International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2024/47 Volume 11, Issue 6, November – December (2024)

REVIEW ARTICLE

Security Vulnerabilities in VANETs and SDN-based VANETs: A Study of Attacks

Upinder Kaur
Maharaja Agrasen University, Baddi (Himachal Pradesh), India.
upinder1981@gmail.com

Aparna N. Mahajan
Maharaja Agrasen University, Baddi (Himachal Pradesh), India.
aparnanmahajan@yahoo.co.in

Sunil Kumar
Guru Jambheshwar University of Science & Technology, Hisar (Haryana), India.
sunilkaushik27@gmail.com

Kamlesh Dutta
National Institute of Technology, Hamirpur (Himachal Pradesh), India.
kdnith@gmail.com

Received: 04 August 2024 / Revised: 17 October 2024 / Accepted: 29 October 2024 / Published: 30 December 2024

Abstract – Vehicular ad hoc networks (VANETs) suffer from several challenges due to advancements in technology such as 5G and the continuous growth in the number of vehicles. These challenges include handling scalability, traffic management, security, flexibility etc. The researchers believe that integrating the Software Defined Networking (SDN) architecture with traditional VANETs could result in a promising solution that will address the aforementioned challenges of traditional VANETs by leveraging the inherent features of SDN. These features include programmable network behavior, virtualization, centralized control mechanism, and network automation. The integration of SDN with VANETs helps in partially mitigating the security attacks associated with traditional VANETs. However, the dynamic and distributed nature of VANETs, when integrated with the centralized control mechanism of SDN introduces new kind of security vulnerabilities. This paper presents a comprehensive review of security vulnerabilities and attacks in both traditional VANETs as well as in SDN-based VANETs. The review begins by categorizing the security attacks against VANETs in accordance with the network communication protocol stack. The potential impacts of these attacks on the operation of vehicular ad hoc networks are being assessed. The paper then explores the extent to which integrating the SDN can mitigate security vulnerabilities in traditional VANETs. Finally, this paper presents the study related to the security attacks against SDN-based VANETs in accordance with the three-layer architecture of SDN. These attacks demonstrate how the unique features (central control mechanism, programmability, and flow-based controlling) of SDN introduce new security vulnerabilities in SDN-based VANETs across the control, data, and application planes. The potential impacts of these attacks on the operation of SDN-based VANETs architecture are also being assessed. Through a systematic classification and analysis of security attacks in VANETs as well as in SDN-based VANETs, this paper will serve as a valuable resource for researchers in understanding the security landscape of VANETs as well as SDN-based VANETs, and motivate them to design the effective defensive solutions to secure the network operations of these critical systems.

Index Terms – VANETs, SDN, SDN-based VANETs, security vulnerabilities, security attacks, encryption and authentication, intrusion detection systems.

1. INTRODUCTION

In today's world, people are spending more and more time in transportation, so vehicles have become an important component of the travel experience. In this context, Vehicular Ad hoc Networks (VANETs) have emerged as a promising solution to improve road safety, enhance passenger comfort, and optimize travel and traffic efficiency. VANET is a kind of Mobile ad hoc network (MANET) that facilitates the communication among the moving vehicles on roads [1]. The development of VANETs has also contributed to the success of ITSs by allowing communication between vehicles and roadside infrastructure, as well as among vehicles themselves. VANETs support vehicle-to-vehicle communication (V2V), vehicle-to-infrastructure at the roadside communication (V2I), and vehicle-to-pedestrian communication (V2P) as shown in

REVIEW ARTICLE

Figure 1. In VANETs, the V2X term is used to represent the communication between Vehicles to Everything (X) (i.e. V2V, V2I, and (V2P)). In recent years, Heterogeneous Vehicular Networks (HetVNets) have emerged as an important development that enriches traditional VANETs with different wireless technologies (DSRC, WiFi, WiMax, etc.) and cellular technology (4G / 5G) [2-3]. Internet of Vehicles (IoVs) has evolved as an innovative development to enhance the performance of new generations of heterogeneous vehicle networks by providing connected vehicles with more sophisticated technological and commercial capabilities [4]. A vehicle in VANETs is an intelligent mobile node equipped with advanced wireless communication technologies that enable efficient communication with roadside infrastructure and other vehicles on the road. A vehicle network is based primarily on three basic elements: intelligent vehicles, roadside equipment, and communication between vehicles. VANETs offer several characteristics including ad-hoc network formation, highly dynamic network topology, frequency spectrum allocation, V2X communication system, geographically dispersed, scalable, real-time data transmission, autonomy, unlimited power supply, high computational capacity, driver protection, etc.

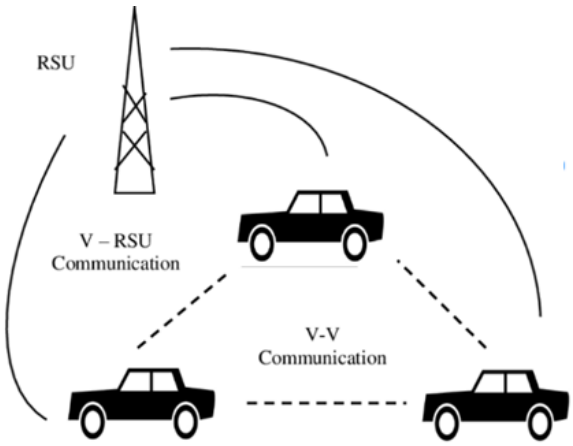

Figure 1 Vehicular Ad-Hoc Networks Architecture Diagram

VANETs have significantly transformed the transportation systems industry by providing an extensive range of applications across multiple domains such as automated toll collection, collision avoidance, driver assistance systems, dynamic routing, emergency vehicle notification, environmental monitoring, infotainment services, intelligent traffic signal control, pedestrian safety, public transportation management, road condition monitoring, road safety warnings, roadside assistance, smart parking, supply chain management, traffic law enforcement, traffic management, vehicle platooning, etc [5]. Despite having several attractive characteristics and interesting application possibilities, VANET has several challenges that impede its successful deployment, implementation, and operation. Some of them are high mobility, scalability, poor reliability, limited bandwidth, network connectivity, intermittent connectivity, heterogeneous vehicle management, weak network security, interference and signal attenuation, lack of uniform standards, and low intelligence levels [5]. One of the most critical challenges facing VANETs is network security. VANETs are particularly vulnerable to various kinds of security threats and attacks due to inherent characteristics such as high mobility, dynamic topology, wireless communication systems and decentralized nature. The researchers believe that integrating the Software Defined Networking (SDN) architecture with VANETs could result in a promising architecture that will address the aforementioned challenges of traditional VANETs by leveraging the inherent features of SDN [6-8]. These features include programmable network behavior, virtualization, centralized control mechanism and network automation. It has been observed that SDN-based VANETs helps in mitigating the security attacks associated with traditional VANETs up to a limited extent. Even the dynamic and distributed nature of VANETs, when integrated with the centralized control mechanism of SDN introduces new security vulnerabilities and opens the doors for new attacks to be launched against the SDN-based VANETs [7-8]. The motivation and objectives of this study are described here, giving the readers a clear understanding of the driving forces behind the study and the specific goals it seeks to achieve.

1.1. Motivation

The convergence of SDN with VANETs can address the security concerns of traditional VANETs to a limited extent. Thus, there is still a need to identify the main security issues associated with SDN and VANETs technologies, both separately and together.

1.2. Objectives

- To investigate the extent to which the integration of the SDN architecture with traditional VANETs might mitigate the security vulnerabilities that are associated with traditional VANETs.
- To investigate how the integration of the SDN architecture with traditional VANETs might lead to new and unseen security vulnerabilities as a result of the inherent characteristics of SDN.

In this paper, an attempt is made first to present the comprehensive review of security attacks in traditional VANETs along with the security vulnerabilities in VANETs. The security attacks are categorized based on the communication protocol layer within the VANETs architecture along with their nature, impact, and security attributes being compromised. Thereafter, a study is being carried out to demonstrate how integrating the SDN architecture with traditional VANETs can mitigate the impact of these critical attacks. The integration of the centralized

REVIEW ARTICLE

control mechanism of SDN with the dynamic and distributed nature of VANETs introduces new security vulnerabilities and opens the door for new attacks to be launched against SDN-based VANETs. Therefore, in the last section, an analysis of new kind of security attacks in SDN-based VANETs is carried out along with their characteristics, impact, and the targeted components within the SDN-based VANETs architecture.

The structure of this paper is as follows: Section 2 provides an overview of SDN and VANET technologies, discussing them both individually and in combination. Section 3 outlines the security requirements for traditional VANETs and SDN-based VANETs. In Section 4, the paper examines the security vulnerabilities and attacks in traditional VANETs, as well as the extent to which SDN integration can mitigate these threats. Section 5 delves into the security vulnerabilities and attacks specific to SDN-based VANETs, which arise from SDN's intrinsic features such as its centralized control, programmability, and flow-based control, when coupled with VANET's dynamic nature. Section 6 presents the future research directions based on the study carried out in this paper. The conclusion of the paper is presented in Section 7.

2. BACKGROUND

2.1. Vehicular Ad-Hoc Networks (VANETs)

The general architecture of VANETs consists of two primary categories of components: in-vehicle equipment, such as On-Board Units (OBUs) and Application Units (AUs), and roadside infrastructure, which includes Roadside Units (RSUs) located externally to vehicles [9]. OBUs are hardware devices installed on intelligent vehicles that allow wireless communication between vehicles and RSUs. OBU consists of a Resource Command Processor (RCP), read/write memory for data storage, and a specialized interface to connect with other OBUs. These devices make each vehicle act as a router and send and receive messages to and from other vehicles or RSUs within their communication range. RSUs are the equipment placed at the roadside and which constitute the fixed infrastructure of the vehicle networks. These units can inform nearby vehicles by broadcasting information related to traffic, weather, and road-specific conditions such as maximum speed, passing clearance, etc. RSUs can also act as a base station by allowing communication between two distant vehicles or simply relaying information sent by a vehicle. The application layer of the network is expected to serve a wide range of safety and non-safety applications. Application Unit (AU) is designed for driver interaction and utilizes the application programming provided by the service provider to communicate with OBU. It is equipped with input and output interfaces such as personal digital assistants (PDA). The AUs connect to the OBUs via either wired or wireless communication technologies for accessing the network and applications. In V2V communication, vehicles send and receive messages about their location, speed, brake status, and steering angle with the surrounding vehicles in their transmission range to support different applications and services. In V2I communication, the vehicles either connect directly or via a number of hops to fixed roadside units (RSUs) to send, receive, and process the traffic data.

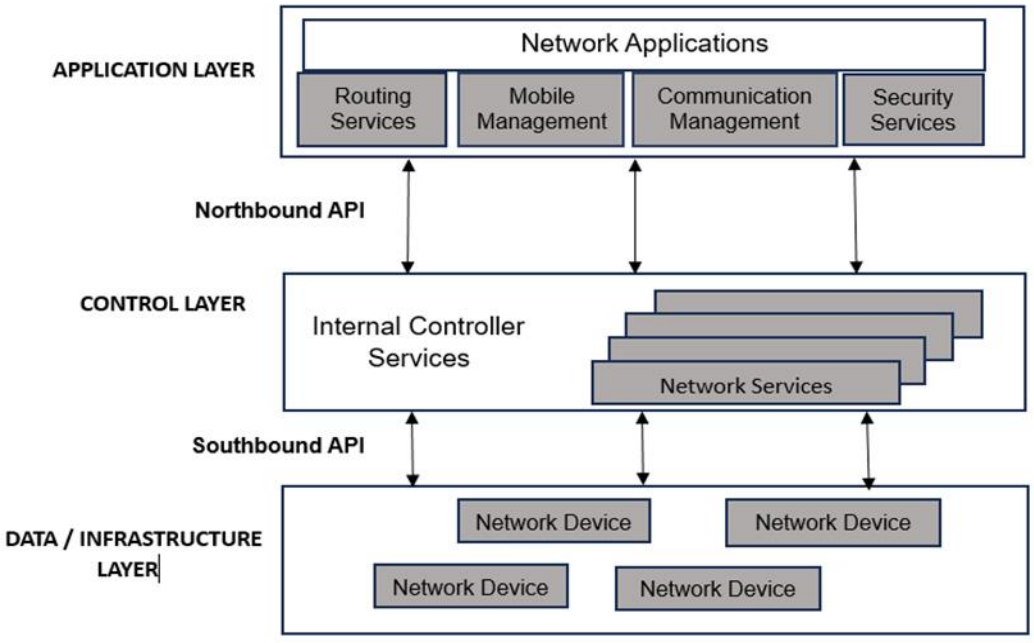

Figure 2 Software Defined Networking Architecture Diagram

REVIEW ARTICLE

V2X communication depends on two key wireless technologies: Dedicated Short-Range Communications (DSRC) and cellular networks (4G/5G) [2-3]. DSRC operates under the IEEE 802.11p and IEEE 1609 standards, as part of the Wireless Access in Vehicular Environments (WAVE) framework. Similar to WiFi, DSRC is specifically designed for short-range communication, enabling high-speed, low-latency wireless connections between vehicles (V2V) and between vehicles and infrastructure (V2I). The main reason behind using the DSRC is its simplicity, high security, minimum control signaling, and the broadcast nature of real-time transmission in case of any emergency conditions such as information related to road blockage, accidents, traffic interruption, etc. However, it suffers from retransmission and message collision in high-density vehicles. Currently, cellular technologies such as 3G/UMTS and 4G/LTE also support V2X communication in VANETs. V2X communications with cellular technology is known as C-V2X (cellular vehicle-to-everything). The roadmap for the implementation of 5G-based V2X services on VANETs has already been created by technical groups like Qualcomm and 3GPP (3rd Generation Partnership Project) [10]. The advanced features of 5G technology including high bandwidth, low latency, highly secure, and high-density connections will significantly enhance V2X communications in VANETs [11].

