2024 Eighth International Conference on Parallel, Distributed and Grid Computing (PDGC) | 979-8-3315-2134-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/PDGC64653.2024.10984030

Denial of Service (DoS) Attacks in SDN-Based VANETs: A Study

Jyotsana Sardana
Dept. of Computer Science & Engg.
Guru Jambeshwar University of Science and Technology, Hisar (Haryana), India
sardana.0410@gmail.com

Sunil Kumar
Dept. of AI & Data Science
Guru Jambeshwar University of Science and Technology, Hisar (Haryana), India
sunilkaushik27@gmail.com

Dharminder Kumar
Dept. of Computer Science & Engg.
Gurugram University, Gurugram (Haryana), India
dr_dk_kumar_02@yahoo.com

Kamlesh Dutta
Dept. of Computer Science & Engg.
National Institute of Technology, Hamirpur (H.P.), India
kd@nith.ac.in

***Abstract*—Vehicular ad hoc networks (VANETs) play a vital role in ensuring the success of Intelligent transport systems (ITS), but the architecture of VANETs is vulnerable to several security attacks. There are also some challenges associated with VANETs such as the management of large-scale dynamic heterogeneous networks and secure communication over the network. The research community stressed on the integration of Software-defined Networking (SDN) with traditional VANETs to address these challenges. The SDN enhances the functionality of traditional VANETs by adding a centralised control mechanism, programmability, and flexibility features.The SDN also mitigates some security issues in VANETs to a limited degree. However, SDN's inherent features introduce new security vulnerabilities mainly in the control plane. This paper first examines the characteristics of SDN when integrated with VANETs. Then, this paper discusses the new security vulnerabilitiesthat arise as a result of the integration of SDN into VANET architecture. The mostcritical security attack in SDN-based VANETs is Denial of Service (DoS) attack. This paper also examines different types of DoS attacks in SDN-based VANETs along with their potentialdefence mechanisms. Finally, this paper highlights the future research directions in the domain of securing the network operations of SDN-based VANETs.**

Keywords—SDN-based VANETs, Vulnerabilities, Security Threats, Denial of Service (DoS) attacks.

I. INTRODUCTION

The increase in the number of vehicles on the roads has also raised significant traffic and safety-related challenges such as accidents, traffic congestion, and network inefficiency. Vehicular ad hoc network (VANET) has emerged as an important and integral component of the Intelligent Transportation System (ITS) and a potential solution to handle traffic and safety-related challenges on the roads [1]. It plays a very significant role in reducing road accidents, enhancing road safety, and improving overall traffic management. VANET is a subclass of Mobile Ad-hoc Network (MANET) where vehicles act as mobile nodes.In VANETs, multiple-level communications are possible such as Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-pedestrians (V2P),and infrastructure-to-infrastructure (I2I) through DSRC and cellular technology (4G / 5G) to deliver the safety and non-safety messages properly among the nodes [2]. There are numerous applications of VANETs such as emergency alert and response, platooning, real-time traffic updates/notifications, collision avoidance, prediction of road topology, parking spot location, navigation, entertainment etc.Besides these attractive applications of VANETs, some challenges are associated with VANETs. These challenges include the management of large-scale dynamic heterogeneous networks, secure communication over the network, quality of service (QoS) etc [3].The research community stressed on the integration of Software-defined Networking (SDN) with traditional VANETs to address these challenges. The SDN has the potential to address these challenges by offering centralized control, programmability, and efficient network management [4]. According to Sultana, Grover, and Tripathi [5], integrating SDN with VANETs offers a promising solution for enhancing dynamic resource allocation, centralized control, and overall network flexibility. The inherent characteristics of SDN also facilitate the effective deployment of intrusion detection and prevention systems, effective trafficmonitoring and filtering, and better congestion control.However, the integration of SDN with VANETs introduces several new security challenges, particularly Denial of Service (DoS) attacks, which can significantly disrupt normal network operations [6].

The integration of SDN with VANETs creates a vulnerable environment for Denial of Service (DoS) attacks due to the central control mechanism of SDN controller and the distributed nature of VANETs [7]. The sole purpose of DoS attacks is to prevent the intended users from accessing the available resources and services. In SDN-based VANETs, attackers can easily compromise vehicle nodes and SDN controllers to execute DoS attacks [8]. When multiple malicious (compromised) nodes across the network execute DoS attack, it becomes Distributed DoS (DDoS) attack [9]. The DDoS attacks are very dangerous and hard to be addressed in real time. DoS attacks can be classified into two main types: vulnerability-based attacks, which exploit

vulnerabilities in the target's system, and flooding attacks, which overwhelm the network with massive amounts of bogus traffic/service requests [10,11]. The distributed and cooperative architecture of VANETs and the centralized mechanism of SDN controllers are exploited by the attackers to launch DoS attacks. These attacks cause network resource overload, communication loss, and unavailability of services [5]. These attacks are particularly very dangerous in SDN-based VANETs. They can have a severe impact on critical vehicular applications such as collision avoidance systems and real-time traffic updates.The disruption in these applications could have catastrophic consequences. It would undermine the safety and efficiency of vehicular communication systems[12].

According to Cloudflare's report [13], DNS-based DDoS attacks have seen an 80% annual increase, accounting for 33% of total attacks, followed by HTTP DDoS attacks (37%) and other Layer 3/4 attacks (30%). These attacks have a significant global impact. The Stormwall report [14] highlights a growing trend of DDoS attacks motivated by geopolitical factors. Israel, despite its relatively small size, has become the fourth most targeted country for DDoS attacks globally, following China (12.6%), the USA (12.2%), and India (11.7%). This emphasizes the urgent need for effective defensive mechanisms to counteract DoS attacks and ensure the reliability, trustworthiness, and safety of networks. The research community are working towards designing security solutions for SDN-based VANETs but paid limited attention towards designing security solutions to counteract the DoS attacks. To the best of our knowledge, while many studies have acknowledged the severity of DoS attacks, a detailed layer-wise analysis of these attacks within SDN-based VANETs remains unaddressed. The main objective of this paper is to present the layer-wise analysis of DoS attacks within SDN-based VANETs along with their defensive mechanisms.

