Hindawi
Security and Communication Networks
Volume 2021, Article ID 9997771, 20 pages
https://doi.org/10.1155/2021/9997771

Review Article

Security in Vehicular Ad Hoc Networks: Challenges and Countermeasures

Jabar Mahmood,[1] **Zongtao Duan**,[1] **Yun Yang**,[1] **Qinglong Wang**,[1] **Jamel Nebhen**,[2] **and Muhammad Nasir Mumtaz Bhutta**[3]

[1]*School of Information and Engineering, Chang'an University, Xi'an 710064, China*
[2]*Prince Sattam Bin Abdulaziz University, College of Computer Engineering and Sciences, P.O. Box 151, Alkharj 11942, Saudi Arabia*
[3]*Department of Information Systems, College of Computer Sciences and Information Technology, King Faisal University, Al Ahsa, Saudi Arabia*

Correspondence should be addressed to Yun Yang; yangyun@chd.edu.cn

Received 10 March 2021; Accepted 21 June 2021; Published 30 June 2021

Academic Editor: Azeem Irshad

Recently, vehicular ad hoc networks (VANETs) got much popularity and are now being considered as integral parts of the automobile industry. As a subclass of MANETs, the VANETs are being used in the intelligent transport system (ITS) to support passengers, vehicles, and facilities like road protection, including misadventure warnings and driver succor, along with other infotainment services. The advantages and comforts of VANETs are obvious; however, with the continuous progression in autonomous automobile technologies, VANETs are facing numerous security challenges including DoS, Sybil, impersonation, replay, and related attacks. This paper discusses the characteristics and security issues including attacks and threats at different protocol layers of the VANETs architecture. Moreover, the paper also surveys different countermeasures.

1. Introduction

Aiming at ensuring the safety and facilitating the passengers and driver, the VANETs are getting much popularity and attention from the researchers [1–3]. VANETs are the networks of vehicles communication and road infrastructures to extend road safety and infotainment [4]. The wireless sensors are fitted within vehicles, accompanied with positioning devices and maps. Through On-Board Unit (OBU), the vehicles are connected with road-side units (RSUs) to share intervehicle and vehicle to RSU, the safety related and otherwise information [5, 6]. The VANETs consist of short-range communication infrastructure. Therefore, the source and destination share information through intermediate nodes. Like OBU, RSU, the trusted authority (TA) is also an entity of the VANETs architecture and is responsible for controlling and supervising the whole network [7, 8].

The remaining paper is ordered as follows: Section 2 explains the VANTEs overview in detail and describes the characteristics of VANETs. Section 3 is divided into two parts. The first part provides detailed security issues in VANETs, the security attacks on the physical layer; the second part presents other security attacks on different layers of VANETs and also describes the protocol layers threat. Section 4 describes the various challenges and solutions in VANETs, and Section 5 concludes the article.

2. Overview of VANETs

The VANETs architecture contains the OBU, RSU, and TA. There are two types of communication technologies in VANETs architecture, i.e., (1) vehicle to vehicle (V2V) and (2) vehicle to infrastructure (V2I) communication as shown in Figure 1. V2V contact vehicles converse with one another and exchange the traffic-related information inside the

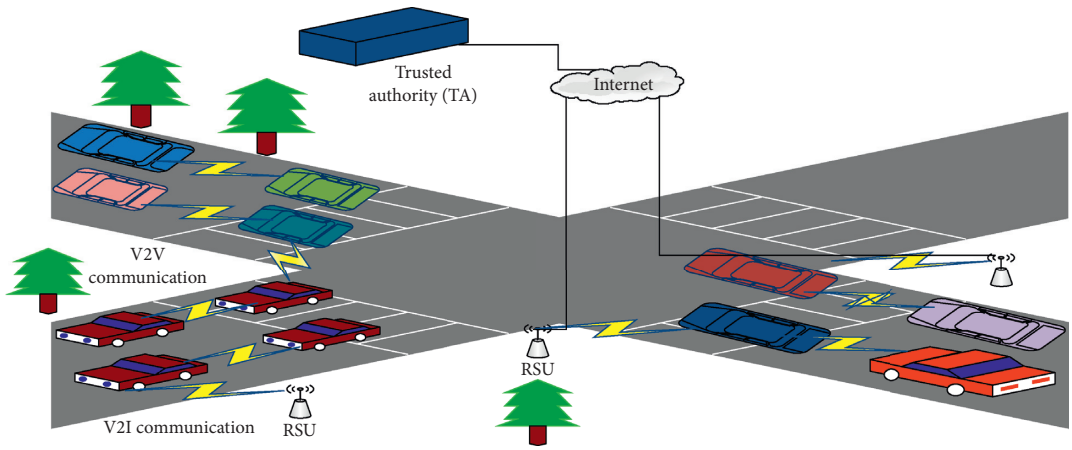

Figure 1: VANETs architectures.

wireless network range [3, 9, 10]. In such networks, when any unforeseen incident happens, such as accident or traffic blockage on the road, instantly a vehicle sends an alert signal to the other nodes or vehicles in the network suggesting to avoid that particular road or area. The vehicle, employing V2I communication, shares the information with RSU which is part of infrastructure installed on the road. The V2I-based communication notifies the driver about traffic and weather updates to keep an eye on the nearby environment [3, 9, 11]. RSU and OBU are registered by a trusted authority [12, 13], which is used to keep up and supervise the VANETs system. The road-side unit positions itself on the road for authentication and communication between TA and OBU. With the use of dedicated short-range communication (DSRC) [6], the OBU fitted in each vehicle can transmit traffic information to nearby vehicles and RSU [10].

2.1. Characteristics of VANETs. VANETs is a dynamic ad hoc network that enables the vehicles converse with one another using fixed and mobile nodes offering numerous services, however with narrow access to the network's infrastructure. Compared to the MANETs, the VANETs have high mobility features and normally vary in topology [10]. In VANETs, vehicles or nodes move arbitrarily in the network, and their movement transforms the network topology. VANETs topology is complex and dynamic because of the strong mobility factor of nodes [9]. The features of VANETs are mentioned below.

2.1.1. High Mobility. Because of the high mobility, the VANETs have good versatility relative to MANETs, and they play a significant role in modelling VANETs protocol. In VANETs, every node moves quickly; thus, vehicles' mobility minimizes the communication time in the network [10, 14].

2.1.2. Driver Protection. The VANETs might get better driver protection, improve traveller console, and support a better flow of traffic. The core benefit of VANETs is that nodes communicate straight to everyone [10].

2.1.3. Vibrant Network Topology. In VANETs, the topology design is vibrant because the vehicle speed of mobility is very high. Therefore, the forecast of node position is very tough to compute. The high speed of vehicle networks is extra weak to attacks, and it is incredibly complicated to identify intruders and vehicles if something is wrong in a network [10].

2.1.4. Variable Network Density. Due to high-speed mobility vehicles, traffic congestion or even lousy weather, the network may experience frequent or intermittent disconnection among nodes. In this situation, the nodes may receive proper guidance from the V2I infrastructure [9, 10].

2.1.5. The Medium of Transmission. Due to open wireless nature, these kinds of networks inherit all security vulnerabilities as posed to other traditional wireless networks [10].

2.1.6. No Power Limits. In MANETs, power is a grave problem; however, in VANETs the power is not a big problem since the OBU in vehicular entities bear sufficient battery and power resources necessary to carry out its communicative tasks [9, 14].

2.1.7. Restriction of Transmission Power. Wireless Access to Vehicle Environment (WAVE) limits the transmission power, which varies from 0 to 28.8°dBm with the corresponding coverage distance ranging from 10°m to 1 km. Thus, the narrow power transfer may change the distance from the VANTS coverage [10].

2.1.8. Network Strength. The signal strength of the network in VANETs depends on the traffic congestion, since it might gain more strength if there is no congestion or less traffic on the road. On the other hand, in case of traffic jams the signal quality might experience degradations [10].

2.1.9. Extensive Scale Network. In VANETs, the network is highly scalable, since such kind of networks may experience highways, downtown areas, point of entries, and exit in the

cities; hence, a massive number of nodes can be dynamically added or adjusted into the system [9, 10].

2.1.10. Extensive Computational Processing. In VANETs, a large number of resources such as processors, colossal memory GPS, and antenna are embedded in vehicles. Such resources may require a massive computational capabilities and guidance to provide enhanced and trustworthy wireless communication for getting accurate information, i.e., live location, speed, and route of the vehicle [9, 10].

3. Security Issues in VANETs

The security issue is very crucial in VANETs which ensures safety for the drivers as well as passengers. This is obligatory to design essential algorithms to assure safety and protection. The security challenges as posed to VANETs are availability, authentication, integrity, confidentiality, nonrepudiation, pseudonymity, privacy, mobility, data and location verification, access control, and key management issues [9, 10, 15, 16].

3.1. Security Issues. In this section, we provide details about various security issues in VANETs.

3.1.1. Availability. Availability [17] is considered a significant factor in VANETs security. This ensures that all resources are accessible forever in a network in the face of vulnerabilities and denial of service attack-based attempts. Cryptography and trust-based algorithms and protocols are helpful to protect the VANETs from these attacks [9, 10, 17, 18].

3.1.2. Authentication. Authentication enables the right participants to enter the network after dual verification. It also ensures that the sender or user who sends a message is not an intruder. Besides, the privacy of the user is preserved using pseudonyms [17–19].

3.1.3. Integrity. Integrity or data integrity ensures that there is no change in the original data packets sent by the sender. Alternatively, it must be protected from the adversary on the way. Data accuracy is one of the fundamental security issues in VANETs. Digital signature, public key infrastructure, and cryptography revocation mechanism may be employed to ensure the integrity between the sender and receiver [9, 10].

3.1.4. Confidentiality. Confidentiality means to hide data from adversaries. In confidentiality we make sure only authenticated users access the data with the help of encryption and decryption. In this way the data remains confidential, while the other unauthorized users may not access this confidential information [9, 20].

3.1.5. Nonrepudiation. This feature ensures that the source of the originating message may not deny the fact that it has generated a particular message. Alternatively, this feature binds the content with the originator of a particular message. [9, 10, 19].

3.1.6. Pseudonymity. The pseudonymity refers to hiding the original identity. The legal participants may use pseudonyms instead of using original identities. In this manner, the legitimate entities may communicate anonymously without revealing their true identities. This ensures protected privacy for the subscribers [18].

3.1.7. Privacy. In VANETs, the privacy refers to concealing driver identity as well as the location's information from other unauthorized users in the network [9, 18, 21].

3.1.8. Scalability. The capability of the network to respond to the dynamically changing requirements is termed as scalability. The frequently changing topology of the vehicular network is another challenge for the researchers [18].

3.1.9. Mobility. Mobility is ubiquitous in VANETs because nodes communicating in VANTEs change their location very quickly and frequently in a network. VANETs nature is dynamic because every second, the node position is changed. This mobility factor focuses on the need of more secure and dynamic algorithms maintaining quality of service requirements [18].

3.1.10. Data Verification. It is used to eliminate malicious messages in the network. This ensures to test the accuracy of data and verify the legitimacy of participating nodes [9].

3.1.11. Access Control. Access control is used to monitor and check the policy rights and roles for all participating nodes in the network [9, 15].

3.1.12. Key Management. Key management refers to the key used in encryption or decryption process during communication between the nodes. The key management and issuance are resolved during the designing of security protocols for the network [18, 22].

3.1.13. Location Verification. A reliable mechanism for the verification of location is required in VANETs, because this is necessary to protect from various attacks during communication and is also helpful in the data validation process [18].

