IoT-Driven solutions for VANET trustworthiness: Examining misconduct and position security challenges

Meenu Shukla| Vaibhav Srivastava| Mayank Deep Khare| N. Vishnu Venkatesh

Abstract Vehicular ad hoc networks (VANETs) improve the traffic management and road safety by exchanging real-time data between automobiles and roadside infrastructure. Reliable Intelligent Transport Systems (ITS) solutions tend to boost VANET data security, integrity and dependability. These systems communicate VANET data between infrastructure and automobiles using sensors, Internet of Things (IoT) devices and communication technologies. IoT-driven solutions improve VANET route design. Traffic management and safety improve with ITS-connected cars and infrastructure. Remote communication technologies enhance traffic management and decision-making by sending real-time data between cars and infrastructure. Smart parking systems use real-time parking availability data from IoT sensors and devices to maximize space use and reduce congestion. Security and misbehavior are dependable problems in 40 IoT-driven VANET studies. Miscommunication and unstandardized are the main security issues which pose hazards. This review shows VANETs that require authentication, encryption and anomaly detection to prevent attacks and IoT for transportation sector. This extensive review covers VANET reliability and IoT-driven real-time traffic monitoring, ITS, remote communication and intelligent parking systems. This review analyzes the metrics to assess the many detection techniques which includes, misconduct-Aware On-Demand Collaborative Intrusion Detection System (MACIDS) and Collision-Induced Dissociation Spectroscopy (CIDS). (i) Accuracy (ii) False Positive Rate, (iii) precision, (iv) recall (v) False Negative Rate and (vi) F1-Score in VANET security in Attack Detection Rates (ADR), misbehavior detection, evaluation metrics and detection algorithms were studied using CIC-IDS data. Due to misconduct and security issues, a strong IoT-driven solutions are required to improve VANET trustworthiness and offers a secure and reliable vehicular communication networks for safer and more efficient transportation systems.

Keywords: traffic observation, intelligent transport system (ITS), remote communications, wireless connectivity, attack detection rates, radio transmissions

1. Introduction

VANETs are one area that has benefited from the quick expansion of the IoT in recent years. VANETs are essential in advance to road safety and traffic management, as well as real-time communication and the exchange of information between vehicles and infrastructure (Quyoom et al 2020). However, the emergence of complex IoT-driven solutions has given birth to some key concerns of VANET reliability, potential misconduct and essential security challenges linked to location accuracy. Issues over the security of data transmitted across VANETs are growing. Significant threats to network security, such as malicious assaults, data falsification and unauthorized access arise from the proliferation of networked IoT devices (Hussein et al 2022). Therefore, maintaining a high level of trustworthiness while lowering misconduct risks is a significant aim of developing and implementing IoT-driven solutions for VANETs. To coordinate traffic flow, accident prevention and location-based services, automobiles must be placed in the network (Śtepiń and Poniszewska-Marańska 2021). Protecting sensitive location data is problematic since VANETs are vulnerable to spoofing, jamming and eavesdropping, which might damage the network. These security challenges and VANET location accuracy must be addressed to maintain vehicle communication network dependability and efficacy (Ahmed et al 2022). Untruthfulness and insecurity of employment are two major problems that might derail VANET deployment and operation. Illegal activity such as unauthorized access, tampering with data and dos attacks can compromise the reliability and safety of the whole network. Since it’s the backbone of many life-saving applications, including accident
avoidance and traffic management, keeping track of locations is very important. This review examines the challenges of position
security as well as misconduct and analyzes IoT-driven solutions for VANET trustworthiness.

2. Trustworthiness in VANET

If vehicles in VANET can safely and correctly exchange information with one another and with fixed infrastructure, the
VANET can be considered trustworthy. It includes the ability to identify and prevent harmful behavior or unauthorized access,
the security of sensitive data, the validity of vehicle identifiers and the integrity of networks. Safer roads and more efficient
public transportation are the results of a dependable VANET that can send and receive data between vehicles and stationary
infrastructure without fear of interference in Figure 1.