The remainder of the paper is structured into VI sections. Section II provides the study of related work in the domain of security of SDN-based VANETs. Section III describes the architecture of SDN-based VANETs. Section IV carries out the study of denial of service (DoS) attacks in SDN-based VANETs by classifying them layer-wise. The future research directions in the domain of security of SDN-based VANETs are highlighted in section V and finally, section VI concludes the paper.

II. Related Work

Rampaul, Patial, and Kumar [12] analyzed various attackers in VANETs, focusing on DoS and DDoS scenarios in V2V and V2I communications. In [15], Krishna and Reddy presented a layer-wise classification of DDoS attacks in VANETs, highlighting their network impact, and potential countermeasures. Singh and Behal [16] reviewed 70 DDoS detection and mitigation mechanisms in SDN, classifying them into information theory-based, machine learning, ANN-based, and heterogeneous methods, and also addressed deployment challenges. Similarly, Wang and Li, [17] explored DDoS detection techniques in SDN, categorizing them into entropy-based, machine learning, and deep learning approaches, while addressing data preprocessing and security challenges. In [18], Tamakloe et al. analyzed DoS and DDoS attacks on SDN, discussing their impact, vulnerabilities, and mitigation strategies. The mitigation techniques were classified into statistical analysis, machine learning, deep learning, policy-based techniques and moving target defense techniques. Additionally, the authors also examined anomaly detection, flow rule updates, and entropy-based models for attack detection and prevention. Eliyan, Fayez, and Di Pietro [19] focused on internal and external approaches for detection, mitigation, and prevention. The solutions are classified into categories such as detection, mitigation and prevention with highlighting each approach utilizing specific tools and techniques to address the security challenges in SDN. In [20], Adhikary et al. presented a hybrid detection approach combining SVM kernel methods (AnovaDot and RBFDot) to detect DDoS attacks in VANETs. This approach achieved higher accuracy and efficiency by simulating real-time network conditions like collisions and packet drops.

III. Architecture of SDN-based VANETs

A. VANETs

The architecture of VANET consists of three main components: vehicles, roadside units (RSUs), and network infrastructure [3]. VANET communications operate in two domains: the ad hoc domain and theinfrastructure-based domain [4]. VANET is highly vulnerable to security attacks due to inherent characteristics of VANET such as distributed nature,high mobility, and reliance on wireless communication [5].The exponential riseof vehicles in the network results in critical challenges such as scalability management, handling heterogeneous nodes, and providing swift responses to vehicle requests. To meet these challenges, an architecture is required to be integrated with VANET which provides centralized control, flexibility, automation, decoupled network control and forwarding functions [6].

B. Software-defined Network (SDN)

SDN has drastically changed the conventional network design by separating the control plane (handlesnetwork administration) from the data plane (handles traffic forwarding) [21]. SDN improves the flexibility and efficiency of the network as compared to traditional networks [21]. OpenFlow protocols are used in SDN forproper interaction of data and control layers with each other. The centralized control mechanisms, flexibility, handling scalability, automation, programmability, and simplified network management are the main features of SDN[22]. Due to these attractive features, SDNhas become the foundation of modern network technologies. SDN has diverse applications in areas like smart cities, smart grids, smart healthcare systems, vehicular networks, 5G systems etc [23]. The architecture of SDN consists of three separate layers: data layer, control layer and application layer. The data layer consists of OpenFlow-enabled switches and devices that manage packet forwarding based on flow rules defined by the SDN controller

[24].The control layer utilizes SDN controllers such asNoX (network operating system) and PoX(Python-based controller) to manage network operations on a wide scale.The SDN controller provides a bird's-eye view of the entire network with comprehensive knowledge and control over all network components (switches, routers, and links). This global perspective enables the controller to optimize network traffic, ensure quality of services and implement security policies across the entire network in a way that traditional networking architecture couldn't achieve. SDN brings flexibility and efficiency through centralized control, programmability, and third-party application integration. However, these features also introduce significant challenges. SDN suffers several key challenges such as single point of failure, scalability bottlenecks, and control plane overload due to its centralized control, even making the controller a prime target of attackers [25]. The programmability characteristic introduces development complexity and risks of bugs and vulnerabilities. The reliance on third-party applications introduces security risks and lack of trust and standardization issues [26].

C. SDN-based VANETs

The integration of SDN with VANET enhances the capabilities of VANET by addressing its challengessuch management of large-scale dynamic heterogeneous networks, secure communication over the network and quality of service (QoS). By leveraging features of SDN, this integrationenables effective resource management and adaptive network control in VANET [5,8].This integrated design improves vehicle-to-everything (V2X) communication, congestion control, and real-time traffic management[3]. The programmability features improve efficiency, and effective utilization of dynamic resources[4]. The centralized control mechanism also addresses some of the security concerns associated with traditional VANETs [5]. All these features make SDN-based VANETs a modern vehicular network environment.The three-layer architecture of SDN-based VANETsprovides a comprehensive framework as shown in Figure 1. It is a model of efficient network management and communication.

- **Application Layer**: The application layer provides servicessuch as traffic management, mobile management, resource management, security services, and routing services to end users [2]. The application layer interacts with the control layer through northbound APIs (e.g., REST) for high-level management [3].
- **Control Layer:**The SDN controller in the control layer plays a crucial role. It analyzes network traffic, manages traffic flow, enforces policies, and allocates resources. In order to support ongoing network operations effectively, the control layer collects information from the data layer via southbound APIs (e.g., OpenFlow) and transmits it to the application layer via northbound APIs [23].
- **Data Layer:** The data layer is responsible for processing and forwarding data as directed by the SDN controller. This layer assists in making real-time decisions on routing, traffic management, and security by leveraging the control layer's functionalities through OpenFlow protocols. The vehicles and infrastructure of VANETs become integral components of this layer [24].

