HP JSDR2025
Hummingbird Publications
Journal of Scientific Development Research
www.hummingbirdjournals.com
© August, 2025
Vol. 9 No. 9

A Review of Security Threats and Defence Mechanisms in Vanets

[1]Usman Ismail Abdulmalik; [2]Mustapha Kassim; & [2]Temitope Betty Williams

[1]Department of Computer Science, Federal Polytechnic, Kaura Namoda, Nigeria.
[2]Department of Computer Science, Federal Polytechnic, Mubi, Nigeria.
Corresponding Author: usmaniamailbox@yahoo.com
DOI: https://doi.org/10.70382/hujsdr.v9i9.007

Keywords: VANETs; Security threats; Defence mechanisms

Abstract

Vehicular Ad Hoc Networks (VANETs) have emerged as a critical component of intelligent transportation systems, enabling real-time communication among vehicles and infrastructure to enhance road safety, traffic management, and driving efficiency. However, due to their highly dynamic nature and reliance on open wireless communication channels, VANETs are vulnerable to various security attacks such as Denial of Service (DoS), Sybil attacks, message tampering, and eavesdropping. To mitigate these security threats, several defence strategies proposed by researchers have been examined. These strategies encompass the use of Multivariate Stream Analysis (MVSA) to identify DDoS attacks, privacy-preserving authentication methods to combat Sybil attacks, and enhanced intrusion detection systems to recognize grey hole attacks. In addition, techniques such as route tracing and node identification are recommended for addressing black hole attacks, while DoS attacks can be prevented through encryption methods and dynamic channel switching. The paper aims to highlight the strengths and limitations of current security solutions and suggests future research directions to develop more robust and adaptive security architectures for VANETs. By addressing these security concerns, the safe deployment and

operation of VANETs in real-world environments can be significantly improved.

Introduction

Vehicular Ad Hoc Networks (VANETs) have significantly advanced modern transportation by enabling seamless communication between vehicles and roadside infrastructure. These networks facilitate a wide range of applications, including cooperative collision prevention, efficient traffic control, and various infotainment services. By utilizing wireless communication protocols, VANETs are a driving force behind the evolution of Intelligent Transportation Systems (ITS), contributing to the development of automated vehicles. As a cutting-edge technology, VANET addresses critical issues related to road safety and service delivery, and ongoing research continues to explore its expanding potential (Shetty & Manjaiah, 2022).

Operating in a highly dynamic and fast-changing environment, VANETs consist of mobile vehicles and stationary infrastructure components. As a subset of Mobile Ad Hoc Networks (MANETs), each vehicle in VANET acts as an independent communication node, capable of initiating contact with other nodes without prior knowledge or centralized coordination. The network primarily comprises two components: the On-Board Unit (OBU) found in vehicles, which contributes to the network's mobility, and the Road Side Unit (RSU), which acts as a fixed communication hub, facilitating data exchange between vehicles (Abuarqoub et al., 2022).

VANETs blend vehicular mobility with road-based infrastructure to promote both safety and entertainment. Vehicles are outfitted with wireless sensors, GPS modules, and digital maps, enabling real-time communication between OBUs and RSUs. This short-range interaction supports the exchange of vital safety information as well as other data. To ensure reliable data transmission, VANETs rely on intermediate nodes to forward messages from the source to the destination. The network supports two main communication types: Vehicle-to-Vehicle (V2V), which enables direct exchange between cars, and Vehicle-to-Infrastructure (V2I), where vehicles interact with roadside units. These communications, typically using the IEEE 802.11p standard, cover distances ranging from 100 to 900 meters. Designed to function in an infrastructure-less environment, VANETs offer robust communication capabilities that enhance both connectivity and safety (Ajay & Shah, 2018; Shahid et al., 2018; Javed et al., 2019; Quyoom, Mir & Sarwar, 2020).

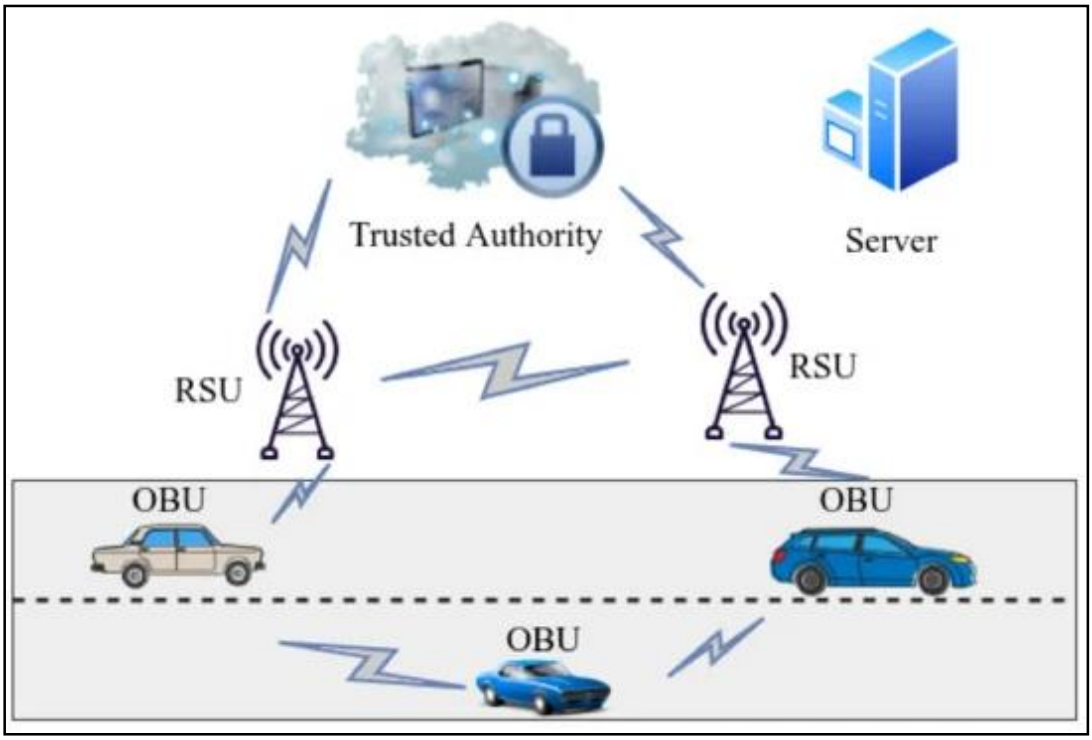

Figure 1: VANET Architecture

Security remains a paramount concern in Vehicular Ad Hoc Networks (VANETs), much like in other emerging areas within Information and Communications Technology (ICT). The consequences of security breaches in VANETs can range from financial losses to life-threatening situations. Previous studies emphasize the importance of security within VANET research (Javed et al., 2019). Privacy and security continue to present major obstacles due to the inherent vulnerabilities of VANETs (Quyoom et al., 2020). Although VANETs provide significant benefits and enhanced connectivity, the advancement of autonomous vehicle systems introduces new and complex security challenges, including Denial-of-Service (DoS) attacks, Sybil attacks, impersonation, and other malicious threats (Mahmood et al., 2021). Tackling these issues is vital to maintain the reliability, safety, and user confidence in VANET deployment.

While existing literature has documented various vulnerabilities and corresponding defensive strategies, this study aims to deepen the understanding by reviewing and analyzing these weaknesses along with effective mitigation techniques. The research focuses particularly on classifying and explaining the different categories of attacks targeting VANETs. It also evaluates numerous scholarly contributions that propose detection mechanisms and countermeasures designed to reinforce VANET security. This work seeks to advance the field by synthesizing current knowledge on VANET threats and recommending strategies to address these risks efficiently.