Figure 1 VANET Trustworthiness with IoT.

VANET’s characteristics: VANET scan assess user’s trustworthiness using various trust management techniques and some VANET features need more practical,
reliable and scalable trust management systems (Sharma et al 2021). Automatic connection to other vehicle nodes: VANETs are unique amongst networks
because of this trait. Unlike regular grids, where users must sign up to become members, VANETs are formed automatically according to the distance each
ehicle can communicate (Katiyar et al 2020). As a result, unlike in other networks, the nodes in a VANET have no incentive to establish mutual trust with one
another. Availability resources: Every vehicle has computer resources, including memory and processor speed (Salem et al 2022). Speed: In a VANET, unlike
most other networks, the nodes move at different rates. As a result, the topology is changing and no two neighbors are ever the same (Srivastava et al 2020).
Thus, reputation values are computed at first acquaintance rather than kept current. This highlights the need for trust bootstrapping in a VANET environment.
Vehicle network intermittent on VANET: New communication networks are established by vehicles regularly. VANETs are unchanging, but the cars that
comprise them are constantly changing. VANETs are categorized as transitory since they appear and disappear. Traditional trust methods, initially designed
for massive ad-hoc networks, are challenging to implement in VANETs because of their opportunistic nature, whereby vehicle nodes meet one another without
previous preparation (Sharma et al 2021). These VANET characteristics increase the probability of node-to-node contacts, giving cars a solid incentive to
cooperate and to be reliable. Possibilities: A VANET is a network where motor vehicles can talk to one another and the infrastructure that lines the roads (Kazi
et al 2022). Guided: Road topology restricts the vehicle mobility since vehicles must obey traffic restrictions.

3. IoT-Driven Solutions for VANET

IoT-driven in VANET systems improves the connection, efficiency and safety. IoT devices, sensors and communication
technologies enable real-time data collection, analysis and dissemination in these systems. This allows automobiles,
infrastructure and other linked entities to communicate effortlessly. VANETs can help create more innovative, safer and more
efficient transportation networks by integrating IoT-driven solutions to control traffic flow, enhance road safety via accident
prevention systems and deliver practical location-based services in Figure 2 (Saad et al 2023).