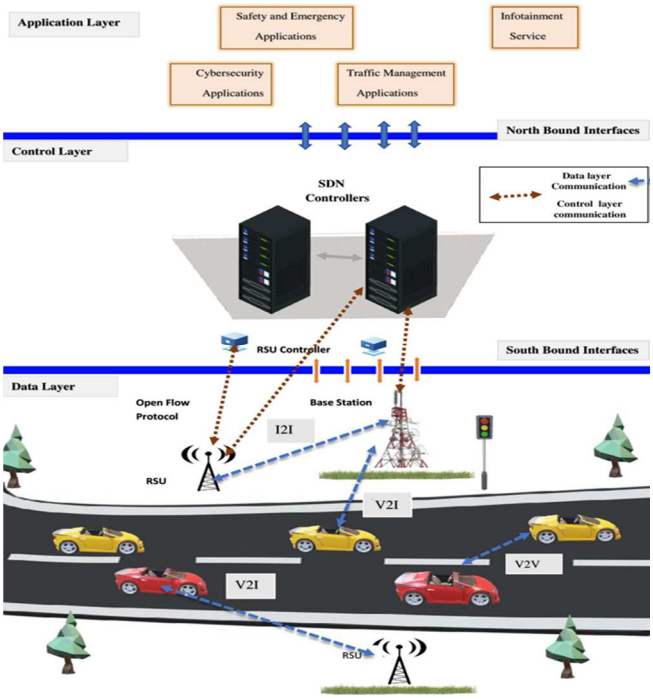

Fig 1. Architecture of SDN-based VANETs

The integration of SDN with traditional VANETs offers an effective solution to the security challenges posed by dynamic and decentralized vehicular environments. SDN separates the data and control planes, allowing centralized and flexible programmable network environment management.

TABLE I. VULNERABILITIES IN INTEGRATING SDN IN VANETS

Vulnerability	Root Cause	Attacks	Impact
Controller Vulnerability [25]	Centralized architecture, single-point-of-failure	Controller saturation due to packet flooding, controller compromised	DDoS attacks overload the controller, disrupting all network services.
Open Programmable Interfaces [26]	Unrestricted access to northbound and southbound APIs	Interface exploits, configuration overload	Malicious applications exploit open interfaces; compromised devices to launch DDoS.
Flow-based Forwarding [27]	Limited capacity of switch flow tables	Flow table overflow, flow rules manipulation	Tampered flow rules, reroute traffic, create disruptions, deplete resources, and deny legitimate requests.
Programmability [28]	Insufficient authenticatio n and lack of rate limiting	Network topology poisoning, misrouting traffic, integrity compromise	Misrouting critical data through fake/unsecure routes; altered or dropped packets affect safety-critical applications.
Dynamic Network Topology [6, 7]	Frequent topology changes due	Denial of service, false data injection,	Safety message delays, increased latency, routing overhead, network

	to high node mobility	node overload, routing protocol exploitation	congestion, compromised data integrity and availability.

The integration of SDN with VANET enhances its ability to address some of the security threats through central control mechanisms, dynamic resource allocation and responses in real-time. SDN can detect and mitigate DoS attacks to a limited extent by reconfiguring the network and isolating malicious entities [29]. The centralized control mechanism of SDN ensures consistent enforcement of security policies as well as detection and mitigation of security attacks in real time. The centralized control, dynamic resource allocation, programmability, and flow-based forwarding features of SDN help to optimize traffic management, ensure security, and reduce congestion, providing a more secure and efficient communications infrastructure in VANETs [30]. SDN mitigates some security attacks in traditional VANETs but also introduces new vulnerabilities in SDN-based VANETs due to its centralized control, programmability, flow-based forwarding, and the dynamic network topology and high mobility in VANETs. Table 1 highlights how various vulnerabilities in SDN-based VANETscan be exploited by attackers to launch diverse types of attacks. The root causes and severe impacts on network security are also detailed in the table.

IV. Denial of Service Attacks in SDN-based VANETs

When SDN is integrated with VANETs, it is vulnerable to several security attacks due to the unique vulnerabilities of both systems. DoS attack is indeed one of the most critical security attacks in SDN-based VANETs due to its potential to disrupt the functionality of the entire network [10]. VANETs are already prone to attacks such as DoS and Sybil attacks due to their dynamic topology and reliance on wireless communication [7,8,22]. The SDN controller being a single point of failure is the prime target of attackers and is highly vulnerable to excessive traffic or malicious requests. The excessive traffic or malicious requests can overwhelm the SDN controller's capacity to manage or reroute data effectively, and lead to DoS attacks across the network [31]. This results in significant network disruptions, including delays in safety-critical communications (e.g., collision avoidance alerts, and accident notifications), ultimately causing a severe decline in the overall performance of VANETs. This integration approach amplifies the security risks, necessitating advanced defense mechanisms to protect against such vulnerabilities.This section classifies DoS attacks against SDN-based VANETs into three categories based on the layer structure of SDN-based VANETs: Data Layer DoS Attacks, Control Layer DoS Attacks and Application Layer DoS Attacks.

A. Data Layer DoS Attacks in SDN-based VANETs

DoS attacks targeting the data layer overload devices such as SDN switches, RSUs, and vehicles responsible for network communication, leading to severe network congestion and degraded service quality[32,33]. For example, a compromised vehicle can send continuous beacon messages to overload nearby RSUs and an attacker node can exploit SDN switches by flooding them with crafted flow-mod requests. The most popular DoS attacks targeting the data layer are described here:

- **Flooding Attack:** The flooding attacks in SDN-based VANETs overwhelm the network with malicious traffic, causing congestion and disrupting Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2X) communications [15,34]as shown in Fig. 2. These attacks target vehicles, RSUs, and communication channels, leading to delayed or lost packets, degraded performance, increased latency, and reduced bandwidth [35]. By employing time series analysis of packet flows and constructing flow trees, the Sentinel defense mechanism [36] has an average mitigation rate of over 78% in different densityscenarios, although its performance degrades as the number of vehicles increases in the network. To counter such threats, machine learning-based approaches have been proposed by researchers [37,38]. In [37], a gradient-boosting classifier effectively detects abnormal traffic in V2I communications with high accuracy and low false alarm rates. In [38], the proposed model combines statistical analysis with techniques - autoencoders and LSTM networks, achieving 99.42% accuracy,99.15% precision, 99.38% recall, and 99.27% F1-score, and improving road safety through secure communications.

