CHAPTER 2
REVIEW OF LITERATURE

2.1 Introduction

This chapter aims to explore effective strategies for mitigating attacks in Vehicular Ad-Hoc networks VANET, drawing insights from the existing literature. VANET offer a promising future for Intelligent Transportation System (ITS). VANET enable communication between vehicles and infrastructure for improved safety, traffic management, and efficiency. However, VANET are vulnerable to various cyber-attacks, particularly Denial-of-Service (DoS) attacks that can disrupt critical communication and compromise network stability. Detection based, prevention based and mitigation based approaches have been proposed in the literature. Due to the nature of open wireless medium used in VANET, there are chances of a number of possible attacks by which the network is exposed leading to fairly high chances of possible attacks. The main goal of the attackers is to create problem for legitimate (genuine) users, and as a result services are not accessible which concludes in denial of service.

Researchers provided a number of survey studies that have proposed taxonomies with respect to DoS attacks with the scope of attacks have so far been limited. There is a need to identify new attacks and come up with continuously adapting detection and mitigation strategies. While significant progress has been made, securing VANET against DoS attacks remains an ongoing challenge. Securing VANET against DoS attacks is vital for ensuring the safety, efficiency, and reliability of future transportation systems. This chapter also presents the result of the literature study conducted to understand the current status of the researches related with providing security to VANET.

By leveraging the insights from existing research as discussed in this chapter, paved the way for addressing the adaptability in the mitigation strategies for DoS attacks in VANET in this thesis.

2.2 Manifestation of DoS Attacks in VANET

DoS attacks introduces useless traffic, suspends services and spread within the VANET. In addition, the DoS attacks also manifest to compromise the integrity,

availability, and safety of the communication within the network through extended level. Considering the extended level, DoS attacks prevail as DDoS attacks impacting VANET with congestion, disrupted communication and degraded network performance.

The manifestation of DoS attacks in terms of the protocol layers are the consideration in this thesis especially application layer, transport layer and network layer. The security concerns based on DoS and DDoS attacks in the layers in Amandeep Verma *et al.,* (2021) considered are highlighted as below:

- Application layer DoS attacks affect service access, gather trust information about vehicles
- Transport layer DoS attacks introduce delays, packet loss and packet corruptions, resource consumption, unavailability of services
- Network layer Dos attacks interrupt the communication, paralyze the network

DoS attacks threatening the VANET are highlighted by Amandeep Verma *et al.,* (2024) based on launching of attacks. The DoS attacks are spread across the network and become a serious threat as DDoS attacks when launched from different locations. The literature also covered the DDoS attacks in VANET. The DoS attacks and the security solutions provided by the researches have been discussed in this chapter. VANET hold immense potential but require careful consideration of both performance and security.

The review due to mitigation techniques are focused based on the following factors:

i. VANET performance and security attacks
ii. Security techniques based on Cryptographic and Machine Learning based IDS, Swarm Intelligence
iii. Artificial Immune System based solutions

The following sections provide a comprehensive understanding of the existing defense techniques against DoS attacks on the above mentioned factors for mitigation to thwart the threatening on the performance of the VANET.

2.3 Review on VANET Performance and Security Attacks

Achieving optimal performance in VANET goes hand-in-hand with robust security measures for vehicles to communicate with each other (V2V) and roadside infrastructure (V2I), enabling applications like collision avoidance, traffic management, and even automated driving. Efficient security protocols and performance optimization techniques are crucial for the successful deployment of this technology.

This review delves deeper into past research works on addressing security in VANET to provide the performance.

Zhou *et al.,* (2024) suggested protocol presented a unique AKA method that supports multiple identity authentications at once by using vehicle features as IDs. Based on robust cryptographic assumptions, the extended Canetti-Krawczyk (eCK) security model ensured message unforgeability and session key indistinguishability. Its efficacy and efficiency are demonstrated in high-density VANET settings through formal security verification using ProVerif and performance assessments utilizing JPBC and Veins simulations. Despite these advancements, the dynamic nature of vehicular settings and possible scalability under very large networks still provide difficulties for practical implementation.

Amit Kumar Singh *et al.,* (2021) newly proposed vehicular delay tolerant network-based communication using machine learning classifiers for filtering efficient vehicular nodes, so that packets can be delivered from source to destination. Classification technique is a suitable strategy to anticipate and classify the traffic and decide the in all probability, and VDTN nodes to be experienced in a given way which can be utilized to settle on increasingly educated steering choices, diminishing overhead in pestilence-based steering draws near.

Sadkhan *et al.,* (2021) identified the Security Challenges with Cognitive Radio Environments for VANET. To implement a robust VANET infrastructure that allows for effective contact between parties, these requirements must be taken into account. Current security architectures and well-known security specification protocols are described in detail. The second approach relies on reclassifying the various VANET attacks and

remedies discussed in the literature. The third approach compares these innovations in VANET using well-known security principles. The model not provided with the enough statistical analysis to support the comparison between VANET and MANET security attacks.

Wang *et al.,* (2020) presented a hybrid conditional privacy-preserving authentication protocol based on the PKI certificate and identity-based signature. The trust authority (TA) assigns the unique long-term certificate for every registered node. Only the vehicle with valid certificate can apply the anonymous short term identity from the current RSU to sign safety-related message. The identity-based signature avoids the CRL checking and the complex bilinear paring operation. When vehicle is compromised, TA can easily revoke its identity by the only long-term certificate. To further enhance efficiency, the vehicle can verify the messages received by single or batch authentication. The method does not consider the possibility of collusion attacks among multiple malicious vehicles.

Shawky *et al.,* (2023) presented a group key distribution system based on blockchain that is specifically designed for VANETs and uses smart contract technology to enable safe and effective key management. Following initial authentication using Public Key Infrastructure (PKI), the Road Side Unit (RSU) serves as the group manager in this method, allocating and updating group session keys among valid vehicles via smart contract functionalities implemented on the Ethereum MainNet. A symmetric key cryptography-based group signature (GS) technique was incorporated to provide safe and lightweight message authentication, meeting privacy and security needs in dynamic vehicular contexts. It discusses message authentication and key distribution, although it skips over dynamic key extraction methods.

