaj, S. El Houssaini, M. Hain, and M. A. El Houssaini, “A New Multivariate Approach for Real Time Detection of Routing Security Attacks in VANETs,” Information (Switzerland), vol. 13, no. 6, pp. 1-19, 2022, [Online]. Available: https://doi.org/10.3390/info13060282.

[12] A. K. Goyal et al., "A Comprehensive Cost Analysis of Intra-Domain Handoff with Authentication Cost in PMIPv6 for Vehicular Ad Hoc Networks (VANETs)," Electronics (Switzerland), vol. 11, no. 10, 2022, [Online]. Available: https://doi.org/10.3390/electronics11101625.

[13] M. U. Ghazi, M. A. Khan Khattak, B. Shabir, A. W. Malik, and M. Sher Ramzan, "Emergency Message Dissemination in Vehicular Networks: A Review," IEEE Access, vol. 8, pp. 38606-38621, 2020, [Online]. Available: https://doi.org/10.1109/ACCESS.2020.2975110.

[14] N. H. Hussein, C. T. Yaw, S. P. Koh, S. K. Tiong, and K. H. Chong, "A Comprehensive Survey on Vehicular Networking: Communications, Applications, Challenges, and Upcoming Research Directions," IEEE Access, vol. 10, pp. 86127-86180, 2022, [Online]. Available: https://doi.org/10.1109/ACCESS.2022.3198656.

[15] M. Arif, G. Wang, M. Zakirul Alam Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges," Vehicular Communications, vol. 19, p. 100179, 2019, [Online]. Available: https://doi.org/10.1016/j.vehcom.2019.100179.

[16] M. M. Hamdi, Y. A. Yussen, and A. S. Mustafa, "Integrity and Authentications for service security in vehicular ad hoc networks (VANETs): A Review," 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 2021, [Online]. Available: https://doi.org/10.1109/HORA52670.2021.9461327.

[17] R. Hussain, F. Hussain, S. Zeadally, and J. Y. Lee, "On the Adequacy of 5G Security for Vehicular Ad Hoc Networks," IEEE Communications Standards Magazine, vol. 5, no. 1, pp. 32-39, 2021, [Online]. Available: https://doi.org/10.1109/MCOMSTD.001.2000066.

[18] A. Islam, S. Ranjan, A. P. Rawat, and S. Maity, "A comprehensive survey on attacks and security protocols for VANETs," Lecture Notes in Networks and Systems, vol. 171, pp. 583-595, 2021, [Online]. Available: https://doi.org/10.1007/978-981-33-4543-0_62.

[19] M. Houmer and M. L. Hasnaoui, "A risk and security assessment of VANET availability using attack tree concept," International Journal of Electrical and Computer Engineering, vol. 10, no. 6, pp. 6039-6044, 2020, [Online]. Available: https://doi.org/10.11591/ijece.v10i6.pp6039-6044.

[20] F. Oberti, "Cybersecurity for future interconnected and smart vehicles," School of Politecnico di Torino (ScuDo), p. Page 2, 2024.

[21] D. Zelle, C. Plappert, R. Rieke, D. Scheuermann, and C. Krauß, "ThreatSurf: A method for automated Threat Surface assessment in automotive cybersecurity engineering," Microprocessors and Microsystems, vol. 90, p. 104461, 2022, [Online]. Available: https://doi.org/10.1016/j.micpro.2022.104461.

[22] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," Knowledge-Based Systems, vol. 189, p. 105124, 2020, [Online]. Available: https://doi.org/10.1016/j.knosys.2019.105124.

[23] I. Naqvi and A. Chaudhary, "A Systematic Review of the Intrusion Detection Techniques in VANETS," TEM Journal, vol. 11, no. 2, pp. 900-907, 2022, [Online]. Available: https://doi.org/10.18421/TEM112-51.

[24] A. K. Goyal, G. Agarwal, A. K. Tripathi, and G. Sharma, "Systematic Study of VANET: Applications, Challenges, Threats, Attacks, Schemes and Issues in Research," 2022, [Online]. Available: https://doi.org/10.1201/9781003097198-3.

[25] K. Vamshi Krishna and K. Ganesh Reddy, "Classification of Distributed Denial of Service Attacks in VANET: A Survey," Wireless Personal Communications, vol. 132, no. 2, 2023, [Online]. Available: https://doi.org/10.1007/s11277-023-10643-6.