3.2. Attacks on the Physical Layer of VANETs (Security Attacks in VANETs). This section on attacks in VANETs can be divided into three parts. In the first part, we discuss the attackers based on their nature, behaviour, and efficiency. In the second part, we discuss the various attacks on physical layer, and the third part focuses on the rest of the attacks in VANETs. Now we discuss the types of the attackers according to nature, behaviour, and efficiency:

(i) Active vs. passive: in the case of an active assault, the assailant gets the information from the network, changes the original message's information, and forwards it to the receiver. Usually, in an active assault, the assailant wants to decrease the network's efficiency or get access to the network for unauthorized services [23]. In the case of the passive assault, the assailant does not send or receive any message on a network by eavesdropping the wireless network and collecting information about the network or seeking potential vulnerabilities [24, 25].

(ii) Insider vs. outsider: insider attacker means that the authorized member who is part of the network has full information about the network and can access network efficiently. On the other side, outsider attackers are intruders who are not authorized and cannot access the network directly. That is, if they want to initiate an attack they must collect knowledge about the network first and then attack [24, 26, 27].

(iii) Malicious vs. rational: the attacker's intention is to attack the network and gain personal benefits. A malicious attacker may upset the network's performance with an objective to affect the legal users of the network [23, 28]. On the other hand, a rational attacker may intentionally launch an attack on the network to get some information in order to damage the network [24, 26].

(iv) Local vs. extended: in the case of local attackers, they launch attacks on a limited scope and cover the limited area or region like some RSU and node [27]. However, extended attackers cover bigger region or area comparatively. The extended attacker aims to degrade the network's performance or shut down the whole network [25].

3.2.1. Eavesdropping Assault. Eavesdropping assault is a type of passive assault and is done in the privacy of the network. Assailant collects the secret information, and the attacker secretly monitors the traffic flow of the network or the existing location and actions of a specific vehicle. This type of assault cannot be detected easily because the attacker performs its activity without any kind of reaction [25, 29]. Figure 2 shows that Car C regularly monitors ATM's cash van's facts and leaks such information to the intruder. ID revelation assault is a subcategory of eavesdropping where the assailant exposes the identity vehicle and uses it to track the under-attack vehicle.

3.2.2. Denial of Service Assault. In DoS-based assault [30–32], the assailant attacks the service provider's services. In this attack, even the legitimate users are unable to acquire services in the network. The assailant may initiate this attack any time and jam the communication channel. This kind of assault can be launched in two ways. On the first hand, the attacker may engulf the resource with numerous requests, while that resource may not be able to respond to legal user requests. This type of attack can be extended by sending a large number of requests for messages and jamming the communication. Therefore, RSU cannot accommodate several requests that OBU might have submitted [29, 33, 34]. In Figure 3, a DOS attack is demonstrated where auto F is an attacker in the car who denies access to RSU services for users of Cars A, C, D, E, and H.

3.2.3. Distributed Denial of Service Assault. Distributed Denial of Service (DDOS) [35] could be more damaging for the ad hoc vehicular environment since the attacker may attack the network in a distributed manner. An attacker may use various time slots for different vehicles to submit a message. The only objective of the assailant is to bring the network down [27, 29]. In Figure 4, a Distributed Denial of Service attack is demonstrated where the two cars, i.e., Car Q and U, attack the services provided by RSU, while the Cars M, N, O, and P denied the attackers Q and R, S and T, deprived of access to RSU services by the car in the attacker.

3.2.4. Illusion Assault. It involves deception with the manipulation of vehicle's inside information, for instance, speed and location, by tampering the hardware physically. By providing the wrong information of vehicles using internal devices or sensors, it misguides the other network nodes. For instance, it may show another person by cloning the location of the other vehicle [25].

In the case of in-transit traffic tampering assault, a malicious node may deliberately cause delay, corruption, replay, or alteration of a message to spoil the VANETs communication. This type of replay assault [36, 37] includes message replay where the assailant records the message received from certified nodes and then resends after sometime to create some misunderstanding or disturb the traffic. In Figure 5, it is shown that the attacker spoofs the message and sends back to the node; the original message was created by "M" assailant to create misunderstanding and replacing it as "tn." This assault could be launched in two ways, one is using an on-board unit by using a particular part of the hardware. The duplicate messages remain unsuccessful in locating the neighbor 's accurate driving status, for example, speed, location, direction, etc. [25, 38].

3.2.5. Message Modification/Alteration. In a message modification attack, the attacker changes the information of the vehicle integrated into a message (for example, speed, position, or direction) for its own benefit. It is a potential hazard for the security of the other nodes in the network [25].

3.2.6. Jamming Assault. An assailant intentionally generates large amount of messages in a network and creates congestion on wireless channel that might affect the performance of network [25]. The assailant may initiate jamming attack by transmitting a strong radio signal to interrupt the entire communication by declining the signal to noise ratio.

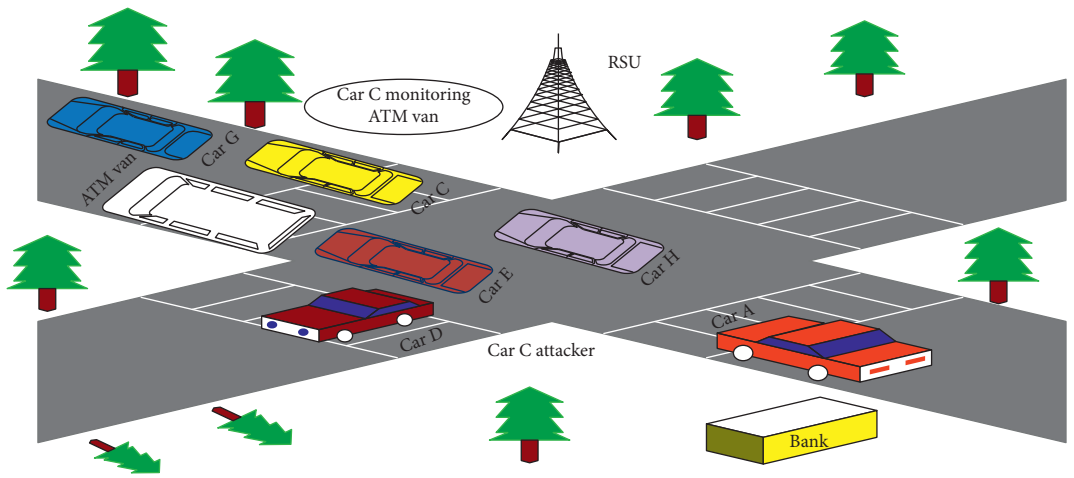

Figure 2: Eavesdropping assault.

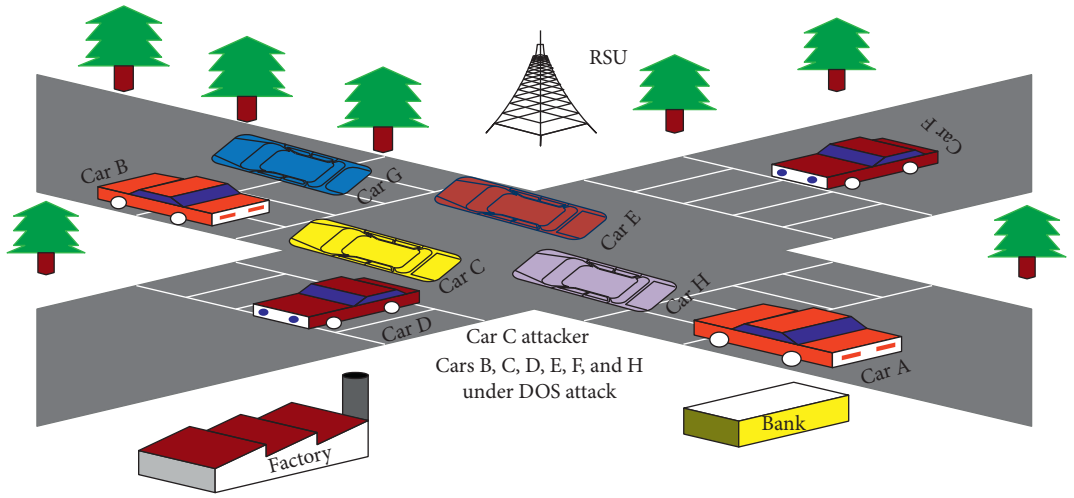

Figure 3: DOS assault.

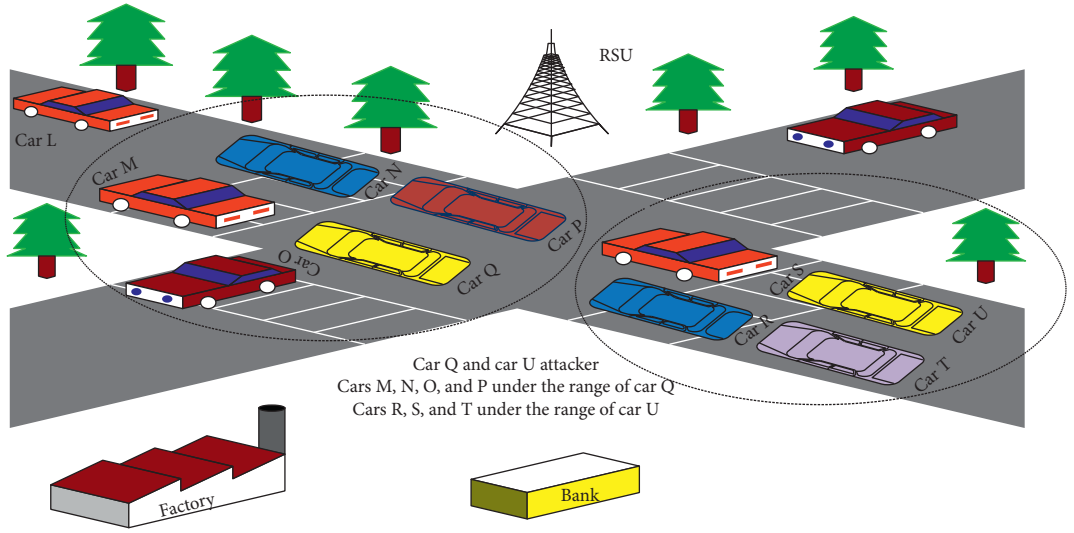

Figure 4: DDOS assault.

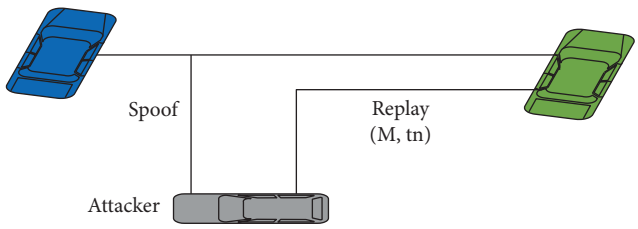

Figure 5: Message replay.

In this, the jammer continuously sends a signal by interfering with the communication of other vehicles in a network. In VANETs, jamming is considered a big threat for its security. Figure 6 shows that the assailant is jamming the network. The victim nodes are always perceived to be busy in a network, since they are unable to send or receive messages in this jammed area. When jamming signal is enabled, the sender sends the data packet, and the receiver does not receive the intended data packet. Therefore, the packet delivery ratio (PDR) is meager. These data packets carry essential information, such as weather conditions, road conditions, accidents, etc. Many incidents may happen if that critical information is not delivered to the nodes in due course of time.

3.3. Other Attacks in VANETs. In this section, we discuss remaining assaults that occurred on VANETs layers during communication.

3.3.1. Sybil Assault. In Sybil assault [39, 40], the assailant generates numerous identities of vehicles and broadcasts the incorrect information on the network. In the case of Sybil assault, data are broadcasted with fictitious identity. This assault is implemented from an OBU upon other OBUs after authentication for acquiring personal benefits. According to this scenario, the assailant creates several identities and sends a message in a network to the authentic user, such as additional traffic on the road, and therefore alters a route. One delusion is generated by the assailant, and the same message is sent to various vehicles. The authentic user will receive the same data packets from various vehicles because the illusion is always created in a network and believes its node will alter the route. This decision goes in favour of the attacker, while the route becomes clear, thus the attacker enjoys the trip [29, 41]. Figure 7 represents a Sybil assault in which an assailant in Car C creates numerous identities and sends those data packets with false identities to other users, which creates an illusion that the road has enormous traffic. After receiving such data packets, Car B and Auto D may decide alternative routes, and, currently, Car C gets a free road.

