A Comprehensive Survey on Vehicular Communication Security

Tayssir Ismail[1,*], Haifa Touati[2], Nasreddine Hajlaoui[3], Mohamed Hadded[4], Paul Muhlethaler[5], Samia Bouzefrane[1] and Leila Azouz Saidane[6]

[1]*CEDRIC Lab, Conservatoire National des Arts et Metiers, Paris, France*
[2]*Hatem Bettaher IResCoMath Research Lab, University of Gabes, Tunisia*
[3]*Unit of Scientific Research, Applied College, Qassim University, SA*
[4]*Abu Dhabi University, UAE*
[5]*INRIA Paris, France*
[6]*CRISTAL Lab, National School of Computer Science, University of Manouba, Tunisia*
E-mail: tayssir.ismail@lecnam.net, haifa.touati@cristal.rnu.tn, nasreddine.hajlaoui@fsg.rnu.tn, mohamed.elhadad@adu.ac.ae, paul.muhlethaler@inria.fr, samia.bouzefrane@cnam.fr, leila.saidane@ensi.rnu.tn
[*]*Corresponding Author*

Received 16 March 2024; Accepted 03 June 2024

Abstract

Significant advancements in Cooperative and Autonomous Driving via Vehicle-to-everything (V2X) communications owe much to the rapid expansion and technological progress in vehicular communications, promising benefits like enhanced traffic flow and reduced energy consumption. However, this reliance on connected vehicles opens new security vulnerabilities. This study provides a comprehensive overview of challenges in existing vehicular communications, with a specific focus on security attacks categorised by their impact on MAC, routing, and cross-layer levels. To ensure secure vehicular communication, we analyse existing solutions for both single and cross-layer

Journal of Cyber Security and Mobility, Vol. 13_5, 1007–1038.
doi: 10.13052/jcsm2245-1439.1359

attacks, evaluating their strengths and limitations from a security standpoint. Additionally, we innovate by addressing vulnerabilities across MAC, routing, and cross-layer interactions, offering practical insights and a unique approach to mitigating their combined impact. Our findings suggest that enhancements are needed for MAC layer security in TDMA protocols, and that routing protocols must be designed with better security features to manage high overheads and real-time requirements.

Keywords: Vehicular networking, V2X technologies, security threats, intrusion detection, misbehaviour detection.

1 Introduction and Motivation

Vehicular networking has emerged as a pivotal component for cooperative automotive applications, playing a crucial role in enhancing both safety and efficiency. Notably, autonomous cooperative driving, facilitated by V2X technologies, has become a strategic focal point for car manufacturers. This approach aims to augment perception capabilities through the exchange of sensor data and it success is heavily reliant on robust vehicular communication technologies, operating in three distinct modes: vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and a hybrid combination of V2V/V2I. Within this framework, Vehicular Ad-Hoc Network (VANET) applications are categorised into safety-related, with a primary goal of accident prevention, and non-safety-related applications that focus on enhancing passenger comfort and providing access to various services. As VANET applications have become more widespread, attackers are increasingly motivated to disrupt vehicular communications, potentially causing significant losses. This has prompted an accelerated pace of research on attacks targeting vehicular networks and the development of mitigation solutions, particularly with the increased prominence of autonomous vehicles. Despite the extensive body of security research in vehicular networks, our study distinctly focuses on surveying MAC, routing, and cross-layer attacks within vehicular networks, along with an examination of the proposed solutions found in the existing literature. The contributions of this paper include:

- We explore security threats targeting vehicular communication, categorising these attacks according to their impact across the layers of the MAC, routing, and cross-layer protocols. This approach helps us unveil vulnerabilities and understand associated risks.

- We conduct a thorough examination of existing literature on vehicular communication security, incorporating an in-depth qualitative comparison. This meticulous analysis establishes a solid foundation for identifying research gaps, offering valuable insights to enhance mitigation strategies that fortify vehicular network resilience.
- Our study identifies lessons learned and pinpoints open research challenges within the field. These challenges collectively shape a roadmap for future research endeavours in vehicular communication security, guiding the exploration of innovative and secure protocols.

The rest of the paper is organised as follows. We review related works in Section 2. Section 3 details MAC, routing, and cross-layer attacks in vehicular communication and Section 4 offers an in-depth analysis of existing techniques for detecting and mitigating these attacks. In Section 5, we summarise lessons learned and identify outstanding issues in the field. Finally, Section 6 concludes the paper.

2 Related works

Recently, different surveys have been published regarding vehicular communication security. A summary of existing surveys is shown in Table 1. In 2018, three survey papers [1–3] were published. In [1], the authors discussed and classified misbehaviour detection mechanisms in Cooperative Intelligent Transportation Systems (C-ITS). In [2], Sharma et al. surveyed Intrusion Detection Systems (IDS) proposed for VANETs. They analysed and compared each IDS technique along with its merits and shortcomings. In [3], Lu et al. gave a comprehensive analysis of various trust management models in VANETs.

In 2019, the trajectory of VANET research remained steadfast with two seminal surveys [4, 5]. In [4], the authors conducted a thorough review of AI-driven vehicular safety, categorising research studies across diverse application domains. Simultaneously, Kelarestaghi et al. [5] addressed security challenges in VANET access technologies, revealing threats and providing an overview of mitigation mechanisms.

In 2020, Hussain et al. [6] made a significant contribution to VANET literature by analysing and comparing trust establishment and management mechanisms. Their work highlights the vulnerabilities and limitations of existing approaches in this domain. This review not only underscores the complexities of trust-related paradigms, but also serves as a rallying point for the advancement of robust trust mechanisms in vehicular networks.

In 2021, authors of [7] carry out an analysis of existing solutions. The research highlights the most common security problems and the different types of attack that affect ITS. It also investigates the applicability of Machine Learning (ML) algorithms with signature-based IDS to strengthen security measures in VANETs.

In 2023, [8, 10] comprehensively addressed VANETs security. [8] provided an in-depth examination of MAC protocols, fading channels, routing protocols, security, and clustering techniques, highlighting the integration of AI techniques to enhance VANET security and suggesting future research avenues. Parallelly, Li et al. [9] analysed and compared AI-enabled trust solutions categorised under Trust Management, IDS, and Recommender Systems. Sangwan et al. [10] reviewed misbehaviour assaults in VANETs, categorising them based on architecture, method, node-centricity, and data-centricity, and emphasised the relevance of ML methods in misbehaviour detection.

The above surveys comprehensively cover the security challenges of VANETs and their mitigation techniques. The attacks covered address different security issues such as availability, integrity, confidentiality, etc. However, in this study, we focused on covering the attacks that mainly target the availability of services where cooperation is required to ensure network operation. In addition, we comprehensively cover these attacks with recent state-of-the-art methods that indicate existing VANET security problems and their solutions, which target MAC, routing, and cross-layer protocols. Conversely, the cross-layer class was not covered as a distinct section in most surveys. Furthermore, the mitigation solutions discussed in our study do not revolve exclusively around a particular category, unlike the approaches detailed in [2] and [3], which focus on IDS and trust management solutions respectively.

3 Communication Attacks in VANETs

Compared to traditional wireless networks, VANET protocols exhibit specific vulnerabilities that attackers exploit to compromise network security. The first vulnerability stems from the high mobility and dynamic topology of VANETs. The constant movement of vehicles results in a highly dynamic network topology, making it difficult to maintain stable connections and implement consistent security measures. Attackers can exploit this instability to launch routing attacks, such as Wormhole or Black Hole attacks, which are less effective in the relatively static topology of traditional wireless networks. A second vulnerability arises from the decentralized network architecture.