2.2. Software Defined Networking (SDN)

Software Defined Networking (SDN) is a novel network architecture characterized by two main principles: (i) logical separation of the control plane (responsible for managing the network operations) from the data plane (responsible for handling the data transmission) and (ii) logically centralization of network intelligence through one or more SDN Controllers that govern the entire network [12]. SDN architecture provides a blueprint for creating automated, flexible networks using a blend of open-source software and standard networking hardware. At its foundation, SDN has a hierarchical three-layer structure that allows for the smooth integration of programmable control and dynamic management into the current network environment as shown in Figure 2. SDN architecture consists of three layers: the application layer, the control layer, and the data layer.

- Data layer: The data layer is the lowest in SDN architecture as shown in Figure 2. This layer represents the network's forwarding and processing capabilities. This layer is often referred to as the infrastructure layer. The data plane refers to all the networking devices that receive and forward data packets based on the predefined flow rules defined by controller.
- Control layer: The control layer is the middle layer between the data layer and the application layer in SDN architecture as shown in Figure 2. The control layer represents the logically centralized software entity known as the SDN controller, which serves as both the brain of the SDN architecture and a network operating system. The SDN controller manages rules and traffic flows to optimize network resources. The controller, which runs on a server, offers fine-grained management over the data plane, including routing, monitoring, and load balancing. It keeps track of the network's global status in real-time, feeds application layer commands to networking components, and returns an abstract representation of network data and events.
- Application layer: As shown in Figure 2, the application layer is the highest layer in an SDN architecture. All of the network applications and services that are installed on the SDN controller are managed by it. In order to provide services like configuration, communication, security, and network management, the application layer assists the control layer. The Application Programming Interfaces (APIs) allow the SDN application layer to interface with the SDN controller and vice versa. These APIs assist in optimizing network management and performance.

Software-Defined Networking (SDN) employs unified communication interfaces to facilitate seamless interaction across its three layers:

- Northbound API: This interface enables communication between network applications (application layer) and the SDN controller (control plane). Most commonly APIs used as Northbound APIs are NETCONF, OpenFlow, and REST. These APIs allow applications to request and define specific network behaviours [13].
- Southbound API: This interface facilitates interaction between the data plane equipment (network switches) and the SDN controller (control plane). Most commonly APIs used as Southbound APIs are OpenFlow, Cisco OpFlex, and NETCONF. OpenFlow is governed by the Open Networking Foundation and it is the most widely adopted standard, enabling efficient control and communication between network switches and controllers [14].

2.3. Software Defined Networking Based Vehicular Ad-Hoc Networks

Recently, researchers are exploring ways to leverage the benefits of SDN to enhance the performance of traditional vehicle networks. Several SDN-based architectures have been proposed in the literature by the research community for vehicle networks referred to as Software Defined Vehicular Ad-hoc Networks (SDVN) [6-8,15].

Figure 3 presents the block diagram of SDN-based VANETs, illustrating the key components and their interactions within the architecture. The integration of SDN into vehicular networks offers several significant benefits, including the following:

REVIEW ARTICLE

- Centralized Control: SDN design separates the control plane from the data forwarding plane by centralizing network information and control in a software controller (SDN Controller). This helps in easier management, configuration, and optimization of network behaviour.
- Flexibility and Scalability: SDN provides flexibility in network architecture and scaling. It supports several network designs and scales more effectively than conventional networking systems by adjusting workloads and traffic patterns. SDN also simplifies the management, configuration, and integration of new heterogeneous technologies in heterogeneous vehicle networks [16,17].
- Programmability: Open APIs allow network administrators and operators to dynamically configure and manage network resources depending on changing demands and applications using SDN.
- Programmable Policies and QoS: SDN provides fine-grained control over network rules and QoS parameters. Administrators can design rules centrally and enforce them uniformly throughout the network resulting in optimal performance and resource use.
- Virtualization: SDN enables network virtualization by creating separate logical network segments (virtual networks) for multi-tenancy and utilization of resources efficiency.
- Automation: Automating network administration using SDN, streamlines operations and reduces configuration errors. SDN automation improves efficiency, agility, and responsiveness to network changes and demands.
- Traffic Engineering: SDN allows for intelligent traffic engineering and load balancing across the network.
- Cost Efficiency: SDN lowers operational costs by simplifying network management, reducing hardware dependency through virtualization, and optimizing resource utilization. It supports more efficient use of network resources and infrastructure.
- Openness and Innovation: SDN promotes innovation and ecosystem growth via open standards and APIs. It simplifies the integration of third-party apps and services, encouraging the development of new network services and applications.
- Security Enhancements: SDN enhances network security by combining centralized monitoring, policy enforcement, and rapid threat response. It enables more effective threat detection and mitigation via micro-segmentation, sensitive data isolation, and interaction with security technologies.

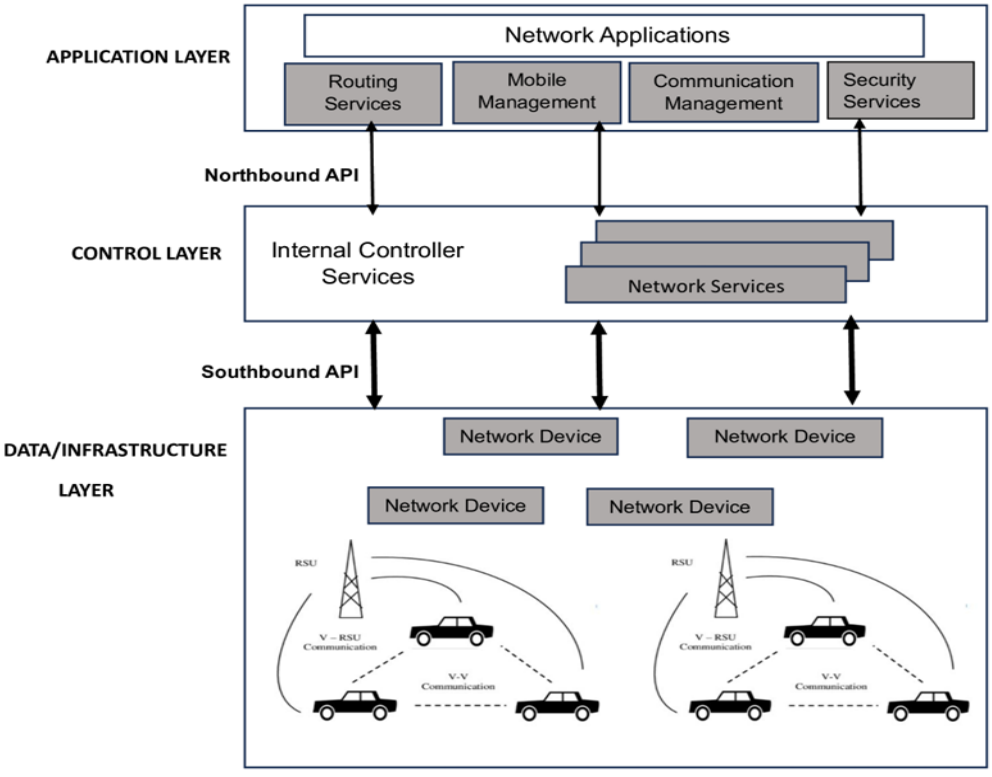

Figure 3 Block Diagram of Software Defined Networking Based Vehicular Ad-Hoc Networks Architecture

REVIEW ARTICLE

3. SECURITY REQUIREMENTS IN VANETS AND SDN-BASED VANETS

Security requirements in SDN-based VANETs are essential to ensure the three main pillars of secure communication i.e. confidentiality, integrity, and availability (CIA) [18]. Key security requirements include:

- Authentication: The process of ensuring that only authorised vehicles, infrastructure components, and network entities are able to access the network and the service it provides. In SDN-based VANETs, vehicles and RSUs constantly communicate to share critical information such as traffic conditions, road blockage alerts, accidents alerts, traffic interruption alerts, vehicle status, or navigation data. Therefore, authentication ensure that only legitimate entities (vehicles, controllers, or RSUs) participate in the network operations to prevent the malicious nodes from injecting false or harmful data in the network.
- Confidentiality: The process of ensuring that the protection of information in the system so that an unauthorized vehicle, infrastructure component, and network entity cannot access it. In SDN-based VANETs, protecting the confidentiality of transmitted data (traffic conditions, road blockage alerts, accidents alerts, traffic interruption alerts, vehicle status, or navigation data) is essential. Therefore, strong encryption methods are required to be deployed in the network.
- Data Integrity: The process of ensuring that the data transferred across the network is not altered or tampered with during transmission. In SDN-based VANETs, ensuring the integrity of data is very essential because any tampering with the transmitted messages (traffic conditions, road blockage alerts, accidents alerts, traffic interruption alerts, vehicle status, or navigation data) could lead to disastrous consequences such as accidents or traffic disruptions.
- Availability: The process of ensuring that network services are always accessible to legitimate vehicles, infrastructure components and network entities. The main functioning of SDN-based VANETs rely on continuous data exchange to maintain optimal traffic flow and safety. The absence of availability in the network could leads to accidents or inefficiencies in transportation.
- Access Control: The process of ensuring to access the network resources based on rules that have been defined in advance. Not all entities in SDN-based VANETs should have equal access to all network resources or information for improving both the reliability and efficiency of the network.
- Non-repudiation: The process of ensuring that the sender of a message cannot later deny having sent it. Non-repudiation in SDN-based VANETs ensures that any actions taken by a vehicle, driver, or controller can be verified at a later stage. This property helps in preventing the entities from denying responsibility for malicious activities or traffic violations. This is essential for accountability and legal enforcement.

By meeting these security requirements, VANETs and SDN-based VANETs may provide secure communication infrastructure that will enhance the vehicle safety and reliability.

4. SECURITY ATTACKS AGAINST VANETS

The security vulnerabilities in VANETs arise from following inherent and external factors [19]. Some of them are discussed here:

- High Mobility and Dynamic Topology: High speeds of vehicles and the frequent changes in network architecture pose significant challenges in maintaining consistent security measures.
- Real-Time Communication Requirements: The low-latency communication for safety-critical applications in VANETs can clash with the time-consuming processes of secure authentication and encryption procedures leading to security vulnerabilities.
- Decentralized Architecture: Security enforcement and trust maintenance are challenging in decentralized network architecture making VANETs susceptible to different kinds of attacks.
- Heterogeneity of Devices: The presence of diverse devices in VANETs presents security challenges owing to their varying capabilities and security features.
- Scalability Issues: Due to limited computing capabilities, it is challenging to provide secure communication as the number of vehicles in the network grows exponentially.
- Open Wireless Medium: Wireless communication is more vulnerable to interference and eavesdropping than wired networks. In comparison to wired networks, physical security measures are less effective in preventing unauthorised access.
- Trust and Identity Management: Trust building among nodes in a very dynamic and open environment is very challenging leading to identity spoofing risks.
- Complex Attack Surface: Due to VANETs' complicated design, attackers are exploiting the physical, data connection, network, transport, and application layers to launch different types of attacks.

REVIEW ARTICLE

- Insider Threats: Compromised VANETs nodes allow attackers to launch internal attacks. This is a major security risk owing to the fact that established trust connections exist between the nodes.
- Insufficient Security Standards: VANET security standards are undergoing evolution and their incomplete adoption cause inconsistent in implementation across manufacturers and devices leading to security vulnerabilities.

In the following subsections, we categorize the security attacks targeting VANETs based on the network communication protocol stack. These attacks are classified into several layers: attacks on the physical layer, attacks on the data link layer, attacks on the network layer, attacks on the transport layer, and attacks on the application layer. Furthermore, these subsections also aim to illustrate the degree to which the integration of SDN with VANETs can mitigate these security concerns, highlighting which attacks can be effectively addressed and which can only be mitigated to a limited extent.