3.1. Real-Time traffic observation in IoT-Driven Solutions

Building smart cities is dependent on tools that can track traffic in real-time. There is a plethora of resources available
to learn more about intelligent traffic management systems that utilize the IoT network. Autonomous traffic sensing is the
backbone of smart city infrastructures and it relies on the use of intelligent wireless sensors to analyze traffic patterns, predict
congestion and regulate traffic routes dynamically. When done appropriately, it generates awareness that leads to more
effective resource and infrastructure management (Syed et al 2021). The first stage in traffic management is to locate and
quantify congestion points. Images or videos collected by vision systems are the starting point for calculating traffic congestion
metrics, including flow, occupancy and density. Based on these measurements, the traffic warning messages are broadcasted
by cell phones, radios, TVs, light signals, dynamic, changeable message signs, or display devices. Web apps accessible from a mobile device are a hot topic in the academic community. Congestion estimations are used by the majority of modern live traffic information upgrades to modify signal timing. An IoT-based technology can adapt traffic signals to changing foot and vehicle volumes (Johari and Krishna 2021). Ultrasonic sensors scan highways for autos and provide data to a Loop Detector Camera (LCD) screen and server. It shows warning lights when a motorist runs a red light and sounds an alarm if it senses a suspicious conduct (Fahim et al 2021). The data layer includes sensors, cameras and Radio Frequency Identification (RFIDs). The application layer manages the traffic light based on volume and provides a daily online report. Traffic density is calculated and traffic signals are adjusted instantly using video surveillance and sensors. Internet-linked cars can collect real-time traffic statistics. Linked automobiles provide individual vehicle monitoring, improving emergency vehicle management. Connecting roadside equipment like traffic lights to the car network improves traffic event dependability (Channi and Kumar 2021). Emergency vehicles must be handled carefully due to their time-sensitive services. By controlling traffic signals, emergency vehicle scheduling can be automated, lowering response times. These facilities are designed for roads. This research examines roadside messaging unit traffic information efficacy, as drivers in this study do not have cell phones. A patented roadside traffic indicator is supposed to be installed (Humayun et al 2022). The graphical messaging device displays signs, colors and messages about future traffic conditions. Research indicates that drivers react to dynamic roadside messaging signs. Roadside message devices on bridges, toll plazas, tunnels, etc., can give portable or permanent emotional message signs. Mobile gadgets warn of unusual traffic data (Xu et al 2020). Roadside gadgets display overflowing highways, upcoming events, environmental news, traffic patterns and more. Senior drivers stand to gain the most from these communication devices, according to the data. Public message devices worked in Beijing Olympics transportation. The effort monitored and distributed traffic information via message boards, radios, TVs, the internet and car displays. High development costs were incurred by the system due to complex hardware and software. Since then, other studies have been conducted to provide traffic updates. Electronic displays at crossroads will display traffic congestion with three colors (Sun et al 2021). This approach calculates real-time traffic density from vehicle-detecting devices of average speed. The scientists evaluate real-time traffic videos using image processing and optical flow to predict road congestion. Traffic lights and smartphone applications allow real-time highway modifications to evaluate the above studies (Rodríguez-Rangel et al 2020). On smart campuses, digital display boards can convey the rush-hour traffic information of misconduct. In future study, we'll cover the wireless sensors that detect, categorize and estimate vehicle speed.

![IoT Driven Solutions for VANET](https://www.malque.pub/ojs/index.php/mr)

**Figure 2** IoT Driven Solutions in VANET.

### 3.2. **Intelligent Transport System (ITS) in IoT-Driven Solutions**

The proliferation of cars has presented the transportation management system with new obstacles. It has prompted a change away from traditional approaches to transportation management in favor of more creative, out-of-the-box ideas that can solve issues in the present and in the future. The IoT is a system of interconnected electronic devices, appliances and other items that could collect, exchange data and perform many additional functions, that can be linked to one another and the internet for data gathering, processing and sharing (Guevara et al 2020). This paves the way for merging the physical and digital
Shukla et al. (2023)

worlds, making the latter more self-sufficient. ITS employs cutting-edge technology and techniques, which might be a handle tool for dealing with this intricate problem. The ultimate purpose of ITS is to provide advanced and simplified travel alternatives for the passengers; therefore, one way of looking at it is as a comprehensive transportation management and service system. IoT sensor networks are used to make these novel approaches transportation management possible (Sharma et al 2022). These sensors contribute to real-time data collection and serve as input to many data pipelines and processing nodes that are linked together. Travelers can rely on ITS to collect data, analyze it and communicate the results to address concerns about road safety, congestion management, traffic law enforcement and accommodating passengers’ ever-evolving requirements. It is necessary to optimize energy use across the system while running on a low-power source like batteries. ITS is made up of a number of subsystems, each having its own energy requirements and modes of operation. Optimizing energy usage is a primary goal in the design, development and implementation of an intelligent transportation system. Energy consumption might be minimized during sensor data processing via multi-sourcing or storage partitioning. ITS infrastructures can be made more energy efficient by the coordination of energy management at specific segments and the potential of collecting power at the system level (Xu et al 2020). ITS must overcome the same operational hurdles as conventional systems to enhance production and efficiency. Optimal duty cycle and latency determining routing algorithms, time-based resource scheduling and asynchronous intelligent learning-based resource management can help to solve communication issues like congestion, conflicts and resource allocation (Rathore et al 2021). ITS allows for comprehensive, high-quality transportation management and service systems because of its efficacy and efficiency.