[26] M. A. Hezam Al Junaid, A. A. Syed, M. N. Mohd Warip, K. N. Fazira Ku Azir, and N. H. Romli, "Classification of Security Attacks in VANET: A Review of Requirements and Perspectives," MATEC Web of Conferences, vol. 150, 2018, [Online]. Available: https://doi.org/10.1051/matecconf/201815006038.

[27] M. A. Elsadig et al., "Connected Vehicles Security: A Lightweight Machine Learning Model to Detect VANET Attacks," World Electric Vehicle Journal, vol. 16, no. 6, pp. 1-29, 2025, [Online]. Available: https://doi.org/10.3390/wevj16060324.

[28] W. El-Shafai, A. T. Azar, and S. Ahmed, "AI-Driven Ensemble Classifier for Jamming Attack Detection in VANETs to Enhance Security in Smart Cities," IEEE Access, vol. PP, p. 1, 2025, [Online]. Available: https://doi.org/10.1109/ACCESS.2025.3552544.

[29] R. Hussain, "Integration of VANET and 5G Security: A review of design and implementation issues," Future Generation Computer Systems, vol. 101, pp. 843-864, 2019, [Online]. Available: https://doi.org/10.1016/j.future.2019.07.006.

[30] I. Naqvi and A. Chaudhary, "Intrusion Detection in VANETs: A Review," 9th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO), 2021, [Online]. Available: https://doi.org/10.1109/ICRITO51393.2021.9596141.

[31] C. Huang, M. Yao, X. Wang, Q. Gan, and Y. Lin, "An Improved and Privacy-Preserving Mutual Authentication Scheme," Security and Communication Networks, 2021, [Online]. Available: https://doi.org/10.1155/2021/6698099.

[32] B. K. Soujanya and F. Azam, "Ensuring Security and Privacy in VANET: A Comprehensive Survey of Authentication Approaches," Journal of Computer Networks and Communications, vol. 2024, no. 1, 2024, [Online]. Available: https://doi.org/10.1155/2024/1818079.

[33] I. A. Sumra, A. Abdullah, I. Ahmad, and A. Alghamdi, "Towards improving security in VANET: Some new possible attacks and their possible solutions," Journal of Internet Technology, vol. 17, no. 4, pp. 821-829, 2016, [Online]. Available: https://doi.org/10.6138/JIT.2016.17.4.20160501c.

[34] D. Ramsamooj, P. Sharma, and H. Liu, "GenVRAM: Dataset Generator for Vehicle to Roadside Attacks and Misbehavior," IEEE Access, vol. 12, pp. 86176-86193, 2024, [Online]. Available: https://doi.org/10.1109/ACCESS.2024.3416840.

[35] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing Vehicle-to-Everything (V2X) Communication Platforms," IEEE Transactions on Intelligent Vehicles, vol. 5, no. 4, pp. 693-713, 2020, [Online]. Available: https://doi.org/10.1109/TIV.2020.2987430.

[36] S. Gyawali, Y. Qian, and R. Q. Hu, "Machine Learning and Reputation Based Misbehavior Detection in Vehicular Communication Networks," IEEE Transactions on Vehicular Technology, vol. 69, no. 8, pp. 8871-8885, 2020, [Online]. Available: https://doi.org/10.1109/TVT.2020.2996620.

[37] I. A. Sumra, H. Bin Hasbullah, and J. L. Bin AbManan, "Attacks on security goals (confidentiality, integrity, availability) in VANET: A survey," Advances in Intelligent Systems and Computing, vol. 306, pp. 51-61, 2015, [Online]. Available: https://doi.org/10.1007/978-981-287-158-9_5.

[38] S. Gillani, F. Shahzad, A. Qayyum, and A. Mehmood, "A Survey on Security in Vehicular Ad Hoc Networks: Major Security Threats in VANETs," pp. 59-74, 2013, [Online]. Available: https://doi.org/10.1007/978-3-642-37974-1_5.

[39] N. C. Velayudhan, A. Anitha, and M. Madanan, "Sybil Attack with RSU Detection and Location Privacy in Urban VANETs: An Efficient EPORP Technique," Wireless Personal Communications, vol. 122, no. 4, pp. 3573-3601, 2022, [Online]. Available: https://doi.org/10.1007/s11277-021-09102-x.