Akhter *et al.,* (2021) developed multi-level blockchain-based privacy-preserving authentication protocol, which introducing a hierarchical architecture consisting of a Global Authentication Center (GAC) and multiple Local Authentication Centers (LACs). This approach used blockchain's decentralized and immutable nature to enable scalable, secure, and fast authentication processes within and across vehicular clusters. Notably, the protocol incorporates a modified IEEE 802.11 control packet format to mitigate traditional MAC issues. The system prioritizd emergency vehicles by enabling expedited

authentication and message transmission, enhancing safety-critical communication. Security was reinforced through RSA-1024 digital signatures, ensuring message confidentiality, integrity, and authenticity. However, consensus mechanisms for managing vehicle behavior and detecting malicious activity remain a future enhancement.

Zabeeulla *et al.,* (2023) suggested a security architecture for 5G-based VANETs by integrating SDN with Self-Organizing Maps (SOM) to form a SOM-SDN framework aimed at enhancing data communication safety. The proposed system used the dynamic adaptability of SDN to manage network traffic and the anomaly detection capability of SOM to identify potential threats, particularly DDoS attacks. By avoiding the need to establish separate control planes, the model reduced latency and control overhead, making it highly efficient for real-time vehicular environments. The proposed framework is not efficient enough to handle the high throughput requirements of VANET.

Kaur and Kakkar *et al.,* (2025) introduced a comprehensive security framework incorporating a novel SecureAuth protocol combined with an optimal attack detection mechanism. The SecureAuth protocol enhanced authentication robustness by integrating security primitives such as interpolation, hashing functions, and EX-OR operations, thereby strengthening resistance against common VANET threats. Routing and CH selection were optimized through a hybrid approach utilizing fuzzy logic and the Fractional Aquila Remora Optimizer (Fr-ARO), which ensured efficient network formation and data forwarding. Attack detection was achieved by employing a Deep Maxout Network (DMN), whose parameters were finely tuned using the Fractional Aquila Spider Monkey Optimization (FASMO) algorithm, resulting in improved detection accuracy. The model reduce adaptability under varying network conditions or attacker strategies.

Azam *et al.,* (2022) introduced an ensemble-based collaborative framework using Majority Voting (Hard and Soft) for detecting Sybil attacks in VANETs. The method integrated multiple classifiers such K-Nearest Neighbor (KNN), Naïve Bayes, Decision Tree, SVM, and Logistic Regression in a parallel fashion, where the final prediction was based on collective decision-making. This ensemble strategy aimed to enhance prediction robustness, reduce false positives, and increase overall accuracy. Despite its promising

performance, the proposed framework is limited in terms of scalability and adaptability to evolving attack patterns.

Nandy *et al*., (2021) suggested an elliptic curve cryptography (ECC)-based secure and pseudo-identity-based privacy-preserving authentication protocol to enhance security in VANETs. The scheme eliminated the dependency on a TA and removes the requirement of a secure communication channel during the registration phase, addressing critical issues in infrastructure-less environments. It integrated pseudo-ID-based authentication for anonymity and employed symmetric-key cryptography with session keys for efficient message encryption. Security resilience was verified using Burrows–Abadi–Needham (BAN) logic and the AVISPA tool, ensuring robustness against known attacks. A mathematical correctness proof validates the protocol's theoretical soundness. However, the scheme's current limitation lies in the lack of real-time testbed validation and absence of an integrated intrusion detection mechanism to enhance holistic VANET security.

Wang *et al.,* (2024) presented an efficient and secure data access control scheme for cloud-assisted VANETs by integrating Attribute-Based Encryption (ABE) with intrusion detection and policy privacy preservation. The proposed framework addressed challenges in secure data sharing by implementing partial policy hiding through anonymization of policy attribute values and employing a hybrid deep learning model, combining a Sparse Stacked Autoencoder (SSAE) and a three-layer Bidirectional Long Short-Term Memory (BiLSTM) network, to detect and filter malicious user access requests. Furthermore, the scheme utilizes an edge-based architecture where computationally intensive encryption and decryption tasks were offloaded to RSUs with verifiable outsourced operations. However, the model does not consider the possibility of insider attacks or other advanced attacks.

Zhang *et al.,* (2022) proposed a novel software-defined trust based VANET architecture (SD-TDQL) in which the centralized SDN controller is served as a learning agent to get the optimal communication link policy using a deep Q -learning approach. The trust of each vehicle and the reverse delivery ratio are considered in a joint optimization problem, which is modeled as a Markov decision process with state space,

action space, and reward function. Expected transmission count (ETX) is used as a metric to evaluate the quality of the communication link for the connected vehicles' communication. Moreover, a trust model has been designed to avoid the bad influence of malicious vehicles. Simulation results prove that the proposed SD-TDQL framework enhances the link quality.

Santhosh Kumar Sripathi Venkata Naga *et al.,* (2022) developed a comprehensive survey on the classification of various types of certificate-less authentication schemes and their features. The schemes are classified based on their type of authentication, the techniques used, the attacks they address, and their security requirements. This survey highlights the performance comparison of various authentication schemes and presents the gaps in them, thereby providing insights for the realization of intelligent transportation systems.

Fábio Gonçalves *et al.,* (2021) suggested an Intelligent Hierarchical Security Framework for VANET making use of Machine Learning (ML) algorithms to enhance attack detection, and to define methods for secure communications among entities, assuring strong authentication, privacy, and anonymity. The ML algorithms used in this framework have been trained and tested using vehicle communications datasets, which have been made publicly available, thus providing easily reproducible and verifiable results. The obtained results show that the proposed Intrusion Detection System (IDS) framework is able to detect attacks accurately, with a low False Positive Rate (FPR). Furthermore, results show that the framework can benefit from using different types of algorithms at different hierarchical levels, selecting light and fast processing algorithms in the lower levels, at the cost of accuracy, and using more precise, accurate, and complex algorithms in nodes higher in the hierarchy.

Table 2.1 summarizes various techniques and methods used to improve security in VANET, their significance, and their limitations.

Table 2.1: Review of VANET Performance and Security Attacks

Author and Year	Techniques / methods	Significance	Limitations
Zhou et al., (2024)	Authentication Key Agreement Protocol for VANET	This protocol enhances VANET security by enabling efficient multi-identity authentication with strong formal guarantees. It significantly reduces computational and storage overhead, making it practical for high-density, resource-constrained vehicular networks.	This model face challenges related to the dynamic nature of vehicular environments and potential scalability under extremely large networks.
Sadkhan et al., (2021)	Cognitive Radio Environments.	Current security architectures and well-known security specification protocols are described in detail. The second approach relies on reclassifying the various VANET attacks and remedies discussed in the literature.	The model not provided enough statistical analysis to support the comparison between VANET and MANET security attacks.
Wang et al., (2020)	Hybrid conditional privacy-preserving authentication protocol.	The identity-based signature avoids the CRL checking and the complex bilinear paring operation. When vehicle is compromised, TA can easily revoke its identity by the only long-term certificate.	The method does not consider the possibility of collusion attacks among multiple malicious vehicles.
Shawky et al., (2023)	Blockchain-based group key distribution	The proposed scheme enhances the security and efficiency of group key distribution in VANETs using blockchain-based smart contracts.	It does not explore dynamic key extraction techniques.