3.3.2. Node Impersonation Assault. Node impersonation attack is another name for a message tempering attack [29]. In VANETs, every vehicle has a unique identifier and uses it to send the message and verify if something wrong happens in the network. In node impersonation assault, the assailant changes the original data packet and claim that the data packet comes from a genuine user [27, 29]. Figure 8 shows that Vehicle D sends messages about the mishap to place x before acquiring help. However, the assailant junction C will inform the data packet and forward it to the ambulance to happen at place Y.

3.3.3. Black Hole Assault. Black hole assault [42–45] is a category of routing assault in which a malicious node attracts the victim's node on the network. Furthermore, it assures transmitting data through it by presenting the shortest path to the receiver node [29, 46]. The victim node chooses that shortest path and sends the data packet; any malicious node may drop the message or misuse the message for its own [41, 47, 48]. Figure 9 depicts that Car K desires to submit messages to Car P and Car Q, but it has no routing path for those nodes. Therefore, Car K activates the route detection process. Route request is redirected to Car B and Car L. Now, a malicious vehicle, Car L, claims that it has the shortest route to arrive at Car P and Car Q. According to the availability response, Car K sends every data packet to Car L and becomes a black hole assault victim.

3.3.4. Worm Hole Assault. Worm hole assault [49] is another type of routing assault. In a worm hole attack, a malicious node receives the message from the authenticated user at any place in the network, and, with the help of another malicious node, it creates a tunnel between two malicious vehicles [29, 46]. Figure 10 shows a wormhole assault in VANETs.

3.3.5. Gray Hole Assault. Gray hole assault is an extended version of black hole assault, wherein the malicious node also shows itself as part of the network. It sends a request message to victims' nodes and shows as the shortest path route node; in gray hole attacker [50] also received the data packets but did not drop all packets like black hole attack. It only dropped few data packets. In Figure 11, Car H shows that part of the network and presents the shortest path for communication to Car G. It is complicated to identify this type of attack because it is not continuous. It is created for limited time period for a specific purpose [29].

3.3.6. Masquerading Assault. In a masquerading attack, the attacker sends packets on behalf of other vehicles by using the identity of those vehicles [51]. In Figure 12, the C shows itself as a police van, and, through that deception, the node makes the other nodes reduce their speed or stop the node.

3.3.7. Global Positioning System Spoofing Assault. Global positioning system spoofing attack is another name for location faking assault. According to this category of assault, the assailant tries to vary their present location identity and forward fake information from the GPS by using such a method, by not showing the existing location to other nodes and pretending to be in an incorrect location to others. This

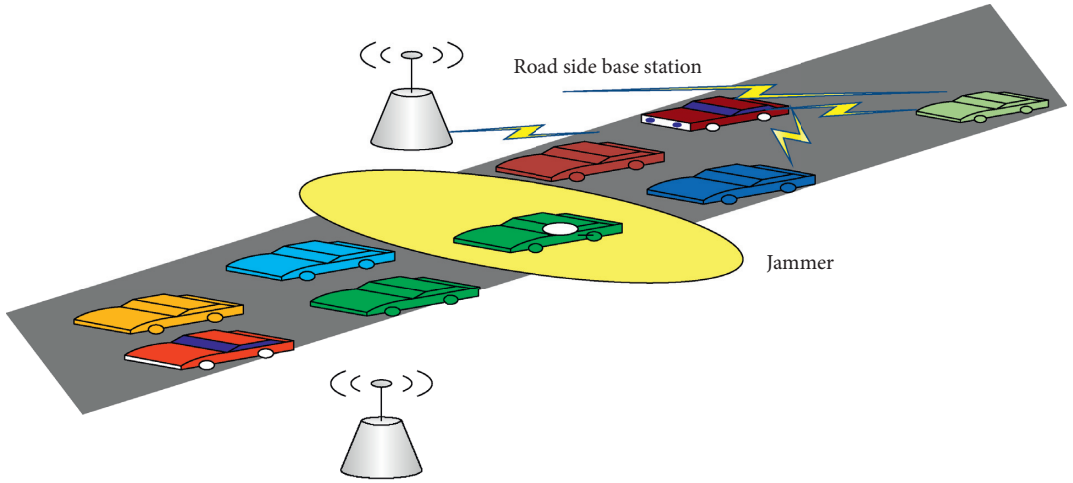

Figure 6: Jamming assault.

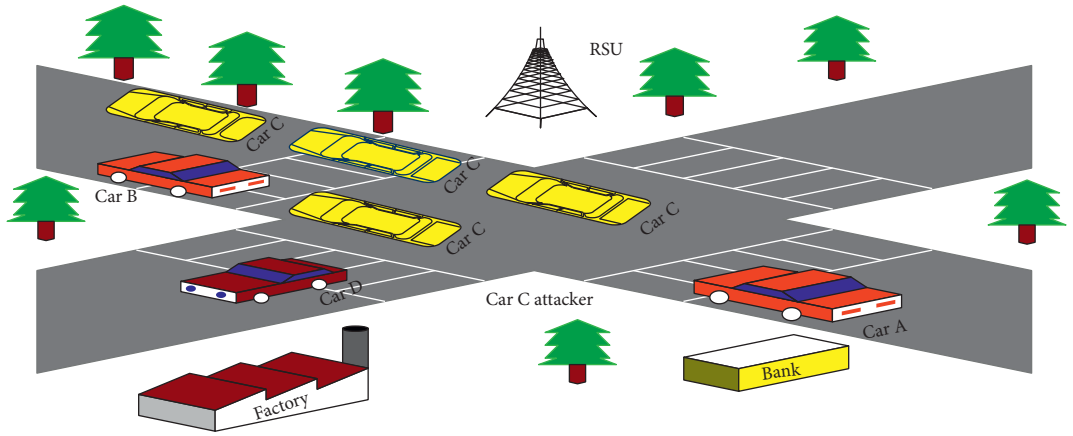

Figure 7: Sybil assault.

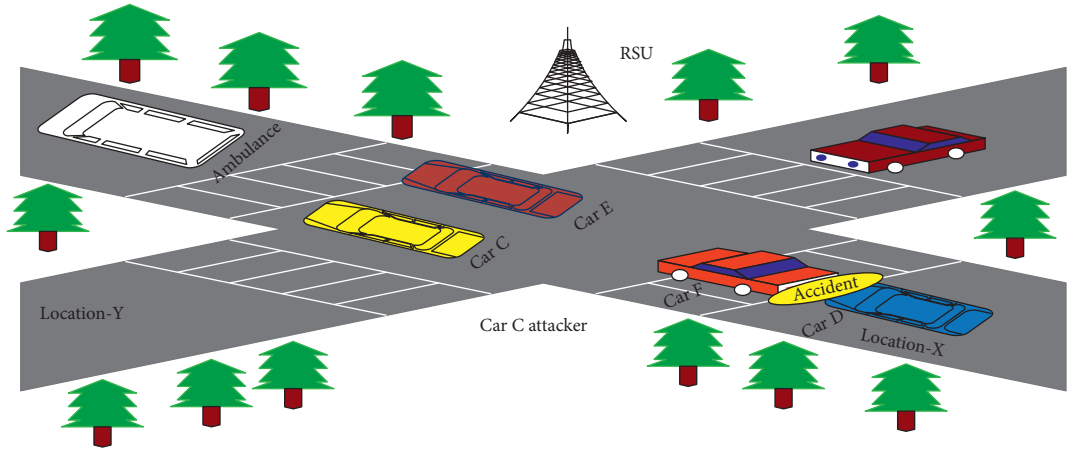

Figure 8: Node impersonation assault.

assault is done by the attacker with the help of set of nodes [29]. In Figure 13, three nodes are moving on the Road-ID 8; however, they do not show their present location and forward the network's incorrect information. RSUs acquiring such details show that there is no node on Road-ID 8.

3.3.8. Brute Force Assault. In the ad hoc network, the sender vehicle sends the message to the receiver vehicle with the help of other nodes if the receiver vehicle is beyond its range. Thus, for the sake of security, the sender nodes or vehicles encrypt the message and submit towards the target via any

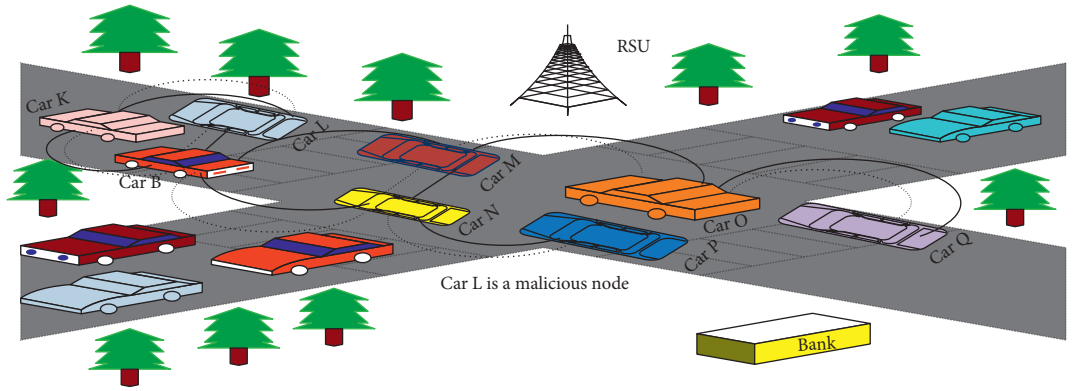

Figure 9: Black hole assault.

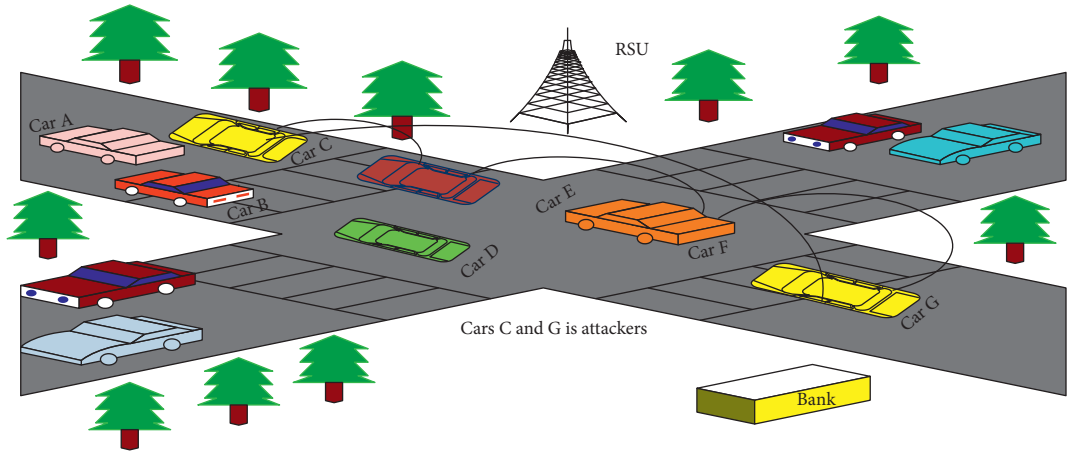

Figure 10: Worm hole assault.