Table 1 Comparison of our contribution with related survey papers

Ref	Year	Contribution	Limitations	Common Points With our Survey
[1]	2018	Survey of misbehaviour detection mechanisms in C-ITS	Absence of cross-layer detection mechanisms	Security analysis of C-ITS
[2]	2018	Survey of VANETs IDS and comparison of their detection strategies	Focus only on IDS solutions and do not investigate different security solutions	Review of IDS in VANETs
[3]	2018	Analysis of attack and trust management models to secure VANETs	Focus only on trust models solutions	Analysis of the trust management models used in VANETs
[4]	2019	Assessing AI use in V2X applications, including AI algorithm comparisons	Partial investigation of the attacks	Review of RL models used in VANETs
[5]	2019	Analysis of vulnerabilities in VANETs and discussion of main mitigation techniques	Classification by different access technologies, not by attacks.	Vulnerabilities assessment and discussion of potential mitigation techniques
[6]	2020	Trust management solutions reliant on reputation system to evaluate vehicle reliability	Trust-centric survey	Analysis of trust establishment approaches in VANETs
[7]	2021	ITS security and existing attacks mitigation techniques	Does not encompass the real-time and dynamic nature of cybersecurity threats	Attacks classification and comparison of defence strategies
[8]	2023	Survey of AI-based techniques to enhance VANETs security	Several attacks are not included, like Black Hole, DoS...	Covered layers, namely MAC and routing layers.
[9]	2023	Review of ML-based trust solutions in VANETs	Trust-centric survey	Analysis of trust establishment approaches in VANETs.
[10]	2023	Survey of ML-based methods to detect misbehaviour in VANETs	Absence of cross-layer detection mechanisms	Node-centric misbehaviour detection.
Our survey	2024	In-depth survey of MAC, routing, and cross layer attacks and solutions and future research directions	-	Attack Taxonomy + Detection Mechanisms + In-depth Analysis + Open research issues.

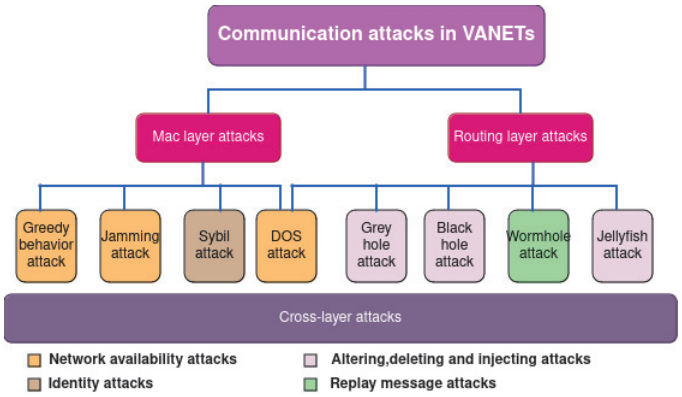


Figure 1 Attack scenarios in VANETs.

VANETs lack a centralized authority, complicating the enforcement of security policies and making it difficult to manage trust among nodes. Attackers can exploit this vulnerability by using for example Sybil attacks to create multiple fake identities, disrupting network operations and communication integrity, a challenge that is more manageable in the centralized structure of traditional wireless networks. Finally, real-time communication requirements introduce another vulnerability in VANETs. The need for real-time data exchange limits the time available for comprehensive security checks and encryption processes. Attackers may exploit this vulnerability by launching Denial of Service (DoS) attacks to overwhelm the network, causing delays that are particularly harmful given the real-time requirements of VANET communications. Traditional networks, with less stringent real-time constraints, can better tolerate and mitigate such attacks.

In this section, we systematically classify these attacks based on their impact on MAC, routing, and cross-layer functionalities, as depicted in Figure 1.

3.1 MAC Layer Attacks

MAC layer protocols in VANET improve channel utilisation, network lifetime and node coordination. They are broadly divided into contention-based protocols (e.g. CSMA/CA, EDCA) and schedule-based protocols (e.g. TDMA). Contention-based protocols prioritise accessing the channel and address issues like hidden terminals, while schedule-based protocols efficiently allocate resources, ensuring reliable and quality service for real-time

applications. Protocols that are based on TDMA guarantee reliability and quality of service by using mechanisms such as assigning specific time slots to each vehicle to prevent collisions and maintaining accurate timing through synchronisation. These protocols include collision avoidance, reserving slots for important messages to be delivered on time, and adjusting slot assignment to maximise bandwidth efficiency depending on traffic conditions. MAC layer misbehaviour's include selfish behaviour and malicious behaviour. Selfish behaviour among vehicles can exacerbate traffic congestion, leading to detrimental consequences for both safety and network efficiency. Selfish actions, such as withholding critical traffic information or intentionally causing congestion to gain personal advantages, can increase accident rates and delay emergency response vehicles. This jeopardizes the safety of all road users. Furthermore, traffic congestion resulting from selfish behaviour reduces the overall throughput of the network and increases communication latency. Malicious behaviour, disrupting communication with strong signals or fake packets, posing detection challenges and degrading network performance. Common MAC layer attacks in VANETs include:

- **Greedy behaviour attack:** falls under the "selfish" misbehaviour category, aiming to monopolise network resources. Greedy nodes do not respect channel access policies, prioritise their own access, and penalise others for not cooperating [11]. In VANETs, this selfish behaviour disregards network rules, resulting in issues like misleading routing, traffic congestion, and collisions.
- **Jamming attack:** it is a form of DoS attack that disrupts legitimate data traffic by transmitting interfering radio signals, leading to potential data corruption. This includes various types such as *Constant Jammer*, emitting random signal bits continuously; *Deceptive Jammer*, sending valid packets with a valid header but useless payload; *Random Jammer*, alternating between jamming and sleeping periods; and *Reactive Jammer*, monitoring ongoing communication and introducing noise into detected packets to render them unusable by the receiver.
- **Sybil attack:** poses numerous threats in VANET when false identities are used in network messages by imitating regular nodes. Malicious nodes use network dynamics to carry out Sybil attacks, where they create numerous fake identities within the network. These attacks disrupt traffic management, compromise safety by spreading false information about traffic conditions and vehicle positions, and erode trust among network participants. Consequently, Sybil attacks can lead to traffic congestion,

increased collision risks, delayed emergency responses, and degraded overall network reliability and performance.