Author and Year	Techniques / methods	Significance	Limitations
	scheme	It significantly reduces computation and communication costs while ensuring robust message authentication.	
Akhter et al., (2021)	Multi-level blockchain-based privacy-preserving authentication protocol	The proposed multi-level blockchain authentication enhances security and privacy in VANETs by enabling decentralized, fast, and scalable vehicle verification. It improves communication reliability through modified MAC protocols and prioritizes emergency vehicle access for timely message delivery.	Consensus mechanisms for managing vehicle behavior and detecting malicious activity remain a future enhancement
Zabeeulla et al., (2023)	Hybrid security framework.	The proposed SOM-SDN framework significantly enhances real-time threat detection and reduces network latency in 5G-based VANETs.	The proposed framework is not efficient enough to handle the high throughput requirements of VANET.
Kaur and Kakkar et al., (2025)	SecureAuth protocol	The proposed SecureAuth protocol significantly enhances VANET security by combining advanced authentication, optimized routing, based attack detection, which improves network reliability and resilience against diverse cyber threats while maintaining efficient resource utilization.	The model reduces adaptability under varying network conditions or attacker strategies.

Author and Year	Techniques / methods	Significance	Limitations
Azam et al., (2022)	Ensemble-based collaborative framework using Majority Voting	The ensemble-based framework uses majority voting across multiple classifiers to improve Sybil attack detection in VANETs, enhancing robustness and reducing false positives. By combining diverse algorithms, it achieves higher accuracy through collaborative decision-making.	The proposed framework is limited in terms of scalability and adaptability to evolving attack patterns
Nandy et al., (2021)	ECC-based secure and pseudo-identity-based privacy-preserving authentication protocol	This protocol employs ECC and pseudo-identity authentication to provide secure, anonymous communication without relying on a trusted authority or secure registration channels. Its lightweight symmetric-key encryption supports efficient message confidentiality, while formal verification ensures strong security guarantees.	There is a lack of real-time testbed validation and absence of an integrated intrusion detection mechanism to enhance holistic VANET security
Wang et al., (2024)	Attribute-Based Encryption (ABE) with intrusion detection and policy privacy preservation	VANETs are critical for enabling secure and intelligent transportation systems through efficient data sharing. The proposed scheme enhances access control and intrusion detection by offloading heavy cryptographic operations to RSUs, improving system responsiveness.	The model does not consider the possibility of insider attacks or other advanced attacks.

The significance and limitations of each method are also mentioned in the table. These methods focus on improving authentication and privacy; others focus on efficient message dissemination or attack detection. However, most of the methods have some limitations, such as not being able to handle advanced attacks, handling a large number of vehicles, or being robust enough to handle variations in data quality or network conditions. Overall, the table provides an overview of the different approaches and their strengths and weaknesses highlighting the need for the continuous VANET performance by securing its operations against DoS attacks and its types with more robust techniques.

The study initially focused on VANET Security. The Security framework included approaches including authentication, detection, and secure message dissemination were highlighted and the approaches implemented for securing VANET against attacks including DoS attacks. VANET performance with scalability, jitter leading delayed communication and loss still existed as the limitations to be focused.

The literature study is preceded further based on the Detection, Prevention and Isolation approaches with Cryptography-based, Machine Learning-based, Trust-based and Artificial Immune System-based to secure VANET against DoS and DDoS attacks. The following subsections provide such approaches securing VANET against DoS attacks and its types.

2.4 Review on Security Solutions handling DoS attacks and its types in VANET

The prevalent impact of DoS attacks and its types in VANET as discussed in chapter 1 provided the need for securing VANET from such attacks hindering network resources or services to the safety critical applications. The Defense landscape in chapter 1 exhibited the broadened security domains available to secure VANET. The sections below portray the security solutions under the following categories:

- Cryptography-based
- ML-based IDS
- AIS

2.4.1 Review on Cryptography-based Techniques in VANET

VANET is essential for enhancing road safety, traffic management, and providing a variety of services to drivers. However, the open nature of VANET makes them

vulnerable to various security threats, including eavesdropping, message tampering, and denial of service (DoS) attacks. To mitigate these threats, cryptography-based techniques have been extensively researched and implemented. This review provides an overview of recent advancements in cryptography-based techniques in VANET, focusing on their applications, benefits, and limitations.

Sajini *et al.,* (2023) introduced an enhanced security framework for VANETs based on American Standard Code for Information Interchange-centered ECC (ASCII-ECC), targeting message authenticity and secure data dissemination. Initially, vehicles and users register with a TA and their respective OBUs. Then, Median-centered K-Means (MKM) algorithm was employed for dynamic cluster formation and Cluster Head (CH) Selection, the Modified Cockroach Swarm Optimization (MCSO) algorithm determined the shortest communication path. Secure communication was executed using ASCII-ECC for authorized vehicles, whereas unauthorized requests were identified and blocked by TA. The proposed scheme does not provide a mechanism for revoking the compromised identities, which could result in security vulnerabilities.

Bala *et al.,* (2023) implemented a Blockchain-enabled Trust and Location-dependent Privacy Preserving (BTLB-PP) authentication system to tackle security and privacy challenges in VANETs by integrating trust management based on the Dirichlet distribution and blockchain technology. The system allowed vehicles to collaborate only with trustworthy nodes by evaluating the reliability of claimed and collaborative vehicles while constructing anonymous obfuscation regions to protect location privacy. Utilizing a private blockchain and smart contracts, it securely recorded and updated trust values of vehicles in a decentralized, tamper-proof manner accessible by all participants, thereby preventing malicious behavior and fake identities. The system is vulnerable to collusion attacks, where malicious vehicles manipulate trust evaluations to gain unauthorized access or evade detection.