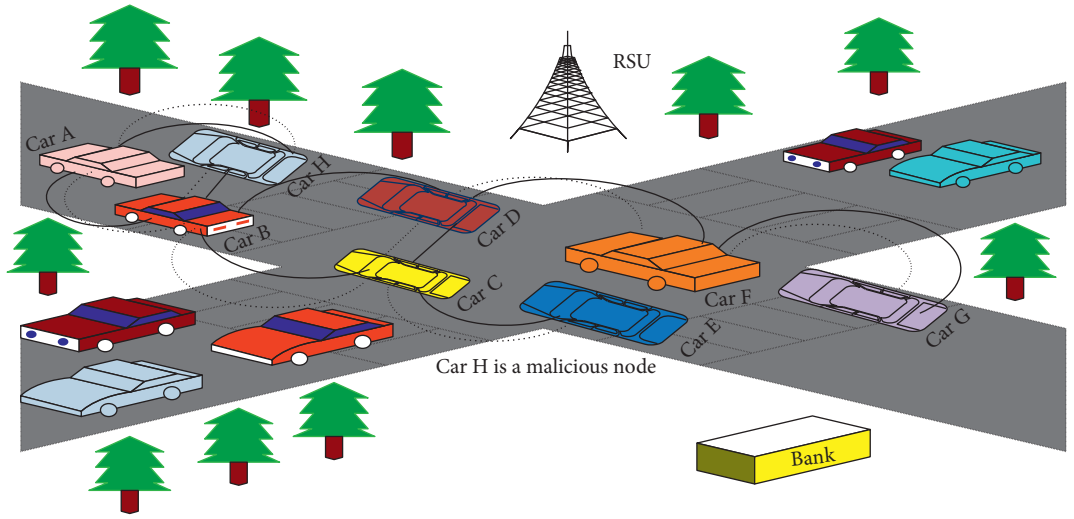

Figure 11: Gray hole assault.

intermediary node. This type of attack is a cryptography assault wherein the intermediary node will serve as an assailant that strives to decrypt the message through various decryption techniques [29, 52]. Figure 14 shows that Car L wants to send information to Car Q, while Car Q is far away. Thus, Car L sends the encrypted data packet to Car Q through Car N that is a malicious node which may attempt brute force assault and decrypt the message through a variety of decryption techniques.

3.4. Threats in Protocol Layer of VANETs. VANETs Routing Protocols (RP) consist of two groups, one is topology-based and the other is position-based routing. Every node is well

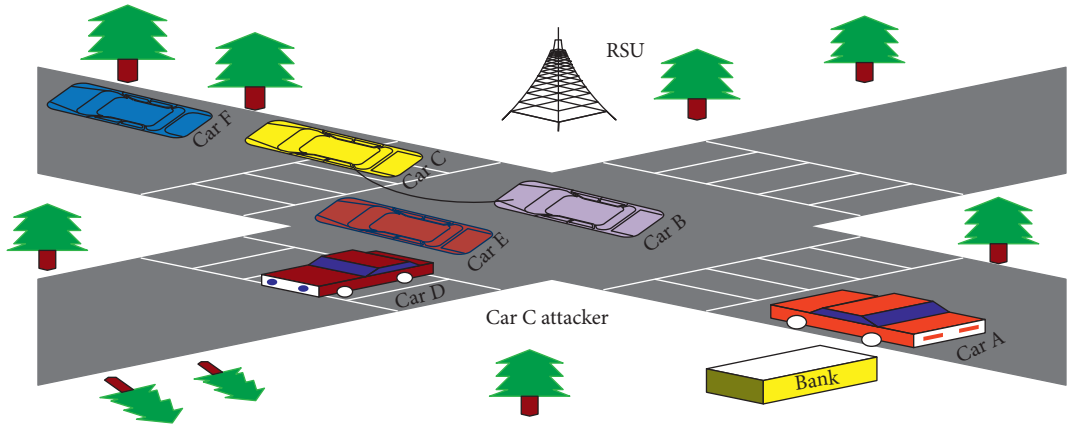

Figure 12: Masquerading assault.

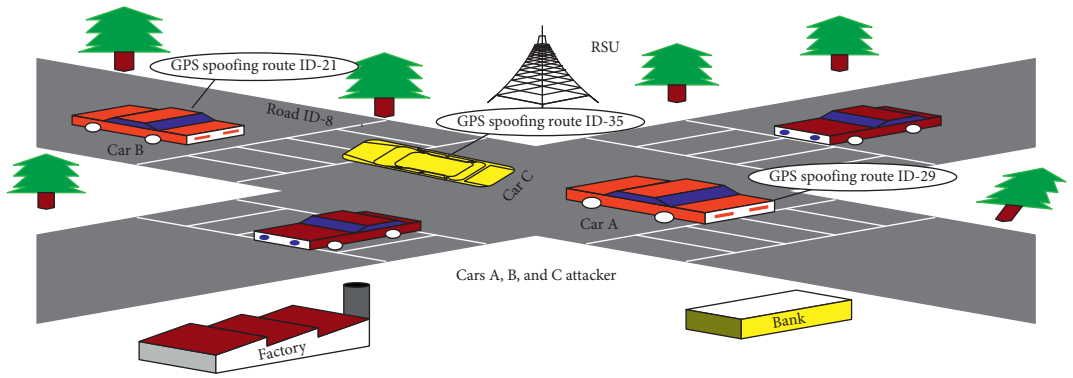

Figure 13: GPS spoofing assault.

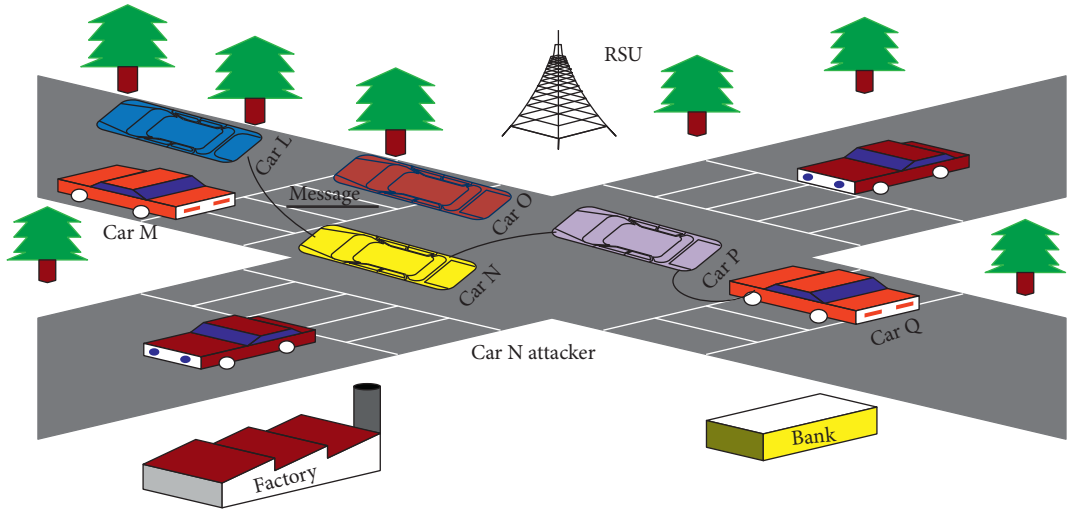

Figure 14: Brute force assault.

aware of the network layout in topology-based RP and sends messages using the accessible nodes and network connection information. One of the other side position-based RP nodes must be aware of the other node's location or position in which packet is being forwarded [53]. Figure 15 shows the two types of VANET routing protocols.

3.4.1. Topology-Based Protocol. The fundamental principle of the table-driven protocol is predetermining the route or path. It must gradually update the routing table every time the routing table is updated and share with neighboring node regularly [54]; therefore, while one node desires to communicate with another node, they already know about

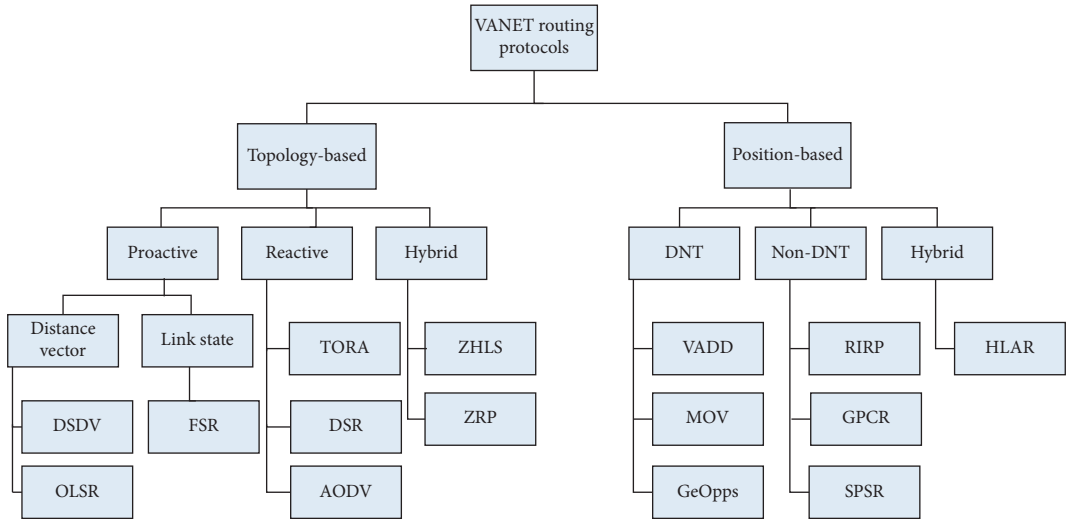

Figure 15: Routing protocols.

the path. One significant advantage of proactive protocols is the availability of path when the node wants to communicate on a network, but bandwidth decline is due to the generation of traffic caused by the swap of control packets [53, 55]. Proactive protocol examples are OLSR, DSDV, and GSR.

(i) Advantages:

Tracing the location of the route is not needed
Low latency when running in real time

(ii) Disadvantages:

Vacant routes consume an important session of the unoccupied bandwidth

3.4.2. Optimized Link State Routing. In MANETs, OLSR [56] is the table-driven routing protocol. OLSR can be regarded as the strength of a link-state algorithm for its benefits in relation to finding the path of any node whenever needed. Initially, using a particular node called multipoint relays (MPRs) [57], OLSR decreases the overhead from flooding of control traffic. In MPRs, select only those communication nodes that are the best path to provide from the source only to the destination, so MPRs help control traffic. Secondly, in OLSR requisite, just partial link states are flooded with an objective to present the shortest path routes [53, 58]. OLSR neighbor list table consists of up-to-date information which can be obtained from the neighboring nodes after exchanging its link-state information with those neighboring vehicle/nodes at regular intervals. As in link-state protocols, the routing messages created on a link are changed dynamically. This minimizes the number of control messages sent over the network which considerably [59] can deal with the blockage in traffic in VANETs, by forwarding and relaying the message to the nodes [58, 60].

3.4.3. Destination Sequenced Distance Vector. Bellman and ford have developed a centralized algorithm for assessing the shortest paths in weighted graphs. It was designed by Bertsekas and Gallager to execute in a distributed vogue called Distributed Bellman-Ford (DBF) algorithm [53, 61]. In DBF, all single nodes keep up the cost to arrive at each familiar destination. Hence, DBF comprises entries in the routing table. The routing table has no entry at the start, and all nodes start issuing a periodic broadcast message to its 1-hope neighborhood. The main drawback of this protocol is that it leads to count-to-infinity and looping problems. The loop may appear if the information regarding the assessment of shortest route becomes outdated. The primary purpose behind the origin of DSDV is to avoid the formation of loops. In DSDV the nodes converse with other network nodes. Each node has a routing table that refers to another network node that stores the necessary information concerning accessible destinations and the number of hopes to reach every node routing table. To maintain reliability in dynamically varying topologies, every vehicle/node exchanges its routing information with other neighbor vehicle/node at regular intervals or instantly while new information is updated in the routing table [54]. Every vehicle/node has its unique sequence number with each path as mentioned below:

(i) The target Internet protocol address
(ii) Number of hops requisite to arrive at the target location
(iii) The sequence number of the information received about that target location as initially marked by the target location

3.4.4. Global State Routing. Global state routing is a table-driven routing protocol; the link state algorithm is the basis of the global state routing protocol. It modifies and extends the connection state algorithm by limiting the message's middle vehicle/node renewal information. Each node in GSR holds a list of neighboring nodes, a topology table, and the next table of hope [59]. The neighbor list table consists of up-to-date information which can be obtained from the

neighboring nodes after exchanging its link-state information with those neighboring vehicle/nodes at regular intervals. As in link-state protocols, the routing messages created on a link are changed dynamically. This minimizes the number of control messages sent over the network considerably [59].