3.2 Routing Layer Attacks

In VANETs, routing layer protocols have to maintain stable links between fast-moving vehicles and to guarantee efficient routing and self-organisation, which is crucial for timely communication in VANETs. Attacks on the routing layer can allow attackers to control, manipulate, or delete the information being routed in the network, which can be used for the attacker's benefit or to completely disrupt the network. If attackers gain control over routing information in VANETs, they could execute various attacks such as routing loops, black hole attacks, and selective forwarding, leading to significant network disruption. This disruption may cause increased latency, packet loss, and even network partitioning, severely impacting the reliability and efficiency of vehicular communication. As illustrated in Figure 1, the most common routing attacks in VANETs are:

- **Black Hole attack:** in this attack, attackers trick by offering to relay packets with false metrics, appearing to be the best forwarders. They attract the packets but drop or consume them instead of forwarding them, thus preventing delivery to the destination.
- **Gray Hole attack:** It is an intelligent version of a black hole attack where the attacker node creates the illusion that it routes the received packets in a normal manner, but it selectively drops packets of some specific type or those received from specific vehicles.
- **Wormhole attack:** Wormhole nodes position themselves strategically to intercept messages and create a private tunnel for faster communication. This control enables them to disrupt the network and compromise data security. They create shortcuts to prevent the discovery of legitimate nodes and cause network disruption.
- **Jellyfish attack:** The attacker introduces delays in packets instead of dropping them silently, as is done in black hole attacks. The attacker gains trust before initiating delays, making it difficult to distinguish from network congestion. Attackers use trust-building methods, aiming to go undetected by mimicking authentic network traffic patterns. Initially, attackers may engage in normal communication behaviour, participating in routing activities and responding promptly to network requests. They might also mimic the behaviour of legitimate nodes, adhering to established protocols to establish credibility. By blending

in with genuine network traffic, attackers aim to evade suspicion and gain the trust of other network participants. Once they have established a facade of trustworthiness, attackers then gradually introduce delays, leveraging the cover of existing network congestion to conceal their malicious activities. This attack includes three types: delay variance, periodic dropping, and reorder attacks.

- **DoS attack:** In its basic form, consists of a malicious node overwhelming the resources of valid nodes by sending far more requests than the system can handle. Consequently, the legitimate vehicles can no longer communicate with each other.

3.3 Cross-layer Attacks

Traditional layered protocols face difficulties in fast-moving VANETs due to rapid changes in topology and density, prompting a transition to cross-layer protocols. These innovative designs integrate information from multiple layers. By integrating MAC parameters into routing decisions, cross-layer protocols aim to improve VANET communication efficiency. This integration offers several advantages. For instance, by considering parameters like channel occupancy, signal strength, and collision rates, the routing protocol can dynamically select relay vehicles with optimal communication conditions, leading to more efficient and reliable data transmission in VANETs. Moreover, integrating access parameters into routing decisions allows cross-layer protocols to optimise routing paths based on factors like contention window and backoff mechanism parameters in contention-based MAC protocols, and slot allocation in TDMA-based protocols. This helps reduce collision and contention overhead and ensures efficient time slot utilisation, thereby reducing latency and improving overall throughput. However, this approach can also introduce certain disadvantages. The increased complexity of the routing protocol may lead to higher computational overhead and energy consumption. Additionally, dynamically selecting relay vehicles based on MAC parameters could potentially introduce scalability issues as the network size grows, requiring frequent updates and impacting stability. Furthermore, implementation and compatibility problems may arise when integrating MAC parameter-based routing decisions across heterogeneous VANET environments.

Integrating MAC parameters into routing choices provides benefits such as increased throughput, enhanced quality of service, decreased latency, and improved resource optimisation. In contrast, drawbacks consist of higher

protocol complexity, scalability obstacles, implementation and compatibility problems, and the possibility of less than ideal routing choices. Recent advances focus on improving the efficiency of security message transmission, with MAC-aware routing protocols using CSMA/CA and TDMA MAC protocols. Attackers in this specific category will take advantage of weaknesses in each layer involved. Vehicles are constantly gathering valuable information from other vehicles or from the environment to provide the required functionality, such as traffic jam detection or deceleration warning systems. vehicles could exchange useful information, such as accident notifications, road conditions, etc., to facilitate traffic management. However, some of them use the collected information to deviate from the protocol specifications to achieve a given goal, to the detriment of the honest participant. This degrades the overall performance of the network. It can be said that the attack patterns remain the same as for single-layer attacks, as illustrated in Figure 1 but the information surface exploited by the attacker is larger. Therefore, they can be more sophisticated and effective than attacks that target a single layer. Detecting and neutralising multi-layer attacks poses major challenges because of the complex and interconnected structure of modern networks. The challenges consist of the necessity for comprehensive visibility across every level, the excessive amount of monitoring data, changing threat strategies, restricted resources and knowledge, compatibility problems between security tools, high numbers of inaccurate results, and the complication of organising a successful incident response.

4 Existing Mitigation Techniques Against Attacks in VANETs

Misbehaving nodes in critical VANETs applications pose serious risks, including potential loss of lives. In this section, we review security solutions proposed in the literature to each attack identified in **Section 4**. We start with single-layer (i.e. MAC and routing) detection techniques, followed by cross-layer detection schemes.

4.1 Solutions to Mitigate MAC Layer Attacks

In this section, we provide a detailed description of solutions proposed in the literature to mitigate MAC layer attacks as detailed in Table 2.

Table 2 Summary of solutions to mitigate MAC Layer attacks

Ref	Year	Attack	Security Goal		Proposed Solution
			Detection	Prevention	
[12]	2014	Greedy behaviour	✓	✓	Linear regression + Watchdog based on fuzzy logic decision scheme
[13]	2015				
[14]	2017	Greedy behaviour	✓		TFT based strategies: Group Reputation and Cooperative Detection
[15]	2019	Jamming Eavesdropping	✓	✓	Deep reinforcement learning
[16]	2022	Jamming	✓	✓	Estimate the jammer-receiver distance
[17]	2018	DDoS	✓	✓	Calculate threshold of bandwidth consumption and data rate / Node isolation
[18]	2022	DoS/DDoS	✓		MDASTI: Collecting data from the MAC frames/ Detecting anomalies using MAD
[19]	2023	DoS/DDoS	✓		DAMASCO: Monitoring the number of transmitted packets / Using MAD to detect attackers

4.1.1 Solutions to mitigate greedy behaviour attacks

Mejri et al. proposed GDVAN in [12, 13], which integrates linear regression, watchdog, and fuzzy logic. They identify greedy nodes through two phases: suspicion and decision. In the suspicion phase, GDVAN uses correlation coefficient to analyse speeds and directions of nearby vehicles in VANETs. A high correlation suggests normal behaviour, while a significant difference may indicate suspicious activity. Linear regression is also used to model behavior over time, with steep slopes possibly indicating sudden changes or suspicious activity. Both methods are flagged for further investigation. The decision phase employs a fuzzy logic scheme. Watchdog supervision tracks metrics, like transmission duration and connection attempts, confirming an attack if thresholds are exceeded. In [14], Terri et al. use game theory modelling. A Tit-For-Tat (TFT) strategy is used to introduce Group Reputation (GR) and Cooperative Detection (CD) strategies to detect greedy nodes.

4.1.2 Solutions to mitigate jamming attacks

Abuzainab et al. [15] use reinforcement learning to enhance the resilience of communication against jamming. Their solution helps nodes avoid communication gaps caused by jamming attacks and enables real-time network defence decisions through distributed cooperation. In [16], the focus shifts from jamming detection to jammer localisation. Their approach utilises jammer signal strength to estimate the jammer-receiver distance and proposes a simplified algorithm for localisation and rerouting. The algorithm uses signal strength analysis to determine how close jammers are to vehicles in the network, which helps in estimating distances. Rerouting involves steering vehicles away from jammed roads by increasing the weight of those routes, prompting vehicles to seek alternative paths and maintain smooth communication.