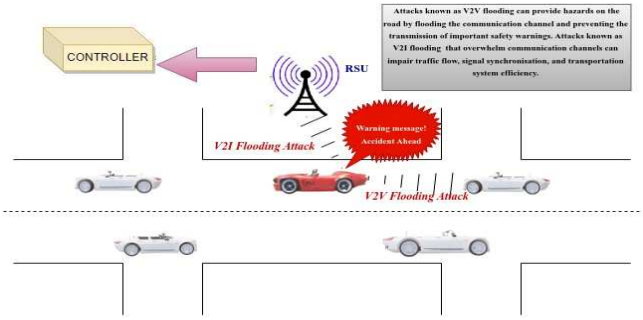

Fig 2. Flooding Attack

- **Flow Table Exhaustion**: The functionality of switches used in SDN rely on Ternary Content Addressable Memory (TCAM) for packet processing. However, the limited size of TCAMposes a significant vulnerability. DoS attacks often target switches' flow tables by flooding them with more packets than the TCAM can accommodate, leading to overload [39]. In the data layer, the network switches route packets based on predefined flow rules. If a switch encounters a packet that doesn't match any of these rules, it either discards it or sends a packet-in request to the controller for further instructions, exacerbating network congestion. Yu et al. [40] proposed a detection system using the PACKET_IN message to address this critical issue. This approach significantly reduces the attack response time and lessens the

burden on the controller. The working mechanism of this system is based on the threshold value of incoming packets.This system leverages a centralized controller for decision-making and flow feature extraction to analyse traffic patterns using an SVM classifier based on the OpenFlow protocol. This approach demonstrated effective detection rates of 97.49% for ICMP traffic and 98.59% for TCP traffic with exceptionally low false alarm rates of 0.3% and 0.32% respectively.

- **Packet-in Flooding**:A packet-in flooding attack targets the control layer by flooding the switch's flow table with a large number of packets, regardless of whether they match any flow rules. The author in [41] explored the impact of packet-in flooding attacks, which overwhelm the controller by generating excessive packet-in message requests. This leads to a high packet-in ratio (PAPI), significantly decreasing throughput—sometimes to zero—and increasing latency for legitimate traffic. To address these vulnerabilities, the author also proposed an adaptive load-balancing technique to distribute traffic evenly across multiple paths and real-time anomaly detection to identify abnormal network activities.

- **Spoofing Attack**:Spoofing attacks occur when an attacker impersonates the physical or logical identity such as MAC address or IP address of a legitimate node (switch or vehicle). The attacker pretends to be a legitimate node and insertsfalse information into the network. This allows the attacker to drop, alter, or reroute the legitimate packets, disrupting communication and compromising the integrity and functionality of network [42]. DDoS attacks primarily target the control layer by overwhelming the network with excessive requests and injecting false network topology information. This disrupts the routing and management functions of the network, rendering it incapable of efficiently directing traffic and handling communication between nodes. This attack indirectly affects the data layer by causing delays in data transmission and leading to the loss of legitimate data packets. In [43], authors presented an anomaly detection technique that combines a deep autoencoder neural network (based on restricted Boltzmann machine) with network tomography for anomaly detection. This technique achieves up to 99% accuracy in detecting anomalies. This approach effectively classifies DoS, SYN flooding, and ARP spoofing attackswith a maximum error rate of only 3%.

- **Exploiting routing protocols:** The attackers exploit vulnerabilities in routing protocols like AODV, DSR, and OLSR within SDN-based VANETs to disrupt network functionality. In routing table poisoning attack, where malicious nodes inject false routing information, causing incorrect entries in routing tables and misrouting of packets. In blackhole attack, the malicious nodes advertise having optimal routes to the destination to attract traffic and then drop all received packets [44, 45]. Grayhole attack is similar to the blackhole attack but here attacker selectively drops selective packets instead of all, making the attack more difficult to detect [46]. In Sybil attack, the attacker node uses multiple identities to create the illusion of multiple nodes, influencing routing decisions and network topology [46]. Wormhole attack involves malicious nodes creating a tunnel, deceiving legitimate nodes into thinking they are part of a valid route, and potentially isolating network sections [46].These attacks are very severeandneed to be addressed in the path of successful deployment of SDN-based VANETs [7]. In [44], an intrusion detection technique was proposed to detect and isolate black hole attacks in the AODV protocol. The black hole attacks are detected using the destination sequence number, hop count, and average packet processing and queuing delays. In [47], authors proposed a collaborative framework for detecting Sybil attacks in networks using majority voting. The framework operates by ensembling individualclassifiers such as Logistic Regression, Decision Tree, Naïve Bayes, SVM, and K-Nearest Neighborin parallel. Hard and soft majority voting mechanisms are employed for the final prediction. The results show that majority voting soft outperforms majority voting hard in detecting Sybil attacks, achieving a higher accuracy of 95%.

- **Replay Attack:**An attacker captures and retransmits valid data or messages, causing unintended repetition of commands or data packets. The replay attack disrupts the network's operation and may trigger unwanted actions [8].In [48], ML-based models were evaluated for detecting replay attacks in VANET using the VeReMi extension dataset. The experimental results show that the random forest model performs better than other ML models.

The communication link-based DoS attacks in SDN-based VANETs disrupt data transmission between entities like vehicles, RSUs, and controllers. Attackers overload communication links or exploit protocol vulnerabilities, causing delays, dropped packets, or network unavailability [49]. These attacks may also involve jamming wireless signals or injecting malicious traffic, compromising the integrity of data transmission and degrading network performance.Some DoS attacks that occurred in communication links are:

- **Signal Jamming:** In a jamming attack, the attacker deploys a powerful jammer near a critical location to disrupt radio frequencies, causing communication failure between V2V and V2I systems, leading to traffic congestion and network compromise [50]. In V2V communications, attackers can place jammers inside a vehicle to target safety-critical applications such as collision avoidance systems as shown in Fig.

3. This disruption prevents vehicles from receiving real-time data, resulting in processing delays, network congestion, and overall degradation in network performance. In [51], a solution was proposed to detect RF jamming attacks using unsupervised machine learning. In this solution, a novel metric (the variation in relative speed between the jammer and the receiver) is used.This approach effectively distinguishes intentional jamming from unintentional interference andshows high detection accuracy in various scenarios.