Rajkumar and Kumar (2024) presented an improved certificate-less signature aggregation method based on ECC that was intended to guarantee complete privacy protection and strong security in VANETs. Because VANETs were extremely dynamic and resource-constrained, the approach minimizes verification delays and communication

overhead on road-side devices by utilizing aggregation and point addition techniques. Its resilience is further supported by formal security proofs based on the Random Oracle Model and Diffie-Hellman assumptions. By employing distributed data authentication, this method solves the key escrow issue while doing away with the conventional certificate administration complexity. Notwithstanding these benefits, the system is vulnerable to some sophisticated assaults, such side-channel or insider attacks, which the present architecture does not adequately handle.

Sudhakar *et al.,* (2024) developed a system called Enhanced Timed Efficient Stream Loss-Tolerant Authentication (ETESLTA) to guarantee private and secure communication. By including a revolutionary cuckoo filter mechanism for accurate vehicle identification inside RSU detection zones, the ETESLTA framework expands upon earlier TESLTA methods. Important procedures including initialization, registration, mutual authentication, message broadcasting and verification, and vehicle revocation are all included in the suggested ETESLTA strategy. It seeks to minimize memory use while preserving strong privacy and broadcast authentication. The cuckoo filter's probabilistic design introduces false positives, which affect authentication accuracy in situations with a high vehicle density.

Shayea *et al.,* (2022) presented ECC with Generic Algorithm based Privacy-Aware Secure Routing (ECC-GA-PASR), a combination of two techniques, such as optimum RSU distribution and ECC-based authentication, to improve the security and computational overhead of high-speed VANETs. The generic algorithm (GA) was utilized to optimize the RSU distribution, and the ECC method was employed to enhance the authentication in trusted authority. However, there is a need to providing hybrid security so that an increase in speed, which should not affect the performance of the network.

Shawky *et al.,* (2023) created a Blockchain-based Secret Key Extraction (BCSKE) technique that uses blockchain technology and physical-layer-based key creation to solve the authentication issues in VANETs. To confirm legitimacy and safely exchange probing packets for channel estimate, the suggested methodology started with authentication based on public-key cryptography. Channel reciprocity was used to derive

a secret key using the channel phase response. With the introduction of a blockchain-enabled reconciliation system, a trusted third party (TTP) used smart contracts to broadcast the repair sequence, allowing for safe retrieval by authorized vehicles. Symmetric key cryptography (SKC), which drastically lowers communication and computational cost, was used for further message authentication after the shared key was created. The scheme lacks forward secrecy, as compromised key, which affect the confidentiality of prior communications.

Nova *et al.,* (2023), developed a novel security framework Floyd–Warshalls algorithm and modified advanced encryption for VANETs to address the persistent issue of Sybil attacks while maintaining privacy and ensuring secure data transmission. Vehicles were clustered using Kernel k-Harmonic Means (KKHM), using high-dimensional feature space for improved accuracy. CH were then selected via the Floyd-Warshall Algorithm (FWA) based on shortest path metrics. To detect malicious CHs, a DNN was trained on relevant features, with its parameters optimized using a newly introduced Gradient-Based Elephant Herding Optimization (GBEHO) algorithm which further improved through Gaussian chaos mapping and enhanced position update strategies using random wandering and variation operators. Finally, the Modified Advanced Encryption Standard (MAES) ensured secure transmission of data from CHs to the cloud. The proposed scheme does not provide protection against message tampering or replay attacks.

Aghabagherloo *et al.,* (2022) presented Conditional privacy-preserving authentication (CPPA) technique that improves security by using a private key update approach and a tamper detection mechanism, therefore eliminating the requirement for continuous RSU connection. Through conditional methods that maintain anonymity and unlinkability, the approach ensured traceability and revocability while allowing vehicles to verify messages independently of RSU interaction. By showing resistance to physical OBU compromise and guaranteeing safe message verification, the scheme's security was explicitly shown in the random oracle model. Even while the plan lessens reliance on RSUs and lessens the effects of TRD compromise, it still depends on recurring key updates, which makes synchronization difficult in extremely dynamic vehicle settings.

Abdelfatah *et al.,* (2021) presented a Secure VANET Authentication Protocol (SVAP) that distributed the network parameters without the need for secure channels by utilizing Chebyshev chaotic maps to secure communication between the infrastructure and automobiles. Uniquely, the protocol combined symmetric key cryptography for lightweight processing and public key signatures for non-repudiation, overcoming the two main limitations of lack of non-repudiation in symmetric schemes and computational overhead. The proposed scheme does not provide a mechanism for revoking compromised identities, which could result in security vulnerabilities.

Al-Shareeda and Manickam *et al.,* (2022) introduced a modular square root-based to resist DoS attacks (MSR-DoS) scheme for enhancing the security and efficiency of communication in vehicular networks. While maintaining crucial security features like source authenticity, message integrity, pseudonym-based privacy preservation, unlinkability, traceability, and revocability, the suggested MSR-DoS scheme used MSR operations to achieve notable computational cost reductions, especially in message signing and verification. However, the present architecture depends on a centralized cloud-based infrastructure and mostly concentrates on individual message verification. The primary drawbacks are the inability to do batch verification and the reliance on cloud computing, which result in scalability and latency problems in real-time situations.

Soujanya B K et al., (2024), suggested security properties and challenges among VANET. Next, the essential and significant features of a secure VANET system, such as confidentiality and integrity of data, and the availability of network systems have been reported, the authenticity of nodes and messages, and the refusal to deny data once it has been transmitted is detailed. Later, it outlined the requirement of the ITS which makes the survey unique. More importantly, the report on the most recent developments in VANET concentrates on the authentication schemes that have been proposed recently. The security features and authentication resistance against attacks, along with the overhead and efficiency of these schemes, are thoroughly examined and contrasted. A detailed analysis of V2V, V2I, and V2X authentication is been reported. Various cryptographic schemes have been discussed along with some advanced techniques such as Blockchain and hybrid schemes. An overview of the integration of 5G/6G networks is documented.

Applications of VANET have been discussed in detail along with some open challenges in VANET.