4.1.3 Solutions to mitigate DoS attacks

In [17], an improved detection and mitigation of DDoS model is proposed. Initially, the bandwidth usage of each node is monitored, the mitigation phase is triggered if a vehicle's usage surpasses a threshold. This phase identifies the source of control packet transmission and aims to isolate malicious vehicles. The proposed signature verification technique offers a more efficient approach than current methods, focusing on simplicity. However, it lacks detailed explanation regarding threshold calculation. Additionally, while existing signature detection techniques are known to increase detection time, the suggested solution does not fully tackle this issue, leading to concerns about its effectiveness in real-time scenarios. In [18], MDASTI,

a host-based DoS detection system for ITS is proposed. It uses a statistical model based on median calculation from broadcast requests to identify malicious vehicles and maintains a local reputation list for node filtering. MDASTI evaluates four key attack characteristics: Flooding, Packet Storm, Disassociation, and Traffic Source, by analysing received packets at each host to detect anomalies and potential attacks. MDASTI uses a simple statistical model that relies on calculating the median to detect unusual actions. These techniques work by examining statistical characteristics in a set of data and creating criteria for rejecting based on assumptions about the distribution of the data. However, effectiveness may be limited in complex settings. In [19], DAMASCO is introduced as a decentralized IDS for VANETs, offering cooperative security against DoS/DDoS attacks. It incorporates a lightweight probabilistic function to analyse and filter packets at each node within the network using Median Absolute Deviation (MAD) to identify potential malicious nodes and attack characteristics. DAMASCO operates using a decentralised model, providing a level of simplicity that is ideal for running on devices with restricted computational capabilities, due to the algorithm's low complexity. Nevertheless, there is no system in place to stop trusted nodes like emergency vehicles from being unfairly blacklisted. Furthermore, assessment done through simulation is reliable but may not capture real-life complexities.

4.2 Solutions to Mitigate Routing Layer Attacks

In this section, we elaborate on the solutions proposed in existing literature to mitigate routing layer attacks, as outlined in Table 3.

4.2.1 Solutions to mitigate black hole attacks

Mostefa et al. [20] utilise TFT to categorise nodes into allow-list, watch-list, and deny-list. Nodes exhibiting malicious behaviour are first gray-listed and then blacklisted upon repeat offences, leading to network isolation. In [21], the authors present DPBHA, a solution for detecting and preventing black hole attacks in VANETs. DPBHA dynamically calculates a threshold value from sequence numbers of Route Reply (RREP) packets and generates a forged Route Request (RREQ) packet. The threshold value is determined based on the difference between the sequence number of the last received RREP and the existing Routing Table (RT). Once the threshold value is calculated, the source node compares the sequence number of each received RREP with this dynamically determined threshold value. RREPs with sequence

Table 3 Summary of solutions to mitigate routing attacks

Ref	Year	Attack	Security Goal		Proposed Solution
			Detection	Prevention	
[20]	2020	Black hole	✓		TFT based solution: nodes are classified to: allow-list, watch-list, and deny-list .
[21]	2022	Black hole	✓	✓	DPBHA: calculates a dynamic threshold value from sequence numbers of RREP packets.
[22]	2023	Black hole	✓		RSUs compute a dynamic threshold value Classify vehicles into legitimate, suspicious and attackers, identified based on node credibility values.
[23]	2023	Black hole	✓		Q-learning-based: Local information module / Remote information module / Learning module.
[24]	2020	Black hole / Gray hole	✓	✓	Trust-based TRPM: Information gathering / Trust composition / Trust application
[25]	2022	Grey hole / Black hole	✓	✓	TrustV: game theory based: use the iterated prisoner's dilemma game.
[26]	2023	Grey hole /Black hole	✓	✓	Markov Decision Process to choose the best rout Q-learning to learn the trust value of links
[27]	2024	Grey hole	✓	✓	Cluster-based: CH monitors suspicious activities and observes data transmission to identify attackers
[28]	2017	Wormhole	✓	✓	WPD:Packets monitoring/ Lower greatest hop bound / Path verification
[29]	2019	Wormhole	✓	✓	Route discovery/ WPWP packet transmission/ Storing intermediate vehicle ids/ Identifying wormhole node.
[30]	2020	Wormhole	✓	✓	Compare RREP's round trip with threshold to detect wormhole attack
[31]	2020	DoS	✓		P-secure: Detect attackers based on threshold and Processing new request to join network
[32]	2022	DoS	✓	✓	FA-AODV: Attacker identification if packet drop level exceeds the predefined threshold
[33]	2023	DoS	✓	✓	Cluster-based DoSRT: Direct-trust computation of sender / Indirect-trust computation / Total trust computation / Attacker list generation

numbers higher than the threshold value are identified as potentially malicious nodes, facilitating the early detection of black hole attacks. In [22], a hybrid method is proposed to detect black hole attackers early, combining dynamic thresholds and node credibility. Roadside Units (RSUs) compute dynamic thresholds and classify vehicles into three categories: Legitimate (Category 1), Suspicious (Category 2), and Identified Attackers (Category 3). Node credibility aids in identifying attackers within Category 2, countering various black hole attack scenarios. In [23], a RL framework is proposed for VANET neighbour selection, integrating an adaptive trust management system. It dynamically updates neighbourhood information to capture potential attacker behaviour changes. The framework employs Q-learning for intermediate node selection, using trust and link lifetime as criteria for reliable communication. To detect black or grey hole attackers, the framework comprises three main components: local information, remote information, and learning modules.

4.2.2 Solutions to mitigate gray hole attacks

In contrast to a Black Hole attack, which disrupts communication by dropping all received packets without discrimination, a Gray Hole attack strategically drops or alters packets based on specific criteria, such as packet type, content, or sender, showing a more subtle and calculated way to disrupt network operations. Even though Black Hole attacks are visibly disruptive, Gray Hole attacks present a more hidden danger, which could make them more challenging to identify and address.

Baccari et al. [24] propose a trust-based model for TDMA-aware Routing Protocol for Multi-hop communications (TRPM) to counter Black Hole, Gray Hole, and DoS attacks. The model consists of three modules: Information gathering, Trust composition, and Trust application. It continuously monitors positive and negative events, calculates neighbour's Frame Information Trust (NFT) and Forwarding Trust (FT), and reserves slots only for nodes exceeding a trust threshold. [25] presents TrustV, a hybrid reputation system utilizing game theory, particularly the iterated prisoner's dilemma game, for cooperation decisions. TrustV effectively deals with uncertainties in HetVNETs by modeling cooperation as a game, identifying selfish and malicious nodes over time. Mianji et al. in [26] propose QL-TRT, a Q-learning-based method for identifying and preventing black hole and grey hole attacks in VANETs. Using a Markov Decision Process, vehicles select trustworthy neighbors for routing while avoiding potential threats. Link trustworthiness is assessed based on packet forwarding ratios, energy consumption, and transmission

time. Q-learning determines optimal route selection by assigning link trust values. In [27], Kaur et al. propose a cluster-based method for detecting and preventing gray hole attacks. The solution comprises two phases: cluster leaders (CHs) monitor suspicious activity during transmission and classify malicious nodes as suspicious. Next, suspicious nodes are further examined for gray holes by observing data transmission. Multiple transmissions accompanied by packet drops confirm that a node is a gray hole. The CH notifies the parties concerned of the node's "grey hole" ID and continues monitoring before removing the node from the list of suspect nodes if it behaves normally.

4.2.3 Solutions to mitigate wormhole attacks

In [28], Albouq et al. introduce the Wormhole-Protocol-Detector (WPD), a lightweight protocol to detect and avoid wormhole attacks. WPD operates in three phases: packets monitoring, lower greatest hop bound, and path verification. WPD monitors the network and detect out-of-range packets, indicating a potential wormhole attack. Then, the protocol estimates Hop Count Between Source and Destination Nodes In the final phase, malicious nodes creating fake shortcut paths are identified by employing neighbour discovery and verification processes to confirm the legitimacy of neighbouring nodes.