3.5. Reactive Protocols (On-Demand). The fundamental principle of reactive protocols is path allocation when the vehicle wants to communicate with another vehicle. Routing protocols have the key advantage of saving bandwidth in the reactive protocol when the node sends a message to the first path to be discovered. When a path is final from source to an intended destination, it is updated in the routing table and is then used for communication among source node to an intended destination node, and this path remains occupied with another node till the communication is completed [60, 62] (Reactive Protocols Example: AODV and DSR).

(i) Advantages:

To update the routing table, periodic flooding in the network is not required. Flooding is only done when required.
It saves the bandwidth.

(ii) Disadvantages:

For path discovery latency is high.
Too much flooding of the network disrupts the node's communication.

3.5.1. Ad Hoc On-Demand Distance Vector (AOVD). AOVD [28, 47, 61, 63], in MANETs, AODV protocol, is used for on-demand routing purposes with reactive routing. In the AODV protocol, routing table is maintained to store the next node routing information, i.e., for the target location nodes, and each routing table is used for a specific time period. If the path is demanded within a specific time, it becomes expired. Later, if a node wants to communicate, then again it finds a new route. In AODV, when the source node sends data, it checks the routing table and sends if the route is available. Otherwise, it needs to start the pathfinding process again to discover the finest route source to the target location for the purpose of transmitting packets through the broadcasting of route/path request (RREQ) message to its neighbor node. AODV was geared towards reducing the distribution of control traffic and stopping data traffic overhead, improving scalability and efficiency [16, 53, 58, 60, 64]. Figure 16 shows that in AODV the messages RREQ and RREP are used. In this figure, node S wants to communicate with node D, and all nodes are connected to their neighbor nodes and submit an RREQ message while every node sends REEQ message to the neighbor node. After receiving the RREQ message, every node sends back an RREP message. When all RREP messages are received, the source node chooses the best path and starts communication [57].

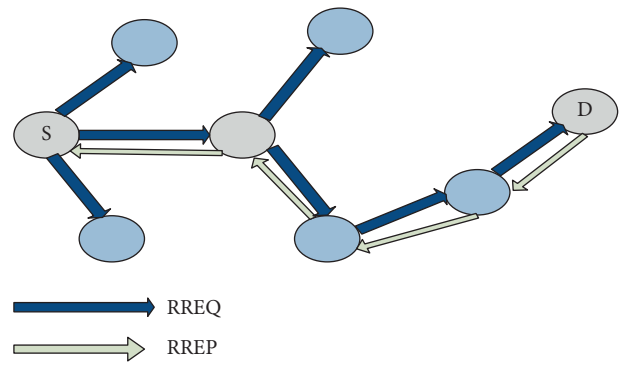

Figure 16: AODV RREQ and RREP message.

3.5.2. Dynamic Source Routing Protocol. DSR [65, 66] is a type of reactive routing protocol. If the vehicle desires to communicate with another vehicle in the network, it will search for a path and send packets to the intended destination. First, the vehicle searches a path after broadcasting a Route Request (RREQ), and this request passes through different nodes till the destination node where data need to be transferred. After they receive the path demand message, the intended destination broadcasts a Route Reply (RREP) packet back to the source vehicle with a unique ID. The dynamic source routing protocol stores the path information. If any unbroken connection or vacant path exists, then information is processed through path repairs. If there is any error on the path, the vehicle will send the Route Error message to the network [66]. DSR protocol is used in VANETs to maintain the network information and submit information about the traffic towards road-side unit [58, 66]. Table 1 shows the features of three routing protocols.

3.5.3. Security Issues for These Protocol Types. The AODV is a part of a reactive routing protocol. AODV's key benefit is that it is uncomplicated, takes less memory, and does not produce additional communication traffic along with the active connection. In AODV, the assailant might publicize a path with a slighter interval metric than the actual interval or publicize routing updates with a big sequence number after annulling all routing updates from supplementary nodes. An additional upgrade edition of AOVD proposed to solve these issues is secure AODV that presents more protected substantiation and truthfulness in AODV through the multihop link [67]. DSR protocol is another type of reactive protocol. The dissimilarity between them utilizes source routing sooner than relying on the routing table at every intermediary node. In DSR, another option is available; i.e., the data packets in this protocol can be forwarded on a hop-by-hop basis. It is feasible to vary the source route as planned in the attacker's route request or route reply packets in dynamic source routing. In DSR, removing a node from a list, changing the order, or adding a new node to a list are potential hazards [67]. In DSDV, significant security issues are scalability and also inappropriate DSDV for extremely dynamic VANETs.

Table 1: Contrast of AODV, DSDV, and OLSR features.

Protocol property	AODV	OLSR	DSDV
Reactive	Agreed	Not	Not
Route maintained in	Route table	Route table	Route table
Quality of service support	Not	Agreed	Not
Multicast routes	Not	Agreed	Not
Distributed	Agreed	Agreed	Agreed
Unidirectional link	Not	Agreed	Not
Support multicast	Agreed	Agreed	Not
Periodic broadcast	Agreed	Agreed	Agreed

3.6. Position-Based Protocol. The geographic location of the destination is determined in location-based routing. The positioning-based RP is generally proposed for the ad hoc network and does not use the network address to send data from the source to the intended target location. In VANETs, the transmission range is lower due to this frequent crash in the routing path. It is also due to gaps and crashes in the network. The problem of fading effect in urban highway environments, like tunnels and giant buildings, causes severe signal loss [68, 69]. Table 2 provides a summary of position-based protocol challenges and countermeasures.

Position-based routing is separated into three major groups detailed as follows:

(i) Nondelay tolerant

(ii) Delay tolerant

(iii) Hybrid

3.6.1. Nondelay Tolerant Network. The position-based first category is based mainly on greedy forwarding. Greedy perimeter stateless routing (GPSR) [70] protocol is used in greedy forwarding. GPSR uses only city scenarios because the dilemma is routing loops, an overlong path structure, and incorrect packet orders enhancing [69]. GPSR is proposed for MANETs; GPSR has a stumpy packet delivery ratio. Another protocol used for connectivity-aware routing is called A-STAR [68] for city buses for maintaining the path-based information. This algorithm might help to find the shortest route by giving connectivity among the vehicular nodes [69].

3.6.2. Delay Tolerant Network. Delay tolerant network [68] is also known as disruption tolerant network [1], delay-tolerant network, and store-carry-and-forward process-based network. Most of the current VANETs protocol had been proposed for immobile destinations. Vehicle-assisted data delivery (VADD) [70] is based on a carry-and-forward mechanism. A protocol connectivity-aware minimum delay geographic routing (CMGR) is similar to VADD. If we compare the CMGR and VADD, CMGR performs better as compared to VADD [69].

3.6.3. Hybrid Protocol. The hybrid protocol is a fusion of a Non-DTN and a disruption tolerant network. Geo-DTN + Nav for geographic transmission is a paradigm of hybrid protocol. In the hybrid protocol, we suppose that the target is standing still, being the reason for delay when one node switches to another. In GeoDTN + Nav [56], the message first switches to the perimeter node before moving to the disruption tolerant network for the enhanced broadcast of the message [69].

3.6.4. Issues for These Protocol Types. The crucial issue of GPRS is packet loss, and high delay could result in the loss of many hopes; as a result, perimeter mode forwarding may be expanded. STAR's reliability is drastically diminished by using a static street map to route packets of approximately possible radio obstacles, such as city buildings. GPCR uses no external static street map, so it is not easy to discover the intersection specifications. VADD is affected by the dynamic nature of the vehicular ad hoc network. It may cause a significant delay in delivery due to the traffic density [70].

3.7. Issues in the Application Layer of VANETs. The primary purpose of the protocol in the application layer is to minimize the end-to-end delay. However, sending emergency messages should arrive at the target vehicle by maintaining the deadline to supply service quality. In other applications, for instance, infotainment services delay is inevitable [71]. Vehicular information transfer protocol [72] is an application layer communication protocol to assist disseminated and ad hoc services infrastructure in VANETs. Two primary attacks on the application layer are malevolent code assault and repudiation assault. In malicious code attacks, malicious vehicles that want to attack networks send malicious codes like a virus, Trojan horse. These types of attacks damage the vehicle application and affect their services. In the repudiation attack [32], for instance, an application runs on a network that is used to control, track, and log user action, hence encouraging malevolent manipulation or spoofing of the recognition of new actions [71].

4. Solutions in VANETs

This section provides a brief review of the works furnished in the domain of VANETs security solutions. Table 3 provides a summary of challenges and countermeasures in VANETs.

4.1. Authenticated Routing for Ad Hoc Networks. The ARAN [73] routing protocol is based on AODV. In ARAN, a third party called certificate authority (CA) is responsible for sending a signed certificate to the nodes, upon receiving a certification request to CA. Asymmetric encryption techniques are used to verify the authenticity of secure path detection, and time tags are used to clear the path [75].

ARAN essentially has five steps:

(i) Certification

(ii) Authentic path finding

(iii) Authentic path setup

(iv) Path maintenance

(v) Key revocation

Table 2: Summary of position-based protocols challenges and countermeasures.

Challenges	Environment (traffic)	Countermeasures
Local optimal and link break	City traffic environment (no use of static external map)	GPSR protocol [70]
Maintain path base information	Static street map	A-STAR protocol [68]
Predictable vehicle mobility	City traffic environment	VADD and CMGR protocols [69, 70]

Table 3: Summary of challenges and countermeasures in VANETs.

Challenges	Techniques/technology	Countermeasures
Replay assault Impersonation assault Eavesdropping assault	Asymmetric encryption techniques are used to verify the authenticity of secure path detection, and time tags are used to clear the path.	Authenticated routing for ad hoc network protocol [73]
DoS assault Routing assault Impersonation assault	It uses the authentication process through one-way hash function.	Secure and efficient ad hoc distance vector protocol [74]
DoS assault Routing assault Replay assault	This protocol uses symmetric cryptographic operations. The one-way hash and MAC functions are used for substantiation and are transmitted via a shared key between nodes.	Ariadne [75]
Routing assault Impersonation assault Bogus information	It uses digital signature and hash function.	SAODV [75]
Routing assault Impersonation assault Bogus information	It uses digital signature and hash function.	A-SAODV [75]
Session hijacking	Cookies are allocated for each session for session management.	One time cookie [75]
Sybil assault	Identifying a malicious node is achieved by discovery of two or supplementary nodes with similar trajectories motion.	Robust method for Sybil assault detection [76]
Impersonation assault	It uses registration ID technique.	Holistic protocol [75]

In the ARAN path, the authentication process is done in every step by adding each middle node's sign and certificate, so this protocol solves the impersonation problem.

4.2. Secure and Efficient Ad Hoc Distance Vector Protocol. Working over DSDV, the secure and efficient ad hoc distance vector protocol (SEAD) [74] uses the authentication process hash function. SEAD uses destination sequence number to ensure path freshness, which assists in avoiding the wrong path. To ensure path authenticity, the SEAD uses hashing on each intermediate node [75].