Adi El-Dalahmeh *et al.,* (2024), evaluated seven cryptographic algorithms, including Blowfish, data encryption standard, triple data encryption standard, Rivest–Shamir–Adleman, advanced encryption standard (AES),advanced encryption standard with elliptic curve cryptography (AES-ECC), and advanced encryption standard with elliptic curve Diffie-Hellman (AES-ECDH),in a simulated SDN-based VANET. The findings show AES-ECDH as the most effective overall, though the best choice depends on specific deployment scenarios and application needs

Bayat *et al.,* (2020) introduced a novel authentication scheme for VANET, suggesting a new solution for secure vehicle communications. The proposed scheme is a road side unit (RSU) based scheme in which the master key of the Trusted Authority (TA) is embedded in a tamper-proof device provided at the RSUs. Compared with the schemes that store the master key in the on-board units, our scheme is more practical because of a secure and high-speed communication link between TA and RSUs. The proposed protocol is vulnerable to impersonation and replay attacks due to the lack of freshness of the messages exchanged between vehicles.

Alfadhli *et al.,* (2020) developed a lightweight multi-factor authentication and privacy-preserving security solution for VANET. Combination of physically unclonable functions (PUF) and one-time dynamic pseudo-identities as authentication factors is focused. Furthermore, it eliminates the heavy dependency on the system key by decentralizing the wide precinct of the certificate authority (CA) into regional domains and achieves robust control of domain keys. A detailed analysis demonstrates that our scheme efficiently meets the VANET security requirements and offers more suitable communication and computation costs and features than existing schemes. The proposed approach relies on a centralized entity for certificate revocation, which can be a single point of failure and affect the system's scalability. The proposed approach relies on a centralized entity for certificate revocation, which can be a single point of failure and affect the scalability of the system.

Mahmood A. Al-Shareeda et al., (2021) proposed SE-CPPA scheme is based on the cryptographic hash function and bilinear pair cryptography for the signing and verifying of messages. Through security analysis and comparison, the proposed SE-CPPA scheme can accomplish security goals in terms of formal and informal analysis. More precisely, to resist impersonation attacks, the true identity of the vehicle stored in the tamper-proof device (TPD) is frequently updated, having a short period of validity. Since the MapToPoint hash function and a large number of cryptography operations are not employed, simulation results show that the proposed SE-CPPA scheme outperforms the existing schemes in terms of computation and communication costs. Finally, the proposed SE-CPPA scheme reduces the computation costs of signing the message and verifying the message by 99.95% and 35.93%, respectively. Meanwhile, the proposed SE-CPPA scheme reduces the communication costs of the message size by 27.3%.

Bindu *et al.,* (2020), a novel multi-scroll attractor (MSA) based chaotic Henon maps encryption approach is proposed. The vehicular ad hoc networks are vulnerable to security threats while communication is established in wireless made proper encryption scheme can aid in establishing effective and secure communication. Conventionally group key agreement model (GKA) scheme is widely used for enabling security in VANET networks which is insignificant because of their over-exploitation of resources in the network. The proposed scheme does not provide protection against message tampering or replay attacks.

Abdueli Paulo Mdee *et al.,* (2022) presented the impacts of LPPSs on vehicular applications, contrary to most of the existing surveys that focus on detailed comparative analysis of LPPSs. This is the first survey comprehensively debating the effects of LPPSs on vehicular applications to the best of our knowledge. As a result, this survey will help identify techniques that work best for certain applications. In addition, it will help highlight necessary modifications to the LPPSs to preserve the Quality of Services (QoS) of VANETs applications.

Ogundoyin *et al.,* (2020) proposed an efficient CPPA scheme for VANET based on elliptic curve cryptography without relying on any hardware device. The scheme satisfies the security and privacy requirements of VANET, solves private key compromise

problems, and provides countermeasures against privilege escalation. The scheme is existentially secure against an adaptive chosen message and identity attacks in the random oracle model based on the hardness of the elliptic curve discrete logarithm problem. The proposed scheme does not provide a mechanism for revoking compromised identities, which could result in security vulnerabilities.

Table 2.2 summarizes various techniques and methods for ensuring security in vehicular ad hoc networks (VANET).

Table 2.2: Review of Cryptographic Techniques in VANET

Author and Year	Techniques / methods	Significance	Limitations
Sajini et al., (2023)	ASCII-ECC	The proposed scheme is a TA-based security framework in which vehicle and user registration is performed via OBUs, ensuring identity verification and authorization. The use of ASCII-ECC enhances message confidentiality, offering better performance and resistance to unauthorized access in dynamic VANET environments.	The proposed scheme does not provide a mechanism for revoking the compromised identities, which results in security vulnerabilities.
Bala et al., (2023)	BTLB-PP authentication system	This system significantly enhances VANET security by enabling reliable, privacy-preserving vehicle authentication through blockchain-based trust management. It ensures secure collaboration among vehicles while protecting location privacy and preventing malicious activities.	Vulnerable to collusion attacks, where malicious vehicles manipulate trust evaluations to gain unauthorized access

Author and Year	Techniques / methods	Significance	Limitations
Rajkumar and Kumar (2024)	Certificate-less signature aggregation method based on ECC	This method uses the certificate less signature aggregation and formal security proofs to guarantee complete privacy protection and strong security in VANETs.	This system vulnerable to some sophisticated attacks, such side-channel or insider attacks, which are not adequately handle by this method.
Sudhakar et al., (2024)	ETESLTA for VANETs	By providing a lightweight yet robust authentication mechanism, ETESLTA ensures that vehicles securely exchange information without compromising user privacy or overwhelming system resources.	The cuckoo filter's probabilistic design introduces false positives, which affect authentication accuracy in situations with a high vehicle density.
Shayea et al., (2022)	ECC-GA-PASR	This method significantly improves high-speed VANET performance by optimizing RSU distribution using a GA, which enhances network coverage and efficiency and integrating	There is a need to providing hybrid security to increase speed.

Author and Year	Techniques / methods	Significance	Limitations
		authentication strengthens security while minimizing computational overhead.	
Shawky et al., (2023)	BCSKE	This scheme enhances authentication efficiency in VANETs by reducing cryptographic overhead through physical-layer key extraction and ensures secure and tamper-proof key reconciliation.	The proposed scheme lacks forward secrecy, as compromised key, which affect the confidentiality of prior communications
Nova et al., (2023)	Floyd–Warshalls algorithm and modified advanced encryption for VANETs.	The proposed security framework significantly enhances Sybil attack detection accuracy while preserving user privacy in VANETs, also ensures efficient and secure data transmission.	The proposed scheme does not provide protection against message tampering or replay attacks.
Aghabagherloo et al., (2022)	Efficient and Physically Secure Privacy-Preserving Authentication Scheme	The proposed scheme enhances VANET security by ensuring anonymity, unlinkability, and tamper detection even under physical attacks. It achieves lower communication overhead without relying on continuous RSU interaction, making it both efficient and resilient.	It still depends on recurring key updates, which makes synchronization difficult in extremely dynamic vehicle settings.