[40] R. Hostak and I. Baronak, "Security in VANET," pp. 0-20, 2023.

[41] Y. Khayati and T. Mazri, "Security study of routing attacks in vehicular AD-HOC networks (VANETs)," ISPRS Archives, vol. 44, no. 4/W3, pp. 267-272, 2020, [Online]. Available: https://doi.org/10.5194/isprs-archives-XLIV-4-W3-2020-267-2020.

[42] A. Anwar, A. Anwar, L. Moukahal, and M. Zulkernine, "Security assessment of in-vehicle communication protocols," Vehicular Communications, vol. 44, p. 100639, 2023, [Online]. Available: https://doi.org/10.1016/j.vehcom.2023.100639.

[43] M. A. R. Baee, L. Simpson, E. Foo, and J. Pieprzyk, "The Security of '2FLIP' Authentication Scheme for VANETs: Attacks and Rectifications," IEEE Open Journal of Vehicular Technology, vol. 4, pp. 101-113, 2023, [Online]. Available: https://doi.org/10.1109/OJVT.2022.3217552.

[44] T. Pavithra and B. S. Nagabhushana, "A Survey on Security in VANETs," 2nd International Conference on Inventive Research in Computing Applications (ICIRCA), pp. 881-889, 2020, [Online]. Available: https://doi.org/10.1109/ICIRCA48905.2020.9182823.

[45] A. Quyoom, A. A. Mir, and A. Sarwar, "Security Attacks and Challenges of VANETs: A Literature Survey," Journal of Multimedia Information System, vol. 7, no. 1, pp. 45-54, 2020, [Online]. Available: https://doi.org/10.33851/jmis.2020.7.1.45.

[46] K. V. Krishna and K. G. Reddy, "VANET Vulnerabilities Classification and Countermeasures: A Review," Majlesi Journal of Electrical Engineering, vol. 16, no. 3, pp. 63-83, 2022, [Online]. Available: https://doi.org/10.52547/mjee.16.3.63.

[47] H. Setia et al., "Securing the road ahead: Machine learning-driven DDoS attack detection in VANET cloud environments," Cyber Security and Applications, vol. 2, p. 100037, 2024, [Online]. Available: https://doi.org/10.1016/j.csa.2024.100037.

[48] S. Tanwar, J. Vora, S. Tyagi, N. Kumar, and M. S. Obaidat, "A systematic review on security issues in vehicular ad hoc network," Security and Privacy, vol. 1, no. 5, pp. 1-26, 2018, [Online]. Available: https://doi.org/10.1002/spy2.39.

[49] K. Singh and S. Sharma, "Advanced Security Attacks on Vehicular AD HOC Network (VANET)," International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 2, pp. 3057-3064, 2019, [Online]. Available: https://doi.org/10.35940/ijitee.b7687.129219.

[50] V. Nampally and M. R. Sharma, "A Survey on Security Attacks for VANET," Security Challenges, vol. 5, no. 10, 2017.

[51] A. C. Ali Hussein and A. K. Elhajj, "Fourth International Conference on Software Defined Systems (SDS), Valencia, Spain, 8-11 May 2017," pp. 67-74, 2020.

[52] M. Arif et al., "Applied sciences and challenges," Applied Sciences, vol. 10, no. 9, 2020.

[53] S. A. Soleymani, S. Goudarzi, M. H. Anisi, M. Zareei, A. H. Abdullah, and N. Kama, "A security and privacy scheme based on node and message authentication and trust in fog-enabled VANET," Vehicular Communications, vol. 29, p. 100335, 2021, [Online]. Available: https://doi.org/10.1016/j.vehcom.2021.100335.

[54] T. Nandy, R. Md Noor, R. Kolandaisamy, M. Y. I. Idris, and S. Bhattacharyya, "A review of security attacks and intrusion detection in the vehicular networks," Journal of King Saud University - Computer and Information Sciences, vol. 36, no. 2, p. 101945, 2024, [Online]. Available: https://doi.org/10.1016/j.jksuci.2024.101945.

[55] N. Phull and P. Singh, "A review on security issues in VANETs," 6th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 1084-1088, 2019.

[56] Z. Lu, G. Qu, and Z. Liu, "A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy," IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 2, pp. 760-776, 2019, [Online]. Available: https://doi.org/10.1109/TITS.2018.2818888.