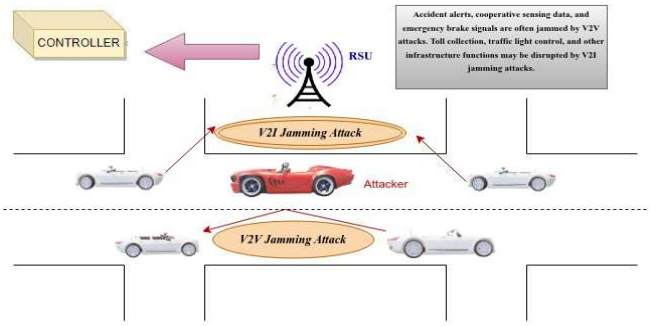

Fig 3. Jamming Attack

Impact of Data Layer DoS Attacks in SDN-based VANETs

a) **Bandwidth consumption / Link Saturation**: During flooding attacks, the network bandwidth can be overwhelmed with utilization reaching up to 90%, preventing legitimate data transmission [13,17].

b) **Packet Loss**: Flooding and jamming attacks can lead to a significant increase in packet drop and packet loss rates, particularly in congested VANETs [16,52].

c) **Latency**: DoS attacks targeting the data layer can result in significant delays in packet transmission [19].

B. *Control Layer DoS Attacks in SDN-based VANETs*

In SDN-based VANETs, the control layer is responsible for the central management of network resources, including routing decisions, flow control, and overall traffic management. A DoS attack targeting the control layer exploits the vulnerabilities inherent in the centralized architecture of SDN. The attackers aim to overload or disrupt the SDN controller by flooding it with excessive requests or malicious traffic, leading to a disruption of network services and degradation of network performance[53].

- **Controller Saturation**: In SDN-based VANETs, attackers may exploit the data layer by sending numerous packet requests without corresponding flow rules, causing network switches to overload the controller with packet-in requests [29].This leads to controller saturation, where the controller's resources become overwhelmed, hindering its ability to manage the network and causing performance degradation or a DoS attack[30]. To address these issues, various detection and mitigation techniques have been proposed by the researchers.In [54], a statistical defence mechanism using statistical process control was proposed for detecting DDoS attacks in SDN-based VANETs. It enables real-time monitoring to identify malicious activities effectively. In [55], authors presented two security schemes for SDN-based VANETs: JChOA, a trusted routing algorithm combining Jellyfish Search and Chimp Optimization, and JChOA_RideNN, an attack detection and mitigation framework using a Rider Optimization-based neural network tuned by JChOA. improves energy (0.947 J), while JChOA_RideNN achieves 93.9% precision and 93.1% recall in detection of malicious entities. In [56], an IDS was proposed for detecting DDoS attacks in VANETs using the Radial Basis Function (RBF) kernel of SVM and Grid Search Cross-Validation (GSCV) for parameter optimization.With optimal RBF-SVM, the model achieved 99.22% detection rate. In [57], different machine learning classifiers were assessed for detecting DDoS attacks in SD-VANETs. The highest performance with an accuracy of 99.35% was obtained by combining the Minimum Redundancy Maximum Relevance (MRMR) feature selection algorithm and a decision tree classifier optimized using Bayesian optimization. In [58], an approach was proposed consisting of five phases: registration, key generation, data encoding, authentication, and decoding. The intrusion detection utilizes a Rider-based neural network (RideNN), optimized with Rider-based Sea Lion Optimization (RBSLO). The RBSLO-based RideNN achieves high performance with 92.5% precision, 95.4% recall, and 94% F-measure.

- **Controller Compromised:** The attacker gains unauthorized access by compromising the controller, enabling it to modify or inject incorrect flow rules. These altered rules are then propagated to the data layer, disrupting network operations. The primary target of the attack is the controller's flow rule management, which controls the switch's flow table entries [59]. As a result, the switches apply malicious flow rules that reroute traffic or drop packets, ultimately leading to a denial of service. In [60], authors used a deep network approach with stacked sparse autoencoders (SSAE) to detect DDoS attacks in SDN-based VANETs. This approach improves detection accuracy by 96.9%. Similarly, Radial Basis Function Kernel (RBF) of SVM algorithm-based models in [61] achieve 99.4 % detection accuracy for DDoS attacks. In this model, Grid Search Cross-Validation (GSCV) technique is used for parameter optimization and RBFof SVM algorithm is used for accurate classification and detection.

Impact of Control Layer DoS Attacks in SDN-based VANETs

a) **Request latency**: The latency for flow rule requests increased due to the overload on the controller [19].

b) **Controller throughput:** The controller's throughput may drop by as much as 80%, severely slowing down the decision-making process for network management [13].

c) **Network Degrade:**Prolonged controller failure can cause network disruptions lasting several minutes, potentially crippling network operations in the worst-case scenario [59].

C. Application Layer DoS Attacks in SDN-based VANETs

Application layer DoS attacks target critical software applications and services in vehicles and infrastructure, such as traffic management, collision avoidance, navigation, and communication platforms [17]. Attackers exploit vulnerabilities like high processing demands or weak authentication to overwhelm these systems, disrupting functionality and denying access to legitimate users [29].Many VANET applications use APIs to interact with other systems. Attackers exploit vulnerabilities in these APIs to send malformed or malicious requests, leading to application crashes.

- **Position Falsification Attack**:Attackers primarily target the application layer by manipulating or falsifying the position of vehicles, which disrupts critical location-based services such as collision avoidance, traffic management, and navigation services. In [62], a multi-class approach was proposed to detect various attacks in the VeReMi dataset using classifiers like Naive Bayes, SVM, and Random Forest. The Random Forest classifier achieved the best results with 0.99 precision and 99.16% accuracy.

- **Third-party Attacks**:Third-party applications pose serious security risks such as malicious add-ons performing that conduct deep packet inspection to gain control over the network. Strong authorization and authentication techniques are required to verify external components and strict access controls are required to limit data access. These security measures safeguard critical software applications and services [17,29].

Impact of Application Layer DoS Attacks in SDN-based VANETs

a) **Response Time**: Applications under attack can experience a 50-200% increase in response times [13,59].

b) **Service Downtime**: Critical services such as traffic management may face downtime, compromising both safety and operational efficiency [31].