CLASSIFICATION OF SECURITY ATTACKS IN VANETS

Various types of attacks can occur in ad-hoc environments, particularly within the vehicular domain. The impact of these attacks on the system largely depends on the intentions of the attackers. Attackers may exhibit malicious behaviour for several reasons, such as exploiting system resources they are not authorised to use, obtaining confidential data, or disrupting the network's efficient functionality. The attacks can be classified on the basis of membership, on the basis of activity and on the basis of intensions (Mishra, Singh & Kumar, 2016). The attacks are described by Mishra *et al*. (2016), Shahid *et al*. (2018) and Mahmood *et al*. (2021) as follow:

1. Attack on the Basis of Membership

In the context of network security, authorised or unauthorised nodes can engage in malicious activities that impact the network. The membership status of the node significantly influences the nature of the attack and its potential prevention strategies. Attacks based on membership can be categorised into two types: insider attacks and outsider attacks (Mishra *et al*., 2016).

a) **Inside Attacks:** Also known as internal attacks, involve authorised network members who engage in malicious activities for personal gain or to disrupt the network. These insiders can have a more significant impact compared to external attackers (Mishra *et al*., 2016). Any authenticated node within the network has the potential to harm the network or specific nodes and may have access to public keys (Shahid *et al.,* 2018). An insider attacker is characterised by being an authorised member with comprehensive knowledge of the network, enabling efficient access and potential exploitation of network resources (Mahmood *et al*., 2021).

b) **Outside Attacks:** Also known as external attacks, involve intruders attempting to infiltrate a network through impersonation or other malicious tactics (Mishra *et al*., 2016). These attackers are characterised by having limited resources to compromise network assets (Shahid *et al*., 2018). Outsider attackers are individuals or nodes that are not authorised and do not have direct access to the network. To initiate an attack, they typically need to gather information about the network first before attempting to exploit vulnerabilities (Mahmood *et al.*, 2021).

2. Attack on the Basis of Activity

Attacks on the basis of activity are classified into two categories based on their nature and impact: active attacks and passive attacks (Mishra *et al*., 2016).

i. **Active Attacks:** Active Attacks involve attempts by malicious actors to modify network information and generate malicious packets and signals, which are typically more impactful than passive attacks (Mishra *et al.*, 2016). These attackers have the capability to access network signals and transmit packets or signals (Shahid *et al.*, 2018). In an active attack, the attacker intercepts network information, alters the content of original messages and then transmits them to the intended recipients. The primary objectives of active attacks usually include disrupting the network's efficiency or gaining unauthorised access to network services (Mahmood *et al.*, 2021).

ii. **Passive Attacks:** Passive Attacks involve attackers who do not modify network information but instead silently monitor and observe the network activities (Mishra *et al.*, 2016). These attackers may engage in eavesdropping on wireless channels to intercept communications (Shahid *et al.*, 2018). In a passive attack, the attacker does not actively send or receive messages but rather listens to network communications to gather information about the network or identify potential vulnerabilities (Mahmood *et al.*, 2021).

3. Attack on the Basis of Intension

Attacks on the basis of intension are often categorised based on the intentions or objectives of the attackers. These categories include malicious, rational and network-based attackers (Mishra *et al.*, 2016).

i. **Rational Attackers:** In these attacks, the attackers aim to derive personal benefit from their actions, making their motivations more foreseeable (Mishra *et al.*, 2016). They cause harm to network assets for personal gain and their behaviour is somewhat predictable (Shahid *et al.*, 2018). A rational attacker may intentionally initiate an attack on the network to obtain information or to disrupt its operations (Mahmood *et al.*, 2021).

ii. **Malicious Attackers:** In these attacks, the attackers do not seek personal benefit directly from their actions. Their primary motive is to disrupt the proper functioning of the network. VANET deals with critical and sensitive information, which makes it an attractive target for such malicious attackers (Mishra *et al.*, 2016). These attackers do not harm the network for personal gain but instead exploit it to cause financial losses or disrupt services (Shahid *et al.*, 2018). Their intention is to undermine the network and its operations. A malicious attacker may intentionally disrupt the network's performance with the aim of affecting legitimate users (Mahmood *et al.*, 2021).

iii. **Network Attacks:** These attacks are the most severe as they directly impact the functionality of the entire network and its nodes. Examples include Denial

of Service (DoS), Sybil attacks and similar types (Mishra *et al*., 2016). Mahmood *et al*. (2021) further categorise these attacks into local and extended types. Local attacks target a limited scope, affecting specific RSUs and nodes within a restricted area. In contrast, extended attacks cover larger regions and aim to significantly degrade the network's performance or even shut it down entirely (Mahmood *et al*., 2021).

TYPES OF SECURITY ATTACK IN VANETS

In VANETs, despite advancements, numerous challenges persist, particularly attacks that target its security components (Quyoom *et al*., 2020). These attacks aim to compromise different aspects of the security system (Kaurav & Dutta, 2021). Al Junaid *et al*. (2018) categorise these attacks into Availability, Authentication/Identification, Confidentiality, Privacy and Nonrepudiation attacks, while Abuarqoub *et al*. (2022) classify them into Bonet, Fabrication and Routing attacks. However, this study focuses on discussing and reviewing common attacks in general, as described by Abdulkader et al. (2017), Ajay & Shah (2018), Al Junaid *et al*. (2018), Yao *et al*. (2018), Arif *et al*. (2019), Quyoom *et al*. (2020), Kaurav & Dutta (2021) and Abuarqoub *et al*. (2022) as follows:

1. Distributed Denial of Service (DDoS) Attack

This type of attack involves launching an assault from multiple locations simultaneously. it is orchestrated using numerous compromised nodes, or Zombies, to generate attack traffic. VANETs are highly susceptible to DDoS attacks due to their decentralised network structure, which supports Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications. DDoS attacks can severely impact network performance, including bandwidth, processing power, throughput and overall system operation. In VANETs, such attacks pose significant risks to public safety, potentially leading to accidents, traffic congestion and other hazardous conditions in Intelligent Transportation Systems (ITS) (Abuarqoub *et al.,* 2022). These attacks are particularly dangerous because they originate from multiple locations, spreading their impact across the network (Al Junaid *et al*., 2018). Figure 2 illustrates a DDoS attack.

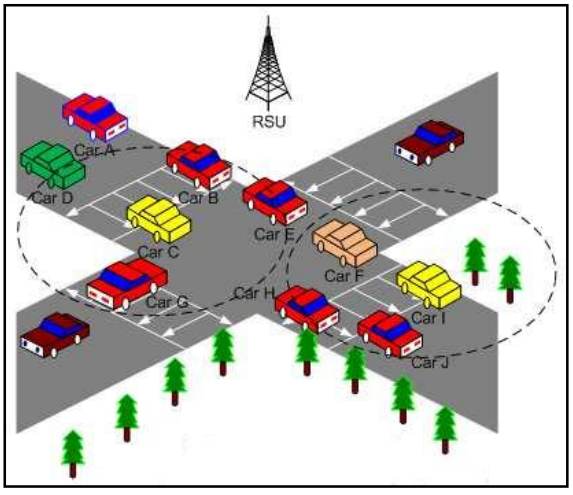

Figure 2: Distributed Denial of Service (DDoS) Attack

2. Sybil Attack

This attack involves an attacker creating numerous fake identities to manipulate the network. These false identities, known as Sybil nodes or virtual nodes, are used to deceive legitimate users. For example, the attacker might simulate heavy traffic on a particular route by sending multiple messages to vehicles, suggesting congestion and prompting them to change their route. By creating this illusion and sending similar messages to multiple vehicles, the attacker induces them to believe the information comes from different sources, thus influencing their route decisions. This manipulation benefits the attacker by clearing a path on their chosen route or redirecting users to undesired locations (Ajay & Shah, 2018). VANETs, due to their critical nature, are highly vulnerable to Sybil attacks, necessitating robust detection algorithms to safeguard them (Abuarqoub *et al*., 2022). Figure 3 illustrates a Sybil attack.