4.1. Security Attacks Against Physical Layer in VANETs

It is the responsibility of the physical layer to ensure that raw bit streams are sent smoothly from one node to another across physical media. When attacks are launched against the physical layer, they have the potential to significantly hinder the communication between two entities and to jeopardize the network's general operation [20]. Some of the most popular types of security attacks on the physical layer in VANETs are shown in Table 1 and degree of mitigation of security attacks against physical layer in VANETs through integration of SDN is shown is Table 2.

Table 1 Security Attacks Against Physical Layer in VANETs

Sr. No	Name of Attack	Description	Impact	Security Attribute Compromised
1	Jamming Attack [21]	An attacker intentionally broadcasts high-power radio frequency signals to interfere with legitimate communication.	Result in loss of connection and prevent vehicles from sharing critical and emergency messages.	Availability
2	Eavesdropping [22]	An unauthorized attacker listens to the conversation between two authorized nodes to extract confidential communication parameters.	Breaches privacy and can lead to the misuse of intercepted data.	Confidentiality.
3	GPS Spoofing [23]	An attacker transmits fake GPS signals to mislead vehicles about their actual location.	Misrouting, accidents, or navigation errors.	Integrity, Authentication.
4	Interference [24]	Intentional or accidental interference from other electronics devices operating in the same frequency band.	Result in loss of connection, data loss, and hinder vehicles from sharing critical and emergency messages.	Availability
5	Node Tampering [25]	An attacker tampers with a vehicle's communication hardware to gain full control over the compromised node	Lead to the injection of malicious data and unauthorized control of the vehicle's communication capabilities	Integrity, Authentication, Confidentiality
6	Node Impersonation Attack [26]	An attacker alters its identity to impersonate a legitimate node at the physical layer.	This attack misleads the network about the presence or activities of legitimate vehicles.	Authentication, Integrity.

REVIEW ARTICLE

Table 2 Mitigation of Security Attacks Against Physical Layer in VANETs Through Integration of SDN

Sr. No.	Name of Attack	SDN Usage	Potential of SDN to Mitigate the Attack	Additional Mechanism Required	SDN Feature Used
1	Jamming Attack	Reroutes traffic away from jammed frequencies or nodes	Mitigatable up to a limited extent	Anomaly detection for signal strength changes	Due to Central Control Mechanism
2	Eavesdropping	Ensures only authorized devices access the network	Mitigatable up to a limited extent	Strong encryption and authentication policies	Due to Programmability
3	GPS Spoofing	Monitors anomalies in location data	Mitigatable up to a limited extent	Secure positioning systems, cryptographic verification	Due to Programmability
4	Interference Node	Optimizes channel allocation and transmission power	Mitigatable up to a limited extent	Interference detection systems, improved signal processing	Due to Flow-based Controlling and Forwarding
5	Tampering Node	Enforces strict access control and authenticates devices	Mitigatable up to a limited extent	Hardware security modules, tamper-resistant hardware	Due to Central Control Mechanism
6	Node Impersonation Attack	Manages certificates, keys, and digital identities centrally	Mitigatable up to a limited extent	Strong encryption and authentication policies	Due to Programmability

SDN introduces additional functionalities such as centralized control mechanism, programmability, and flow-based management to traditional VANETs which significantly improve the mitigation of security attacks at the Physical Layer. Table 2 presents the degree of the mitigation of security attacks against the physical layer in VANETs through the integration of SDN. To achieve complete protection against these attacks, additional mechanisms including strong encryption and authentication techniques, anomaly detection techniques and tamper-proof hardware should be installed in the network.

4.2. Security Attacks Against Data Link Layer in VANETs

The transport of data from node to node with error control and flow control is the main responsibility of the data link layer. However, this layer is susceptible to security attacks that interrupt the communication, compromise data integrity and have serious impact on the performance of the network [27]. Some of the most popular types of security attacks on the data link layer in VANETs are listed in Table 3. Table 4 presents the degree of the mitigation of security attacks against the data link layer in VANETs through the integration of SDN.

Table 4 illustrates that the integration of SDN with traditional VANETs can partially mitigate several data link layer attacks in VANETs. However, in most cases, additional mechanisms like strong encryption and authentication policies, anomaly and collision detection algorithms and secure communication protocols are required for more comprehensive protection.

4.3. Security Attacks Against Network Layer in VANETs

The network layer is responsible for routing the data packets from vehicles to vehicles or infrastructure. An attack on this layer has the potential to dramatically disrupt communication, which may result in the instability of the network and degradation in network efficiency [27].

Some of the most popular types of security attacks on the network layer in VANETs are shown in Table 5 and degree of mitigation of security attacks against network layer in VANETs through integration of SDN is shown is Table 6. Table 6 shows how SDN features like centralized control, programmability, and flow-based controlling and forwarding can be leveraged to mitigate network-layer security attacks in VANETs, with varying levels of success depending on the attack and the additional mechanisms required.

4.4. Security Attacks Against Transport Layer in VANETs

The transport layer is responsible for ensuring the reliable flow of data from vehicles to vehicles or infrastructure (end to end device). Attacks on this layer have the potential to disrupt the end-to-end communication, reduce the performance of the network, and compromise the integrity of the data. Some of the most popular types of security attacks on the transport

REVIEW ARTICLE

layer in VANETs is shown in Table 7 and degree of mitigation of security attacks against transport layer in VANETs through integration of SDN is shown is Table 8.

Table 3 Security Attacks Against Data Link Layer in VANETs

Sr. No	Name of Attack	Description	Impact	Security Attribute Compromised
1	Traffic Analysis Attack [24]	The attacker passively listens to network traffic to capture and analyse sensitive information.	Breaches privacy and can result in the misuse of collected sensitive information.	Confidentiality
2	Beaconing Attack [28]	An attacker sends frequent, false beacon messages causing network congestion.	Results in increased network load and reduced performance	Availability, Integrity
3	Replay Attack [29]	The attacker repeats or delays previously captured valid data frames.	Causes erroneous network responses due to misleading information flow	Integrity, Authentication
4	Identity Spoofing [30]	An attacker gains access network in an unauthorized way by spoofing MAC address.	Misleads other vehicles and causes potential network chaos	Authentication , Integrity
5	Collision Attack [31]	The attacker transmits data frames simultaneously with another node, causing collisions.	Degrades network performance and causes data loss	Availability
6	Resource Exhaustion Attack [16]	An attacker floods the network with fake frames to consume bandwidth, memory, and processing capacity	Reduces network efficiency and can lead to network failure	Availability
7	Bit Flipping Attack	An attacker alters bits within a data frame to corrupt the data.	Causes data corruption and increases retransmissions	Integrity
8	Man-in-the-Middle Attack [32]	A malicious node intercepts and potentially alters communication between two legitimate nodes.	Results in loss of data confidentiality and data manipulation	Confidentiality , Integrity, Authentication

Table 4 Mitigation of Security Attacks Against Data Link Layer in VANETs Through Integration of SDN

Sr. No.	Name of Attack	SDN Usage	Potential of SDN to Mitigate the Attack	Additional Mechanism Required	SDN Feature Used
1	Traffic Analysis Attack	Monitors and controls traffic flows to detect and prevent unauthorized traffic analysis	Mitigatable up to a limited extent	Anomaly detection, traffic encryption	Due to Central Control Mechanism
2	Beaconing Attack	Centralized control to verify and authenticate beacon messages	Mitigatable	Secure beacon message protocols	Due to Programmability
3	Replay Attack	Uses time-stamping and sequence checking to detect replayed messages	Mitigatable up to a limited extent	Cryptographic techniques, secure timestamping	Due to Flow-based Controlling and Forwarding

REVIEW ARTICLE

4	Identity Spoofing	Manages digital identities and certificates centrally	Mitigatable up to a limited extent	Strong encryption and authentication policies	Due to Programmability
5	Collision Attack	Dynamically reroutes traffic and adjusts transmission parameters to avoid collisions	Mitigatable up to a limited extent	Collision detection algorithms	Due to Flow-based Controlling and Forwarding
6	Resource Exhaustion Attack	Centralized resource management to monitor and control resource usage	Mitigatable up to a limited extent	Rate limiting, anomaly detection	Due to Central Control Mechanism
7	Bit Flipping Attack	Monitors data integrity and uses error-checking mechanisms	Mitigatable up to a limited extent	Redundant transmission, error-correcting codes	Due to Programmability
8	Man-in-the-Middle Attack	Centralized authentication and encryption of all communications	Mitigatable up to a limited extent	Strong encryption and mutual authentication	Due to Central Control Mechanism

Table 5 Security Attacks Against Network Layer in VANETs

Sr. No	Name of Attack	Description	Impact	Security Attribute Compromised
1	Sybil Attack [17]	The attacker produces multiple fictitious identities to disturb normal VANET operations by spreading fake messages	Results in incorrect information about traffic density, routing, and resource allocation.	Authentication, Integrity
2	Wormhole Attack [33]	Two malicious nodes establish a private link between distant locations to replay messages.	Results in short paths controlled by the malicious nodes, disrupting routing protocols.	Integrity, Authentication
3	Replay Attack [34]	The attacker fraudulently repeats or delays valid data packets to create confusion or trigger unintended actions	Cause network loops and erroneous responses due to misleading information	Integrity, Authentication
4	Black Hole Attack [35-36]	A malicious node falsely advertises itself as having the best route to the destination, and then drop all of the packets received by it on being an immediate node on the selected route.	Causes loss of data packets and disrupted communication	Availability.
5	Gray Hole Attack [37]	An attacker selectively drops packets, creating intermittent communication issues.	Causes data loss, unreliable delivery, and degraded network performance	Availability
6	Routing Table Overflow Attack [38]	The attacker floods the network with bogus announcements to consume resources and overflow routing tables	Exhausts bandwidth, memory, and processing capacity, causing network crashes.	Availability, Integrity

REVIEW ARTICLE

7	Selfish Node Attack [39-41]	Selfish nodes send their own packets via other nodes but refuse to forward packets from other nodes	Disrupts communication and decreases network reliability	Availability
8	Routing Table Poisoning Attack [42]	Fake routing information is broadcasted by the attacker node to poison the routing tables of other benign nodes.	Results in transmission through non-existent routes, leading to network instability.	Integrity.
9	Sinkhole Attack [43]	An attacker node attracts data traffic by falsely claiming to have the best route, then drops or manipulates the packets	Causes data loss, misrouting, and disrupted communication	Availability, Integrity
10	Location Disclosure Attack [44]	The attacker monitors traffic to gather information about nodes and routes for malicious purposes	Compromises the privacy of vehicles and routes	Confidentiality.
11	Position Falsification [45]	The attacker sends false or manipulated information about position to disrupt location-based services	Misleads information about navigation and routing	Integrity, Authentication
12	Identity Spoofing [46]	The attacker advertises fake identities (by spoofing IP address) to gain unauthorized access or disrupt network functioning	Misleads other nodes and causes network chaos	Authentication, Integrity
13	Packet Dropping [47]	The attacker intentionally drops data and routing packets to disrupt communication.	Causes data loss, reduced reliability, and disrupted communication	Availability
14	Malicious Flooding [48]	The network is flooded with bogus packets by the attacker node to consume network bandwidth and other resources.	Leads to network congestion and degraded performance	Availability
15	Node Impersonation [49]	The attacker quickly alters its identity and provides fake information to other nodes.	Misleads communication and causes data breaches	Authentication, Integrity
16	Collusion Attack [50]	Multiple malicious nodes collaborate to launch attacks and disrupt network functioning.	Amplifies the impact and increases network instability	Integrity, Availability
17	Routing Loop Attack [51]	The attacker advertises routes to create routing loops and waste resources.	Consumes resources and increases transmission delays	Availability, Integrity

Table 6 Mitigation of Security Attacks Against Network Layer in VANETs Through Integration of SDN

Sr. No.	Name of Attack	SDN Usage	Potential of SDN to Mitigate the Attack	Additional Mechanism Required	SDN Feature Used
1	Sybil Attack	Centralized management of identities to detect and prevent multiple identities from a single node	Mitigatable	Strong authentication and digital identity management	Due to Central Control Mechanism