3.3. Remote Communication Technologies in IoT-Driven Solutions

The use of remote communication systems between vehicles and other objects is explored. Components both inside and outside of the car could share data using this system. Vulnerabilities in remote communication technologies might be targeted by attackers who want to harm a moving car or bus from a distance. This implies that hackers might steal blueprints for automobile communication systems even if they don’t have a direct physical access to the ports. If user defenses are vulnerable on distant communication, user should reconsider (El-Rewini et al 2020). Figure 3 classifies several forms of communication technology, including Zigbee, RFID, WiMAX and WiFi; wireless access in-vehicle systems and remote keyless entry systems.

![Figure 3 Wireless connectivity in the vehicle's system.](image)

3.3.1. Wireless connectivity in the vehicle’s system

Dedicated Short Range Communications (DSC) is a subset of wireless communication technology known for its short range. This system relies on the 802.11p protocol. This connection offers high-speed, direct communication between vehicles and the surrounding infrastructure, as well as rigorous security. The cellular network is unnecessary for this setup. Simplified schematic of how DSRC can be implemented in vehicle-to-vehicle connections (Oladimeji et al 2023). Roadside Unit (RSU) signifies the roadside vehicle to infrastructure and V2I refers to the corresponding communication system.
Another name for a keyless entry system is a remote central locking system. This technique represents to the use of a remote-controlled electronic lock. If unlock this door manually, or it can sense your presence when user get close (Abu et al. 2022). A keypad activates the lock. The keypad can be found near the car driver’s entry. Lincoln and Ford automobiles use this design.

3.3.2. WiMAX and WiFi

WiMAX is supposed to provide wireless fidelity. One possible means of communication between infrastructure and automobiles is WiFi. WiMAX is faster than WiFi. WiMAX stands for Worldwide Interoperability for Microwave Access. The abbreviation for IEEE 802.16 is WiMAX. WiMAX has several advantages, including high security, low latency, Quality of Service (quality of service) and interoperability with all-IP core networks. For voice, video and V2V communication, OFDMA, called OFDM, enables WiFi and WiMAX systems to operate at incredible speeds on a single platform. The advantage of OFDM is that it helps WiMAX overcome the effects of multipath fading while maintaining a high data rate. WiFi and WiMAX can use the MIMO system’s channel to improve wireless performance and double capacity without using more bandwidth or power from the transmitting antenna (Kumar et al. 2021). As a result, spectral efficiency can be improved exponentially. Vehicle communication might be impacted by MIMO systems as well. Massive MIMO is a crucial technology for 5G communication.

3.3.3. Zigbee

Zigbee uses wireless protocols for WSN applications to meet low-cost, long-battery demands. IEEE 802.15.4 powers Zigbee. This unit supports frequencies of 2.4 GHz, 868 milliseconds and 900 MHz. Zigbee provides engage networking. Routers and receivers use ZigBee in numerous applications with wireless mesh networking. Zigbee uses a spread spectrum technique called direct sequencing. Offset-QPSK modulates Zigbee. Channel measurement and spacing are 5 and 2MHz. The forward collision warning system utilizes Zigbee. FCWS scans the road ahead using lasers, sensors and cameras to inform drivers (Bharati et al. 2020). A wireless, Zigbee-based driving aids system. A roadside gadget and a mobile Zigbee unit make up this system. Mobile unit alerts driver with audio. To decrease accidents, a drink-and-drive prevention system monitors the alcohol levels of driver.

3.3.4. RFID

RFID identifies an item by use of radio transmissions. An RFID reader in a system can read or recognize tags affixed to things. Toll collection, vehicle performance tracking and traffic management are some of the uses for radio frequency identification technology, in addition to vehicle tracking.

3.4. Smart Parking Systems

The architecture of an intelligent parking system consists of embedded technologies and several application frameworks. Requests from the application layer, such as those for reserved parking places, are fulfilled by the network layer. The transaction layer communicates with users request for parking services at the network layer (Zulfiqar et al. 2020). In summary, the protocol for a consensus process at the payment layer and every park provider simultaneously update the shared database. Intelligent parking system design is built on four tiers: application, network, transaction and physical. Figure 4 depicts the layer of smart parking system.