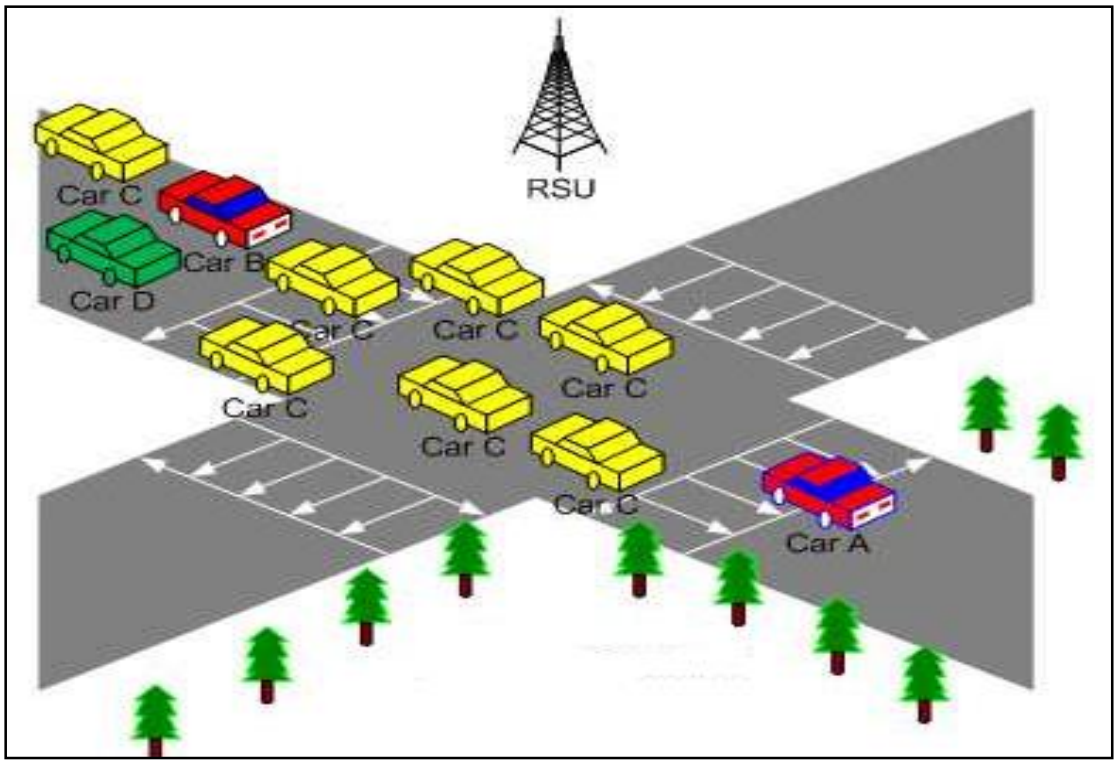

Figure 3: Sybil Attack

3. Impersonation Attack

This attack, also known as a message tampering attack, involves an attacker gaining unauthorised access to a node's identity, allowing them to transmit false information across the network. The attacker can impersonate another node, intercept messages, modify their content for personal gain and relay them to other nodes (Abuarqoub *et*

al., 2022). By tampering with the message content obtained from its original source, the attacker manipulates the data to serve their own interests (Arif *et al*., 2019). This can involve deliberately spreading false information to create communication confusion or to obtain unauthorised privileges within the network. In the context of VANET, such alterations to critical messages can lead to severe consequences and financial losses (Ajay & Shah, 2018). Figure 4 illustrates an Impersonation attack.

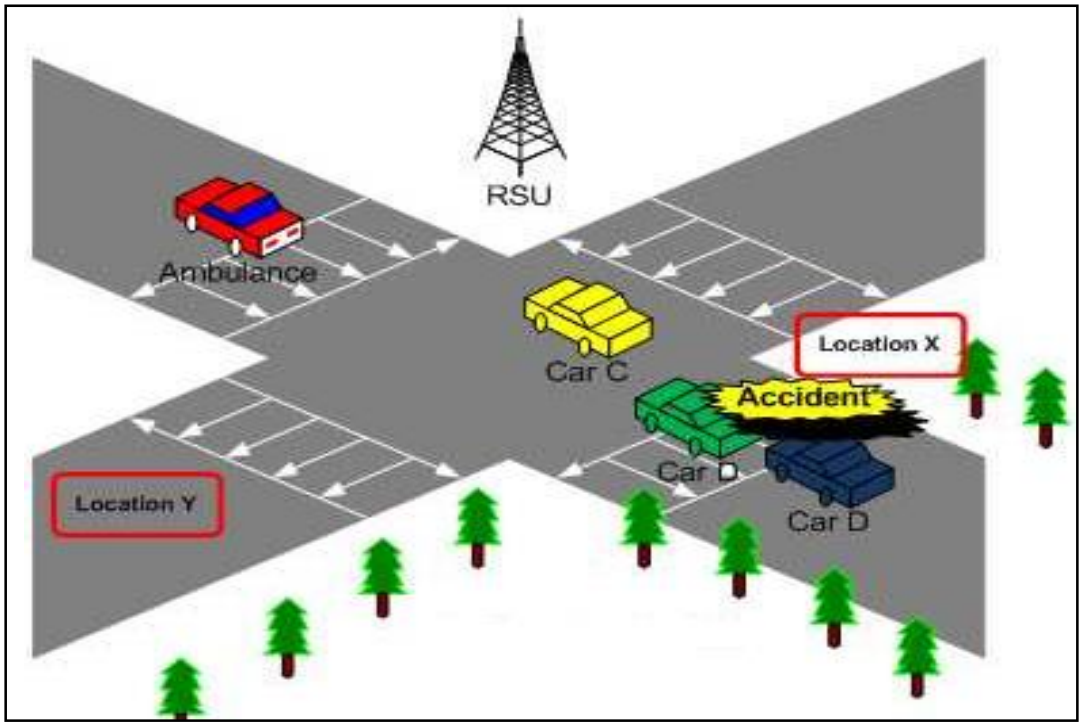

Figure 4: Impersonation attack

4. Blackhole Attack

This type of attack is known as a routing attack, where an attacker entices legitimate nodes to route their packets through it by falsely advertising the shortest path. Once it receives the packets, it drops them (Ajay & Shah, 2018). In this attack, the attacker introduces a malicious node into the network. This node intercepts Packet Data Units (PDUs) intended for the destination node and pretends to offer a shorter path for routing the packets to the destination. Consequently, the attacker can amplify the impact of the attack by deploying multiple malicious nodes across the network (Abuarqoub *et al*., 2022). The malicious node manipulates the routing protocol by falsely claiming to have an optimal route for forwarding packets to their destination. Detecting such attacks is challenging because the malicious node initially behaves cooperatively in the communication, only to reroute packets to disrupt network

operations before returning to normal activities (Arif *et al.*, 2019). Figure 5 illustrates a Black Hole attack.