REVIEW ARTICLE

2	Wormhole Attack	Monitors and detects abnormal traffic patterns indicative of wormhole attacks	Mitigatable up to a limited extent	Secure localization and timing verification	Due to Central Control Mechanism
3	Replay Attack	Uses time-stamping and sequence checking to detect replayed messages	Mitigatable up to a limited extent	Cryptographic techniques, secure timestamping	Due to Flow-based Controlling and Forwarding
4	Black Hole Attack	Centralized monitoring to detect and isolate malicious nodes dropping traffic	Mitigatable up to a limited extent	Collaborative detection algorithms	Due to Central Control Mechanism
5	Gray Hole Attack	Monitors traffic patterns to detect selective forwarding	Mitigatable up to a limited extent	Anomaly detection algorithms	Due to Central Control Mechanism
6	Routing Table Overflow Attack	Controls routing table entries to prevent overflow attacks	Mitigatable	Routing table management	Due to Central Control Mechanism
7	Selfish Node Attack	Monitors and enforces cooperative behaviour among nodes	Mitigatable up to a limited extent	Incentive mechanisms, behaviour monitoring	Due to Central Control Mechanism
8	Routing Table Poisoning Attack	Verifies routing updates and maintains integrity of routing tables	Mitigatable up to a limited extent	Secure routing protocols	Due to Programmability
9	Sinkhole Attack	Detects and isolates nodes that attract and drop traffic	Mitigatable up to a limited extent	Anomaly detection, reputation systems	Due to Central Control Mechanism
10	Location Disclosure Attack	Monitors location data and detects anomalies	Mitigatable up to a limited extent	Encryption, secure localization techniques	Due to Central Control Mechanism
11	Position Falsification	Cross-checks position information with multiple sources	Mitigatable up to a limited extent	Secure localization techniques	Due to Programmability
12	Identity Spoofing	Manages digital identities and certificates centrally	Mitigatable up to a limited extent	Strong encryption and authentication policies	Due to Programmability

REVIEW ARTICLE

13	Packet Dropping	Detects and mitigates nodes dropping packets	Mitigatable up to a limited extent	Traffic analysis and anomaly detection	Due to Flow-based Controlling and Forwarding
14	Malicious Flooding	Limits and controls the rate of traffic to prevent flooding	Mitigatable	Rate limiting, anomaly detection	Due to Central Control Mechanism
15	Node Impersonation	Centralized authentication of all nodes	Mitigatable up to a limited extent	Strong encryption and mutual authentication	Due to Central Control Mechanism
16	Collusion Attack	Monitors collaborative behaviour of nodes to detect collusion	Mitigatable up to a limited extent	Anomaly detection, behaviour monitoring	Due to Central Control Mechanism
17	Routing Loop Attack	Detects and corrects routing loops	Mitigatable	Loop prevention mechanisms, routing protocols	Due to Programmability

Table 7 Security Attacks Against Transport Layer in VANETs

Sr. No	Name of Attack	Description	Impact	Security Attribute Compromised
1	Session Hijacking [52]	An attacker hijacks and takes control of an active session between two nodes by predicting packet sequence numbers	Unauthorized access to session data, data manipulation, and disrupted communication	Confidentiality, Integrity
2	Man-in-the-Middle Attack [32]	A malicious node intercepts and potentially alters communication between two legitimate vehicles	Loss of data confidentiality, injection of malicious data, and data manipulation	Confidentiality, Integrity, Authentication
3	Denial of Service (DoS) Attack [1, 52-56]	To block a victim from accessing available network resources, an attacker floods them with a huge number of bogus packets.	Network congestion, unavailability, and degraded performance	Availability
4	Distributed Denial of Service (DDoS) Attack [1, 52-56]	Multiple nodes perform a DoS attack in a coordinated manner.	Severely degraded network performance, service disruption, and potential network collapse.	Availability
5	TCP SYN Flood Attack [57]	An attacker sends numerous TCP SYN requests, exhausting the target node's resources.	Resource exhaustion, denial of new connections, and potential node crash.	Availability.

REVIEW ARTICLE

6	ACK Storm Attack [58]	An attacker sends a high volume of TCP ACK packets to create an ACK storm.	Resource consumption, network congestion, and degraded performance.	Availability.
7	Port Scanning [59]	An attacker scans target nodes for open ports to identify potential vulnerabilities.	Identification of vulnerabilities for further attacks.	Confidentiality , Integrity.
8	Jellyfish (JF) Attack [60-61]	An attacker delays, drops, or reorders data packets to degrade network throughput.	Increased latency, potential data corruption, and degraded performance	Availability, Integrity.
9	Packet Injection [62]	An attacker injects malicious packets into an existing communication stream.	Misinformation, data corruption, and potential exploitation of services.	Integrity, Authentication .
10	Fragmentation Attack [63]	An attacker sends fragmented packets to bypass security mechanisms and inject malicious data.	Data corruption and bypassing of intrusion detection systems	Integrity, Authentication
11	Replay Attack [34]	An attacker fraudulently repeats or delays valid packets	Erroneous network responses, data corruption, and unauthorized actions	Integrity, Authentication

Table 8 Mitigation of Security Attacks Against Transport Layer in VANETs Through Integration of SDN

Sr. No.	Name of Attack	SDN Usage	Potential of SDN to Mitigate the Attack	Additional Mechanism Required	SDN Feature Used
1	Session Hijacking	Monitors and controls session states and data flows	Mitigatable up to a limited extent	Strong session encryption, authentication	Due to Flow-based Controlling and Forwarding
2	Man-in-the-Middle Attack	Centralized authentication and encryption of all communications	Mitigatable up to a limited extent	Strong encryption and mutual authentication	Due to Central Control Mechanism
3	Denial of Service (DoS) Attack	Monitors and controls traffic to detect and mitigate abnormal traffic patterns	Mitigatable up to a limited extent	flow rate limiting, anomaly detection	Due to Central Control Mechanism
4	Distributed Denial of Service (DDoS) Attack	Centralized traffic analysis to detect and mitigate distributed attack patterns	Mitigatable up to a limited extent	Distributed detection systems	Due to Central Control Mechanism
5	TCP SYN Flood Attack	Controls and limits the rate of SYN packets	Mitigatable	SYN cookie mechanism, flow rate limiting	Due to Programmability
6	ACK Storm Attack	Monitors and limits the rate of ACK packets	Mitigatable	Rate limiting	Due to Programmability
7	Port Scanning	Detects and blocks unauthorized port	Mitigatable	Intrusion detection	Due to Central

REVIEW ARTICLE

		scanning activities		systems	Control Mechanism
8	Jellyfish (JF) Attack	Monitors traffic patterns to detect and mitigate delays introduced by malicious nodes	Mitigatable up to a limited extent	Anomaly detection	Due to Flow-based Controlling and Forwarding
9	Packet Injection	Centralized verification and authentication of packets	Mitigatable up to a limited extent	Strong packet authentication	Due to Central Control Mechanism
10	Fragmentation Attack	Monitors and verifies packet fragments	Mitigatable up to a limited extent	Strong packet reassembly and verification	Due to Programmability
11	Replay Attack	Uses time-stamping and sequence checking to detect replayed messages	Mitigatable up to a limited extent	Cryptographic techniques, secure timestamping	Due to Flow-based Controlling and Forwarding

Table 9 Security Attacks Against Application Layer in VANETs

Sr. No	Name of Attack	Description	Impact	Security Attribute Compromised
1	Message Tampering / Data Corruption [64]	Malicious entities introduce errors or alter messages exchanged between vehicles or infrastructure	Leads to information modification, misleading alerts, compromised reliability, and potential exploitation	Integrity, Authentication
2	Privacy Breach [65]	Unauthorized access and disclosure of sensitive information about vehicles, drivers, or passengers.	Results in identity theft, misuse of personal data, and privacy violations	Confidentiality
3	Illusion Attack / Fake Traffic Information / False Alert Generation [66]	An attacker disseminates false alerts about road conditions to mislead vehicles or infrastructure.	Causes confusion, potential accidents, traffic jams, incorrect routing, and safety risks.	Integrity
4	Unauthorized Data Access [67]	Gaining unauthorized access to prohibited or sensitive data in VANET applications.	Leads to accessing, manipulating critical information, and potential exploitation	Confidentiality, Authentication
5	False Data Injection [68]	Injecting malicious or false data into VANET applications to mislead systems	Results in misleading decisions, compromised functionality, and safety risks	Integrity.
6	Malware Injection [69]	Injecting malicious software into VANET applications to compromise security or functionality.	Causes data theft, service disruption, security compromise, and malware spread.	Confidentiality, Integrity, Availability.

REVIEW ARTICLE

7	Collaborative Attack [70]	Multiple attackers work together to compromise VANET applications	Increases attack surface and difficulty in detection and mitigation	Integrity, Authentication.
8	On-off Attack [71]	An attacker frequently switches between benign and malicious behavior.	Causes inconsistent system performance and challenges in attack identification and mitigation.	Integrity.
9	Firmware or Software Exploitation [72]	Exploiting vulnerabilities in vehicle firmware or software for unauthorized access or manipulation	Compromises vehicle control, data integrity, and potentially disrupts the network	Integrity, Authentication.

Table 8 shows how SDN's core features such as centralized control, programmability and flow-based controlling can effectively mitigate various attacks at the transport layer though additional mechanisms like encryption and authentication, anomaly detection, and rate limiting are often required for full protection.

4.5. Security Attacks Against Application Layer in VANETs

The application layer encompasses the software and protocols that make it possible for certain applications and services to be provided to infrastructure and vehicles. The security attacks at this layer will results in the manipulation of data, and violation of security and privacy. Some of the most popular types of security attacks on the application layer in VANETs are shown in Table 9 and degree of mitigation of security attacks against application layer in VANETs through integration of SDN is shown is Table 10.

Table 10 Mitigation of Security Attacks Against Application Layer in VANETs Through Integration of SDN

Sr. No.	Name of Attack	SDN Usage	Potential of SDN to Mitigate the Attack	Additional Mechanism Required	SDN Feature Used
1	Message Tampering / Data Corruption	Centralized monitoring and verification of message integrity	Mitigatable up to a limited extent	Strong encryption and message authentication	Due to Flow-based Controlling and Forwarding
2	Privacy Breach	Ensures access control and monitors data access centrally	Mitigatable up to a limited extent	Strong encryption and access control policies	Due to Central Control Mechanism
3	Illusion Attack / Fake Traffic Information / False Alert Generation	Centralized validation and verification of traffic information	Mitigatable up to a limited extent	Secure data verification mechanisms	Due to Flow-based Controlling and Forwarding
4	Unauthorized Data Access	Centralized enforcement of access control policies	Mitigatable	Strong authentication and authorization	Due to Central Control Mechanism
5	False Data Injection	Verifies data integrity and authenticity before forwarding	Mitigatable up to a limited extent	Cryptographic verification of data	Due to Flow-based Controlling and Forwarding
6	Malware Injection	Monitors and controls the flow of data to detect and block malicious content	Mitigatable up to a limited extent	Intrusion detection systems, malware signatures	Due to Programmability

REVIEW ARTICLE

7	Collaborative Attack	Monitors and analyses collaborative behaviours to detect anomalies	Mitigatable up to a limited extent	Anomaly detection algorithms	Due to Central Control Mechanism
8	On-off Attack	Centralized monitoring of node behaviour to detect and mitigate on-off patterns	Mitigatable up to a limited extent	Anomaly detection, behaviour analysis	Due to Central Control Mechanism
9	Firmware or Software Exploitation	Centralized management and verification of firmware and software updates	Mitigatable up to a limited extent	Secure boot mechanisms, cryptographic verification	Due to Programmability

Table 10 demonstrates how SDN's centralized control, programmability, and flow-based control mechanisms can be leveraged to mitigate security attacks at the application layer in VANETs. However, the success of these mitigations often depends on the integration of additional mechanisms such as strong encryption and message authentication, intrusion detection systems and secure data verification.