3.4.1. Layer of Application

At the top of the architectural stack, the application layers allow users to interact with their system, a web application, or a mobile application. Customers can look for and reserve the parking spaces they like. Likewise, the supplier of parking services could send offers to the integrated systems and parking-related information, including available parking spaces, to the providers. The best possible service is provided to end users by the layer because of their direct interaction with the integrated system.

3.4.2. Layer of Network

The network layer ensures smooth communication between integrated systems, users and parking lots. There is a layer in the system that links information about users and parking garages. The layer consists of various communication technologies, such as Local Area Network (LAN) and Wide Area Network (WAN), which parking service providers, customers and internet-connected objects (Biyik et al. 2020). They could be equipped with Bluetooth, WI-FI and other wireless technologies. Together with the existing GSM technology, they come in 4G and 5G versions.

3.4.3. Layer of Transaction

https://www.malque.pub/ojs/index.php/mr
All communications in a network must take place at this level. Smart contracts and consensus mechanisms allow users and parking lots to exchange information in a trusted environment. The public ledger is managed by the parking garage at this level. The transaction layer uses immutable technologies like blockchain to ensure the integrity of the transactions and data transfers (Zaidi et al 2021).

3.4.4. Layer of Physical

The physical layers provide an in-depth look into the system’s inner workings and electrical structure (Englander et al 2020). The physical layer relies on the data gathered from physical sensors and how that data is processed and managed. In this layer, several types of sensors play a crucial role. Sensor use an IoT device that can be identified by its availability, as described in the physical layers.

Figure 4 layer of smart parking system.

4. Detection of security attacks in VANET

VANET security threats, challenges and objectives like Authenticity, Confidentiality and Availability. DoP, Jamming and GPS Spoofing Attacks can corrupt location data, causing navigation and traffic management errors. Malware, Broadcast Tampering, Black-hole and Gray-hole attacks can harm network data and communication (Salim et al 2020). Eavesdropping, Traffic Analysis and Tunneling Attacks could reveal sensitive data and communication secrecy. Sybil, greedy behavior, spamming and free-riding attacks can impair network resource authenticity and availability, hurting trust and VANET efficiency. Compelling VANET data and resource protection is required due to these security challenges in Table 1. The many forms of security breaches and their definitions are shown in Table 2. In the context of a research analysis utilizing the CIC-IDS data, Table 3 illustrates the performance evaluation of the IDS system in detecting various attack types, including Botnet, Brute Force, DoS and Port attacks, with the corresponding numbers of records and the achieved ADR in percentage for each category. Figure 5 represents the graphical representation of the number of security attack records of data. Figure 6 denotes the visual presentation or visualization of the number of attack records are identified or detected by the system in the CIC-IDS data. Finally, Figure 7 depicts the graphical representation or visualization of the Attack Detection Rates (ADR) achieved by the system in identifying the security attacks in the CIC-IDS data (Karthiga et al 2022).

Table 1 Types of security attacks in VANET.

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Confidentiality</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadcast tampering attacks</td>
<td>Traffic analysis attack</td>
<td>GPS spoofing attack</td>
</tr>
<tr>
<td>Denial-of-Position (DoP) Attack</td>
<td>Eavesdropping Attack</td>
<td>Free riding attack</td>
</tr>
<tr>
<td>Malware attack</td>
<td>Jamming attack</td>
<td>Tunneling attack</td>
</tr>
<tr>
<td>Greedy behavior attack</td>
<td>Spamming attack</td>
<td>Sybil attack</td>
</tr>
<tr>
<td>Black-hole and gray hole attack</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Figure 5 Number of security attack records using the CIC-IDS dataset. 
Source: https://www.hindawi.com/journals/wcmc/2022/5069104/

Figure 6 Correctly Detected Records in the CIC-IDS dataset 
Source: https://www.hindawi.com/journals/wcmc/2022/5069104/

Table 2 Types of Security Attacks and Definitions.