In [29], a new algorithm is proposed to detect and isolate tunnelling attacks using the Wormhole Path Watcher Packet (WPWP) technique. The process involves four steps: route discovery, WPWP packet transmission, storing intermediate vehicle identifiers, and identifying the wormhole node. The WPWP algorithm uses special packets to monitor network paths for suspicious delays or hop counts during route discovery. These packets are strategically crafted to traverse the network along the route being discovered, gathering crucial information about the path characteristics. They record timestamps at various points, capturing the time taken for each hop and the number of hops encountered. By comparing the expected path characteristics, such as expected delay and hop count, with the observed values recorded by WPWP packets. If suspicious delays or hop counts are detected, WPWP packets are sent to confirm wormhole presence. Intermediate vehicle identifiers are stored if a wormhole is suspected. The algorithm iterates until a reliable path is found, then identifies and isolates the wormhole node based on duplicate identifiers. In [30], Ali et al. assessed the impact of wormhole attacks on the AODV routing protocol. They also propose a detection and prevention method, which begins with route discovery. Source vehicles

broadcast RREQ packets to neighboring vehicles, recording sending times. Upon receiving RREQs, vehicles reply with RREP packets, and round-trip times are calculated. A threshold is determined based on average round-trip times and the number of received RREPs. If a received RREP's round-trip time is below the threshold and the path involves only two vehicles, a wormhole is detected.

4.2.4 Solutions to mitigate DoS attacks

In [31], the P-secure approach propose to early detect DoS attacks through two phases. In the first phase, vehicle data, including location, speed and number of messages, are collected, with threshold values set manually. If the data received exceeds the threshold, a potentially malicious vehicle is flagged. In the second phase, new network connection requests are checked against the previous valid database to minimise false requests. In [32], the FA-AODV algorithm is proposed to counter DoS attacks. Nodes operate in "promiscuous mode" to monitor packet communication with neighbours. Nodes that exceed a predefined packet drop threshold are considered malicious and excluded from future transmissions. Marker nodes broadcast messages to identify malicious nodes and remove their packets. In [33], DoSRT introduces a cluster-based DoS Resistant Trust model. It assesses vehicle trust through message exchange frequency to counter DoS attacks. DoSRT monitors neighbour vehicle behaviour continuously and comprises four modules: Direct-trust computation of sender, Indirect-trust computation, Total trust computation, and Generate attacker list.

The P-secure method offers robust security through advanced encryption and anomaly detection, enabling early detection and prevention of DoS attacks. However, it may introduce some latency due to heavy processing. The FA-AODV algorithm, which utilises fuzzy logic and ant colony optimisation, adjusts rapidly to network variations, providing moderate to high precision and rapid response rates, yet it may be less efficient in highly dynamic circumstances because of the burden of upholding pheromone trails. The DoSRT model stands out for its precise accuracy and quick reactions within a cluster-based system, effectively identifying and handling attacks with minimal extra costs, proving especially useful in large, constantly changing networks. In general, P-secure guarantees strong security in stable situations, FA-AODV excels in moving conditions, and DoSRT offers a balanced, scalable fix for large, changing networks.

4.3 Solutions to Mitigate Cross-layer Attacks

Previous studies in securing vehicular networks typically address protection of individual OSI layers separately. However, integrating layers to share data enhances network performance and operational efficiency. The advantage of incorporating multi-layer information for attack detection has garnered considerable interest. Cross-layer schemes aim to monitor features across multiple layers, enabling more accurate detection of single-layer attacks and thereby improving overall network detection performance. Our research considers the MAC and routing layers, demonstrating a cross-layer detection solution, that leverages data from these layers to effectively identify attackers. The solution collects relevant data based on the protocols used and the characteristics of targeted attacks, using a detection algorithm to monitor multiple metrics to identify and/or isolate malicious nodes. Detected malicious nodes are excluded as next hops, and their identity is broadcast to prevent the selection of routing paths by other nodes. To illustrate the gereral cross-layer detection principal we will delve into a specific example that encompasses the MAC and routing layers. Subba et al. in [34] present a multi-layered VANET intrusion detection framework, comprising a Local IDS (LIDS) for neighborhood vehicle monitoring. LIDS utilizes specifications like RSSI, PDR, PFR, and DPR to detect malicious vehicles. Subsequently, a Cluster IDS (CIDS) employs game theory to monitor reported malicious vehicles by CHs. CHs and malicious vehicles engage in a non-cooperative game, optimizing their strategies based on potential consequences. Malicious nodes are identified and categorized by a Global Decision System (GDS), which aggregates reports from multiple CHs and broadcasts their identities via RSUs to prevent communication with normal vehicles.

In this section, we explore the remedies proposed in earlier research to to tackle cross-layer layer attacks, as enumerated in Table 4.

4.3.1 Cross-layer solutions to mitigate black hole attacks

Hierarchical architectures are proposed to address black hole attacks in VANETs, such as the QoS-OLSR protocol [35, 36]. In [35], the authors propose to monitor both VANET-OLSR and MAC layers to detect black holes targeting Multi-Point Relays (MPRs). This solution enhances detection by employing a cooperative intrusion detection system based on cross-layer architecture, where watchdogs compare transmitted and received packets to identify malicious nodes. In [36], the authors improved their cross-layer solution by aggregating the physical layer detection with the MAC and

Table 4 Summary of solutions to mitigate cross-layer attacks

Ref	Year	Attack	Security Goal		Proposed Solution
			Detection	Prevention	
[34]	2018	Malicious vehicle	✓	✓	Local IDS / Cluster IDS / Global Decision System
[35]	2014	Black hole	✓		*Cooperative watchdog *Mac monitoring
[36]	2016				
[37]	2017	Black hole	✓	✓	*Cross-layer data collection/ Detection stage/ Decision stage
[38]	2023	Black hole	✓	✓	Checking incoming RREP packets to determine their authenticity
[39]	2017	DDoS	✓	✓	Analysing signal properties/ Incorporating results into routing table/ Isolating malicious nodes

routing layer detection and improved the detection rate. Shurman et al. [37] developed a cross-layer IDS to counter black hole attacks. They modified the Ad Hoc On-Demand Distance Vector (AODV) routing protocol for this purpose, involving three stages. Firstly, cross-layer data collection gathers features from different layers. Next, these features are used to identify black hole nodes using fuzzy theory. Finally, a decision is made for each node, removing it from the network if identified as a black hole. Rabiaa et al. [38] introduced CRAOMDV, a cross-layer ad-hoc multi path routing scheme for secure data transmission in VANETs. It exchanges data between network and MAC layers to detect and evade attackers, removing routes with malicious nodes. CRAOMDV also selects alternative paths to prevent data loss, emphasising the need for efficient cost metrics for optimal route discovery.

4.3.2 Cross-layer solutions to mitigate DoS attacks

Since a DoS attack usually aims to exhaust the available resources, determining threshold values is the most preferable method among the solutions mentioned above. In general, the dynamic determination of threshold values for DoS attack detection in VANETs enables a more adaptive, accurate, and efficient detection mechanism compared to static thresholds. By continuously adjusting thresholds based on real-time network observations, dynamic thresholding enhances the resilience and effectiveness of VANET security measures against evolving threats. In contrast, static thresholds lack the flexibility to account for dynamic network conditions, potentially leading to decreased detection accuracy and responsiveness in the face of changing attack patterns. Ansari et al. proposed in [39] a cross-layer approach that combines signal properties from the MAC layer and routing information through the MAC/Network interface to deal with DDoS flooding attacks from different layers. It maintains minimal detection overhead due to its non distributed, node-centric detection approach. However, this scheme fails to maintain detection accuracy when the signal-to-noise ratio (SNR) and node density are low. Another drawback of this scheme is that the attacker can deliberately blacklist a legitimate node by changing its entry in the routing table.