5. SECURITY ATTACKS IN SDN-BASED VANETS

It is possible to enhance the network administration and flexibility by integrating the functions of SDN with VANETs. However, this strategy also offers a unique set of security risks owing to the integrated approach of both complex architectures. The security vulnerabilities in SDN-based VANETs arise from the inherent features of SDN mainly due to central control mechanism, programmability and flow-based controlling and forwarding [7-8, 73,74]. Some of security vulnerabilities in SDN-based VANETs are discussed here:

- Complex Architecture: Integration of SDN in VANETs complicates the job of finding and securing all the vulnerabilities and even secure interoperability between controllers of SDN and VANET components is also a big challenge.
- Centralized Control Plane Vulnerabilities: The controller being the central sole point for decision-making and all operations of network makes it an easy target for attackers. By compromising the SDN controller, attackers can easily modify network policies and cause network services to malfunction. As a result, the controller's security is a critical issue that must be addressed in order to defend the entire network.
- Mobility and Dynamic Topology: Any effort towards continuous security enforcement is complicated in SDN-based VANETs due to the high mobility of vehicles and frequent changes in network topology.
- Data Plane Vulnerabilities: In an SDN-managed VANET, compromised devices have the ability to introduce malicious traffic and obstruct communication by taking advantage of data plane vulnerabilities that impact both SDN and VANET components. SDN risks to the control and application layers are amplified by vehicle mobility and openness in the data plane. As a result, the data plane should be secured with proper authentication mechanism.
- Interface Vulnerabilities: Insecure northbound and southbound APIs may enable man-in-the-middle attacks in SDN-VANET connection owing to poor encryption and authentication. The security and lack of standardisation of APIs are major issues that are required to be address.
- Resource Constraints: Vehicles' limited processing and storage capacity limit the use of strong authentication and encrypted security protocols, influencing performance and scalability trade-offs in integrated network security measures.
- Insider Threats: Legitimate nodes in VANETs can be compromised for internal attacks, and unlawfully access to SDN controllers or VANET devices can lead to malicious configurations or policies in the networks.
- Trust and Identity Management: Establishing trust among the mobile nodes in integrated networks is very challenging. The security risks involving identity spoofing are heightened due to lack of proper identity management across SDN and VANET components.
- Lack of Standardization: There is a lack of standardised security protocols, which results in uneven security across SDN-VANET settings. This creates challenge in maintaining interoperability and strong security across diverse implementations.
- Real-Time Communication Requirements: The low-latency communication for safety-critical applications in VANETs can clash with the time-consuming processes of secure authentication and encryption procedures in SDN based VANETs which might possibly compromise security protocols in order to fulfil fast response requirements.

REVIEW ARTICLE

- Privacy Concerns: The integration of SDN with VANETs raises concerns about privacy breaches and location tracking without adequate anonymization.
- Network Monitoring and Forensics Challenges: It is highly required to have sophisticated monitoring and analysis tools in order to achieve visibility and identify critical attacks in integrated SDN-VANET networks due to inherent complexity and variety of vulnerabilities that are associated with both architectures.
- Interoperability between Multiple Controllers: In distributed SDN architecture, the interoperability between multiple controllers can also be a source of vulnerabilities to be exploited by the attackers.

In this section, we have described the security attacks against SDN-based VANETs in accordance to the three-layer architecture of SDN. These attacks demonstrate how the unique features of SDN, such as its central control mechanism, programmability, and flow-based controlling, can introduce new security vulnerabilities in VANETs across the control, data, and application planes. These attacks include attacks on the control plane, data plane and application plane along with their impacts, target components in integrated SDN-VANETs and the features of integrated SDN-VANETs exploited by the attacker. The security attacks against data plane/ layer in SDN-based VANETs are shown in Table 11. These security attacks mainly exploit the flow-based controlling and forwarding feature of SDN. The security attacks against control plane/ layer in SDN-based VANETs are shown in Table 12. These security attacks mainly exploit the central control mechanism feature of SDN. The security attacks against application plane/ layer in SDN-based VANETs are shown in Table 13. These security attacks mainly exploit the programmability feature of SDN. In the last, the security attacks against multiple planes and APIs in SDN-based VANETs are shown in Table 14.

Table 11 demonstrates that how the central control mechanism, flow-based controlling and forwarding, and programmability features of SDN can be exploited by the attackers when integrated with VANETs. These features introduce new vulnerabilities in the data plane of SDN-based VANETs that attackers can easily exploit to target the SDN Controller, VANET nodes, SDN switches, and communication channels.

Table 11 Security Attacks Against Data Plane/ Layer in SDN-Based VANETs

Sr. No	Name of Attack	Description	Impact	Target Components	SDN Feature exploited
1	Spoofing Attacks [75]	Attackers impersonate legitimate nodes to inject false information	Misrouting, unauthorized access	SDN Controller, VANET nodes	Central control mechanism, Flow-based controlling and forwarding
2	Flow Table Overflow Attacks [8,76]	Attackers flood SDN switches' flow tables with excessive flow rules.	Controller performance degradation, Switch performance degradation, packet loss	SDN Switches	Flow-based controlling and forwarding
3	Packet Sniffing Attacks [77]	Attackers capture packets to gain sensitive information	Sensitive data leakage	Communication channels	Flow-based controlling and forwarding
4	Wormhole Attacks [7]	Attackers create a tunnel to replay packets in different parts of the network	Route disruption	Communication channels, VANET nodes	Flow-based controlling and forwarding
5	Jamming Attacks [7, 8]	Attackers disrupt communication by overwhelming the network with interference	Communication disruption	VANET nodes, Communication channels	Flow-based controlling and forwarding
6	Routing Loop Attacks [78]	Attackers create routing loops causing network congestion	Network congestion	SDN Controller, VANET nodes	Flow-based controlling and

REVIEW ARTICLE

					forwarding
9	Eavesdropping [79]	Attackers capture data packets to extract sensitive information	Data breach, privacy violation	Communication channels, SDN Switches RSUs, VANET nodes	Flow-based controlling and forwarding
10	Traffic Analysis [80]	Attackers analyze traffic patterns to infer sensitive information	Privacy breach, network reconnaissance	SDN Switches, VANET nodes	Flow-based controlling and forwarding
11	Packet Dropping [81]	Compromised switches drop packets instead of forwarding them	Data loss, service degradation	SDN Switches	Flow-based controlling and forwarding
12	Side-Channel Attacks [82]	Attackers use indirect methods to gather physical information about the network (analysis of power to break cryptography)	Unauthorized information retrieval	SDN Controller, VANET nodes	Flow-based controlling and forwarding
13	False Data Injection Attacks [83]	False data is injected into the network by attackers to mislead the decision-making processes.	Incorrect network decisions, Network disruption, data integrity issues	SDN Controller, VANET nodes, SDN Switches	Programmability, Flow-based controlling and forwarding
14	Blackhole Attacks [84]	Compromised nodes drop packets instead of forwarding them	Packets loss	VANET nodes, SDN Controller	Programmability, Flow-based controlling and forwarding
15	Grayhole Attacks [85]	Selectively dropping packets to avoid detection	Selective packets loss	VANET nodes, SDN Controller	Programmability, Flow-based controlling and forwarding
16	Switch Compromise Attacks [86]	Attackers gain control of SDN switches to manipulate traffic	Traffic manipulation	SDN Switches	Programmability
17	Man-in-the-Middle (MitM) Attacks [87-88]	Attackers intercept and manipulate communication between nodes	Data interception, modification	Communication channels between SDN Controller and nodes, Data Plane	Programmability, Flow-based controlling and forwarding
18	Replay Attacks [7]	Attackers replay captured packets to execute unauthorized actions	Unauthorized actions	Communication channels, SDN Controller, Data Plane	Programmability, Flow-based controlling and forwarding
19	Traffic Sniffing [80]	Accessing and analysing important network data, especially at network joints	Data interception, potential data	Network joints, flow rules	Central control mechanism,

REVIEW ARTICLE

		and important elements	breaches		programmability
20	Buffer Saturation [89]	Filling the buffer with excessive data to prevent normal data processing	Data loss, network performance degradation	Data plane	Flow-based controlling and forwarding
21	Link Layer Discovery Protocol (LLDP) Manipulation [90]	Exploiting LLDP to create incorrect network topologies	Network topology manipulation, data misrouting	Southbound Interface Attacks, Data Plane	Flow-based controlling and forwarding

Table 12 Security Attacks Against Control Plane/ Layer in SDN-Based VANETs

Sr. No	Name of Attack	Description	Impact	Target Components	SDN Feature exploited
1	Decentralized Controller Synchronization Attack [91]	Attackers disrupt synchronization between decentralized SDN controllers managing VANET segments	Segment isolation, network partition	Decentralized controllers, Inter-segment communication	Central control mechanism
2	Multi-Controller Partitioning	Attackers partition SDN-based VANETs by compromising communication between multiple SDN controllers	Controller isolation, network segmentation	SDN Controller communication, VANET nodes	Central control mechanism
3	Topology Poisoning Attacks [92, 93]	Attackers inject false topology information to mislead the controller	Incorrect routing information	SDN Controller, Routing algorithms	Central control mechanism and Programmability
4	Controller Hijacking Attacks [94]	Attackers gain control of the SDN controller to manipulate the operation of the networks	Total control over network	SDN Controller	Central control mechanism
5	Control Message Tampering [95]	Control messages sent between the controller and network devices are tempered by attackers	Incorrect network state, misconfiguration	SDN Controller, SDN Switches	Central control mechanism and Programmability
6	Control Plane Isolation [96]	Attackers isolate the control plane from data plane devices	Loss of network control, service disruption	SDN Controller, SDN Switches	Central control mechanism
7	Inter-Controller Communication Attack	Attackers disrupt communication between multiple controllers in a distributed SDN environment	Controller isolation, network segmentation	SDN Controllers	Central control mechanism

REVIEW ARTICLE

8	Control Plane Manipulation [97]	Attackers manipulate control plane messages to disrupt or alter network operations	Network instability, service disruption	SDN Controller, VANET nodes	Central control mechanism, Programmability
9	Hierarchical Authorization Escalation [98]	Attackers exploit hierarchical authorization structures in SDN to escalate privileges and gain unauthorized access	Unauthorized control, policy violation	Authorization frameworks, SDN Controller	Central control mechanism
10	Controller Resource Exhaustion [99]	Attackers consume the controller's resources to degrade its performance	Sluggish network response, service degradation	SDN Controller	Central control mechanism
11	Time Synchronization Manipulation [100]	Attackers manipulate time synchronization protocols in SDN-based VANETs to disrupt coordinated actions	Traffic coordination failure, safety risks	Time synchronization protocols, Control Plane, VANET nodes	Flow-based controlling and forwarding, Programmability
12	Link Fabrication Attacks [101]	Attackers create fake links in the network topology	Fake network topology	SDN Controller	Central control mechanism, Programmability
13	Policy Violation Exploitation [102]	Attackers exploit gaps in policy enforcement mechanisms of SDN controllers to gain unauthorized access	Unauthorized network access, data breach	SDN Controller, Security policies	Central control mechanism, Programmability
14	Virtual Network Isolation Bypass [103]	Attackers bypass virtual network isolation mechanisms in SDN to gain unauthorized access to sensitive traffic	Data leakage, privacy violation	Virtualized network components, SDN Controller	Programmability
15	Protocol-level Vulnerability Exploitation [104]	Attackers exploit vulnerabilities in SDN-based protocol implementations to gain unauthorized control over network functions	Protocol compromise, network instability	Protocol implementations, SDN Controller	Programmability
16	Deformed Control Packets Injection [80]	Injecting suspicious control packets to induce abnormal switch behaviour and expose network vulnerabilities	Abnormal network behaviour, potential vulnerability exploitation	Control Plane, SDN Switches, control packets	Programmability, Central control mechanism
17	Centralized Botnet Command and Control [105]	Utilizing central control to issue commands	Coordinated attacks, large-scale disruptions	SDN Controller, vehicles nodes	Central control mechanism

REVIEW ARTICLE

18	Password Guessing or Brute Force [80]	Predicting or brute-forcing user passwords to gain network access	Unauthorized access, potential data breaches	Non-SDN devices	Central control mechanism, programmability
19	Controller Compromise [106]	Compromise of the central controller by attackers affects the Data plane's security	Network-wide compromise if the controller is compromised	SDN controller, Data plane	Central control mechanism

Table 12 demonstrates that the control plane in SDN-based VANETs is highly vulnerable to attacks that exploit the central control mechanisms and programmability, making it a key target for attackers. These attacks can result in serious consequences, including network partitioning, data breaches, unauthorized access, and controller compromise, ultimately disrupting the overall functionality of the VANET.

Table 13 emphasizes that the application plane in SDN-based VANETs is particularly vulnerable to critical attacks exploiting the network's programmability, especially through compromised applications and policies. These attacks can result in severe consequences, including unauthorized network manipulation, data breaches, and service disruptions, directly affecting the security and integrity of VANETs.