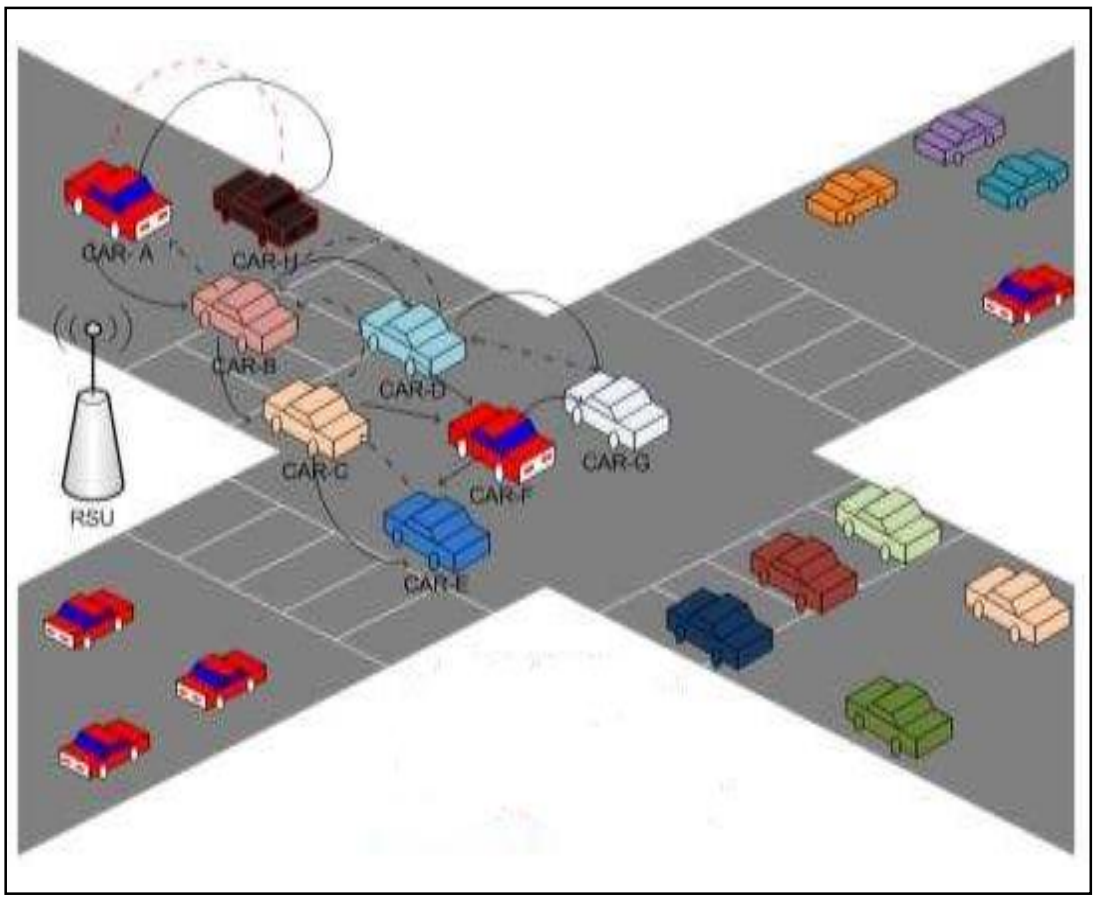

Figure 5: Black hole attack

5. Wormhole Attack

This type of attack is also a routing protocol attack in VANETs. In this scenario, a malicious node intercepts data packets and quickly transfers them to another malicious node located a few hops away (Abuarqoub *et al.*, 2022). The essence of this attack lies in convincing nodes that they are adjacent to each other. Such attacks exploit selective forwarding and eavesdropping techniques (Kaurav & Dutta, 2021), making them difficult to detect within the network. The primary danger posed by a Wormhole attack is its ability to propagate false information among vehicles, thereby disrupting multicast and broadcast routing and potentially compromising the security of routing protocols (Abuarqoub *et al.*, 2022). Attackers favour this method because it allows them to establish a strong strategic presence in VANETs (Al Junaid *et al.*, 2018). Figure 6 illustrates a Wormhole attack.

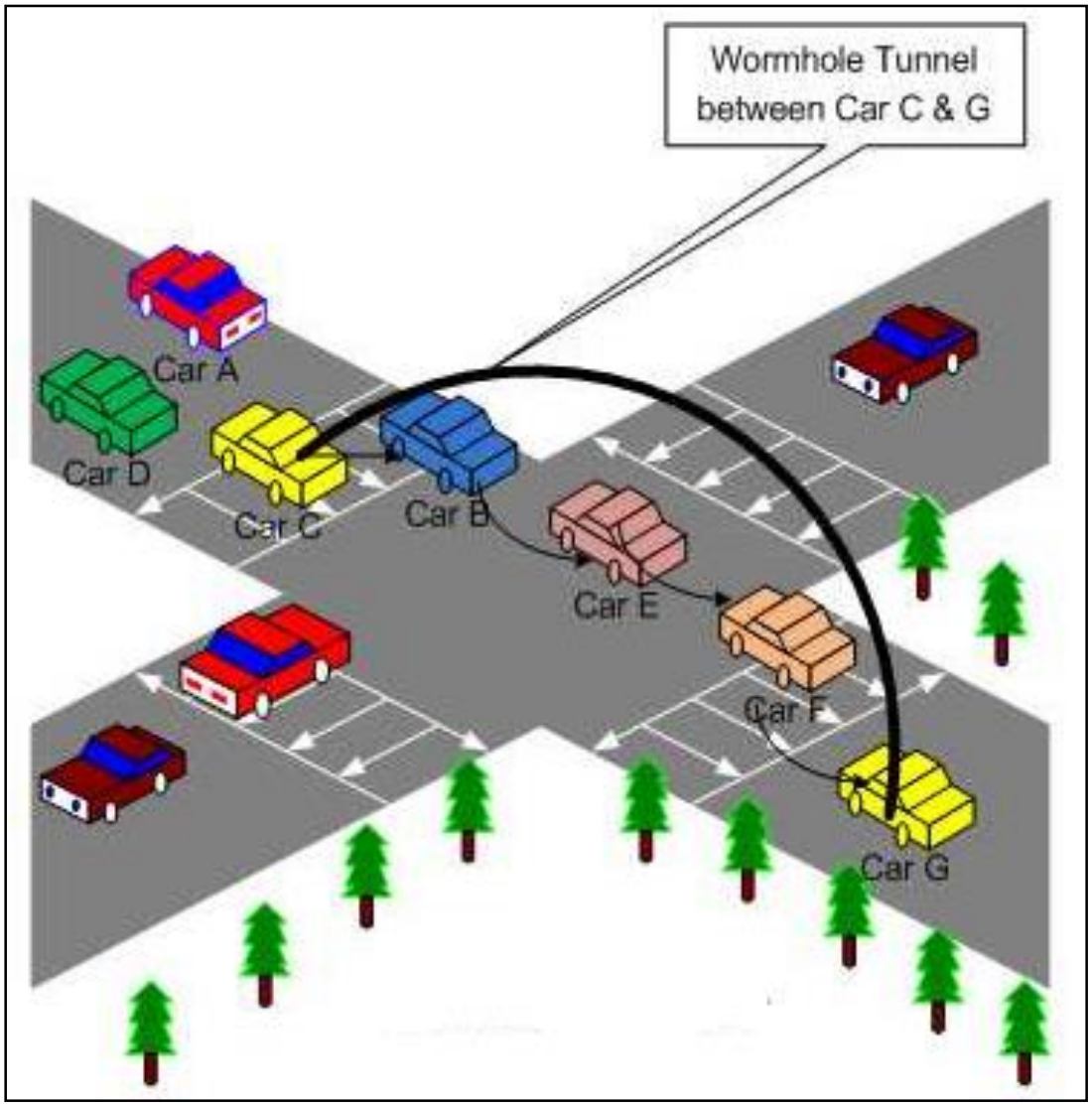

Figure 6: Wormhole attack

6. Grey Hole Attack

This type of attack is also a routing attack in VANETs. It is an extension of the black hole attack where instead of dropping all packets, it selectively drops specific packets. Detecting this attack is challenging because it is not continuous; it occurs intermittently for a limited time and targets specific types of packets (Ajay & Shah, 2018). The Grey hole attack operates in two primary modes: either it allows all data packets to pass through correctly or it selectively drops packets from the received data (Abdulkader *et al.*, 2017). Moreover, the attack is activated for a limited duration, either for a specific period or for specific types of data packets (Abuarqoub *et al.*, 2022). Figure 7 illustrates a grey hole attack.