[57] G. Mahalakshmi et al., "Machine Learning based Feature Selection for Intrusion Detection System in VANET," ResearchGate, 2021.

[58] T. Ismail et al., "A Comprehensive Survey on Vehicular Communication Security," Journal of Cyber Security and Mobility, vol. 13, no. 5, pp. 1007-1038, 2024, [Online]. Available: https://doi.org/10.13052/jcsm2245-1439.1359.

[59] A. Mchergui, T. Moulahi, and S. Zeadally, "Survey on Artificial Intelligence (AI) techniques for Vehicular Ad-hoc Networks (VANETs)," Vehicular Communications, vol. 34, p. 100403, 2022, [Online]. Available: https://doi.org/10.1016/j.vehcom.2021.100403.

[60] R. Sultana, J. Grover, and M. Tripathi, "Intelligent defense strategies: Comprehensive attack detection in VANET with deep reinforcement learning," Pervasive and Mobile Computing, vol. 103, p. 101962, 2024, [Online]. Available: https://doi.org/10.1016/j.pmcj.2024.101962.

[61] M. A. Abdelmaguid, H. S. Hassanein, and M. Zulkernine, "Securing the unforeseen: Enhancing VANET security with dynamic honeypots and attack rate analysis," Vehicular Communications, vol. 55, p. 100946, 2025, [Online]. Available: https://doi.org/10.1016/j.vehcom.2025.100946.

[62] D. Balta, Ü. Çavuşoğlu, and M. Balta, "A Comprehensive Survey On Machine Learning-Based Intrusion Detection System for Vehicular Area Network Architectures," Düzce Üniversitesi Bilim ve Teknoloji Dergisi, vol. 12, no. 3, pp. 1536-1556, 2024, [Online]. Available: https://doi.org/10.29130/dubited.1372131.

[63] A. Hankins, T. Das, S. Sengupta, and D. Feil-Seifer, "Eyes on the Road: A Survey on Cyber Attacks and Defense Solutions for Vehicular Ad-Hoc Networks," IEEE Computing and Communication Workshop and Conference (CCWC), pp. 585-592, 2023, [Online]. Available: https://doi.org/10.1109/CCWC57344.2023.10099187.

[64] J. Liang, M. S. Sheikh, and W. Wang, "A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs)," Sensors (Switzerland), vol. 19, no. 16, 2019, [Online]. Available: https://doi.org/10.3390/s19163589.

[65] H. Kim and J. M. Chung, "VANET jamming and adversarial attack defense for autonomous vehicle safety," Computers, Materials and Continua, vol. 71, no. 2, pp. 3589-3605, 2022, [Online]. Available: https://doi.org/10.32604/cmc.2022.023073.

[66] Y. Huang and M. Ma, "ILL-IDS: An incremental lifetime learning IDS for VANETs," Computers & Security, vol. 124, p. 102992, 2023, [Online]. Available: https://doi.org/10.1016/j.cose.2022.102992.

[67] S. Hakak et al., "Autonomous vehicles in 5G and beyond: A survey," Vehicular Communications, vol. 39, pp. 1-34, 2022, [Online]. Available: https://doi.org/10.1016/j.vehcom.2022.100551.

[68] M. Arif et al., "Applied sciences and challenges," Applied Sciences, vol. 10, no. 9, 2020.

[69] T. Nandy, R. Md Noor, R. Kolandaisamy, M. Y. I. Idris, and S. Bhattacharyya, "A review of security attacks and intrusion detection in the vehicular networks," Journal of King Saud University - Computer and Information Sciences, vol. 36, no. 2, p. 101945, 2024, [Online]. Available: https://doi.org/10.1016/j.jksuci.2024.101945.

[70] S. H. A. Kazmi, F. Qamar, R. Hassan, K. Nisar, and B. S. Chowdhry, "Survey on Joint Paradigm of 5G and SDN Emerging Mobile Technologies: Architecture, Security, Challenges and Research Directions," Wireless Personal Communications, vol. 130, no. 4, pp. 2753-2800, 2023, [Online]. Available: https://doi.org/10.1007/s11277-023-10402-7.

[71] T. Mekki, I. Jabri, A. Rachedi, and L. Chaari, "Software-defined networking in vehicular networks: A survey," Transactions on Emerging Telecommunications Technologies, vol. 33, no. 10, pp. 1-29, 2021, [Online]. Available: https://doi.org/10.1002/ett.4265.