Table 13 Security Attacks Against Application Plane/ Layer in SDN-Based VANETs

Sr. No	Name of Attack	Description	Impact	Target Components	SDN Feature exploited
1	Application Layer Hijacking [107]	Attackers gain control of applications interacting with the SDN controller	Unauthorized network manipulation, data theft	SDN Applications, SDN Controller	Programmability
2	Application Policy Violation [108]	Attackers exploit vulnerabilities in application policies to bypass security measures	Unauthorized access, policy breaches	SDN Applications, SDN Controller	Programmability
3	Application Communication Attack [108]	Attackers intercept and manipulate communication between SDN applications and the controller	Data integrity issues, unauthorized actions	SDN Applications, SDN Controller	Programmability
4	Cloud-based Service Provider Compromise [109]	Attackers compromise SDN-based cloud service providers managing VANET resources to gain unauthorized access	Service disruption, data breach	Cloud infrastructure, Application Plane, SDN Controller	Central control mechanism, Programmability, API
5	Malicious Application Injection [110]	Attackers inject malicious applications to manipulate network behavior	Network disruption, data breaches	SDN Applications, SDN Controller	Programmability
6	Add-ons [111]	Inserting malicious add-ons or plugins to manipulate data or network behaviour	Unauthorized data access, network manipulation	Data transfer and management, Application Plane	Programmability

REVIEW ARTICLE

Table 14 Security Attacks Against Multiple Planes/ Layers in SDN-Based VANETs

Sr. No	Name of Attack	Description	Impact	Target Components	SDN Feature exploited	Planes
1	Denial of Service (DoS) Attacks [112-122]	Attackers overwhelm the network especially SDN controller with traffic, rendering it unusable	Service disruption, network unavailability	SDN Controller, RSUs, VANET Nodes	Central control mechanism, Flow-based controlling and forwarding	Data Plane, Control Plane
2	Distributed Denial of Service (DDoS) Attacks [112-122]	Multiple compromised nodes flood the network, causing a denial of service	Network paralysis	SDN Controller, RSUs, VANET Nodes	Central control mechanism, Flow-based controlling and forwarding	Data Plane, Control Plane
3	Flow Rule Manipulation / Modification [123]	Attackers alter flow rules in switches to misroute traffic	Traffic hijacking, network inefficiencies, data leakage	SDN Switches, Data Plane, Control Plane	Flow-based controlling and forwarding, Programmability	Data Plane, Control Plane
4	Sybil Attacks [7]	Attackers create multiple fake identities to disrupt the network	Network confusion	VANET nodes, SDN Controller	Central control mechanism, Flow-based controlling and forwarding	Control Plane, Data Plane
5	Misconfiguration [124]	Inaccurately configured or left insecure the flow rules stored in the flow tables of OpenFlow switches	Network performance issues, potential misrouting of data	Data Plane, Control Plane, Application Plane, Flow tables, OpenFlow switches	Central control mechanism, Programmability, Flow-based controlling and forwarding	Data Plane, Control Plane, Application Plane
6	Lack of Authentication and Authorization [79]	Absence of robust authentication and authorization mechanisms for applications	Unauthorized access to the network, potential insertion of malicious applications	Data Plane, Control Plane, Application Plane, Applications within the SDN environment	Central control mechanism, Programmability, Flow-based controlling and forwarding	Data Plane, Control Plane, Application Plane
7	API Exploitation [125]	Attackers exploit APIs exposed by SDN applications to gain unauthorized access	Data leakage, unauthorized control	SDN Applications, SDN Controller	Programmability, API	Control Plane, Interfaces
8	Programmable Malware Injection [126]	Injecting malware into the network via programmable interfaces	Network-wide compromise, data breaches.	Application plane, SDN controller	Programmability	Control Plane, Interfaces

Table 14 highlights a range of security attacks that can impact various planes of SDN-based VANETs. It also emphasizes how vulnerabilities stemming from SDN's inherent features can undermine the network's integrity, availability, and confidentiality. The central control mechanism and programmability of SDN play critical roles in both facilitating these attacks and offering potential avenues for their mitigation, underscoring the need for robust security measures across all layers of the network.

REVIEW ARTICLE

6. FUTURE RESEARCH DIRECTIONS

- Researchers should make the effort to discover unseen attacks within the integrated SDN-VANET framework, focusing on vulnerabilities introduced by the integration of SDN.
- Researchers should investigate cutting-edge cryptographic methods to develop stronger authentication and authorization mechanisms for SDN-based VANETs.
- Researchers should explore the applications of machine learning and artificial intelligence to design real-time intrusion detection systems capable of detecting and responding to threats in SDN-based VANETs.
- Researchers should develop real-time anomaly detection systems using big data and analytics to quickly identify and mitigate potential threats in SDN-based VANETs.
- Researchers should investigate the influence of emerging technologies such as AI, quantum computing, and 5G on the security landscape of SDN-based VANETs, focusing on both risks and security enhancements.
- Researchers should develop innovative strategies to enhance the control plane's resilience against attacks such as controller hijacking, control message tampering, and other vulnerabilities unique to SDN.
- Researchers should investigate the use of blockchain technology to implement decentralized trust and security mechanisms for safeguarding communication and data integrity in SDN-based VANETs.
- Researchers should pay attention to the development of integrated security frameworks that span across different network planes (application, control, and data) to improve the overall security posture of SDN-based VANETs.
- Researchers should pay attention to design realistic testbeds and simulation environments for evaluating the security and performance of SDN-based VANETs under various attack scenarios.
- Researchers should develop the secure methods to ensure secure and private data transmission within SDN-based VANETs while allowing efficient communication, especially when handling critical information.

7. CONCLUSION

In conclusion, the convergence of SDN with VANETs can be seen as an innovative solution that can effectively tackle many challenges faced by traditional VANETs. The inherent characteristics of SDN are well suited to address the challenging requirements of traditional VANETs such as requirement of high throughput, efficient management of high mobility of vehicles, low communication latency, and the ability to effectively handle the heterogeneity and scalability of vehicles. However, in this paper, the convergence of SDN with traditional VANETs can be seen as twofold by nature particularly concerning secure network communication. On one hand, the inherent features of SDN assist the traditional VANETs in the effective functioning of various VANETs services as well as in addressing the some of the security vulnerabilities of VANETs. On the other hand, this integrated architecture of SDN with VANETs introduces new security vulnerabilities due to the intrinsic characteristics of SDN. SDN-based VANETs may be more prone to security vulnerabilities than traditional VANETs due to the implementation of the logically centralized network control mechanism and the continued growth in cyber-attacks. Despite these challenges, the researchers have paid little attention to designing robust security solutions for SDN-based VANETs. The study presented in this paper is an attempt to provide researchers the domain knowledge of the specific security issues in both traditional VANETs and SDN-based VANETs. This study will help the researchers in better understanding these vulnerabilities as well as motivate them to design strong security solutions for securing the network operations of SDN-based VANETs. As future work, we recommend that researchers should leverage the potential of emerging technologies including artificial intelligence, machine learning and blockchain technology to design the strong security solutions for SDN-based VANETs.

REFERENCES

[1] 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, Jun. 2020.

[2] S. A. Abdel Hakeem, A. A. Hady, and H. Kim, “Current and Future Developments to Improve 5G-New Radio Performance in Vehicle-to-Everything Communications,” Telecommunication Systems, vol. 75, no. 3, pp. 331–353, Aug. 2020.

[3] S. Sharma, A. Kaul, S. Ahmed, and S. Sharma, “A Detailed Tutorial Survey on VANETs: Emerging Architectures, Applications, Security Issues, and Solutions,” International Journal of Communication Systems, vol. 34, no. 14, pp. 4905, Aug. 2021.

[4] H. Taslimasa, S. Dadkhah, E. C. P. Neto, P. Xiong, S. Ray, and A. A. Ghorbani, “Security Issues in Internet of Vehicles (IoV): A Comprehensive Survey,” Internet of Things, vol. 22, p. 100809, 2023.

[5] F. Cunha, L. Villas, A. Boukerche, G. Maia, A. Viana, R. A. Mini, and A. A. Loureiro, “Data Communication in VANETs: Protocols, Applications and Challenges,” Ad Hoc Networks, vol. 44, pp. 90–103, 2016.

[6] 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.

[7] M. Arif, G. Wang, O. Geman, V. E. Balas, P. Tao, A. Brezulianu, and J. Chen, “SDN based VANETs, Security Attacks, Applications, and Challenges,” Applied Sciences, vol. 10, no. 9, p. 3217, 2020.

[8] 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, 2021.

[9] M. J. Patil and K. P. Adhiya, "A Comprehensive Study on VANET Security," in Proceedings of the International Conference on

REVIEW ARTICLE

Advancements in Smart Computing and Information Security, Cham, Switzerland: Springer Nature, pp. 363–382, 2023.
[10] J. T. Penttinen, "5G Explained: Security and Deployment of Advanced Mobile Communications," John Wiley & Sons, 2019.
[11] S. A. Abdel Hakeem, A. A. Hady, and H. Kim, "5G-V2X: Standardization, Architecture, Use Cases, Network-Slicing, and Edge-Computing," Wireless Networks, vol. 26, no. 8, pp. 6015–6041, Jul. 2020.
[12] K. Nisar, E. R. Jimson, M. H. A. Hijazi, I. Welch, R. Hassan, A. H. M. Aman, 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, 2020.
[13] C. Caba and J. Soler, "APIs for QoS Configuration in Software Defined Networks," in Proceedings of the 2015 1st IEEE Conference on Network Softwarization (NetSoft), pp. 1-5, IEEE, 2015.
[14] F. Holik and J. Horalek, "Implementing SDN into Computer Network Lessons," Journal of Telecommunication, Electronic and Computer Engineering, vol. 9, no. 1–3, pp. 65–69, 2017.
[15] M. M. Islam, M. T. R. Khan, M. M. Saad, and D. Kim, "Software-Defined Vehicular Network (SDVN): A Survey on Architecture and Routing," Journal of Systems Architecture, vol. 114, p. 101961, 2021.
[16] 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.
[17] B. Yu, C. Z. Xu, and B. Xiao, "Detecting Sybil Attacks in VANETs," Journal of Parallel and Distributed Computing, vol. 73, no. 6, pp. 746–756, 2013.
[18] W. B. Jaballah, M. Conti, and C. Lal, "Security and Design Requirements for Software-Defined VANETs," Computer Networks, vol. 169, p. 107099, 2020.
[19] M. Arif, G. Wang, M. Zakirul Alam Bhuiyan, T. Wang, and J. Chen, "A Survey on Security Attacks in VANETs: Communication, Applications, and Challenges," Vehicular Communications, vol. 19, p. 100179, Oct. 2019.
[20] S. Kumar and K. Dutta, "Securing Mobile Ad Hoc Networks," International Journal of Handheld Computing Research, vol. 7, no. 1, pp. 26–76, Jan. 2016.
[21] L. Mokdad, J. Ben-Othman, and A. T. Nguyen, "DJAVAN: Detecting Jamming Attacks in Vehicle Ad Hoc Networks," Performance Evaluation, vol. 87, pp. 47–59, 2015.
[22] D. P. Choudhari and S. S. Dorle, "Maximization of Packet Delivery Ratio for DADCQ Protocol After Removal of Eavesdropping and DDoS Attacks in VANET," in 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1-8. IEEE, 2019.
[23] M. Nandhini, "Transport Safety in VANET by Detecting GPS Spoofing Attack Using Two Navigators," International Journal of Advanced Research in Computer Science, vol. 8, no. 3, 2017.
[24] S. R. Shetty and D. H. Manjaiah, "A Comprehensive Study of Security Attack on VANET," in Data Management, Analytics and Innovation: Proceedings of ICDMAI 2021, Vol. 2, pp. 407-428. Springer Singapore, 2022.
[25] S. Kumar and K. S. Mann, "Detection of Multiple Malicious Nodes Using Entropy for Mitigating the Effect of Denial of Service Attack in VANETs," in 2018 4th International Conference on Computing Sciences (ICCS), pp. 72-79. IEEE, 2018.
[26] R. Mishra, A. Singh, and R. Kumar, "VANET Security: Issues, Challenges and Solutions," in 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 1050-1055. IEEE, 2016.
[27] S. Kumar and K. Dutta, "Security Issues in Mobile Ad Hoc Networks: A Survey," in Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications, pp. 176-221. IGI Global, 2014.
[28] F. Altaf, K. Prateek, and S. Maity, "Beacon Non-Transmission Attack and Its Detection in Intelligent Transportation Systems," Internet of Things, p. 100602, Aug. 2022.
[29] M. A. Mimi, "Using Clustering Scheme: Prevent Reply Attack in Vehicular Ad-Hoc Networks (VANET)," Journal of Discrete Mathematical Sciences and Cryptography, vol. 25, no. 7, pp. 2007-2014, 2022.
[30] K. Verma, H. Hasbullah, and A. Kumar, "Prevention of DoS Attacks in VANET," Wireless Personal Communications, vol. 73, no. 1, pp. 95–126, Apr. 2013.
[31] A. M. R. Tolba, "Trust-Based Distributed Authentication Method for Collision Attack Avoidance in VANETs," IEEE Access, vol. 6, pp. 62747–62755, 2018.
[32] F. Ahmad, A. Adnane, V. N. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the-Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackers' Strategies," Sensors, vol. 18, no. 11, p. 4040, 2018.
[33] P. K. Ravula, S. Uppalapati, and G. R. Karri, "An Early Detection and Prevention of Wormhole Attack Using Dynamic Threshold Value in VANET," International Journal of Vehicle Information and Communication Systems, vol. 9, no. 2, pp. 201–225, 2024.
[34] M. A. Mimi, "Using Clustering Scheme: Prevent Reply Attack in Vehicular Ad-Hoc Networks (VANET)," Journal of Discrete Mathematical Sciences and Cryptography, vol. 25, no. 7, pp. 2007-2014, 2022.
[35] R. K. Dhanaraj, S. H. Islam, and V. Rajasekar, "A Cryptographic Paradigm to Detect and Mitigate Blackhole Attack in VANET Environments," Wireless Networks, vol. 28, no. 7, pp. 3127-3142, 2022.
[36] 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, 2015.
[37] P. Remya Krishnan and P. Arun Raj Kumar, "Detection and Mitigation of Smart Blackhole and Gray Hole Attacks in VANET Using Dynamic Time Warping," Wireless Personal Communications, vol. 124, no. 1, pp. 931-966, 2022.
[38] F. Alifo, D. Martin, and M. Awinsongya, "Wormhole Attack Vulnerability Assessment of MANETs: Effects on Routing Protocols and Network Performance," International Journal of Computer Applications, vol. 185, no. 48, pp. 1-8, 2023.
[39] S. Kumar and K. Dutta, "Trust-Based Intrusion Detection Technique to Detect Selfish Nodes in Mobile Ad Hoc Networks," Wireless Personal Communications, vol. 101, pp. 2029-2052, 2018.
[40] S. Kumar, K. Dutta, and G. Sharma, "A Detailed Survey on Selfish Node Detection Techniques for Mobile Ad Hoc Networks," in 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), pp. 122-127. IEEE, 2016.
[41] N. Jyothi and R. Patil, "An Optimized Deep Learning-Based Trust Mechanism in VANET for Selfish Node Detection," International Journal of Pervasive Computing and Communications, vol. 18, no. 3, pp. 304–318, 2021.
[42] A. H. Magsi, L. V. Yovita, A. Ghulam, G. Muhammad, and Z. Ali, "A Content Poisoning Attack Detection and Prevention System in Vehicular Named Data Networking," Sustainability, vol. 15, no. 14, p. 10931, 2023.
[43] Y. Pramitarini, R. H. Y. Perdana, T. N. Tran, K. Shim, and B. An, "A Hybrid Price Auction-Based Secure Routing Protocol Using Advanced Speed and Cosine Similarity-Based Clustering Against Sinkhole Attack in VANETs," Sensors, vol. 22, no. 15, p. 5811, 2022.
[44] S. Khan, I. Sharma, M. Aslam, M. Z. Khan, and S. Khan, "Security Challenges of Location Privacy in VANETs and State-of-the-Art Solutions: A Survey," Future Internet, vol. 13, no. 4, p. 96, Apr. 2021.
[45] S. Ercan, M. Ayaida, and N. Messai, "Misbehavior Detection for Position Falsification Attacks in VANETs Using Machine Learning," IEEE Access, vol. 10, pp. 1893–1904, 2022.
[46] H. Mustafa, W. Xu, A. R. Sadeghi, and S. Schulz, "End-to-End Detection of Caller ID Spoofing Attacks," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 3, pp. 423–436, 2016.