V. Future Research Directions

In this paper, we have briefly studied vulnerabilities and DoS attacks in SDN-based VANETs. Based on this study, the following research directions are identified for researchers to explore, to enhance the security and resilience of network operations in SDN-based VANETs:

- There is a pressing need to uncover unexplored vulnerabilities and thoroughly examine cross-domain attacks that exploit weak links within this interconnected system.
- Researchers should harness the full potential of AI technologies such as AI, machine learning, and deep learning, to design innovative and effective real-time attack detection and mitigation techniques.
- Researchers should design DoS attack detection engines utilizing hybrid machine learning techniques to enhance detection accuracy and reliability.
- Researchers should explore the potential of federated learning to develop advanced mechanisms for detecting distributed Denial of Service (DDoS) attacks.
- Researchers should explore the integration of blockchain technology to ensure secure communication between controllers and other network components.
- Researchers should focus on deploying distributed and hierarchical SDN controller architectures, rather than relying on a single SDN controller, to eliminate single points of failure and ensure continuous network operations.
- The research community should focus on designing layer-specific security solutions to address DoS vulnerabilities across the data, control, and application layers.
- To secure all layers of SDN-based VANETs against DoS attacks, the research community should also concentrate on designing a cross-layer strategy.
- Researchers should develop effective mechanisms for dynamically reconfiguring flow tables to prevent resource exhaustion.
- To enable proactive defense mechanisms, researchers should investigate how the game theory might be used to predict and counteract emerging DoS attack strategies.
- There is also a pressing need to study how quantum computing may affect the cryptographic primitives used in SDN-based VANETs.
- Researchers should focus on thoroughly understanding the operation of routing protocols to design effective security solutions that prevent DoS attacks from exploiting vulnerabilities within these protocols.
- Researchers should investigate how SDN-based VANETs can securely collaborate with other domains, such as smart cities, IoT, and cloud infrastructure.

- Researchers should propose multi-dimensional trust models to ensure the authenticity and reliability of communication between network components and SDN controllers.
- Researchers should integrate edge and fog nodes for decentralized processing and effective DoS mitigation at the network's periphery.
- Researchers should focus on improving the security of inter-controller communication protocols to protect against data breaches and unauthorized access.
- Researchers should harness the potential of advanced cellular technologies 5G/6G networks to reduce latency and enhance security in SDN-based VANETs
- Researchers should focus on designing application-specific datasets, and evaluation benchmarks for DoS detection and mitigation in SDN-based VANETs.

VI. CONCLUSION

This paper presents a study on vulnerabilities and DoS attacks in SDN-based VANETs, highlighting their severe impact on the availability, reliability, performance, and security of these networks. The DoS attacks are classified into three categories based on the layer structure and their impacts are thoroughly analysed. With the rapid growth of SDN-based VANET deployments, addressing these security challenges is essential to ensure the security, efficiency, and resilience of vehicular networks. The study outlines several key future research directions, aimed at helping the research community in designing advanced and robust security solutions for the real-time detection and mitigation of DoS attacks in SDN-based VANETs.

REFERENCE

[1] M. Chahal, S. Harit, K. K. Mishra, A. K. Sangaiah, and Z. Zheng, "A Survey on software-defined networking in vehicular ad hoc networks: Challenges, applications and use cases," *Sustainable Cities and Society*, vol. 35, pp. 830-840, 2017.

[2] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, "A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for SDN-VANET," *IEEE Access*, vol. 8, pp. 91028–91047, Jan. 2020.

[3] M. S. Sheikh, J. Liang, and W. Wang, "A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs)," *Sensors*, vol. 19, no. 16, p. 3589, Aug. 2019.

[4] A. Di Maio, M. R. Palattella, R. Soua, L. Lamorte, X. Vilajosana, J. Alonso-Zarate, and T. Engel., "Enabling SDN in VANETs: What is the Impact on Security?," *Sensors*, vol. 16, no. 12, p. 2077, Dec. 2016.

[5] R. Sultana, J. Grover, and M. Tripathi, "Security of SDN-based vehicular ad hoc networks: State-of-the-art and challenges," *Vehicular Communications*, vol. 27, p. 100284, Aug. 2020.

[6] H. Shafiq, R. A. Rehman, and B. S. Kim, "Services and security threats in SDN-based VANETs: A survey," *Wireless Communications and Mobile Computing*, vol. 2018, no. 1, p. 8631851, 2018.

[7] W. B. Jaballah, M. Conti, and C. Lal, "Security and design requirements for software-defined VANETs," *Computer Networks*, vol. 169, p. 107099, Jan. 2020,

[8] M. Arif, G. Wang, O. Geman, A. Brezulianu, and J. Chen., "SDN-based VANETs, Security Attacks, Applications, and Challenges," *Applied Sciences*, vol. 10, no. 9, p. 3217, May 2020,

[9] K. Adhikary, S. Bhushan, S. Kumar, and K. Dutta, "Decision Tree and Neural Network Based Hybrid Algorithm for Detecting and Preventing DDoS Attacks in VANETs," *International Journal of Innovative Technology and Exploring Engineering*, vol. 5, pp. 669–675, 2020.

[10] K. B. Adedeji, A. M. Abu-Mahfouz, and A. M. Kurien, "DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges," *Journal of Sensor and Actuator Networks*, vol. 12, no. 4, p. 51, 2023.

[11] K. Adhikary, S. Bhushan, S. Kumar, and K. Dutta, "Evaluating the Performance of Various SVM Kernel Functions Based on Basic Features Extracted from KDDCUP'99 Dataset by Random Forest Method for Detecting DDoS Attacks," *Wireless Personal Communications*, vol. 123, pp. 3127–3145, 2022.

[12] R. Kumar and N. Agrawal, "A survey on software-defined vehicular networks (SDVNs): a security perspective," *The Journal of Supercomputing*, vol. 79, no. 8, pp. 8368–8400, Dec. 2022,

[13] Cloudflare, "DDoS Threat Landscape Report: Q1 2024," *Cloudflare Radar*, 2024. [Online]. Available: https://radar.cloudflare.com/reports/ddos-2024-q1.