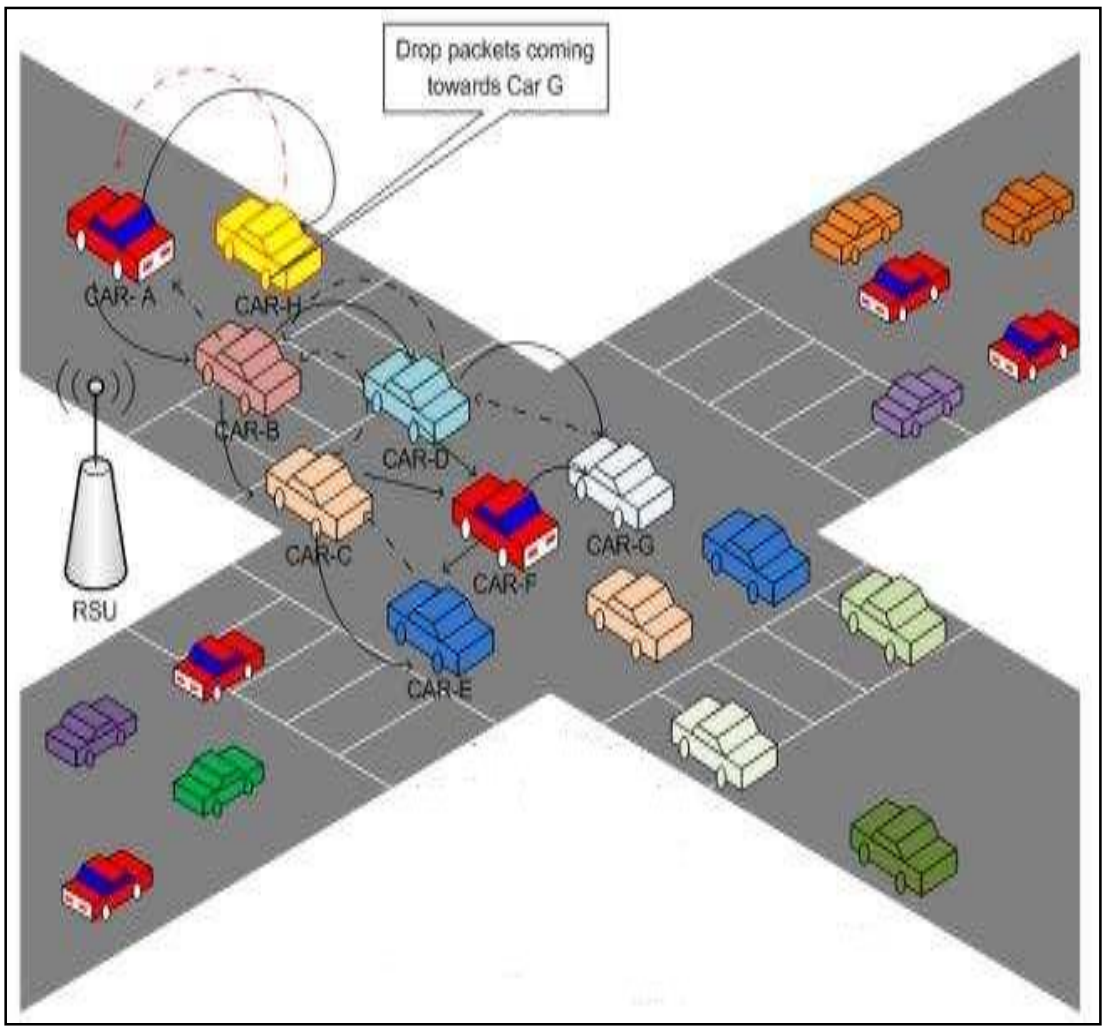

Figure 7: Grey hole attack

7. Denial of Service (DOS) Attack

This attack targets services provided by service providers where legitimate users are unable to access network services despite available resources. The attacker disrupts the main communication medium within the range of the service provider, limiting access to network services (Ajay & Shah, 2018). In VANET environments, attackers typically target the communication media, causing nodes difficulty in accessing the network. The primary goal is to prevent legitimate nodes from accessing network services and utilising network resources. Such attacks can lead to node exhaustion and resource depletion. Attackers may execute DoS attacks by blocking communication channels, overloading networks, or dropping packets (Arif *et al.*, 2019). DoS attacks are considered among the most severe threats in vehicular networks (Quyoom *et al.*, 2020). Figure 8 illustrates a Denial of Service (DoS) attack.

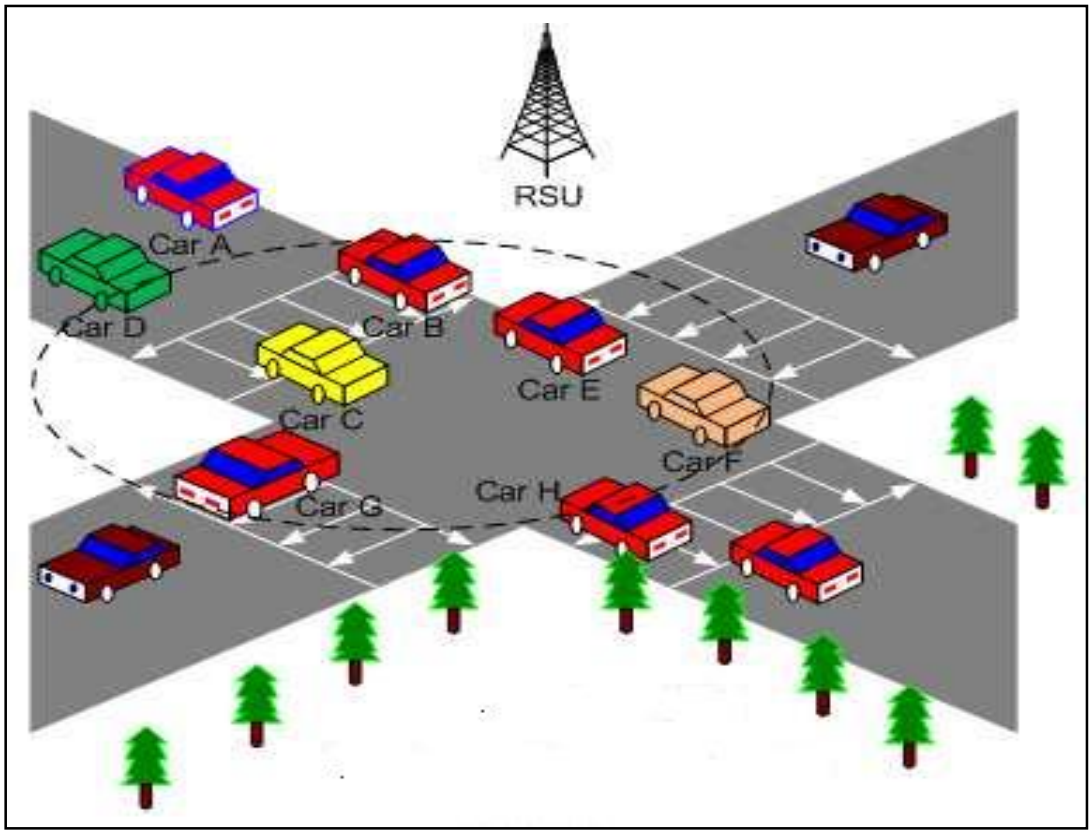

Figure 8: Denial of Service (DoS) attack

PROPOSED DEFENCE MECHANISMS AGAINST SECURITY ATTACKS IN VANET

Several research has been proposed to protect VANETs from the security attacks. This section presents and discusses some of the techniques or approaches that have been proposed by researchers to overcome these threats based on the available literature, these includes:

1. Proposed Defence Mechanisms against Distributed Denial of Service (DDoS) Attack

Kolandaisamy *et al*. (2018) proposed the Multivariant Stream Analysis (MVSA) approach aimed at identifying and reducing the impact of DDoS attacks. MVSA categorises network traffic into safety and non-safety applications, where safety applications involve critical information about travellers and vehicles, while non-safety applications include services like entertainment, fuel savings and electronic tolls. Each packet undergoes analysis to compute network traces consisting of payload, hop count, time to live and packet frequency. Nodes responsible for detecting and mitigating DDoS attacks maintain these traces. Subsequently, MVSA calculates a multivariant stream factor across multiple time intervals to derive a multivariant stream weight (i.e.

the weight of the continuous flow of multiple traffic). Using this weight, MVSA can classify and mitigate DDoS packets and nodes accordingly. Evaluation results indicate a 93% accuracy within a 100ms timeframe.