REVIEW ARTICLE

[47] K. N. Tripathi, G. Jain, A. M. Yadav, and S. C. Sharma, "Entity-Centric Combined Trust (ECT) Algorithm to Detect Packet Dropping Attack in Vehicular Ad Hoc Networks (VANETs)," in Next Generation Information Processing System: Proceedings of ICCET 2020, Volume 2, pp. 23–33. Springer Singapore, 2021.

[48] Y. Xie, Y. Li, and Y. Wang, "Research on Detection Method of Malicious Node Based on Flood Attack in VANET," in 6GN for Future Wireless Networks: Third EAI International Conference, 6GN 2020, Tianjin, China, August 15-16, 2020, Proceedings 3, pp. 373–383. Springer International Publishing.

[49] R. S. Raghav, R. Danu, A. Ramalingam, and G. K. Kumar, "Detection of Node Impersonation for Emergency Vehicles in VANET," International Journal of Engineering Research & Technology (IJERT), vol. 2, pp. 3383–3389, 2013.

[50] W. Xiong, R. Wang, Y. Wang, Y. Wei, F. Zhou, and X. Luo, "Improved Certificateless Aggregate Signature Scheme Against Collusion Attacks for VANETs," IEEE Systems Journal, vol. 17, no. 1, pp. 1098–1109, 2022.

[51] A. Kumar, N. Sharma, and A. Kumar, "End-to-End Authentication Based Secure Communication in Vehicular Ad Hoc Networks (VANET)," Journal of Discrete Mathematical Sciences and Cryptography, vol. 25, no. 1, pp. 219–229, 2022.

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

[53] 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 and Automation, vol. 12, no. 5, pp. 478–486, 2019.

[54] 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.

[55] 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.

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

[57] G. Nayak, A. Mishra, U. Samal, and B. K. Mishra, "Depth Analysis on DoS & DDoS Attacks," in Wireless Communications and Security, pp. 159–182, 2022.

[58] J. Grover, "Security of Vehicular Ad Hoc Networks Using Blockchain: A Comprehensive Review," Vehicular Communications, vol. 34, p. 100458, 2022.

[59] B. Karthiga, D. Durairaj, N. Nawaz, T. K. Venkatasamy, G. Ramasamy, and A. Hariharasudan, "Intelligent Intrusion Detection System for VANET Using Machine Learning and Deep Learning Approaches," Wireless Communications and Mobile Computing, vol. 2022, Article ID 5069104, 2022.

[60] 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.

[61] A. Garg, S. Kumar, and K. Dutta, "An Analytical Survey of State of the Art JellyFish Attack Detection and Prevention Techniques," in 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), pp. 38–43. IEEE, 2016.

[62] B. K. Pattanayak, O. Pattnaik, and S. Pani, "Dealing with Sybil Attack in VANET," in Intelligent and Cloud Computing: Proceedings of ICICC 2019, Volume 1, pp. 471–480. Springer Singapore, 2021.

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

[64] S. A. Asra, "Security Issues of Vehicular Ad Hoc Networks (VANET): A Systematic Review," TIERS Information Technology Journal, vol. 3, no. 1, pp. 17–27, 2022.

[65] P. Mundhe, S. Verma, and S. J. C. S. Venkatesan, "A Comprehensive Survey on Authentication and Privacy-Preserving Schemes in VANETs," Computer Science Review, vol. 41, p. 100411, 2021.

[66] S. Dong, H. Su, Y. Xia, F. Zhu, X. Hu, and B. Wang, "A Comprehensive Survey on Authentication and Attack Detection Schemes that Threaten It in Vehicular Ad-Hoc Networks," IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 12, pp. 13573–13602, 2023.

[67] A. S. Mustafa, M. M. Hamdi, H. F. Mahdi, and M. S. Abood, "VANET: Towards Security Issues Review," in 2020 IEEE 5th International Symposium on Telecommunication Technologies (ISTT), pp. 151–156. IEEE, 2020.

[68] C. Zhao, J. S. Gill, P. Pisu, and G. Comert, "Detection of False Data Injection Attack in Connected and Automated Vehicles via Cloud-Based Sandboxing," IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 9078–9088, 2021.

[69] A. Al-Sabaawi, K. Al-Dulaimi, E. Foo, and M. Alazab, "Addressing Malware Attacks on Connected and Autonomous Vehicles: Recent Techniques and Challenges," in Malware Analysis Using Artificial Intelligence and Deep Learning, pp. 97–119.

[70] M. Kim, I. Jang, S. Choo, J. Koo, and S. Pack, "Collaborative Security Attack Detection in Software-Defined Vehicular Networks," in 2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS), pp. 19–24. IEEE, 2017.

[71] J. Zhang, K. Zheng, D. Zhang, and B. Yan, "AATMS: An Anti-Attack Trust Management Scheme in VANET," IEEE Access, vol. 8, pp. 21077–21090, 2020.

[72] K. V. Krishna and K. G. Reddy, "VANET Vulnerabilities Classification and Countermeasures: A Review," Majlesi Journal of Electrical Engineering, vol. 16, no. 3, pp. 63–83, 2022.

[73] M. Adnan, J. Iqbal, A. Waheed, N. U. Amin, M. Zareei, A. Umer, and E. M. Mohamed, "Towards the Design of Efficient and Secure Architecture for Software-Defined Vehicular Networks," Sensors, vol. 21, no. 11, p. 3902, 2021.

[74] 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, 2020.

[75] R. Amin, I. Pali, and V. Sureshkumar, "Software-Defined Network Enabled Vehicle to Vehicle Secured Data Transmission Protocol in VANETs," Journal of Information Security and Applications, vol. 58, p. 102729, 2021.

[76] D. Tang, Z. Zheng, C. Yin, B. Xiong, Z. Qin, and Q. Yang, "FTODefender: An Efficient Flow Table Overflow Attacks Defending System in SDN," Expert Systems with Applications, vol. 237, p. 121460, 2024.

[77] Y. Gautam, B. P. Gautam, and K. Sato, "Experimental Security Analysis of SDN Network by Using Packet Sniffing and Spoofing Technique on POX and Ryu Controller," in 2020 International Conference on Networking and Network Applications (NaNA), pp. 394–399. IEEE, 2020.

[78] J. Cao, Q. Li, R. Xie, K. Sun, G. Gu, M. Xu, and Y. Yang, "The CrossPath Attack: Disrupting the SDN Control Channel via Shared Links," in 28th USENIX Security Symposium (USENIX Security 19), pp. 19–36.

[79] 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, 2016.

[80] A. N. Alhaj and N. Dutta, "Analysis of Security Attacks in SDN Network: A Comprehensive Survey," in Contemporary Issues in Communication, Cloud, and Big Data Analytics: Proceedings of CCB 2020, pp. 27–37.