4.3. Ariadne. Working on DSR, this protocol uses symmetric cryptographic operations. The one-way hash and MAC functions are used for substantiation and are transmitted via a shared key between nodes. The TESLA uses Ariadne-based authentication for data transmission. The TESLA time interval is used in the route discovery and authentication process [75].

4.4. SAODV. This protocol proposed the integration of security measures into the AODV protocol. All routing correspondence is signed digitally to assure legitimacy, and hash functions are used to guard hop count. The route response cannot be sent in this intermediate node method, even though they know the new path. This problem can be solved by double signature; in addition, it raises the system complexity [75].

4.5. A-SAODV. A-SAODV is an extended version of SAODV, which has an experimental adaptive response decision attribute. Depending on the length of the queue and the threshold conditions, each middle node may come to a decision, whether to send a response to the source node or not [75].

4.6. One-Time Cookie. Usually, cookies are allocated for each session for session management. However, this protocol gives OTC the concept to protect the system from session abduction and SID stealing. OTC produces a token for every request, and these tokens are linked to request using HMAC to avoid the token from being reused [75].

4.7. Elliptic Curve Digital Signature Algorithm. ECDSA [77] algorithm utilizes a digital signature. Additionally, ECDSA ensures the genuineness and protection of the digital

signatures through hash and related symmetric key operations. It can be initiated once both the sender and the receiver agree upon the parameters for elliptical curve domain parameters [75].

4.8. Robust Method for Sybil Attack Detection. RobSAD [76] approach's core principle is that drivers cannot have the same movement pattern for two different vehicles, as every human being drives along with their comfort. Identifying a malicious node is achieved by the discovery of two or supplementary nodes with similar trajectories motion [76].

4.9. Holistic Protocol. This protocol describes the method of authentication by registering the vehicle/node by RSU. The vehicles send Hello message to the RSU during the vehicle registration process; RSU then prepares and sends the Registration ID (consisting of the license number and registration number of vehicle) to the node. Additionally, the verification is complete through a RSU certificate. If the vehicle is genuine, only information will be shared; otherwise, it will be blocked [75].

4.10. Challenges in the Physical Layer of VANETs. Due to the high speed, the signals of VANETs entities undergo multipath fading and Doppler frequency shifts. Hence, due to the effects of the multipath fading and frequency shifts, the need of physical layer communication arises. For testing the application, V2V uses radio and infrared (IR) waves to communicate. The V2V communication occurs through excessive frequencies like micro- and millimetre waves. The waves that belong to the infrared and millimetre category use the line of sight communication [71, 78].

The DSRC physical layer includes the 802.11p OFDM, which operates within 5.9 GHz band (5.885–5.9.5) range with a maximum of 10 MHz channel [78]. The underlying data rate is approximately 3 Mbps, and the default data rate is 6 Mbps. The physical layer in VANETs is a thoroughly researched area. From transmission control to using multiple (or individual) antennas and from evaluation to channel-to-channel selection, there are numerous aspects of the physical layer which contribute to network scalability. Owing to the spread of delays and mobility on several roads, the multipath environment makes communication extremely challenging. Delay-spread frequency selective fading and mobility cause time-selective fading. The need of the line of sight leads to a significant delay owing to dispersal, and Doppler spreads [79]. The challenges to the physical layer in VANETs consist of the following.

4.10.1. Dual and Single Radio. The coincidence among single and double radio is still vague. Although dual-radio has different clear benefits, inserting a second radio into the survival of single radios does not boost protection contact efficiency under the default scheme [79].

4.10.2. Model for Propagation. Vehicular ad hoc networks work in three types of environments: countryside, city, and highway. The free-space model used for the highway is not rigorously exact as the signal passes through the adjacent reflections. The city free-space model can be effected by shadowing and multipath fading. In a rural environment, some other factor, like trees and hills, can cause lots of reflection [79].

4.10.3. Selection of the Channel. An analytical and simulation study is required at the physical layer for the channel selection. A game-theoretic approach can be used for selecting the best channel and data rate [79].

4.10.4. Channel Estimation. We require advanced channel estimation techniques in VANETs to acquire a correct channel state information (CSI) [79].

4.10.5. Variety of Techniques. Fading and interfering effects can be minimized using a range of techniques [79].

4.11. Algorithms in the Protocol Layer of VANETs. The reliance on remote correspondence, control, and handling innovation renders IoV dynamically weak against potential ambushes, such as remote interruption, control, and direction [80]. For itself, compelling validation courses of action envisioning unapproved visitors must be directed to adapt to these issues. Thus, this work focuses on the security and protection by structuring up twofold verification conspiring for Internet of Vehicles as demonstrated by its different situations. In any case, the OBU self-makes an unclear personality and provisional encryption key to open a validation session. Second, the trust master's legitimacy of the node's actual and baffling personality can be confirmed (TA). Table 4 provides a summary of algorithms in protocol layers of VANETs challenges and countermeasures.

Zeng et al. [81] proposed a new route for city VANETs formed by connectivity analysis based on geographical position to conquer the general mistakes of VANETs route in the city area. In combination with a digital city map, LCGL manages the geographical position information about nodes and connections. LCGL selects the shortest connected route to forward the data packet to the route and link length.

As per Sun et al. [82], several open communication protocols overlook the nearness of structures or difficulties accessible amid viable use, mainly in urban regions. These deterrents can cause signal fading or even square direct communication. Numerous vehicles are often left on the road side. As a result of their location, these left vehicles can be utilized as transfers to successfully lessen the shadowing impact of deterrents and even tackle communication issues. In this work, the author exhibited left-vehicle right-hand off-routing communication in vehicle ad hoc networks. The author of [82] proposed a practical left vehicle associate hand-off routing calculation made out of four sections: an occasional Hello packet trade instrument, competitor transfer list update, communication connect quality

Table 4: Summary of algorithms in protocol layers of VANETs challenges and countermeasures.

Paper	Challenges	Countermeasures
Zeng et al. [81]	Connectivity analysis in city based on geographical position	Link connectivity analysis on geographic location (LCGL) routing scheme
Sun et al. [82]	Road side vehicle communication issue	Practical left vehicle associate had off routing
Rahman and Tepe [83]	Channel access conflicts confirming improved channel usage in cross layer V2V and V2I communication\enleadertwodots	Multilevel algorithm removing these issues
Kumar and Mann [84]	Multiple malicious node detection in the network and avoiding DOS assault	Packet detection algorithm
Malla and Sahu [85]	Various existing solutions using cryptographic techniques are time and resources consuming	The proposed solution betters the security in VANETs without using cryptographic techniques
Waraich and Batra [86]	DOS assault recognition	Quick response table and recognition of the DOS attack
Jeffane and Ibrahimi [87]	DOS assault on the physical and MAC layers in IEE standard 802.11p	Packet delivery ratio (PDR) metric to detect the DOS attack
RoselinMary et al. [88]	Detecting the DOS assault before the verification time	Attacked packet detection algorithm
Singh and Sharma [89]	DOS attack is the main challenge to network availability	Proposing an enhanced attacked packet detection algorithm
Quyoom et al. [31]	Detecting the DOS assault	Proposed MIPDA
Issac and Mary [90]	Protection against DOS assault to mitigate packet loss	Updated prediction-based authentication method (PBA)
Sohail et al. [91]	Security challenges in VIoT, such as efficient trust assessment, certified user nonfunctioning and secure information diffusion	Proposing a new scheme, trust enhanced on-demand routing (TER)

evaluation, and hopeful hand-off rundown selection. Simulation results uncover evident advantages for lists, such as the nature of communication, achievement rate, and time delay.

Ad hoc vehicular networks have twisted into an increasing innovation that can gratify the interest of advancing associated vehicles and developing prerequisites for the Canny Transportation Framework (ITS). Authentications are utilized to confirm vehicular correspondence though the declarations of vehicles should be disavowed if every vehicle is found to get out of hand hubs. In VANETs, authentication disavowal Certificate Revocation Lists (CRL) must be instantly conveyed to every single vehicular hub to avoid redundant correspondence with the noxious hubs. Be that as it may, because of developing several testaments, the measure of CRL constantly increases, and, subsequently, it ends up hard overseeing and conveying the CRL in vehicular networks. The author presents a compelling and adaptable plan to convey a declaration denial list in the various leveled engineering of VANETs [92].

Rahman and Tepe [83] stated that the DSRC/WAVE system is standardized to broadcast critical security information with IEEE 802.11p as MAC protocol. Studies show that IEEE 802.11p fights the adverse effects of asymmetric radio communications and mobility problems in V2V and V2I communication. The author provides a well-organized and consistent cross-layer algorithm for problems with V2V and V2I communication. The analysis shows that the multilevel algorithm's proposal removes channel access conflicts and confirms improved channel usage. The solution can be the dissemination of up to three jumps without routing protocol. That is chiefly significant for security and emergency critical message of area vehicle network.

Kumar and Mann [84] considered the safety of VANETs. As per Kumar et al., the security of the vehicles or nodes can be enlarged if the network accessibility is increased. If the denial of service of attack happens on the network, the availability of the network decreases. The authors proposed an algorithm that was proficient at sensing the numerous malicious nodes or vehicles that transfer the unrelated packet to squeeze the network and ultimately stop the network from transmitting the safety information messages. The proposed algorithm simulated on NS-2 and the quantitative values of packet delivery ratio, packet loss ratio, and network throughput demonstrates that by detecting the denial of service attack in a good time, the proposed algorithm improves the network security.

Vehicular ad hoc network aims to improve transportation efficiency and safety. VANETs have open nature of wireless medium, so the number of chances of various attacks in this work increases. The authors proposed a solution for DOS attack which uses the redundancy removal mechanism consisting of rate decreasing algorithms and state transition mechanism as its components.

The protocol of Malla and Sahu [85] uses various existing solutions (channel switching, frequency hopping, multiradio transceivers, and communication technology). The proposed solution betters the security in VANETs without using cryptographic techniques.

Due to high mobility in VANETs, secure routing is a big issue [86]. The topology nature of VANETs is dynamic; paths are regularly updated, and sometimes the communication link breaks due to hurdles such as buildings, bridges, and tunnels. It is challenging to determine the reason for packet drop because persistent connection breaks can cause packet drop, resulting in deterioration of

network performance in vehicular ad hoc networks. This also happens due to the existence of security threats. VANETs are subclass of MANETs and exist in the same attack. Researchers have already developed different security mechanisms for safe routing in MANETs, but these solutions are not compatible with VANETs because of specific attributes. A vehicle can communicate with other vehicles (V2V) as well as communicating to infrastructure (V2I). Waraich and Batra [86] proposed a solution to avoid the DOS attack to ensure routing for both forms of communication. They use the quick response table and recognize the DOS attack.

VANETs are a subgroup of MANETs. It is developed to provide communication between vehicles and fixed equipment (RSU) to give each other's range. VANETs are very sensitive to safety issues. Jeffane and Ibrahimi [87] proposed a new mechanism that focuses on the denial of service attack on the physical and MAC layers in IEE standard 802.11p. This solution uses the packet delivery ratio (PDR) metric to detect the DOS attack.

Security for VANETs is vital because their very presence relates to critical circumstances that are life-threatening [88]. VANETs are a subgroup of MANETs. All nodes or vehicles are equipped with an On-Board Unit (OBU), enabling data from one node to another in the network to be sent and received. In vehicular ad hoc network communication interface provided by the on-road infrastructure, to detect the denial of service attack before verification time, Roselin Mary et al. [88] proposed a new algorithm (attacked packet detection algorithm).