Yu *et al*. (2018) proposed System SDVN (Software Defined Vehicular Network) designed specifically to effectively detect DDoS attacks. Their framework comprises three key modules: the attack detection module, detection trigger module and flow table item collection module. The attack detection module initiates detection based on PACKET_IN messages. A machine learning module utilising Support Vector Machine (SVM) classifier is employed to train samples and construct a detection model for identifying DDoS nodes within the network. The system generates manual DDoS attack traffic using Scapy and hping3. Results from simulations demonstrated improved classification recognition with a lower false alarm rate and reduced time to initiate attacks.

Gao *et al*. (2019) employed a Distributed Network Intrusion Detection System to detect DDoS attacks. Initially, the system collects network traffic and then utilises a Random Forest (RF) classifier within the network traffic module to identify DDoS traffic. Upon detection of a DDoS packet by the classifiers, the system generates an alert. The authors conducted experiments using NSL-KDD and UNSW-NB15 datasets, achieving 98.7% accuracy with RF, which outperformed other machine learning classifiers.

Kolandaisamy *et al*. (2020) proposed Packet Marking Based on Adaptive Stream Region (PMBSR), which demonstrates superior performance over MVSA in terms of drop ratio, delivery ratio and delay. The PMBSR technique begins by generating a neighbour log file and vehicle values based on network density. If the value falls below a predefined threshold, it identifies its region and divides it into multiple time windows. It then computes the circulation rate to determine the route for each time window within the region. Using collected data, it calculates the standard deviation value, identifying nodes that exceed normal deviation as suspicious nodes.

Adhikary *et al*. (2020) employed a hybrid machine learning approach for DDoS attack detection. Their model combines two SVM kernels: AnovaDot and RBFDot. They conducted simulations using a generated dataset where the AnovaDot algorithm was used initially for training. The output from AnovaDot was then combined with the initial dataset and fed into the RBFDot algorithm for predictions. These predictions were evaluated to assess the effectiveness of the hybrid model, demonstrating its applicability in real-time scenarios for achieving accurate results.

2. Proposed Defence Mechanisms Against Sybil Attack

Yao *et al*. (2019) proposed the ASAP-V protocol, aimed at privacy-preserving authentication and Sybil detection in VANETs. The protocol is structured into four

phases. In the Registration Phase, a trusted authority registers vehicle details such as certificates and keys. The Assignment Phase manages pseudonym assignments for vehicles. The Detection Phase focuses on detecting Sybil attacks, while the Prosecution Phase activates upon detecting a Sybil vehicle, instructing other vehicles to cease communication with it. Performance evaluation of the protocol showed effective detection capabilities with low false negatives and false positives even without centralised authority, achieving an average detection time of 1.2 seconds with a beacon interval of 300 ms and 100 vehicles.

Quevedo *et al*. (2020) proposed an intelligent approach using Extreme Learning Machine (ELM) to detect Sybil attacks in VANETs. They defined a movement matrix based on the mobility patterns of normal VANET nodes, which was then utilised with ELM to distinguish between normal and Sybil nodes based on metrics such as time, location, speed and changes in acceleration. This approach achieved a success rate of 99.9% when tested with 800 vehicles. The ELM technique used in this approach can be integrated with other machine learning methods to enhance efficiency and realism of detection results.

Adhikary *et al*. (2020) proposed an Event Based Reputation System (EBRS), which enhances VANET security by requiring each vehicle to obtain a local certificate from its connected Roadside Unit (RSU). Acting as a trusted authority, the RSU facilitates the exchange of session keys among vehicles. When a vehicle broadcasts messages to nearby vehicles, the recipients verify the integrity of the message by checking the sender's certificate from the RSU. EBRS also combats stolen and fabricated identities using reputation and trust values, thus defending against Sybil attacks effectively.

Li & Zhang (2019) proposed a method for detecting Sybil nodes based on RSSI sequence and the Vehicle Driving Matrix (RSDM). Their approach evaluates the evolution of differences between RSSI sequences and the driving matrix to identify Sybil nodes. Through simulations, the method achieved high detection rates with minimal error rates, boasting over 90% accuracy, 0% error rate and low false positive and false negative rates (FPR and FNR).

Syed & Prasad (2019) proposed a two-phase security mechanism aimed at reliably identifying and blocking attacked nodes by detecting Sybil attacks to ensure safety, reliability and security in VANET applications. The first phase employs Public Key Infrastructure (PKI) for secure communications, relying on a trusted Certificate Authority (CA). The second phase utilises Hash Function mechanisms to detect Sybil attacks by analysing collected data assets within a hash set. This combined approach has demonstrated effective prevention and mitigation of security threats in VANET communication systems, particularly in interactions between vehicles and Roadside Units (RSUs).

3. Proposed Defence Mechanisms Against Impersonation Attack

Hussain *et al.* (2016) proposed a method to prevent impersonation attacks using a Trust Authority (TA) and Public Key Infrastructure (PKI). The TA verifies the identity of vehicles when they communicate with new Roadside Units (RSUs) and shares keys accordingly. They also reviewed SPECS (Secure and Privacy Enhancing Communications Schemes), which employs Identity-Based Batch Verification (IBV) for securing V2V communications. SPECS utilises binary search to efficiently verify batches of messages and employs bloom filters for message validation.

Tobin, Thorpe & Murphy (2017) proposed the BUCK algorithm for VANETs, where vehicles broadcast beacon messages to discover neighbouring vehicles and calculate distances. Each vehicle possesses a verified hash value that is cross-checked with RSUs using timestamps to detect impersonation. They also implemented VANET Content Fragile Watermarking (VCFW) to prevent image tampering, embedding unique watermarks in images that are imperceptible to humans but can validate image authenticity.

Quyoom *et al.* (2020) discussed algorithms for detecting and isolating node impersonation, such as the Detection of Malicious Vehicle (DMV) and Outlier Detection algorithms. These schemes utilise RSUs to monitor node behaviour and increase trust values for trusted vehicles. If distrust values exceed a threshold, the vehicle's ID is reported to the Certificate Authority (CA) as malicious.

4. Proposed Defence Mechanisms Against Blackhole Attack

Tobin *et al.* (2017) proposed a solution to detect and prevent black hole nodes in VANETs. The solution consists of three stages: route backtracking, node accusation and blacklisting. Route backtracking allows nodes (source or destination) to trace the route to detect anomalies. If a malicious node is detected, an accusation message is sent to peers, excluding the accused node. The accused node's behaviour is then reviewed and if confirmed malicious, it is blacklisted using its vehicle identifier. Simulations showed a 100% detection rate with no false positives or negatives and the solution operated with an average response time of 5.84 seconds.

Abdulkader *et al.* (2017) introduced the Lifetime Improving Ad-hoc On-Demand Distance Vector (LI-AODV) routing algorithm for VANETs, an enhancement over AODV. LI-AODV aims to identify and mitigate malicious black hole nodes. It begins by flooding Route Requests (RREQs) to obtain Route Replies (RREPs) from network nodes, selecting the best path excluding black hole nodes. The algorithm improves network lifetime and manages load balancing through a scheduling algorithm combining round-robin and Highest Response Ratio Next (HRRN) with HMAC and SHA-384 for security. Simulations with 50 nodes at varying speeds demonstrated LI-

AODV's effectiveness with a 98% detection rate, 1.7% false positive rate and over 92% packet delivery ratio compared to other protocols.

5. Proposed Defence Mechanisms Against Wormhole Attack

Ali, Nand & Tiwari (2017) proposed an algorithm leveraging RSA and symmetric key concepts for secure data transmission in VANETs. The RSA algorithm generates public-private key pairs for encryption and decryption. Data authenticity is ensured by signing with a private key and verifying with the sender's public key. A shared key is broadcasted once across the network for packet decryption, authenticated using source identifiers to thwart wormhole attacks. This method reduces computational overhead compared to continuous key exchange but may increase with network density. The lack of simulation limits practical validation, yet Tesla with Instant Key (TIK) protocol for authentication is outlined.