REVIEW ARTICLE

[81] 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, p. 8631851, 2018.
[82] S. Gao, Z. Li, B. Xiao, and G. Wei, "Security Threats in the Data Plane of Software-Defined Networks," IEEE Network, vol. 32, no. 4, pp. 108–113, 2018.
[83] A. S. Alshra'a and J. Seitz, "Using Inspector Device to Stop Packet Injection Attack in SDN," IEEE Communications Letters, vol. 23, no. 7, pp. 1174–1177, 2019.
[84] M. Erritali, B. Cherkaoui, H. Ezzikouri, and A. Beni-hssane, "Detection of the Black Hole Attack on SDN based VANET Network," in Distributed Sensing and Intelligent Systems: Proceedings of ICDSIS 2020, pp. 67–74. Springer International Publishing, 2022.
[85] N. M. Yungaicela-Naula, C. Vargas-Rosales, J. A. Pérez-Díaz, and D. F. Carrera, "A Flexible SDN based Framework for Slow-Rate DDoS Attack Mitigation by Using Deep Reinforcement Learning," Journal of Network and Computer Applications, vol. 205, p. 103444, 2022.
[86] J. C. C. Chica, J. C. Imbachi, and J. F. B. Vega, "Security in SDN: A Comprehensive Survey," Journal of Network and Computer Applications, vol. 159, p. 102595, 2020.
[87] V. Kiruthika, S. Padmapriya, M. Ganga, and V. Anupriya, "Mitigation of Cyber Attacks in Software Defined Networking Framework," in 2023 First International Conference on Advances in Electrical, Electronics and Computational Intelligence (ICAEECI), pp. 1–6. IEEE, 2023.
[88] T. A. Jawad, A. N. Mahmood, and A. N. Hameed, "Detecting Man-in-the-Middle Attacks via Hybrid Quantum-Classical Protocol in Software-Defined Networks," Indonesian Journal of Electrical Engineering and Computer Science, vol. 31, no. 1, pp. 205–211, 2023.
[89] X. Huang, K. Xue, Y. Xing, D. Hu, R. Li, and Q. Sun, "FSDM: Fast Recovery Saturation Attack Detection and Mitigation Framework in SDN," in 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), pp. 329–337. IEEE, 2020.
[90] I. Al Salti and N. Zhang, "LINK-GUARD: An Effective and Scalable Security Framework for Link Discovery in SDN Networks," IEEE Access, vol. 10, pp. 130233–130252, 2022.
[91] H. Zhou, Y. Zheng, X. Jia, and J. Shu, "Collaborative Prediction and Detection of DDoS Attacks in Edge Computing: A Deep Learning-Based Approach with Distributed SDN," Computer Networks, vol. 225, p. 109642, 2023.
[92] J. Wang, Y. Tan, J. Liu, and Y. Zhang, "Topology Poisoning Attack in SDN-Enabled Vehicular Edge Network," IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9563–9574, 2020.
[93] J. Wang, Y. Tan, and J. Liu, "Topology Poisoning Attacks and Countermeasures in SDN-Enabled Vehicular Networks," in GLOBECOM 2020 - 2020 IEEE Global Communications Conference, pp. 1–6. IEEE, 2020.
[94] H. Zhou, C. Wu, C. Yang, P. Wang, Q. Yang, Z. Lu, and Q. Cheng, "SDN-RDCD: A Real-Time and Reliable Method for Detecting Compromised SDN Devices," IEEE/ACM Transactions on Networking, vol. 26, no. 5, pp. 2048–2061, 2018.
[95] E. M. Onyema, M. A. Kumar, S. Balasubarmanian, S. Bharany, A. U. Rehman, E. T. Eldin, and M. Shafiq, "A Security Policy Protocol for Detection and Prevention of Internet Control Message Protocol Attacks in Software Defined Networks," Sustainability, vol. 14, no. 19, p. 11950, 2022.
[96] S. Wang, S. Chandrasekharan, K. Gomez, S. Kandeepan, A. Al-Hourani, and M. R. Asghar, "SECOD: SDN Secure Control and Data Plane Algorithm for Detecting and Defending Against DoS Attacks," in NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, pp. 1–5. IEEE, 2018.
[97] Z. A. Bhuiyan, S. Islam, M. M. Islam, A. A. Ullah, F. Naz, and M. S. Rahman, "On the (In) Security of the Control Plane of SDN Architecture: A Survey," IEEE Access, 2023.
[98] R. Deb and S. Roy, "A Comprehensive Survey of Vulnerability and Information Security in SDN," Computer Networks, vol. 206, p. 108802, 2022.
[99] M. P. Singh and A. Bhandari, "New-Flow Based DDoS Attacks in SDN: Taxonomy, Rationales, and Research Challenges," Computer Communications, vol. 154, pp. 509–527, 2020.
[100] H. Li, D. Li, X. Zhang, G. Shou, Y. Hu, and Y. Liu, "A Security Management Architecture for Time Synchronization Towards High Precision Networks," IEEE Access, vol. 9, pp. 117542–117553, 2021.
[101] Y. Liu, Y. Wang, and H. Feng, "A Novel Link Fabrication Attack Detection Method for Low-Latency SDN Networks," Journal of Information Security and Applications, vol. 84, p. 103807, 2024.
[102] Q. Li, Y. Chen, P. P. Lee, M. Xu, and K. Ren, "Security Policy Violations in SDN Data Plane," IEEE/ACM Transactions on Networking, vol. 26, no. 4, pp. 1715–1727, 2018.
[103] K. Thimmaraju, G. Rétvári, and S. Schmid, "Virtual Network Isolation: Are We There Yet?" in Proceedings of the 2018 Workshop on Security in Softwarized Networks: Prospects and Challenges, pp. 1–7, Budapest, Hungary, 2018.
[104] I. A. Valdovinos, J. A. Pérez-Díaz, K. K. R. Choo, and J. F. Botero, "Emerging DDoS Attack Detection and Mitigation Strategies in Software-Defined Networks: Taxonomy, Challenges and Future Directions," Journal of Network and Computer Applications, vol. 187, p. 103093, 2021.
[105] K. Shinan, K. Alsubhi, A. Alzahrani, and M. U. Ashraf, "Machine Learning-Based Botnet Detection in Software-Defined Network: A Systematic Review," Symmetry, vol. 13, no. 5, p. 866, 2021.
[106] H. Zhou, C. Wu, C. Yang, P. Wang, Q. Yang, Z. Lu, and Q. Cheng, "SDN-RDCD: A Real-Time and Reliable Method for Detecting Compromised SDN Devices," IEEE/ACM Transactions on Networking, vol. 26, no. 5, pp. 2048–2061, 2018.
[107] J. Cao, R. Xie, K. Sun, Q. Li, and G. Gu, "When Match Fields Do Not Need to Match: Buffered Packets Hijacking in SDN," in Proceedings of the Network and Distributed System Security Symposium (NDSS'20), San Diego, CA, USA, 2020.
[108] S. Scott-Hayward, C. Kane, and S. Sezer, "Operationcheckpoint: SDN Application Control," in Proceedings of the 2014 IEEE 22nd International Conference on Network Protocols, pp. 618–623, IEEE, 2014.
[109] K. Bhushan and B. B. Gupta, "Distributed Denial of Service (DDoS) Attack Mitigation in Software Defined Network (SDN)-Based Cloud Computing Environment," Journal of Ambient Intelligence and Humanized Computing, vol. 10, pp. 1985–1997, 2019.
[110] J. Kim, M. Seo, S. Lee, J. Nam, V. Yegneswaran, and P. Porras, "Enhancing Security in SDN: Systematizing Attacks and Defenses from a Penetration Perspective," Computer Networks, p. 110203, 2024.
[111] Y. Maleh, Y. Qasmaoui, K. El Gholami, Y. Sadqi, and S. Mounir, "A Comprehensive Survey on SDN Security: Threats, Mitigations, and Future Directions," Journal of Reliable Intelligent Environments, vol. 9, no. 2, pp. 201–239, 2023.
[112] 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, 2020.
[113] F. Bensalah, N. Elkamoun, and Y. Baddi, "SDNStat-Sec: A Statistical Defense Mechanism Against DDoS Attacks in SDN based VANET," in Advances on Smart and Soft Computing: Proceedings of ICACIn 2020, pp. 527–540. Springer Singapore, 2021.
[114] R. P. Nayak, S. Sethi, S. K. Bhoi, K. S. Sahoo, T. A. Tabbakh, and Z. A. Almusaylim, "TBDDoSA-MD: Trust-Based DDoS Misbehave Detection Approach in Software-Defined Vehicular Network (SDVN)," Computers, Materials & Continua, vol. 69, no. 3, pp. 2985–2999, 2021.
[115] G. De Biasi, L. F. Vieira, and A. A. Loureiro, "Sentinel: Defense Mechanism Against DDoS Flooding Attack in Software Defined Vehicular Network," in 2018 IEEE International Conference on Communications (ICC), pp. 1–6. IEEE, 2018.
[116] G. O. Anyanwu, C. I. Nwakanma, J. M. Lee, and D. S. Kim, "RBF-SVM Kernel-Based Model for Detecting DDoS Attacks in SDN

REVIEW ARTICLE

Integrated Vehicular Network," Ad Hoc Networks, vol. 140, p. 103026, 2023.
[117] M. A. Setitra and M. Fan, "Detection of DDoS Attacks in SDN based VANET Using Optimized TabNet," Computer Standards & Interfaces, vol. 90, p. 103845, 2024.
[118] 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, 2022.
[119] P. K. Singh, S. K. Jha, S. K. Nandi, and S. Nandi, "ML-Based Approach to Detect DDoS Attack in V2I Communication Under SDN Architecture," in TENCON 2018-2018 IEEE Region 10 Conference, pp. 0144–0149. IEEE, 2018.
[120] J. S. Weng, J. Weng, Y. Zhang, W. Luo, and W. Lan, "BENBI: Scalable and Dynamic Access Control on the Northbound Interface of SDN based VANET," IEEE Transactions on Vehicular Technology, vol. 68, no. 1, pp. 822–831, 2018.
[121] H. Vasudev and D. Das, "A Trust Based Secure Communication for Software Defined VANETs," in 2018 International Conference on Information Networking (ICOIN), pp. 316–321. IEEE, 2018.
[122] 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, 2020.
[123] B. A. Reddy, K. S. Sahoo, and M. Bhuyan, "Securing P4-SDN Data Plane Against Flow Table Modification Attack," in NOMS 2024-2024 IEEE Network Operations and Management Symposium, pp. 1–5. IEEE, 2024.
[124] I. M. Varma and N. Kumar, "A Comprehensive Survey on SDN and Blockchain-Based Secure Vehicular Networks," Vehicular Communications, p. 100663, 2023.
[125] A. Akhunzada and M. K. Khan, "Toward Secure Software Defined Vehicular Networks: Taxonomy, Requirements, and Open Issues," IEEE Communications Magazine, vol. 55, no. 7, pp. 110–118, 2017.
[126] K. K. Karmakar, V. Varadharajan, and U. Tupakula, "Mitigating Attacks in Software Defined Networks," Cluster Computing, vol. 22, pp. 1143–1157, 2019.

Authors

Ms. Upinder Kaur is at present working as Associate Professor in the Department of Computer Science at G.M.N College, Ambala Cantt (Haryana). She received her bachelor's degree from Kurukshetra University, Kurukshetra (Haryana) in 2001 and master's degree in Computer Science from Kurukshetra University, Kurukshetra (Haryana) in 2003. She received her M.Phil. degree in Computer Science from CDLU, Sirsa in 2008. She is pursuing her Ph.D. from Maharaja Agrasen University, Solan (Himachal Pradesh). Her research interests include Network Security, Wireless Networks, Neural Networks and Metaheuristic Algorithms.

Dr. Aparna N Mahajan is at present working as Director, Maharaja Agrasen Institute of Technology, Maharaja Agrasen University, Solan (Himachal Pradesh). She did her graduation in Electrical and Power Engineering from Government College of Engineering, Amravati, Nagpur University in 1981 and then her post graduation leading to M.E. in Power System from Govt College of Engineering, Aurangabad. She did her Ph.D from Banasthali Vidyapith, Banasthali in the field of Electronics and Communication Engineering in the broad area of Vehicular Adhoc Networking. Dr. Mahajan has over 31 years of teaching and administrative experience and has guided a number of undergraduate and postgraduate projects, with a number of publications in National and International journals and conferences to her credit. Her areas of interest, to name a few, include computer networks, data communication, wireless communication, mobile communication etc. She has organized a number of workshops and seminars in these areas as well on personality development & communication skills. Dr. Mahajan was past Chairperson of Women in Engineering, IEEE Delhi Section. She was conferred Outstanding Branch Counselor Award from IEEE Delhi Section and IEEE Head Quarter NewYork in 2015. She was also conferred Best Teacher Award (ECE) in 2006.

Dr. Sunil Kumar is at present working as Assistant Professor in the Department of Computer Science and Engineering and Incharge of Department of Artificial Intelligence and Data Science at Guru Jambheshwar University of Science and Technology, Hisar (Haryana). He received his bachelor's degree in Computer Engineering from Kurukshetra Univesrsity, Kurukshetra (Haryana) in 2002 and master's degree in Computer Science and Engineering from Guru Jambheshwar University of Science and Technology, Hisar (Haryana) in 2007. He has been awarded Gold Medal for standing first in 2005–2007 batch of Master of Technology in Computer Science and Engineering, Guru Jambheshwar University of Science and Technology, Hisar. He earned his Ph.D degree in Computer Science and Engineering from National Institute of Technology, Hamirpur (Himachal Pradesh) in 2017. He also qualified national importance exam GATE and UGC NET. His research interests include Network Security, Wireless Networks, Cloud Computing, IoTs, Artificial Intelligence and Machine Learning. Dr. Kumar has published more than 35 research papers in various International Journals and conferences of repute. He is serving as reviewer with publisher like by IEEE, Springer, Taylor & Francis, Hindawi, Inderscience etc. He has supervised 21 M.Tech. Dissertations. One student has completed his Doctorate under his guidance and other six are pursuing their Ph.D.

Dr. Kamlesh Dutta is associated with the Department of Computer Science and Engineering at National Institute of Technology, Hamirpur. She did her PhD from Guru Gobind Singh Indraprastha University, Delhi; M.Tech. from IIT Delhi; and MS with Honours from Vladimir State Technical University (Russia). She has supervised 11 PhD theses, 35+ M.Tech. Dissertations and published more than 180 papers in international journals and conference proceedings of repute. At present several students are working under her guidance toward their M.Tech and Ph.D. Her area of research includes Information Security, Artificial Intelligence, Machine Learning, Deep Learning, Software Engineering and E-learning. She was empanelled expert for the implementation of IPV6 by DoT. She has organized more than 60 short term training programs, workshops, seminars and conferences for the benefit of Faculty and students. She is on the national and international committees of various international conferences and Journals. She is a lifetime member of ISTE, CSI, ISSS, SIGSEM and SIGDIAL. Dr. Dutta visited Singapore and Australia regarding training under UNDP and Cisco. She has received four best paper awards for her research publications. Dr. Dutta received an outstanding award for her contribution to the Cisco Networking Academy Program. Dr. Dutta has been completed three research projects. Dr. Dutta provided IPV6 Consultancy Services for RINL, Visakhapatnam Steel Plant. She holds two copyrights of India namely: Bhukamp Rodhi E-chakri and Retrofitting E-chakri.

REVIEW ARTICLE

How to cite this article:

Upinder Kaur, Aparna N. Mahajan, Sunil Kumar, Kamlesh Dutta, " Security Vulnerabilities in VANETs and SDN-based VANETs: A Study of Attacks ", International Journal of Computer Networks and Applications (IJCNA), 11(6), PP: 774-802, 2024, DOI: 10.22247/ijcna/2024/47.