4.4 Summary and Comparison

In this section, we summarize and qualitatively compare misbehaviour detection approaches classified by the targeted layer as shown in Figure 2. This evaluation categorizes the effectiveness of these approaches based on target

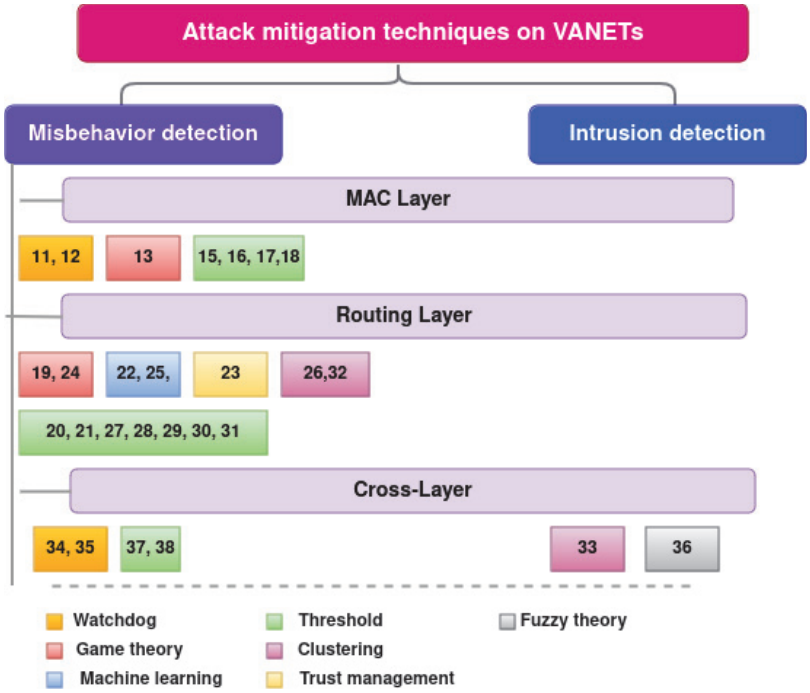


Figure 2 Attack mitigation techniques in VANETs.

layers, offering insights into their strengths and limitations and shedding light on their applicability in real-world scenarios.

This study offers a comprehensive review of attacks on decentralized communications in VANETs and the detection mechanisms proposed in the literature. Tables 2, 3 and 4 summarize the proposed detection solutions, most of which are distribution-based and independent of a dedicated infrastructure. Like other ad hoc networks, VANETs face threats from malicious vehicles, which can disrupt communications and network performance. To guarantee robust network performance, it is imperative to use secure protocols. Our review focuses primarily on MAC and routing layer detection solutions, followed by solutions based on cross-layer detection. Many proposed solutions are based on detecting deviations from normal behaviour, assuming that the presence of an honest majority in the environment defines "normal" behaviour.

In general, solutions for detecting attacks can be reviewed as follows. Greedy behaviour attacks are countered using watchdog mechanisms or

game theory, with the latter gaining traction due to its ability to achieve distributed game equilibrium among network vehicles. Jamming attacks are detected using statically or dynamically determined thresholds. To overcome the complexity and time constraints of traditional algorithms, researchers have integrated intelligent algorithms to enhance decision-making. such as RL which is particularly suited for decentralised wireless networks. PDR monitoring with thresholds is employed for detecting DoS attacks in the MAC layer, while watchdog and trust computations are used to detect black hole and grey hole attacks, relying on assumptions about an honest majority. Trust plays a vital role in vehicle networks, aiding in predicting future behaviour based on reputation acquired from past interactions. Similarly, wormhole attack detection solutions utilise various techniques to estimate the minimum number of hops needed to locate tunnel attacks. IDS are utilised for DoS attack detection in the routing layer and for black hole attack detection in cross-layer solutions, although such cross-layer solutions are still relatively sparse in the literature, particularly in the context of VANETs. Despite considerable research into V2V communication, its security remains challenging, with common defence strategies involving traffic behaviour analysis and anomaly reporting, they typically involve passive measures like triggering alarms or active ones such as isolating malicious nodes.

5 Discussion and Open Research Issues

In this section, we outline the findings from our review of the current state of V2V communication security in VANETs and highlight key challenges. We also identify potential future directions to address these issues and enhance the communication security within VANETs.

5.1 Outcomes

The lessons learned from our in-depth survey can be summarised as follows:

- MAC layer security is vital for decentralised communication in VANETs. While many solutions concentrate on securing the 802.11p protocol, TDMA-based MAC protocols, known for their efficiency over contention-based ones, lack coverage regarding security solutions in the literature.
- Many attacks target the routing layer, which was initially designed without security considerations. However, routing protocols designed with security in mind often entail high overhead and do not meet

real-time operation demands. Therefore, developing a security-aware routing protocol capable of expediting the detection process remains an unresolved issue warranting further investigation.

- Cross-layer solutions enhance network performance by integrating MAC and routing protocols, considering node characteristics and routing paths. However, only a limited number of such solutions are documented in the literature.
- Recent studies on attack detection have been valuable for both scientific and industrial applications. However, proposed solutions often prioritise detecting attacks over preventing misbehaviour. Existing prevention mechanisms may still be vulnerable to unknown attacks and cannot always safeguard the network against internal attackers with authorised access.

5.2 Open Research Issues

Here, we provide an accurate roadmap that can be used for future research on V2V communications:

- The proposed solutions deal with different types of attacks and they employ various methods to detect a specific attack. For future work, there may be a need to investigate attacks that are more protocol or application-oriented.
- Another security challenge relates to scalability: the lack of a clear line of defence for real-time operations is a challenge. Increasing the scale of the network increases the computational and communication load on the security algorithm, which increases both response latency and detection error rate.
- The following challenge is linked to cooperation: many VANET algorithms and protocols assume that data will be broadcast by the communicating vehicles. This feature makes vehicular networks vulnerable to attacks. Furthermore, many security mechanisms rely on the cooperation of vehicles, as local data may not be sufficient to prevent and detect attacks.
- The lack of research papers addressing simultaneous and diverse attack detection in VANETs is a notable gap in the literature. While efforts have been made to develop mechanisms for individual attack types, limited research exists on detecting and mitigating multiple concurrent attacks. Future research should concentrate on multi-level and hybrid approaches integrating ML, reputation systems, and detection algorithms to address

this challenge. Moreover, real-world experiments are essential to validate these approaches across various scenarios and network conditions. Bridging this gap is vital for advancing and adopting VANETs in applications like ITS and smart cities.