Important information shared for vehicle protection is the major issue. The node is self-organized, highly mobile, and of free movement in a vehicular ad hoc network, so any node may communicate with any other node that may (or not) be trustworthy. This is the area of concern inside the VANETs security horizon. The road-side unit is responsible for every node at all times and provides the communication of secure information. The vehicles and the RSU are prone to several security attacks like selfish driver attacks, masquerading attacks, Sybil attacks, and alteration attacks. DOS attack is the main challenge to network availability. Singh and Sharma [89] proposed an enhanced attacked packet detection algorithm, which prohibits network performance deterioration even under this attack. EAPDA checks the nodes, detects malicious nodes, and better gets the throughput with minimized delay, thus improving security.

As per Quyoom et al. [31], the security of VANETs plays a vital role in sustaining essential life. A sensitive, life-related information network must be open at all times for secure communication. Several types of attacks and threads possible in VANET were subject to the network accessibility problem. These attacks include Sybil attacks, misbehaving attacks, incorrect vehicle position information, and selfish driver and jamming attacks. Among these attacks, a significant threat to the information economy is the denial of service attacks. To analyze and detect the DOS attack, the authors proposed a Malicious and Irrelevant Packet Detection Algorithm (MIPDA).

Issac and Mary [90] used the updated prediction-based authentication method (PBA) to protect against VANETs DOS attack to mitigate packet loss caused by vehicle mobility. The primary aim is to reduce the delay in validating emergency vehicles such as ambulances and fire services. The architecture of the PBA is such that the beacons cannot be predicted by the sender vehicles. This process has been shown to be secure as a result.

The IoT plays an essential role in connecting the network with the world and new technologies. However, VANETs being an important segment of IoT have faced various challenges due to the high mobility and dynamic nature of the network. IoT focuses in future to allow internetworking to disseminate information. Previous security solutions to vehicular Internet of Things (VIoT) focus more on privacy protection and security-related challenges using PKI. Sohail et al. [91] proposed a new scheme, trust enhanced on-demand routing (TER). This scheme overcomes the security challenges in VIoT, such as efficient trust assessment, certified user nonfunctioning, and secure information diffusion.

4.12. Solutions in the Application Layer of VANETs. The principal aim for the application layer protocols is to decrease the end-to-end delay caused by sending emergency messages. In other applications, for instance, infotainment services delay is predictable. Vehicular Information Transfer Protocol (VITP) is an application layer communication protocol to support distributed and ad hoc service infrastructure in VANET [71]. Two possible primary assaults in application layer are malevolent code attack and the repudiation attack. In malevolent code assault, malevolent vehicles send malevolent code or programs, for instance, viruses, Trojan horses. These malicious codes damage the vehicle application and affect their services. A repudiation attack, in which attackers control the whole network with the help of the various applications, gets all information quickly and manipulates the message. The application layer is capable of detecting DoS attacks than other layers [71].

Two schemes were proposed in [67]; the first scheme is an application-aware control scheme in which all accessible applications should be periodically registered and updated and forwarded to all other VANETs nodes. The second scheme includes the unified routing scheme that will route a packet of precise applications according to demand and safety requirements.

5. Conclusion

Consisting of mobile information and communication infrastructure, the VANETs play an important role in road safety and travel comfort. However, as technology is growing and VANETs are getting more popular, security vulnerabilities are increasing rapidly, which ultimately restricts the widespread usage of the VANETs. In this article, the security vulnerabilities of VANETs are surveyed. The article also provides layer-specific attack classification in the VANETS protocol stack. Besides, we also provided a discussion on several countermeasures.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

Conceptualization was done by J. M. and Y. Y.; investigation was carried out by Y. Y. and M. N. M. B.; original draft was prepared by J. M. and Y. Y.; review and editing were done by Y. Y. and J. N.; supervision was provided by Z. D. and Q. W.; funding acquisition was made by Z. D.\enleadertwodots. All authors have read and agreed to the published version of the manuscript.

Acknowledgments

This work was supported by Key Research Item for the Industry of Shaanxi Province under grant no. 2018GY-136.

References

[1] R. Geng, X. Wang, and J. Liu, "A software defined networking-oriented security scheme for vehicle networks," *IEEE Access*, vol. 6, pp. 58195–58203, 2018.

[2] N. S. Samaras, "Using basic manet routing algorithms for data dissemination in vehicular ad hoc networks (VANETs)," in *Proceedings of the 2016 24th Telecommunications Forum (TELFOR)*, pp. 1–4, IEEE, Belgrade, Serbia, November 2016.

[3] J. Wantoro and I. W. Mustika, "M-aodv+: an extension of aodv+ routing protocol for supporting vehicle-to-vehicle communication in vehicular ad hoc networks," in *Proceedings of the 2014 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*, pp. 39–44, IEEE, Jakarta, Indonesia, November 2014.

[4] L. Feng, Y. Xiu-Ping, and W. Jie, "Security transmission routing protocol for mimo-vanet," in *Proceedings of the 2014 International Conference on Cloud Computing and Internet of Things*, pp. 152–156, IEEE, Changchun, China, December 2014.

[5] C. Pathak, A. Shrivastava, and A. Jain, "Ad Hoc on demand distance vector routing protocol using dijkastra's algorithm (aodv-d) for high throughput in vanet (vehicular Ad Hoc network)," in *Proceedings of the 2016 11th International Conference on Industrial and Information Systems (ICIIS)*, pp. 355–359, IEEE, Roorkee, India, December 2016.

[6] I. U. Rasool, Y. B. Zikria, and S. W. Kim, "A review of wireless access vehicular environment multichannel operational medium access control protocols: quality-of-service analysis and other related issues," *International Journal of Distributed Sensor Networks*, vol. 13, no. 5, 2017.

[7] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: communication, applications and challenges," *Vehicular Communications*, vol. 19, Article ID 100179, 2019.

[8] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETs): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[9] Z. Afzal and M. Kumar, "Security of vehicular ad-hoc networks (vanet): a survey," *Journal of Physics: Conference Series*, vol. 1427, no. 1, Article ID 012015, 2020.

[10] M. S. Sheikh, J. Liang, and W. Wang, "Security and privacy in vehicular ad hoc network and vehicle cloud computing: a survey," *Wireless Communications and Mobile Computing*, vol. 202025 pages, Article ID 5129620, 2020.

[11] A. Awang, K. Husain, N. Kamel, and S. Aissa, "Routing in vehicular ad-hoc networks: a Survey on single- and cross-layer design techniques, and perspectives," *IEEE Access*, vol. 5, pp. 9497–9517, 2017.

[12] S. A. Chaudhry, "Correcting "palk: password-based anonymous lightweight key agreement framework for smart grid"" *International Journal of Electrical Power & Energy Systems*, vol. 125, Article ID 106529, 2021.

[13] X. Li, Y. Han, J. Gao, and J. Niu, "Secure hierarchical authentication protocol in vanet," *IET Information Security*, vol. 14, no. 1, pp. 99–110, 2019.

[14] A. Sari, O. Onursal, M. Akkaya et al., "Review of the security issues in vehicular ad hoc networks (vanet)," *International Journal of Communications, Network and System Sciences*, vol. 8, no. 13, pp. 552–566, 2015.

[15] Z. A. Abdulkader, A. Abdullah, M. Taufik Abdullah, and Z. Ahmad Zukarnain, "Vehicular ad hoc networks and security issues: survey," *Modern Applied Science*, vol. 11, no. 5, Article ID 30, 2017.

[16] R. C. Poonia, D. Bhargava, and B. S. Kumar, "Cdra: cluster-based dynamic routing approach as a development of the aodv in vehicular ad-hoc networks," in *Proceedings of the 2015 International Conference on Signal Processing and Communication Engineering Systems*, pp. 397–401, IEEE, Guntur, India, January 2015.

[17] P. Agarwal, "Technical review on different applications, challenges and security in vanet," *Journal of Multimedia Technology & Recent Advancements*, vol. 4, no. 3, pp. 21–30, 2017.

[18] V. K. Tripathi and S. Venkaeswari, "Secure communication with privacy preservation in vanet-using multilingual translation," in *Proceedings of the 2015 Global Conference on Communication Technologies (GCCT)*, pp. 125–127, IEEE, Thuckalay, India, April 2015.

[19] A. Kumar and M. Bansal, "A review on vanet security attacks and their countermeasure," in *Proceedings of the 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*, pp. 580–585, IEEE, Solan, India, September 2017.

[20] P. Caballero-Gil and X. Wang, "Security issues in vehicular ad hoc networks," *Mobile Ad Hoc networks: Applications*, pp. 67–88, 2011.

[21] A. Irshad, M. Usman, S. A. Chaudhry, H. Naqvi, and M. Shafiq, "A provably secure and efficient authenticated key agreement scheme for energy internet based vehicle-to-grid technology framework," *IEEE Transactions on Industry Applications*, vol. 99, p. 1, 2020.

[22] S. Hussain and S. A. Chaudhry, ""Comments on "biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment"" *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10 936–10 940, 2019.

[23] N. K. Chaubey, "Security analysis of vehicular ad hoc networks (VANETs): a comprehensive study," *International Journal of Security and Its Applications*, vol. 10, no. 5, pp. 261–274, 2016.

[24] S. M. Faisal and T. Zaidi, "Timestamp based detection of sybil attack in vanet," *IJ Network Security*, vol. 22, no. 3, pp. 397–408, 2020.

[25] M. B. Mansour, C. Salama, H. K. Mohamed, and S. A. Hammad, "Vanet security and privacy-an overview," *International Journal of Network Security & Its Applications*, vol. 10, no. 2, pp. 13–34, 2018.

[26] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "Vanet security surveys," *Computer Communications*, vol. 44, pp. 1–13, 2014.

[27] I. A. Sumra, I. Ahmad, H. Hasbullah et al., "Classes of attacks in vanet," in *Proceedings of the 2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC)*, pp. 1–5, IEEE, Riyadh, Saudi Arabia, April 2011.

[28] A. Suman and C. Kumar, "A behavioral study of sybil attack on vehicular network," in *Proceedings of the 2016 3rd International Conference on Recent Advances in Information Technology (RAIT)*, pp. 56–60, IEEE, Dhanbad, India, March 2016.

[29] A. N. Upadhyaya and J. Shah, "Attacks on vanet security," *International Journal of Computer Engineering and Software Technology*, vol. 9, no. 1, pp. 8–19, 2018.

[30] K. Mahmood, J. Arshad, S. A. Chaudhry, and S. Kumari, "An enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure," *International Journal of Communication Systems*, vol. 32, no. 16, Article ID e4137, 2019.

[31] A. Quyoom, R. Ali, D. N. Gouttam, and H. Sharma, "A novel mechanism of detection of denial of service attack (dos) in vanet using malicious and irrelevant packet detection algorithm (mipda)," in *Proceedings of the International Conference on Computing, Communication & Automation*, pp. 414–419, IEEE, Noida, India, May 2015.

[32] R. Shringar Raw, M. Kumar, and N. Singh, "Security challenges, issues and their solutions for vanet," *International Journal of Network Security & Its Applications*, vol. 5, no. 5, pp. 95–105, 2013.

[33] H. Hasbullah, I. A. Soomro, and J. Manan, "Denial of service (dos) attack and its possible solutions in vanet," *International Journal of Electronics and Communication Engineering*, vol. 4, no. 5, pp. 813–817, 2010.

[34] D. Rampaul, R. K. Patial, and D. Kumar, "Detection of dos attack in VANETs," *Indian Journal of Science and Technology*, vol. 9, no. 47, pp. 1–6, 2016.

[35] A. Sahi, D. Lai, Y. Li, and M. Diykh, "An efficient DDOS TCP flood attack detection and prevention system in a cloud environment," *IEEE Access*, vol. 5, pp. 6036–6048, 2017.

[36] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, "Securing smart city surveillance: a lightweight authentication mechanism for unmanned vehicles," *IEEE Access*, vol. 8, pp. 43711–743724, 2020.

[37] S. A. Chaudhry, T. Shon, F. Al-Turjman, and M. H. Alsharif, "Correcting design flaws: an improved and cloud assisted key agreement scheme in cyber physical systems," *Computer Communications*, vol. 153, pp. 527–537, 2020.