Author and Year	Techniques / methods	Significance	Limitations
Abdelfatah et al., (2021)	SVAP scheme for VANET.	The proposed protocol ensures lightweight, secure authentication with non-repudiation for VANET, reducing computation and storage overhead while eliminating the need for secure channels during parameter distribution.	The proposed scheme does not provide a mechanism for revoking compromised identities, which could result in security vulnerabilities.
Al-Shareeda and Manickam, (2022)	MSR-DoS scheme	The proposed scheme also supports batch verification to significantly reduce computational costs. According to the analysis of security, our scheme is sufficiently resistant to several common attacks in VANET.	Inability to do batch verification and the reliance on cloud computing, which result in scalability and latency problems

Various techniques and methods have been proposed to address the security concerns in vehicular networks, such as cryptographic schemes, multi-factor authentication, and privacy-preserving authentication schemes. These techniques aim to ensure authentication, integrity, and confidentiality while considering the constrained computational environment of vehicular networks. However, some of these proposed solutions have limitations, such as a lack of efficiency, vulnerability to attacks, and scalability issues.

2.4.2 Review on ML-based IDS in VANET

Vehicular Ad-hoc Networks (VANET) offer a promising future for intelligent transportation, enabling applications like collision avoidance and cooperative driving.

However, the open and dynamic nature of VANET makes them vulnerable to various security attacks. Intrusion Detection Systems (IDS) play a crucial role in safeguarding these networks by identifying and preventing malicious activities.

Traditional signature-based IDS are effective against known attacks, but struggle to adapt to novel threats. Machine Learning (ML) offers a powerful alternative, enabling IDS to learn from network traffic patterns and detect anomalies indicative of attacks. This review explores the potential of ML-based IDS in VANET.

Alladi *et al.,* (2021) propose an anomaly detection framework for VANET based on deep neural networks (DNNs) using a sequence reconstruction and thresholding algorithm. The DNN architectures are deployed on the roadside units (RSUs) that receive the broadcast vehicular data and run anomaly detection tasks to classify a message sequence as anomalous or genuine. Multiple DNN architectures are implemented in this experiment and their performance is compared using key evaluation metrics. Performance comparison of the proposed framework is also drawn against the prior work in this area. The proposed approach requires a large amount of training data, which can be difficult to collect in a VANET environment.

Kathole *et al.,* (2025) introduced an efficient fuzzy ranking with ensemble ML network to detect attacks in VANET. This begins by sourcing network traffic data from online repositories, which is then subjected to a data cleaning phase to eliminate inconsistencies and noise. For effective feature dimensionality reduction and selection, a Modernized Random Parameter-based Green Anaconda Optimization (MRP-GAO) algorithm was introduced to perform Optimal Weighted Feature Selection (OWFS), ensuring the most relevant features were retained. Subsequently, an Ensemble Machine Learning Model (EMLM) was constructed, incorporating Bayesian Network, AdaBoost, SVM, and MLP classifiers to improve detection accuracy through diverse learning strategies. To further refine the classification decision, a fuzzy ranking method was applied to aggregate the ensemble outputs and yield the final attack detection verdict. Despite its improved detection accuracy and adaptability, this system has high computational complexity due to ensemble learning and metaheuristic optimization.

Shu *et al.,* (2020) developed deep learning with generative adversarial networks and explore distributed SDN to design a collaborative intrusion detection system (CIDS) for VANET, enabling multiple SDN controllers to jointly train a global intrusion detection model for the entire network without directly exchanging their sub-network flows. The proposed scheme requires a high number of message exchanges, which can result in high communication overhead and delay.

Bangui *et al.,* (2021) a hybrid ML model to enhance the performance of IDSs by dealing with the explosive growth in computing power and the need for detecting malicious incidents timely. The proposed approach mainly uses the advantages of Random Forest to detect known network intrusions. Besides, there is a post-detection phase to detect possible novel intruders by using the advantages of corsets and clustering algorithms. Variations in network conditions and attacker behaviors can affect the performance of the intrusion detection system.

Gonçalves *et al.,* (2021) Intelligent Hierarchical Intrusion Detection System (IDS) divide the network into four levels, each of them into multiple clusters, enabling the usage of different Machine Learning (ML) based detection techniques. The communications between all the hierarchy entities are secured using Vehicular Ad hoc Network Public Key Infrastructure and Attribute-Based Encryption with Identity Manager Hybrid (VPKIbrID). This hybrid model takes advantage of multiple techniques to fulfill several communication requisites for secure VANET communications.

Kadam, and Krovi, (2021) presented a Hybrid KSVM (KNN and SVM) framework for enhancing security in VANET. The proposed approach integrated the strengths of KNN in handling nonlinear data patterns with the classification capabilities of SVM to effectively detect DDoS attacks. However, this approach is limited to the detection of DDoS attacks only, and its effectiveness against other attack types such as DoS and Sybil attacks remains unexplored.

Anyanwu *et al.,* (2022) proposed solution employed the Radial Basis Function (RBF) kernel of the Support Vector Machine (SVM) classifier and an exhaustive parameter search technique called Grid Search Cross-Validation (GSCV). In this

framework, the proposed architecture can be deployed on each vehicle's On-Board Units (OBUs), which receive the vehicular data and run intrusion detection tasks to classify a message sequence as a DDoS attack or benign. The performance of the proposed algorithm compared to other ML algorithms using key performance metrics. The trade-off between detection accuracy and computational complexity in a VANET environment existed.

Gad *et al.,* (2021) the vast majority of existing research is based on NSL-KDD or KDD-CUP99 datasets. Recent attacks are not present in these datasets. As a result, we employed a realistic dataset called ToN-IoT that derived from a large-scale, heterogeneous IoT network. VANET make the network vulnerable to various types of attacks, such as denial of service (DoS) and distributed denial of service (DDoS). Many researchers are now interested in adding a high level of security to VANET. Machine learning (ML) methods were used for constructing a high level of security capabilities based on intrusion detection systems (IDSs). The proposed intrusion detection system was against different types of attacks and in various VANET scenarios.

Table 2.3 summarizes the techniques and methods proposed based on machine learning in various research papers for securing vehicular networks. The significance of these techniques is highlighted, such as the need for authentication, confidentiality, and privacy preservation in constrained computational environments. However, limitations of these techniques are also pointed out, including the lack of efficient implementation, vulnerability to certain attacks, and dependence on centralized entities that could result in security vulnerabilities.