6 Conclusion

As VANETs become increasingly open, technologically intricate, and characterized by a diverse range of protocols, novel security threats inevitably emerge. Safeguarding against these threats necessitates innovative approaches that can adapt to the evolving landscape of attacks and vulnerabilities. In this paper, we have placed a paramount focus on decentralized architectures due to their cost-effectiveness compared with centralized counterparts, as well as their adaptability across various environmental scenarios. Furthermore, our attention is steadfastly fixed on V2V communications, specifically adopting a node-centric perspective. We firmly assert that this node-centric approach serves as the foremost line of defence in constructing robust security solutions. Our investigation has delved deeply into potential attacks that could affect MAC, routing, and cross-layer protocols. We have meticulously explored a range of defence mechanisms and presented an exhaustive comparative study of existing solutions. Additionally, our work encompasses the categorization of security mitigation strategies, as portrayed in Tables 2, 3 and 4. This categorization seeks to underscore the imperative of prioritizing preventative measures to facilitate the realization of practical VANET applications. Importantly, we have also delineated unresolved challenges and forthcoming obstacles that warrant concerted attention. However, it is important to recognise certain limitations inherent in our study. Although we have thoroughly explored and qualitatively evaluated a range of defence mechanisms, the rapidly evolving landscape of vehicle technology and safety requires constant vigilance and adaptation. Furthermore, the effectiveness of the proposed solutions may depend on real-world implementation challenges and contextual complexities that have not been fully addressed within the scope of this paper. In summary, the detection of attacks within VANETs remains a complex and challenging subject. As we contemplate the road ahead, the potential of cross-layer protocols, coupled with adaptive detection techniques and cryptographic measures, appears to be a promising avenue for future research efforts aimed at strengthening VANET security.

References

[1] Van der Heijden R. W. et al. "Survey on misbehavior detection in cooperative intelligent transportation systems." IEEE Communications Surveys & Tutorials 21, 779–811, 2018.

[2] Sharma, Sparsh, and Ajay Kaul. "A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud." Vehicular communications 12, 138–164, 2018.

[3] Lu, Zhaojun, Gang Qu, and Zhenglin Liu. "A survey on recent advances in vehicular network security, trust, and privacy." IEEE Trans. on Intelligent Transportation Systems 20, 760–776, 2018.

[4] Tong W., et al. "Artificial intelligence for vehicle-to-everything: A survey." IEEE Access, 10823–10843, 2019.

[5] Kelarestaghi K. B., et al. "Survey on vehicular ad hoc networks and its access technologies security vulnerabilities and countermeasures" arXiv preprint, 2019.

[6] Hussain R., Jooyoung L., Sherali Z. "Trust in VANET: A survey of current solutions and future research opportunities." IEEE Trans. on Intelligent Transportation Systems, 2020.

[7] Lamssaggad A., Nabil B., Abdelhakim H., Mounira M. "A survey on the current security landscape of intelligent transportation systems." IEEE Access, 2021.

[8] Karabulut M. A., Shah AFM S., Haci I., Al-Sakib K. P., Atiquzzaman M. "Inspecting VANET with Various Critical Aspects–A Systematic Review." Ad Hoc Networks, 2023.

[9] Li Z., Weidong F., Chunsheng Z., Zhiwei G., Wuxiong Z. "AI-enabled Trust in Distributed Networks." IEEE Access, 2023.

[10] Sangwan A., Anju S., Rishi P. S. "A classification of misbehavior detection schemes for VANETs: a survey." Wireless Personal Comm. 129, 285–322, 2023.

[11] Ismail, Tayssir, Haifa Touati, Nasreddine Hajlaoui, Mohamed Hadded, Paul Muhlethaler, Samia Bouzefrane, and Leila Azouz Saidane. "Impact analysis of greedy behavior attacks in vehicular ad hoc networks." In 2021 10th IFIP International Conference on Performance Evaluation and Modeling in Wireless and Wired Networks (PEMWN), pp. 1–6. IEEE, 2021.

[12] Mejri, M. N., Ben-Othman, J. "Detecting greedy behavior by linear regression and watchdog in vehicular ad hoc networks.", IEEE Global Comm. Conf., 2014.

[13] Mejri, M. N., Ben-Othman, J. "GDVAN: a new greedy behavior attack detection algorithm for VANETs.", IEEE Trans. on Mobile Computing, 759–771, 2016.
[14] Al-Terri D. et al. "Cooperative based tit-for-tat strategies to retaliate against greedy behavior in VANETs." Computer Communications 104, 108–118, 2017.
[15] Abuzainab N., Erpek T., Davaslioglu K., Sagduyu Y.E., Shi Y., Mackey S.J., Yener A. QoS and jamming-aware wireless networking using deep reinforcement learning. IEEE Military Communications Conf. (MILCOM), 610–615, 2019.
[16] Almomani I., Mohanned A., Dimitrios K., Aala A., Leandros M. "An Efficient Localization and Avoidance Method of Jammers in Vehicular Ad Hoc Networks." IEEE Access, 2022.
[17] Guleria C., Harsh K. V. "Improved Detection and Mitigation of DDoS Attack in Vehicular ad hoc Network." 4th Int. Conf. on Computing Communication and Automation (ICCCA), 2018.
[18] Valentini E. P., Rodolfo I. M., Adil A. "An attacks detection mechanism for intelligent transport system." IEEE Int. Conf. on Big Data, 2453–2461, 2020.
[19] Valentini E. P., Geraldo P. R. F., Robson E. D. G., Caetano M. R., Lourenço A. P., Rodolfo I. M. "A Novel Mechanism for Misbehaviour Detection in Vehicular Networks." IEEE Access, 2023.
[20] Mostefa F. Z., Zoulikha M. M., Claude D. "Secure Communications by Tit-for-Tat Strategy in Vehicular Networks." Int. J. Networked Distributed Comput. 8, 214–221, 2020.
[21] Malik A., Muhammad Z. K., Mohammad F., Faheem K., Jung-Taek S. "An efficient dynamic solution for the detection and prevention of black hole attack in vanets." Sensors, 2022.
[22] Lakshmi S., Anita E.M., Jenefa J. A hybrid approach against black hole attackers using dynamic threshold value and node credibility. IEEE Access, 2023.
[23] Sarker O., Hong S., Babar M.A. Reinforcement Learning Based Neighbour Selection for VANET with Adaptive Trust Management. arXiv preprint, 2023.
[24] Baccari S., Hadded M., Touati H., Muhlethaler P. A secure trust-aware cross-layer routing protocol for Vehicular Ad hoc Networks. Jour. of Cyber Sec. and Mobility, 2020.
[25] Quevedo A.M.B.C, Carlos H.O.O.Q., Gomes R. L. , Camara S. F., Celestino J. "A Reputation and Security Mechanism for Heterogeneous

Vehicular Networks." IEEE Symp. on Computers and Comm. (ISCC), 1–6, 2022.

[26] Mianji, E. M., Gabriel-Miro M., Irina T. "Trustworthy Routing in VANET: A Q-learning Approach to Protect Against Black Hole and Gray Hole Attacks." 97th IEEE Vehicular Technology Conf. (VTC), 1–6, 2023.

[27] Kaur G., Meenu K., Amandeep K. "VANET Cluster Based Gray Hole Attack Detection and Prevention." SN Computer Science 5, 1, 2024.

[28] Albouq S. S., Erik M. F. "Detection and avoidance of wormhole attacks in connected vehicles." 6th ACM Symp. on Development and Analysis of Intelligent Vehicular Networks and Applications, 107–116, 2017.

[29] Kanumalli S.S., Anuradha C., Murty P.S.R.C. "Isolation of wormhole attackers in IOV using WPWP packet" Revue d'Intelligence Artificielle, 9–13, 2019.

[30] Ali S., Parma N., Shailesh T. "Impact of wormhole attack on AODV routing protocol in vehicular ad-hoc network over real map with detection and prevention approach" Int. Jour. of Vehicle Inf. and Comm. Sys. 5, 354–373,2020.