<table>
<thead>
<tr>
<th>Type of attacks</th>
<th>classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial-of-Position</td>
<td>A particular kind of assault that seeks to obstruct the precise determination</td>
</tr>
<tr>
<td>Attack (DoP)</td>
<td>of a vehicle's position inside the network, making location-based services</td>
</tr>
<tr>
<td></td>
<td>unavailable and even wreaking havoc on navigation and traffic control</td>
</tr>
<tr>
<td>Jamming Attack</td>
<td>Jamming involves deliberately tampering with wireless communication signals</td>
</tr>
<tr>
<td></td>
<td>to cause communication issues, service disruptions and interruptions in</td>
</tr>
<tr>
<td></td>
<td>transmitting critical data.</td>
</tr>
<tr>
<td>Malware Attack</td>
<td>Deploying malevolent software or code inside a network can jeopardize</td>
</tr>
<tr>
<td></td>
<td>communication security and integrity, resulting in data modification, illegal</td>
</tr>
<tr>
<td></td>
<td>access, or system failure.</td>
</tr>
<tr>
<td>Attack Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Broadcast Tampering Attacks</td>
<td>Include the unapproved alteration or manipulation of messages that are broadcast inside the VANET, which can result in the spread of misleading information and could confuse users or damage the network.</td>
</tr>
<tr>
<td>Blackhole and Grayhole Attack</td>
<td>A hostile node that launches a black-hole assault takes all traffic sent at it; But in a gray-hole attack, part of the packets that the rogue node gets are discarded. Attacks of both kinds impede communication and may result in data loss or network outages (Ahmed et al 2021).</td>
</tr>
<tr>
<td>Greedy Behavior Attack</td>
<td>The term describes the actions of a hateful or self-centered node that prioritizes its benefits over the network's security and performance, potentially causing resource depletion and compromising effective communication in the system.</td>
</tr>
<tr>
<td>Spamming Attack</td>
<td>Spamming involves the unauthorized and excessive transmission of irrelevant or malicious messages in the network, which can lead to the depletion of network resources, congestion, and potential disruptions in the communication flow.</td>
</tr>
<tr>
<td>Eavesdropping Attack</td>
<td>The illegal interception of communication in the network among legitimate organizations has resulted in the compromise of sensitive information, leading to privacy breaches and data leakage.</td>
</tr>
<tr>
<td>Traffic Analysis Attack</td>
<td>Examining network traffic and data flow aims to uncover sensitive information or identify vulnerabilities that could compromise the security of the transmitted data.</td>
</tr>
<tr>
<td>Sybil Attack</td>
<td>It involves an evil actor creating several false identities (Sybil nodes) to manipulate the perception of the network and, in turn, cause disruptions or the spread of misleading information.</td>
</tr>
<tr>
<td>Tunneling Attack</td>
<td>The process involves creating a novel communication pathway that bypasses existing channels, exposing vulnerabilities and compromising the security and integrity of the system (Hasan et al 2022).</td>
</tr>
<tr>
<td>GPS Spoofing Attack</td>
<td>GPS spoofing involves manipulating the GPS signals received by vehicles, providing them with false location data that could result in misleading directions and traffic congestion</td>
</tr>
<tr>
<td>Free Riding Attack</td>
<td>This term describes the unethical practice of using a network's resources without providing anything in return, which can lead to the exhaustion of those resources, network congestion, and threats to the network's integrity and safety (Hussein et al 2022).</td>
</tr>
</tbody>
</table>

![ADR in the CIC-IDS dataset](https://www.hindawi.com/journals/wcmc/2022/5069104/)