Table 2.3: Review on ML-based IDS in VANET

Author and Year	Techniques / methods	Significance	Limitations
Alladi et al., (2021)	Deep neural networks (DNNs) using a sequence reconstruction	Anomaly detection tasks receiving broadcast vehicular data classified message as anomaly or genuine. With	19 anomalies including DoS attack were detected using a single threshold. A

Author and Year	Techniques / methods	Significance	Limitations
	and thresholding algorithm was the anomaly detection framework deployed on RSUs.	multiple DNN architectures, among multiple, the proposed framework detected the anomalous sequences with 98% accuracy.	new potential threshold must be calculated for detecting other anomalies.
Kathole, J et al., (2025)	Efficient fuzzy ranking with ensemble ML to detect and classify attacks in VANET	Enhances attack detection accuracy in VANETs by combining optimal feature selection with ensemble learning, thereby improved network security and reliability in dynamic vehicular environments.	The system has high computational complexity due to ensemble learning and metaheuristic optimization.
Bangui et al., (2021)	Hybrid ML model with Random Forest and post-detection phase with clustering algorithms	Enhanced the IDS performance. Detected known network intrusions and also possible novel intruders were detected in post-detection phase.	Performance of the IDS affected by the variations in network conditions and attacker behaviors.
Anyanwu, G.O., (2022)	Proposed an Intrusion Detection Model (IDM) with the Radial Basis Function (RBF),	Proposed architecture deployed on the OBUs of each vehicle receiving the vehicular data and run intrusion detection tasks to classify a message sequence as a DDoS	Space and memory computational analysis for SDN-VANET is the future direction.

Author and Year	Techniques / methods	Significance	Limitations
	kernel of the SVM classifier and an exhaustive parameter search technique called Grid Search Cross-Validation (GSCV).	attack or benign. Outperformed existing benchmarks with overall accuracy of 99.33%, detection rate of 99.22% and an average squared error of 0.007.	
Kadam, and Krovi, (2021)	Hybrid KSVM	Hybrid KSVM framework significantly enhances the accuracy and reliability of detecting DDoS attacks in VANETs, by combining strengths of KNN and SVM, thereby improving the overall security and safety.	Limited to the detection of DDoS attacks only, and its effectiveness against other attack types such as DoS and Sybil attacks remains unexplored
Gonçalves, F et al., (2021)	Proposed an Intelligent Hierarchical Security Framework for VANET making use of Machine Learning (ML) algorithms.	Enhanced attack detection using the VPKIbrID model and its ABE mode for secure communications among entities, assuring strong authentication, privacy, and anonymity. Attack detection is done at multiple levels, using different algorithms for each level, according to the corresponding needs and characteristics with a low False Positive Rate	Impact of the burden of the amount of data communicated between the different levels, analyzing the usage of compression to reduce the size of the communication data.

Author and Year	Techniques / methods	Significance	Limitations
Gad, A.R et al., (2021)	Proposed IDSs with 8 strategies, in particular logistic regression (LR), naive Bayes (NB), decision tree (DT), SVM, kNN, random forest (RF), AdaBoost, as well as XGBoost.	A realistic dataset called ToN-IoT was employed and tested various ML methods in both binary and multi-class classification problems. XGBoost method outperformed other ML methods with 98% accuracy.	Optimization algorithms for dimensionality reduction to apply in future.

The ML – based IDS techniques mentioned above provided the significance, such as the need for authentication, confidentiality, and privacy preservation in constrained computational environments.

In addition to detecting attacks and securing VANET, the IDS also lacks in variations in network conditions and attacker behaviors can affect the performance of the intrusion detection system and there is a need to develop effective security solutions to ensure the secure and reliable operation of VANET using immune techniques.

The security solutions based on cryptographic techniques and intrusion detection based on machine learning techniques were efficient and provided more accurate results in detection. But to provide a secure implementation of VANET architecture only attack detection is not sufficient it is necessary to provide immunity against attacks by developing AIS-based security solutions. For a truly secure VANET architecture, a proactive approach is crucial. Artificial Immune AIS-based security solutions come in for VANET to have a built-in defense system that can adapt and learn from encountered threats, similar to the human immune system

The section below provides the existing research work based on AIS for securing VANET.

2.4.3 Review on AIS in Securing VANET

Incorporating AIS in VANET makes it to move beyond just reacting to threats and develop immunity against them. This can lead to a more robust and secure communication network for vehicles. Inspired by the human immune system's remarkable ability to learn and adapt to new threats, Artificial Immune Systems (AIS) offer a distributed and adaptive approach to VANET security. Just like our bodies constantly fight off infections, AIS-enabled vehicles can learn from encountered attacks, share information with each other, and continuously improve their defenses. This distributed approach strengthens the overall security of the network, making it more resilient.

Several AIS algorithms are being explored for VANET security, including Negative Selection, Clonal Selection, and Dendritic Cell Algorithms. AIS can be combined with traditional security methods like cryptography and access control to create a layered defense system for VANET. The consolidated view of the existing AIS based security solutions for VANET is emphasized below.

Jamaesha *et al.,* (2024), suggested the Dendritic Cell with Adaptive Trust Q-learning Protocol (dDC-ATQP), which combined reinforcement learning with a biologically inspired trust evaluation mechanism to provide a clever and safe routing technique. In particular, the trust mechanism improves network security and dependability by continually observing and assessing node activity in order to identify and isolate hostile nodes. Concurrently, the adaptive Q-learning-based routing technique lowers latency and boosts transmission efficiency by dynamically choosing the best routes depending on this network conditions. Initial routing performance in quickly changing topologies impacted by the convergence time of Q-learning, and the learning-based trust mechanism impose computational cost in situations with limited resources.

Jim et al., 2022, proposed a new bio-inspired algorithm, namely Artificial Immune System Based Algorithm (AISBA). MANET nodes provide the transmission

capability to receive, transmit and route traffic from a sender node to the destination node. In this paper, we design an artificial immune system-based security method for MANET by simulating the mechanism of the human immune system. Limited evaluation of the impact of AIS-based approach on network efficiency and delay were performed.