Krundyshev, Kalinin & Zegzhda (2018) proposed an artificial swarm algorithm using Intelligent Water Drop (IWD) and trust-based models in VANETs. Trust among nodes in high-speed environments is pivotal, managed through voting-based mechanisms for creating a trusted peer-to-peer network. To address throughput challenges in dense networks, swarm intelligence is integrated. The algorithm is structured into route establishment, maintenance and trust upkeep to detect malicious nodes. Simulations indicate a 40% reduction in delay, 20% increase in throughput and 30% enhanced packet sharing. However, its efficacy without an Intrusion Detection System (IDS) is modest, yet substantial improvements are observed when combined with IDS.

6. Proposed Defence Mechanisms Against Grey Hole Attack

Alheeti, Gruebler & McDonald-Maier (2015) proposed a security system designed to detect grey hole attacks in VANETs. Their approach relies on analysing vehicle behaviour using trace files to identify abnormalities. Initially, they extract data using AWK text processing and apply fuzzification techniques to minimise false alarms. The system integrates with an Intrusion Detection System (IDS) utilising Support Vector Machines (SVM) and Feed-forward Neural Networks (FFNN) for anomaly detection. In their simulations, FFNN outperformed SVM, achieving an accuracy of 99.82% under normal conditions and 99.86% with malicious nodes, with a low false negative rate of 0.12%. In comparison, SVM achieved accuracies of 99.93% and 99.64%, respectively, with a higher false negative rate of 0.30%. The authors emphasize the need for more efficient data extraction methods to enhance system performance in dynamic VANET environments.

7. Proposed Defence Mechanisms Against Denial of Service (DoS) Attack

Hussain *et al*. (2016) proposed a strategy to prevent DoS attacks in vehicular networks using Dynamic Source Routing (DSR) protocols and symmetric cryptography/MAC with authentication. This approach enhances security by employing technologies like frequency hopping and multiple transceivers supported by On-Board Units (OBUs) for channel switching. The authors reviewed the IP-CHOCK model developed by Vinh hoa LA et. al., which significantly strengthens the detection of malicious nodes without requiring secret information exchanges or special hardware. Simulation results demonstrated high detection rates and improved resilience against attacks by accurately identifying forged nodes through IP analysis.

Al-Raba'nah & Al-Refai (2016) proposed an approach to mitigate DoS attacks in VANETs utilising OBUs. Their technique offers four switching options - channel switching, technology switching, frequency hopping spread spectrum (a technique used in wireless communication that enhances security and resistance to interference) and multiple radio transceivers - to counteract DoS attacks based on received malicious messages. Each OBU assesses incoming messages and selects an appropriate switching option, passing the choice to the next OBU in the network. This approach aims to maintain network availability during attacks by improving resilience through diversified communication channels. Additionally, the authors reviewed the work of Roselin Mary et al., who introduced the Attacked Packet Detection Algorithm (APDA). Integrated with Roadside Units (RSUs), APDA identifies and tracks malicious nodes by analysing packet frequency and velocity changes. It maintains a database of validated nodes, pre-emptively detecting DoS attacks to reduce overhead delays and enhance overall VANET security.

8. Other Proposed Defence Mechanisms Against Security Attacks in VANETS

Kumar & Mann (2019) introduced the Multiple Malicious Nodes Detection Algorithm (MMNDA) designed to enhance the detection of both genuine and irrelevant packets in vehicular networks. Unlike existing systems focusing on single node detection, MMNDA targets multiple malicious nodes simultaneously. By analysing velocity and frequency of vehicle nodes, the algorithm improves detection accuracy for DDoS and Sybil attacks while minimising packet loss and extending network lifetime. Moreover, MMNDA facilitates efficient communication between Roadside Units (RSUs) and multiple nodes concurrently, thereby enhancing network efficiency and robustness against attacks.

Jeevitha & Bhuvaneswari (2019) proposed a clustering algorithm for vehicular networks where RSUs assign random IDs to cluster nodes. The algorithm measures time gaps, distances and traffic flow (TF) to classify nodes into an honest or malicious category

using Machine Learning algorithms. Nodes with TF values less than or equal to 1 are deemed honest and added to the registered table, while those with TF values greater than 1 are identified as malicious. This approach aims to optimise network throughput, reduce end-to-end delays, minimise dropped packets and enhance overall network security by effectively detecting and isolating malicious nodes.

Ghazizadeh *et al*. (2019) proposed a method to estimate job completion times in vehicular networks using a three-lane highway simulation with Access Points (APs) spaced every 2000 meters. Each AP covers a 200-meter area, utilising a five-parameter logistic speed-density function to determine vehicular speeds and average processing times ranging from 20 to 30 minutes per transmission. Simulation results showed a maximum relative error of less than 0.24% for uniformly distributed job durations and less than 1.96% for exponentially distributed durations. This method provides accurate estimation of job completion times, crucial for optimising traffic management and resource allocation in VANETs.

Shen *et al*. (2020) proposed a Message Recovery Signature (MSR) mechanism for securing traffic data aggregation in VANETs. MSR ensures properties such as availability, confidentiality and integrity of information processing within VANET systems. Comparative analyses using GMP and PBC simulations demonstrated that MSR offers computationally efficient solutions compared to existing schemes. The proposed mechanism is suitable for deploying in vehicular clouds to enhance traffic data aggregation capabilities and support advanced traffic services efficiently.

CONCLUSION

Vehicular Ad Hoc Networks (VANETs) represent a groundbreaking advancement in modern transportation systems, revolutionizing how vehicles interact with each other and with roadside infrastructure. However, the dynamic and decentralized nature of VANETs also introduces significant security concerns. This paper provides an in-depth exploration of these challenges, beginning with an examination of VANETs' distinct security requirements and structural features. It classifies various security attacks based on criteria such as node participation, type of malicious activity, and attack objectives. The analysis covers major threats like Distributed Denial of Service (DDoS), Sybil, impersonation, black hole, wormhole, grey hole, and Denial of Service (DoS) attacks detailing their characteristics and potential impacts. To counter these threats, the study reviews a range of defensive solutions proposed in the literature, including Multivariate Stream Analysis (MVSA) for detecting DDoS attacks, privacy-focused authentication mechanisms to prevent Sybil attacks, intelligent intrusion detection systems for anomaly recognition, and techniques like cryptographic encryption and channel switching to combat DoS attacks. Overall, this paper delivers a thorough

review of VANET security challenges and outlines practical strategies for enhancing vehicular communication protection. For future advancements, the research suggests exploring blockchain for decentralized trust models, leveraging artificial intelligence and machine learning for real-time threat identification, and employing privacy-preserving technologies such as homomorphic encryption. Additionally, integrating edge computing can enhance responsiveness, while cross-layer security approaches may offer comprehensive protection across network layers.

RFERENCES

Abdulkader, Z. A., Abdullah, A., Abdullah, M. T. and Zukarnain, Z. A. (2017). LI-AODV:lifetime improving AODV routing for detecting and removing black-hole attack from VANET. *Journal of Theoretical and Applied Information Technology*, 95(1), 196-209. http://www.jatit.org/volumes/Vol95No1/19Vol95No1.pdf

Abuarqoub, A., Alzu'bi, A., Hammoudeh, M., Ahmad, A. and Al-Shargabi, B. (2022). A survey on vehicular ad hoc networks security attacks and countermeasures. *The proceedings of the 6th International Conference on Future Networks & Distributed Systems, Uzbekistan*, 701-707. https://doi.org/10.1145/3584202.3584309

Adhikary, K., Bhushan, S., Kumar, S. and Dutta, K. (2020). Hybrid algorithm to detect DDoS attacks in VANETs. *Wireless Personal Communications*, 114(4), 3613-3634. https://doi.org/10.1007/s11277-020-07549-y.

Alheeti, K. M. A. Gruebler, A. and McDonald-Maier, K. D. (2015). On the detection of grey hole and rushing attacks in self-driving vehicular networks. *The proceedings of the 7th Computer Science and Electronic Engineering Conference*, 231-236. https://doi.org/10.1109/CEEC.2015.7332730

Ali, S., Nand, P. and Tiwari, S. (2017). Secure message broadcasting in VANET over Wormhole attack by using cryptographic technique. *The proceedings of the International Conference on Computing, Communication and Automation*, 520-523. https://doi.org/10.1109/CCAA.2017.8229856.