[14] SecurityWeek, "DDoS Hacktivism is Back with a Geopolitical Vengeance," *SecurityWeek*, Dec. 5, 2024. [Online]. Available: https://www.securityweek.com/ddos-hacktivism-is-back-with-a-geopolitical-vengeance/.

[15] K. V. Krishna and K. G. Reddy, "Classification of Distributed Denial of Service Attacks in VANET: A Survey," *Wireless Personal Communications*, vol. 132, no. 2, pp. 933–964, Jul. 2023.

[16] J. Singh and S. Behal, "Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions," *Computer Science Review*, vol. 37, p. 100279, Jun. 2020

[17] H. Wang and Y. Li, "Overview of DDoS Attack Detection in Software-Defined Networks," in *IEEE Access*, vol. 12, pp. 38351-38381, 2024

[18] E. Tamakloe, B. Kommey, E. Akowuah, and D. Opoku, "Detailed review on the Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks in Software Defined Networks (SDNs) and defense strategies," *International Journal of Applied Sciences and Smart Technologies*, vol. 5, no. 2, pp. 271–302, 2023.

[19] E. Eliyan, L. Fayez, and R. Di Pietro, "DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges," *Future Generation Computer Systems*, vol. 122, pp. 149-171, 2021.

[20] K. Adhikary, S. Bhushan, S. Kumar, and K. Dutta, "Hybrid algorithm to detect DDoS attacks in VANETs," *Wireless Personal Communications*, vol. 114, no. 4, pp. 3613–3634, 2020.

[21] T. Mekki, I. Jabri, A. Rachedi, and L. Chaari, "Software-defined networking in vehicular networks: A survey," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 10, Apr. 2021.

[22] B. A. Mohammed, "Review on Software-Defined Vehicular Networks (SDVN)," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 22, no. 9, pp. 376, 2022.

[23] S. Askar, G. A. Qadir, and T. A. Rashid, "SDN-Based 5G VANET: Characteristics, Attacks, and Challenges," *IJSB*, vol. 5, no. 6, pp. 148-162, Aug. 2021. Accepted May 29, 2021.

[24] M. M. Ghonge and P. N, "Software-defined network-based vehicular ad hoc networks: A comprehensive review," *EAI/Springer Innovations in Communication and Computing*, pp. 33–53, 2022.

[25] M. Priyadarsini and P. Bera, "Software defined networking architecture, traffic management, security, and placement: A survey," *Computer Networks,* vol. 192, p. 108047, Apr. 2021.

[26] R. Deb and S. Roy, "A comprehensive survey of vulnerability and information security in SDN," *Computer Networks*, vol. 206, p. 108802, Feb. 2022.

[27] K. Nisar, E. R. Jimson, M. H. A. Hijazi, I. Welch, R. Hassan, A. H. M. Aman, A. H. Sodhro, S. Pirbhulal, and S. Khan."A survey on the architecture, application, and security of software defined networking: Challenges and open issues," *Internet of Things*, vol. 12, p. 100289, Sep. 2020.

[28] M. S. Farooq, S. Riaz, and A. Alvi, "Security and Privacy Issues in Software-Defined Networking (SDN): A Systematic Literature Review," *Electronics*, vol. 12, no. 14, p. 3077, Jul. 2023.

[29] A. K. Jain, H. Shukla, and D. Goel, "A comprehensive survey on DDoS detection, mitigation, and defense strategies in software-defined networks," *Cluster Computing*, vol. 27, pp. 13129–13164, 2024.

[30] U. Kaur, A. N. Mahajan, S. Kumar, and K. Dutta, "Security Vulnerabilities in VANETs and SDN-based VANETs: A Study of Attacks," *International Journal of Computer Networks and Applications*, vol. 11, no. 6, 2024 (accepted for publication on 29.10.2024).

[31] J. K. Chahal, A. Bhandari, and S. Behal, "DDoS attacks &defense mechanisms in SDN-enabled cloud: Taxonomy, review and research challenges," *Computer Science Review*, vol. 53, 2024, Art. no. 100644.

[32] T. Zhang, C. Xu, P. Zou, H. Tian, X. Kuang, S. Yang, and L. Zhong., "How to Mitigate DDoS Intelligently in SD-IoV: A Moving Target Defense Approach," in *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 1097-1106, Jan. 2023.

[33] K. Adhikary, S. Bhushan, S. Kumar, and K. Dutta, "Evaluating the Performance of Various Machine Learning Algorithms for Detecting DDoS Attacks in VANETs," *International Journal of Control Automation*, vol. 12, no. 5, pp. 478–486, 2019.

[34] S. Kumar and K. Dutta, "Direct Trust-Based Security Scheme for RREQ Flooding Attack in Mobile Ad Hoc Networks," *International Journal of Electronics*, vol. 104, no. 6, pp. 1034–1049, 2017.

[35] S. Kumar, K. Dutta, and A. Garg, "FJADA: Friendship-Based JellyFish Attack Detection Algorithm for Mobile Ad Hoc Networks," *Wireless Personal Communications*, vol. 101, pp. 1901–1927, 2018.

[36] G. de Biasi, L. F. M. Vieira and A. A. F. Loureiro, "Sentinel: Defense Mechanism against DDoS Flooding Attack in Software Defined Vehicular Network," *2018 IEEE International Conference on Communications (ICC)*, Kansas City, MO, USA, 2018, pp. 1-6.

[37] P. K. Singh, S. Kumar Jha, S. K. Nandi and S. Nandi, "ML-Based Approach to Detect DDoS Attack in V2I Communication Under SDN Architecture," *TENCON 2018 - 2018 IEEE Region 10 Conference*, Jeju, Korea (South), 2018, pp. 0144-0149.

[38] U. Tariq, "Optimized Feature Selection for DDoS Attack Recognition and Mitigation in SD-VANETs," *World Electric Vehicle Journa*l, vol. 15, no. 9, p. 395, Aug. 2024.

[39] V. Karthik, R. Lakshmi, S. Abraham, and M. Ramkumar, "Residual based temporal attention convolutional neural network for detection of distributed denial of service attacks in software defined network integrated vehicular adhoc network," *International Journal of Network Management,* vol. 34, no. 3, Dec. 2023.