Goyal et al., 2023, developed a Misbehavior Detection using Temporal Fusion Transformer. Trust and Node Cooperation are the most crucial factors on which C-ITS relies as the decisions that are taken by a vehicle are based on the data and information it gets from the network infrastructure that is installed on the roadsides which is basically a pool of information which has been gathered from other vehicles and smart infrastructures that are part of the VANET. The presence of any misbehavior in the network or a compromised node in the transport network system will lead to atrocious results for both traffic and network safety. AIS-based approach may be vulnerable to attacks that specifically target the immune system-based algorithms.

Kumar et al., 2021, developed a Vehicular middleware and heuristic approaches for intelligent transportation system of smart cities. The middleware and heuristic approaches of the vehicular system are essential for designing and analyzing research problems related to smart cities. Limited evaluation on the impact of AIS-based solutions on the quality of service (QoS) provided by the network.

Jagriti and Lobiyal., (2022), introduced the Vehicular Adhoc Networks (VANETs) paradigm's Adaptive Layer Positive Selection Algorithm (ALPSA) to solve the problems of instability and anomaly detection in Virtual Traffic Light (VTL) systems. As self-organized traffic control systems, VTLs frequently have problems like abandoned cars after cluster formation, which lowers traffic safety and efficiency. Through the Positive Selection Algorithm (PSA), the proposed ALPSA combined AIS concepts to dynamically monitor and regulate vehicle involvement. A mobility model that produced clustering metrics to improve the clustering process comes before the method's layered algorithmic structure, which operates in two stages. PSA-generated detectors find non-participating cars, allowing for a quick and flexible reaction to cluster formation or reformation. This method uses behavior-based detection. It is vulnerable to adversarial attacks like Sybil attacks, detector poisoning, and false data injection.

Table 2.4: Review of AIS in VANET

Author and Year	Techniques / methods	Significance	Limitations
Jamaesha et al., (2024)	dDC-ATQP in MANET	This protocol significantly enhances the security and efficiency of MANETs by intelligently detecting malicious nodes and adapting routing decisions in real-time.	In quickly changing topologies impacted by the convergence time of Q-learning, and the learning-based trust mechanism impose computational cost in situations with limited resources
Jim et al., (2022)	Artificial Immune System Based Algorithm (AISBA) without learning stage - principles of Artificial Immune Systems (AIS). Two different Trust models developed distinguishing a genuine node and a selfish node.	Average detection rate achieved - 93.41%. Compared with Secured AODV(SAODV) protocol with 87% (only 37% in SAODV) of PDR, 94% (only 86% in SAODV) detection rate.	Only detection focused. The immune system not able to identify other types of attacks.
Goyal, A et al., (2023)	Trust and Node Cooperation are the most crucial factors.	C-ITS relying on the decisions that are taken by a vehicle are based on the data and information it gets from the network	AIS-based approach vulnerable to attacks that specifically target the immune system-based algorithms.

Author and Year	Techniques / methods	Significance	Limitations
		infrastructure that is installed on the roadsides. Detected misbehaviour in the system using Deep Learning techniques.	
Kumar et al (2021)	Vehicular middleware and heuristic approaches for intelligent transportation system	Detected misbehaviour in the system.	Limited evaluation on the impact of AIS-based solutions on the quality of service (QoS) provided by the network.
Jagriti and Lobiyal., (2022)	ALPSA	ALPSA enhances the reliability of Virtual Traffic Lights by dynamically detecting and managing anomalous vehicle behavior in real time. It significantly improves traffic coordination through reduced detection time and increased clustering accuracy in VANET environments.	This method uses behavior-based detection, it is vulnerable to adversarial attacks like Sybil attacks, detector poisoning, and false data injection.

Table 2.4 provides an overview of various techniques and methods used for improving the security of vehicular ad hoc networks (VANET) using artificial immune systems (AIS) based intrusion detection systems (IDS). These approaches detect and prevent various security attacks in VAET with proving an enhanced

immunity however it has some limitations. The limitations of the proposed methods indicate the need for further research to detect single point of failure and improper blockage of malicious nodes and there is a need to further improve the security of VANET.

Observations from the literature highlight that the security solutions developed resolved the DoS and DDoS attacks by detection and prevention, isolation of DoS attacks still experienced gaps in providing security in VANET.

The research gaps identified are

- Cryptography-based solutions play a crucial role in ensuring the security of VANET communications but have limitations in key management on malicious nodes detection and depend on the system specific requirements.
- Cryptographic techniques and machine learning techniques results in high communication overhead and delay.
- AIS based approaches may be affected by factors such as the size and density of the network, detectors.
- Vulnerability to certain hybrid form of attacks.

The inference obtained from the literature study is the need for securing of VANET against DoS attacks and its types with immunized behavior with services.

2.5 Conclusion

This chapter has presented a comprehensive overview of existing research on securing VANET against DoS attacks. The literature reveals a growing concern about the vulnerabilities of VANET to these attacks and the potential consequences for traffic safety and efficiency. A variety of approaches, including intrusion detection, prevention, trust management, and resource management, have been proposed to mitigate DoS attacks. However, there is a lack of consensus on a unified and comprehensive defense strategy.

Moreover, the concept of self-healing and immunization has emerged as promising approaches to enhance VANET resilience. While some studies have explored these concepts individually, their integration into a holistic security framework remains limited.

The review of existing literature has identified research gaps, including the need for more effective and efficient DoS attack detection methods, the development of robust self-healing mechanisms, and the exploration of advanced security techniques to address emerging threats. These gaps provide opportunities for further research to strengthen VANET security.

2.6 Chapter Summary

The chapter summarizes the key findings and emphasizes the importance of continued research on DoS attacks in VANET. It highlights the need for robust security measures to ensure the safety and reliability of vehicular communication systems. The chapter analyzes various defense strategies proposed in the literature to mitigate DoS attacks in VANET.

From the analysis, it is obvious that VANET security based on various techniques and methods has been reviewed to determine the possibilities for enhancing the security of VANET. These techniques include cryptographic techniques, intrusion detection based on AIS and machine learning based techniques. However, these techniques were with limitations such as such as high communication overhead, lack of efficiency, vulnerability to certain hybrid form of attacks, and a single point of failure for certificate revocation. The hybrid approaches were attempted recently for VANET security based on optimization algorithm, machine learning and deep learning.

The problem still exists to develop effective and efficient countermeasures to protect VANET from various DoS attacks while preserving their real-time performance, reliability, and safety. In this research, one such attempt is made based on hybrid approach combining multiple security mechanisms to create a robust defense against DoS attacks and its types.