Ajay, N. U. and Shah, J. S. (2018). Attacks on VANET security. *International Journal of Computer Engineering & Technology*, 9(1), 8-19. http://www.iaeme.com/ijcet/issues.asp

Al Junaid, H. A. M., Syed, A. A., Warip, M. N. M., Ku Azir, K. N. Z. and Romli, N. Z. (2018). Classification of security attacks in VANET: A review of requirements and perspectives. *MATEC Web of Conferences 150. EDP Sciences.* https://doi.org/10.1051/matecconf/201815006038

Al-Raba'nah, Y. and Al-Refai, M. (2016). Toward secure vehicular ad hoc networks an overview and comparative study. *Journal of Computer and Communications,* 4, 12-27. https://doi.org/10.4236/jcc.2016.416002.

Arif, M., Wang, G., Bhuiyan, Z. A., Wang, T. and Chen, J. (2019). A survey on security attacks in VANETs: Communication, applications and challenges. *Vehicular Communications. Elsevier Inc*. https://doi.org/10.1016/j.vehcom.2019.100179

Gao, Y., Wu, H., Song, B., Jin, Y., Luo, X. and Zeng, X. (2019). A distributed network intrusion detection system for distributed denial of service attacks in vehicular ad hoc network. *IEEE Access*, 7, 154560-154571. https://doi.org/10.1109/ACCESS.2019.2948382.

Ghazizadeh, A. Ghazizadeh, P. Mukkamala, R. and Olariu, S. (2019). Towards Approximating expected job completion time in dynamic vehicular clouds. The *proceedings of the 12th IEEE International Conference on Cloud Computing*, Milan, Italy, 2019, 481-483, https://doi.org/10.1109/CLOUD.2019.00084

Hussain, N., Singh, A. and Shukla, P. K. (2016). In depth analysis of attacks and countermeasures in vehicular ad hoc network. *International Journal of Software Engineering and Its Applications,* 10 (12), 329-368. http://dx.doi.org/10.14257/ijseia.2016.10.12.29

Javed, M. N., Shafiq, H., Alam, K. A. Jamil, J., Sattar, M. U. (2019). VANET's security concerns and solutions: A systematic literature review. *The proceedings of 3rd International Conference on Future Networks and Distributed Systems, Paris, France.* https://doi.org/10.1145/3341325.3342028

Jeevitha, J. R. and Bhuvaneswari, N. S. (2019). Malicious node detection in VANET session hijacking attack. *The proceedings of the IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India*, 1-6. https://doi.org/10.1109/ICECCT.2019.8869452

Kaurav, A. S. and Dutta, S. R. (2021). Detection and prevention from different attacks in VANET: A Survey. *The proceedings of the International Conference on Physics and Energy 2021*. https://doi.org/10.1088/1742-6596/2040/1/012017

Kolandaisamy, R., Noor, R. D., Ahmedy, I., Ahmad, I., Z'aba, M. R., Imran, M. and Alnuem, M. (2018). A multivariant stream analysis approach to detect and mitigate DDoS attacks in vehicular ad hoc networks. *Wireless Communications and Mobile Computing,* 1-13. https://doi.org/10.1155/2018/2874509

Kolandaisamy, R., Noor, R. M., Z'aba, M. R., Ahmedy, I. and Kolandaisamy, I. (2020). Adapted stream region for packet marking based on DDoS attack detection in vehicular ad hoc networks. *The Journal of Supercomputing*, 76 (8), 5948-5970. https://doi.org/10.1007/s11227-019-03088-x.

Krundyshev, V. Kalinin, M. and Zegzhda, P. (2018). Artificial swarm algorithm for VANET protection against routing attacks. *The proceedings of the IEEE Industrial Cyber-Physical Systems*, 795-800. https://doi.org/10.1109/ICPHYS.2018.8390808.

Krundyshev, S. and Mann, K. S. (2019). Prevention of DoS attacks by detection of multiple malicious nodes in VANETs. *The proceedings of the International Conference on Automation, Computational and Technology Management, London, UK*, 89-94. https://doi.org/10.1109/ICACTM.2019.8776846

Li, W. and Zhang, D. (2019). RSSI sequence and vehicle driving matrix based sybil nodes detection in VANET. *The proceedings of the 11th IEEE International Conference on\Communication Software and Networks*, Chongqing, 763-767.https://doi.org/10.1109/ICCSN.2019.8905261.

Mahmood, J., Duan, Z., Yang, Y., Wang, Q., Nebhen, J. and Bhutta, M. N. M. (2021). Security in vehicular ad hoc networks: Challenges and countermeasures. *Security and Communication Networks. Hindawi*. https://doi.org/10.1155/2021/9997771

Mishra, R., Singh, A. and Kumar, R. (2016). VANET security: Issues, challenges and solutions. *The proceedings of the International Conference on Electrical, Electronics and Optimization Techniques*. https://ieeexplore.ieee.org/document/7754846

Quevedo, C. H. O. O., Quevedo, A. M. B. C., Campos, G. A., Gomes, R. L., Celestino, J.and Serhrouchni, A. (2020). An intelligent mechanism for sybil attacks detection incVANETs. *The proceedings of the IEEE International Conference on Communications*, 1-6. https://doi.org/10.1109/ICC40277.2020.9149371.

Quyoom, A., Mir, A. A. and Sarwar, A. (2020). Security attacks and challenges of VANETs: A literature survey. *Journal of Multimedia Information System*, 7(1), 45-54).http://doi.org/10.33851/JMIS.2020.7.1.45

Shahid, M. A., Jaekel, D., Ezeife, C., Al-Ajmi, Q., Saini, I. (2018). Review of potential security attacks in VANET. *The proceedings of the Majan International Conference (MIC)*. https://doi.org/10.1109/MINTC.2018.8363152

Shen, J., Liu, D., Chen, X., Li, J., Kumar, N. and Vijayakumar, P. (2020). Secure real-time traffic data aggregation with batch verification for vehicular cloud in VANETs. *IEEE Transactions on Vehicular Technology*, 69 (1), 807-817. https://doi.org/10.1109/TVT.2019.2946935

Shetty, S. R. and Manjaiah, D.H. (2022). A comprehensive study of security attack on VANET. *Lecture Notes on Data Engineering and Communications Technologies.Springer, Singapore*. https://doi.org/10.1007/978-981-16-2937-2_25

Syed, S. A. and Prasad, B. V. V. S. (2019). Merged technique to prevent sybil attacks in VANETs. *The proceedings of the International Conference on Computer and Information Sciences*, Sakaka, Saudi Arabia, 1-6. https://doi.org/10.1109/ICCISci.2019.8716435.

Tobin, J., Thorpe, C. and Murphy, L. (2017). An approach to mitigate black hole attacks on vehicular wireless networks. *The proceedings of the 85th IEEE Vehicular Technology Conference*. https://doi.org/10.1109/VTCSpring.2017.8108460.

Yao, Y., Xiao, B., Wu, G., Liu, X., Yu, Z., Zhang, K., Zhou, X. (2018). Multi-channel based sybil attack detection in vehicular ad hoc networks using RSSI. *IEEE Transactions on Mobile Computing,* 18(2), 362-375. https://doi.org/10.1109/TMC.2018.2833849.

Yao, Y. Xiao, B., Yang, G., Hu, Y., Wang, L. and Zhou, X. (2019). Power control identification: A novel sybil attack detection scheme in VANETs using RSSI. *IEEE Journal on Selected Areas in Communications*, 37(11), 2588-2602. https://doi.org/10.1109/JSAC.2019.2933888.

Yu, Y. Guo, L. Liu, Y. Zheng, J. and Zong, J. (2018). An efficient SDN-based DDoS attack detection and rapid response platform in vehicular networks. *IEEE Access*, 6, 44570-44579. https://doi.org/10.1109/ACCESS.2018.2854567.