**Figure 7** ADR in the CIC-IDS dataset.
Table 3 ADR analysis using the CIC-IDS dataset in the IDS VANET system.

<table>
<thead>
<tr>
<th>Attack Types</th>
<th>Correctly Detected Records</th>
<th>Number of Records</th>
<th>ADR In %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Botnet Attack</td>
<td>74,192</td>
<td>75,000</td>
<td>98.9</td>
</tr>
<tr>
<td>Brute Force Attack</td>
<td>15,972</td>
<td>17,000</td>
<td>93.9</td>
</tr>
<tr>
<td>Dos Attack</td>
<td>14,789</td>
<td>15,000</td>
<td>98.5</td>
</tr>
<tr>
<td>Portscan Attack</td>
<td>88,762</td>
<td>89,000</td>
<td>99.7</td>
</tr>
</tbody>
</table>

Source: https://www.hindawi.com/journals/wcmc/2022/5069104/

4.1. Misconduct detection in VANETs

A wide variety of intrusion detection methods have been the subject of several research, all aimed to address the unique challenges and requirements of VANETs. Numerous innovative solutions have emerged from these studies, ranging from centralized systems backed by reputable organizations like the Department of Motor Vehicles (DMV) to decentralized frameworks that use the collaborative efforts of vehicles and authorized authorities (Sharma and Kaul 2021). Centralized intrusion detection systems employ large-scale data aggregation processes and XML dependency trees to identify and thwart Sybil attacks and the dissemination of false information. Plausibility checking and hashing pseudonym-based detection techniques highlights the ongoing efforts to fortify VANETs against evolving security threats, underscoring the importance of adaptable and dynamic security frameworks in modern vehicular communication systems (Zhang et al 2020). Strict security measures are necessary to protect data and communication in VANETs. Expert Intrusion Detection Systems (IDS) tailored to the fluid and distributed natures of VANETs have been the subject of the study. These strategies use multi-layered game theory principles and innovative cluster head deployments to protect networks against attacks, including selective forwarding, black holes, DoS, wormholes and Sybil attacks. Security protocols for VANETs are growing complex as lightweight neural network classifiers and context-aware data-centric misconduct detection models. These advancements have allowed the creation of public data like the Vehicular Reference Misconduct Dataset (VeReMi) to evaluate the efficacy of various detection methods. This proactive strategy to strengthening VANETs against new security threats will free up space for more robust and varied security architectures.

4.2. Evaluation metrics

Our comprehensive review findings reveal a detailed analysis and assessment of the data, showcasing significant insights into the number of security attack records, the corresponding detected records and the achieved ADR in the CIC-IDS data. This study examines the effects of misconduct in VANET systems and how they affect detection performance. The research focuses on terms such as (i) F1-Score, (ii) False Positive Rate, (iii) False Negative Rate and (iv) Accurateness to evaluations of Multiple Detection Techniques in Misbehavior-Aware On-Demand Collaborative IDS (MACIDS), shown in Figure 8 and Table 4 and CIDS shown in Figure 9 and Table 5 (Ghaleb et al 2020) help to clarify how the system functions under different misconduct scenarios.

![Figure 8 A comparisons of multiple detection methods in MACIDS. Source: Ghaleb et al 2020](https://www.malque.pub/ojs/index.php/mr)
Table 4 Evaluations of various detection methods in MACIDS.

<table>
<thead>
<tr>
<th>Performance</th>
<th>MACIDS (XBoost)</th>
<th>MACIDS (SVM)</th>
<th>MACIDS (RF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recall</td>
<td>0.95</td>
<td>0.9</td>
<td>0.98</td>
</tr>
<tr>
<td>Accuracy</td>
<td>0.96</td>
<td>0.94</td>
<td>0.97</td>
</tr>
<tr>
<td>FPR</td>
<td>0.04</td>
<td>0.11</td>
<td>0.04</td>
</tr>
<tr>
<td>F1-Score</td>
<td>0.95</td>
<td>0.95</td>
<td>0.97</td>
</tr>
<tr>
<td>FNR</td>
<td>0.05</td>
<td>0.0</td>
<td>0.02</td>
</tr>
<tr>
<td>Precision</td>
<td>0.96</td>
<td>0.92</td>
<td>0.97</td>
</tr>
</tbody>
</table>

Source: Ghaleb et al 2020

Figure 9 A comparison of multiple detection methods in CIDS.