[40] Y. Yu, L. Guo, Y. Liu, J. Zheng and Y. Zong, "An Efficient SDN-Based DDoS Attack Detection and Rapid Response Platform in Vehicular Networks," in *IEEE Access*, vol. 6, pp. 44570-44579, 2018.

[41] A. J. Siddiqui and A. Boukerche, "On the Impact of DDoS Attacks on Software-Defined Internet-of-Vehicles Control Plane," *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, Limassol, Cyprus, 2018, pp. 1284-1289.

[42] A. Haydari and Y. Yilmaz, "RSU-Based Online Intrusion Detection and Mitigation for VANET," *Sensors*, vol. 22, no. 19, p. 7612, Oct. 2022.

[43] A. Ibraheem, Z. Sheng and G. Parisis, "Anomaly Detection and Classification for SDN-Enabled In-Vehicle Network Using Network Tomography-Based Deep Learning," *2024 IEEE Wireless Communications and Networking Conference (WCNC)*, Dubai, United Arab Emirates, 2024, pp. 1-6.

[44] S. Kumar and K. Dutta, "Intrusion Detection Technique for Black Hole Attack in Mobile Ad Hoc Networks," International Journal of Information Privacy, Security and Integrity, vol. 2, no. 2, pp. 81–101, Mar. 2016.

[45] M. ul Hassan, A. A. Al-Awady, A. Ali, Sifatullah, M. Akram, M. M. Iqbal, J. Khan, and Y. A. A. A. Ali, "ANN-Based Intelligent Secure Routing Protocol in Vehicular Ad Hoc Networks (VANETs) Using Enhanced AODV," *Sensors*, vol. 24, no. 3, p. 818, 2024.

[46] S. Kumar and K. Dutta, "Securing mobile ad hoc networks: Challenges and solutions," *International Journal of Handheld Computing Research (IJHCR)*, vol. 7, no. 1, pp. 26-76, 2016.

[47] S. Azam, M. Bibi, R. Riaz, S. S. Rizvi, and S. J. Kwon, "Collaborative learningbased Sybil attack detection in vehicular ad-hoc networks(VANETs),"*Sensors*, vol. 22, no. 18, p. 6934, 2022.

[48] A. Kumar, M. A. Shahid, A. Jaekel, N. Zhang and M. Kneppers, "Machine learning based detection of replay attacks in VANET," *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, Miami, FL, USA, 2023, pp. 1-6.

[49] A. K. Jain, H. Shukla, and D. Goel, "A comprehensive survey on DDoS detection, mitigation, and defense strategies in software-defined networks," *Cluster Computing*, vol. 27, pp. 13129–13164, Dec. 2024.

[50] R. Nayak, S. Sethi, S. K. Bhoi, K. S. Sahoo, N. Z. Jhanjhi, T. Tabbakh, and Z. A. Almusaylim., "TBDDoSA-MD: Trust-Based DDoS Misbehave Detection Approach in Software-defined Vehicular Network (SDVN)," *Computers, Materials & Continua/Computers, Materials & Continua (Print),* vol. 69, no. 3, pp. 3513–3529, Jan. 2021.

[51] D. Karagiannis and A. Argyriou, "Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning," *Vehicular Communications*, vol. 13, pp. 56–63, May 2018.

[52] K. Adhikary, S. Bhushan, S. Kumar, and K. Dutta, " Evaluating the Impact of DDoS Attacks in Vehicular Ad-Hoc Networks," *International Journal of Security and Privacy in Pervasive Computing (IJSPPC)*, vol. 12, no. 4, pp. 1–18, 2020.

[53] M. A. Aladaileh, M. Anbar, I. H. Hasbullah, Y. -W. Chong and Y. K. Sanjalawe, "Detection Techniques of Distributed Denial of Service Attacks on Software-Defined Networking Controller–A Review," in *IEEE Access*, vol. 8, pp. 143985-143995, 2020.

[54] F. Bensalah, N. Elkamoun, and Y. Baddi, "SDNStat-Sec: A Statistical Defense Mechanism Against DDoS Attacks in SDN-Based VANET*," in Advances in intelligent systems and computing,* 2020, pp. 527–540.

[55] U. Kaur, A. N. Mahajan, S. Kumar, and K. Dutta, "Jellyfish search chimp optimization enabled routing and attack detection in SDN based Vanets," *Wireless Personal Communications*, vol. 138, no. 2, pp. 819–859, Sep. 2024.

[56] G. O. Anyanwu, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Optimization of RBF-SVM Kernel Using Grid Search Algorithm for DDoS Attack Detection in SDN-Based VANET," *IEEE Internet of Things Journal,* vol. 10, no. 10, pp. 8477–8490, Aug. 2022.

[57] M. Türkoğlu, H. Polat, C. Koçak, and O. Polat, "Recognition of DDoS attacks on SD-VANET based on combination of hyperparameter optimization and feature selection," *Expert Systems With Applications*, vol. 203, p. 117500, May 2022.

[58] M. K. Pulligilla and C. Vanmathi, "An authentication approach in SDN-VANET architecture with Rider-Sea Lion optimized neural network for intrusion detection," *Internet of Things*, vol. 22, p. 100723, Feb. 2023.

[59] A. Kaur, C. R. Krishna, and N. V. Patil**,** "A comprehensive review on Software-Defined Networking (SDN) and DDoS attacks: Ecosystem, taxonomy, traffic engineering, challenges and research directions," *Computer Science Review,* vol. 55, p. 100692, 2025.

[60] H. Polat, M. Turkoglu, and O. Polat, "Deep network approach with stacked sparse autoencoders in detection of DDoS attacks on SDN-based VANET," *IET Communications*, vol. 14, no. 22, pp. 4089–4100, Dec. 2020.

[61] G. O. Anyanwu, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "RBF-SVM kernel-based model for detecting DDoS attacks in SDN integrated vehicular network," *Ad Hoc Networks*, vol. 140, p. 103026, Nov. 2022,

[62] K. Vermani, A. Noliya, S. Kumar, and K. Dutta, "Ensemble Learning Based Malicious Node Detection in SDN-Based VANETs*," Journal of Information Systems Engineering and Business Intelligence,* vol. 9, no. 2, pp. 136–146, Nov. 2023.