[31] Fotohi R., Yaser E., Mohammad S. G. "A new approach for improvement security against DoS attacks in vehicular ad-hoc network." arXiv preprint, 2020.

[32] Tosunoglu B. A., Cemal K. "FA-AODV: flooding attacks detection based ad hoc on-demand distance vector routing protocol for VANET." Sakarya University Jour. of Computer and Inf. Sciences 5, 304–314, 2022.

[33] Keshari N., Dinesh S., Ashish K.M. "DoSRT: A Denial-of-Service Resistant Trust Model for VANET" Cybernetics and Inf. Technologies, 165–180, 2023.

[34] Subba B., Santosh B., Sushanta K."A game theory based multi layered intrusion detection framework for VANET" Future Gen. Comp. Sys. 12–28, 2018.

[35] Baiad, R., Otrok, H., Muhaidat, S., & Bentahar, J. Cooperative cross layer detection for blackhole attack in VANET-OLSR. In Int. Wireless Communications and Mobile Computing Conf. (IWCMC), 863–868, 2014.

[36] Baiad R. et al. "Novel cross layer detection schemes to detect blackhole attack against QoS-OLSR protocol in VANET" Vehicular Communications 9–17, 2016.

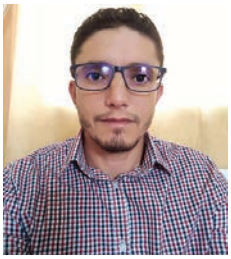
[37] Shurman M. M., et al. “An Enhanced Cross-Layer Approach Based on Fuzzy-Logic for Securing Wireless Ad-Hoc Networks from Black Hole Attacks.”, 2017.
[38] Rabiaa N., Ali C. M., Boukli H. S. “A Cross-layer Method for Identifying and Isolating the Blackhole Nodes in Vehicular Ad-hoc Networks.” Info. Sec. Jour.: A Global Perspective 32, 212–226, 2023.
[39] Ansari A., Mohammed W. “Flooding attack detection and prevention in MANET based on cross layer link quality assessment.” Int. Conf. on Intelligent Computing and Control Systems (ICICCS), 612–617, 2017.

Biographies

Tayssir Ismail received a Master degree from the Faculty of science of Gabes (F.S.G), Tunisia, in 2019. She is currently pursuing the Ph.D. degree at Conservatoire national des arts et métiers (Cnam), Paris, and the National School of Computer Science (ENSI), Tunis. Alongside her Ph.D. studies, she worked as a teaching and research assistant (ATER) at CNAM, Paris, this year. Her research interests cover vehicular networks, security and machine learning.

Haifa Touati received her Ph.D. in Computer Science from the National School of Computer Science (ENSI-Tunisia) in 2011, and her HDR in 2021.

She obtained her engineering and master's degrees in networking from the same institution. She is currently an Associate Professor of Computer Science at the Faculty of Sciences of Gabes (FSG-Tunisia), where she was the supervisor of the Master's degree program in Computer Science and Networking. Additionally, she serves as the Director of the IReSCoMath research laboratory. Her research interests include named data networking, vehicular communications, security, Machine Learning and blockchain technology.



Nasreddine Hajlaoui received his engineer degree in Networks and Communications from the National School of Engineers of Gabes (Tunisia), in 2007 and research M.S. degree in telecommunications from Higher School of Communications of Tunis (Sup'Com) in 2009. He received his Ph.D. degree in Engineering Computer Systems from the University of Sfax, Tunisia, in 2016. He is currently working as assistant professor at Qassim University (KSA) and a member of Hatem Bettaher IResCoMath Lab. His research areas include wireless networking, cloud computing, security and analytical modeling.

Mohamed Hadded joins Abu Dhabi University as an assistant professor of cybersecurity engineering, in the College Engineering/CSIT Department. In 2016, he completed his Ph.D. in computer science Engineering at Telecom

SudParis college in co-accreditation with Sorbonne University (Pierre and Marie Curie Campus). Prior to joining ADU, Dr. Hadded worked as a senior cybersecurity researcher for intelligent transportation systems at IRT SystemX Paris, France from 2021 to 2022. From 2018 to 2022, he also served as an adjunct assistant professor in the Department of Networks and Cybersecurity at Gustave Eiffel University (France). From 2018 to 2021, he worked as a cybersecurity research engineer at VEDECOM institute (Versailles, France). Before that, he worked as a postdoctoral research fellow at the national institute for research in digital science and technology (INRIA, France) from 2017 to 2018. From 2015 to 2017, he worked as a teaching and research assistant (ATER) at Paris 5 and Franche-Comté (UFC) universities. Since 2021, he serves as a Guest Editor on Wireless Communication Technologies in Intelligent Transport Systems at Electronics Journal and a TPC member at several international conferences and workshops on wireless and mobile networking, Telecommunication, and security.

Paul Muhlethaler started at Inria (French National Research Institute in Computer Science) in 1988 where he is now a research director. His research topics focus on protocols for networks, with a speciality in wireless networks. He has worked extensively at ETSI and IETF for the HiPERLAN and OLSR standards. He was one of the authors of the first draft of the OLSR protocol in 1997 and co-author of OLSR v1 standard. He was the first researcher to carry out optimizations of CSMA protocols in Multihop Ad Hoc Networks, thereby highlighting the importance of such optimizations. With F. Baccelli and B. Blaszczyszyn, he designed a complete model of an Aloha multihop ad hoc network which led to the design of one of the first multihop ad hoc network offering a throughput scaling according the Gupta and Kumar's famous law. In 2004, he received the prestigious "Science and Defense" award for his work on Mobile Ad Hoc Networks. His current activity concerns models

and performance evaluations especially in wireless and vehicular ad hoc networks. He has also started to study the use of Machine Learning in wireless networks.

Samia Bouzefrane received the Ph.D. degree in computer science from the University of Poitiers, France, in 1998. After four years at the University of Le Havre, France, she joined the CEDRIC Lab of Conservatoire National des Arts et Métiers (Cnam), Paris, in 2002. She is currently Professor in Cnam. She is the coauthor of many books (Operating Systems, Smart Cards, and Identity Management Systems). She has coauthored more than 120 technical articles. Her current research interests include the Internet of Things, vehicular networks, and security using AI techniques. Since 2019, she has been partly delegated to the French Ministry of Higher Education and Research.

Leila Azouz Saidane is Professor at the National School of Computer Science (ENSI) and the director of CRISTAL research laboratory (Center of Research in Network and System Architecture, Multimedia and Image Processing), at the University of Manouba, in Tunisia. She is the vice-president of TRINET association. She is engineer and has obtained her PhD and her

"doctorat d'état" at the faculty of science of Tunis within the cooperation between this institution, ENSI and INRIA (Institut National de Recherche en Informatique et en Automatisme) in France. She was the Director of ENSI, the Chairperson of the PhD and Habilitation Commission and the supervisor of the Master's Degree program in Networks and Multimedia Systems at ENSI. She was director of department at ENSI and a member of the university council of Manouba. She collaborated on several international projects and supervised several PhDs and masters. She is author and co-author of several papers in refereed journals and international conferences. Research areas: Analytical study of network performance, Probabilistic quality of service in networks, Wireless sensor networks: access methods, routing, energy saving, preventive maintenance, redeployment, scaling up, real-time application, Content-oriented networks, Vehicular networks, WBAN , Smart homes, IoT, Cloud computing.