Table 5 Evaluations of various detection methods in CIDS.

<table>
<thead>
<tr>
<th>Performance</th>
<th>CIDS (RF)</th>
<th>CIDS (XGBoost)</th>
<th>CIDS (SVM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy</td>
<td>0.92</td>
<td>0.93</td>
<td>0.86</td>
</tr>
<tr>
<td>Precision</td>
<td>0.91</td>
<td>0.93</td>
<td>0.8</td>
</tr>
<tr>
<td>Recall</td>
<td>0.95</td>
<td>0.93</td>
<td>0.99</td>
</tr>
<tr>
<td>F1-Score</td>
<td>0.93</td>
<td>0.93</td>
<td>0.89</td>
</tr>
<tr>
<td>FPR</td>
<td>0.11</td>
<td>0.08</td>
<td>0.29</td>
</tr>
<tr>
<td>FNR</td>
<td>0.05</td>
<td>0.07</td>
<td>0</td>
</tr>
</tbody>
</table>

Source: Ghaleb et al 2020

Flaws in the communication infrastructure and non-standard security processes create potential threats. The study emphasizes the need for robust security frameworks with anomaly detection, encryption and authentication to prevent assaults on VANETs and integrate IoT technologies for excellent dependability in the transportation sector. Many VANET-related topics are examined, including intelligent transportation systems (ITS), innovative parking systems, remote communication technologies and real-time traffic observation. Furthermore, the thorough examination sheds light on security threats to VANETs and highlights the significance of effective detection techniques and metrics in enhancing reliability. It concludes by emphasizing how critical it is to deploy potent IoT-driven solutions to enhance VANET credibility and guarantee the development of dependable and secure vehicular communication networks. This will contribute to the development of more secure and efficient transportation networks.

5. Final considerations

Rapid adoption of Internet of Things–driven solutions in VANETs has resulted in significant improvements in network coverage and operation efficacy. But as our lives become more reliant on Internet of Things devices, security and privacy
concerns have been raised concerning VANETs. In-depth examination of these issues highlights the need of enhancing VANET reliability via the implementation of secure and trustworthy IoT-driven solutions. To ensure the reliability of VANETs in the face of evolving threats and challenges, a comprehensive approach is required to include robust security mechanisms, effective misbehavior detection systems and rigorous position authentication procedures. By tackling these issues and tapping into the promise of IoT-driven solutions, VANETs can help to enable safer and more efficient transportation networks for the public benefit. Finally, it underlines the need of using powerful IoT-driven solutions to increase VANET credibility and ensure the growth of trustworthy and secure vehicular communication networks. The creation of safer and effective transportation networks will benefit from this.

Ethical Considerations
Not Applicable.

Conflict of Interest
The authors declare no conflict of interest.

Funding
The current review did not receive any financial support.

References
Hussein NH, Yaw CT, Koh SP, Tiong SK & Chong KH (2022) A comprehensive survey on vehicular networking: Communications, applications, challenges, and upcoming research directions. *IEEE Access*, 10, 86127-80. DOI:10.1109/ACCESS.2022.3198656
Kazi AK, Khan SM & Haider NG (2021) Reliable group of vehicles (RGoV) in VANET. *IEEE Access*, 9, 111407-16. DOI:10.1109/ACCESS.2021.3102216


Xu C, Wu Y, Rong J & Peng Z (2020) A driving simulation study to investigate the information threshold of graphical variable message signs based on visual perception characteristics of drivers. Transportation research part F: traffic psychology and behavior, 74, 198-211. DOI: 10.1016/j.trf.2020.08.023