[38] D. Kushwaha, P. K. Shukla, and R. Baraskar, "A survey on sybil attack in vehicular Ad Hoc network," *International Journal of Computer Applications*, vol. 98, no. 15, 2014.

[39] M. Rahbari and M. A. J. Jamali, "Efficient detection of sybil attack based on cryptography in vanet," 2011, https://arxiv.org/abs/1112.2257.

[40] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IOV," *Ad Hoc Networks*, vol. 61, pp. 33–50, 2017.

[41] T. Zaidi and S. Faisal, "An overview: various attacks in vanet," in *Proceedings of the 2018 4th International Conference on Computing Communication and Automation (ICCCA)*, pp. 1–6, IEEE, Greater Noida, India, December 2018.

[42] V. Bibhu, K. Roshan, K. B. Singh, and D. K. Singh, "Performance analysis of black hole attack in vanet," *International Journal of Computer Network and Information Security*, vol. 4, no. 11, pp. 47–54, 2012.

[43] I. Dhyani, N. Goel, G. Sharma, and B. Mallick, "A reliable tactic for detecting black hole attack in vehicular ad hoc networks," in *Advances in Computer and Computational Sciences*, pp. 333–343, Springer, Berlin, Germany, 2017.

[44] K. C. Purohit, S. C. Dimri, and S. Jasola, "Mitigation and performance analysis of routing protocols under black-hole attack in vehicular Ad Hoc network (vanet)," *Wireless Personal Communications*, vol. 97, no. 4, pp. 5099–5114, 2017.

[45] H. P. Singh, V. P. Singh, and R. Singh, "Cooperative black-hole/grayhole attack detection and prevention in mobile ad hoc network: a review," *International Journal of Computer Applications*, vol. 64, no. 3, pp. 16–22, 2013.

[46] M. A. H. Al Junaid, A. Syed, M. N. M. Warip, K. N. F. K. Azir, and N. H. Romli, "Classification of security attacks in vanet: a review of requirements and perspectives," in *Proceedings of the MATEC Web of Conferences*, EDP Sciences, Article ID 06038, 2018.

[47] S. Lachdhaf, M. Mazouzi, and M. Abid, "Secured aodv routing protocol for the detection and prevention of black hole attack in vanet," *Advanced Computing: International Journal*, vol. 9, no. 1, 2018.

[48] J. Tobin, C. Thorpe, and L. Murphy, "An approach to mitigate black hole attacks on vehicular wireless networks," in *Proceedings of the 2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, pp. 1–7, IEEE, Sydney, Australia, June 2017.

[49] J. Singh and N. Sharma, "Wormhole attack detection by using intrusion detection system in vanet," *International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN*, pp. 2250–3501, 2012.

[50] S. Verma, B. Mallick, and P. Verma, "Impact of gray hole attack in vanet," in *Proceedings of the 2015 1st International Conference on Next Generation Computing Technologies (NGCT)*, pp. 127–130, IEEE, Dehradun, India, September 2015.

[51] N. Phull and P. Singh, "A review on security issues in VANETs," in *Proceedings of the 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 1084–1088, IEEE, New Delhi, India, March 2019.

[52] N. Couture and K. B. Kent, "The effectiveness of brute force attacks on rc4," in *Proceedings of the Second Annual Conference on Communication Networks and Services Research, 2004*, pp. 333–336, IEEE, Fredericton, Canada, May 2004.

[53] B. Hamid and E.-N. El Mokhtar, "Performance analysis of the vehicular ad hoc networks (vanet) routing protocols aodv, dsdv and olsr," in *Proceedings of the 2015 5th International Conference on Information & Communication Technology and Accessibility (ICTA)*, pp. 1–6, IEEE, Marrakech, Morocco, December 2015.

[54] I. Mouhib, M. Smail, M. D. El Ouadghiri, and H. Naanani, "Network as a service for smart vehicles: a new comparative study of the optimized protocol q-aodv and gpsr protocol,," in *Proceedings of the 2016 International Conference on Engineering & MIS (ICEMIS)*, pp. 1–5, IEEE, Agadir, Morocco, September 2016.

[55] A. Datta, "Modified ant-aodv-vanet routing protocol for vehicular adhoc network," in *Proceedings of the 2017 1st International Conference on Electronics, Materials Engineering and Nano-Technology (IEMENTech)*, pp. 1–6, IEEE, Kolkata, India, April 2017.

[56] K. N. Qureshi and H. Abdullah, "Topology based routing protocols for vanet and their comparison with manet," *Journal of Theoretical and Applied Information Technology*, vol. 58, no. 3, pp. 707–715, 2013.

[57] L. Rivoirard, M. Wahl, P. Sondi, M. Berbineau, and D. Gruyer, "Performance evaluation of aodv, dsr, grp and olsr for vanet with real-world trajectories," in *Proceedings of the 2017 15th International Conference on ITS Telecommunications (ITST)*, pp. 1–7, IEEE, Warsaw, Poland, May 2017.

[58] A. Chekima, F. Wong, J. A. Dargham et al., "A study on vehicular ad hoc networks," in *Proceedings of the 2015 3rd International Conference on Artificial Intelligence, Modelling and Simulation (AIMS)*, pp. 422–426, IEEE, Kota Kinabalu, Malaysia, December 2015.

[59] T. P. Venkatesan, P. Rajakumar, and A. Pitchaikkannu, "Overview of proactive routing protocols in manet," in *Proceedings of the 2014 Fourth International Conference on Communication Systems and Network Technologies*, pp. 173–177, IEEE, Washington, DC, USA, April 2014.

[60] A. Nayyar, "Flying adhoc network (fanets): simulation based performance comparison of routing protocols: aodv, dsdv, dsr, olsr, aomdv and hwmp," in *Proceedings of the 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*, pp. 1–9, IEEE, Durban, South Africa, August 2018.

[61] S. Tabar, L. Najjar, and M. Gholamalitabar, "Quality of service in the network layer of vehicular ad hoc networks," in *Proceedings of the World Congress on Engineering and Computer Science*, San Francisco, CA, USA, October 2016.

[62] B. Paul and M. Abu Naser Bikas, "Vanet routing protocols: pros and cons," *International Journal of Computer Applications*, vol. 20, no. 3, pp. 28–34, 2011.

[63] M. N. Amara korba Abdelaziz and G. Salim, "Analysis of security attacks in aodv," in *Proceedings of the 2014 International Conference on Multimedia Computing and Systems (ICMCS)*, IEEE, Marrakech, Morocco, April 2014.

[64] N. Garg and P. Rani, "An improved aodv routing protocol for vanet (vehicular Ad Hoc network)," *International Journal of Science, Engineering and Technology Research (IJSETR)*, vol. 4, no. 16, p. 1024, 2015.

[65] S. Dhankhar and S. Agrawal, "VANETs: a survey on routing protocols and issues," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 3, no. 6, pp. 13427–13435, 2014.

[66] A. Moravejosharieh, H. Modares, R. Salleh, and E. Mostajeran, "Performance analysis of aodv, aomdv, dsr, dsdv routing protocols in vehicular ad hoc network," *Research Journal of Recent Sciences ISSN*, vol. 2277, p. 2502, 2013.

[67] B. Mokhtar and M. Azab, "Survey on security issues in vehicular ad hoc networks," *Alexandria engineering journal*, vol. 54, no. 4, pp. 1115–1126, 2015.

[68] M. K. Nasir, M. K. Sohel, M. T. Rahman, and A. K. Islam, "A review on position based routing protocol in vehicular adhoc network," *American Journal of Engineering Research*, vol. 2, no. 2, pp. 7–13, 2013.

[69] B. Pete and P. Jaini, "Continuous connectivity aware routing in VANET using hybrid protocol," in *Proceedings of the 2015 2nd International Conference on Electronics and Communication Systems (ICECS)*, IEEE, Coimbatore, India, Febuary 2015..

[70] S. Boussoufa-Lahlah, F. Semchedine, and L. Bouallouche-Medjkoune, "A position-based routing protocol for vehicular ad hoc networks in a city environment," *Procedia Computer Science*, vol. 73, pp. 102–108, 2015.

[71] C. S. Evangeline and V. B. Kumaravelu, "Survey on VANET's layered architecture, security challenges and target network selection schemes," vol. 14, no. 24, pp. 4248–4262, 2006, https://www.researchgate.net/journal/Journal-of-Engineering-and-Applied-Sciences-1819-6608.

[72] M. D. Dikaiakos, S. Iqbal, T. Nadeem, and L. Iftode, "VITP: an information transfer protocol for vehicular computing," in *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, pp. 30–39, Cologne, Germany, September 2005.

[73] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "Authenticated routing for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 3, pp. 598–610, 2005.

[74] J.-W. Wang, H.-C. Chen, and Y.-P. Lin, "A secure destination-sequenced distance-vector routing protocol for ad hoc networks," *Journal of Networks*, vol. 5, no. 8, Article ID 942, 2010.

[75] R. Mishra, A. Singh, and R. Kumar, "VANET security: issues, challenges and solutions," in *Proceedings of the 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pp. 1050–1055, IEEE, Chennai, India, March 2016.

[76] C. Kumar Karn and C. Prakash Gupta, "A survey on VANETs security attacks and sybil attack detection," *International Journal of Sensors Wireless Communications and Control*, vol. 6, no. 1, pp. 45–62, 2016.

[77] C. S. Vorugunti and M. Sarvabhatla, "A secure and efficient authentication protocol in VANETs with privacy preservation," in *Proceedings of the Ninth International Conference on Wireless Communication and Sensor Networks*, pp. 189–201, Lecture Notes in Electrical Engineering, Springer, New Delhi, April 2014.

[78] F. D. Da Cunha, A. Boukerche, L. Villas, A. C. Viana, and A. A. Loureiro, "Data communication in VANETs: a survey, challenges and applications," vol. 44, 2014 https://www.researchgate.net/journal/Ad-Hoc-Networks-1570-8705.

[79] U. A. Khan and S. S. Lee, "Multi-layer problems and solutions in VANETs: a review," *Electronics*, vol. 8, no. 2, Article ID 204, 2019.

[80] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure v2v communications in an IOV paradigm," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2740–2749, 2017.

[81] Q. Zeng, Y. Tang, Z. Yu, and W. Xu, "A geographical routing protocol based on link connectivity analysis for urban VANETs," *Journal of Internet Technology*, vol. 21, no. 1, pp. 41–49, 2020.

[82] G. Sun, L. Song, H. Yu, V. Chang, X. Du, and M. Guizani, "V2v routing in a vanet based on the autoregressive integrated moving average model," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 1, pp. 908–922, 2018.

[83] K. A. Rahman and K. E. Tepe, "Towards a cross-layer based mac for smooth v2v and v2i communications for safety applications in dsrc/wave based systems,," in *Proceedings of the 2014 IEEE Intelligent Vehicles Symposium Proceedings*, pp. 969–973, IEEE, Dearborn, MI, USA, June 2014.

[84] S. Kumar and K. S. Mann, "Prevention of dos attacks by detection of multiple malicious nodes in VANETs," in *Proceedings of the 2019 International Conference on Automation, Computational and Technology Management (ICACTM)*, pp. 89–94, IEEE, London, UK,USA, April 2019.

[85] A. M. Malla and R. K. Sahu, "Security attacks with an effective solution for dos attacks in VANET," *International Journal of Computer Applications*, vol. 66, no. 22, pp. 975–8887, 2013.

[86] P. S. Waraich and N. Batra, "Prevention of denial of service attack over vehicle ad hoc networks using quick response table," in *Proceedings of the 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*, pp. 586–591, IEEE, Solan, India, September 2017.

[87] K. Jeffane and K. Ibrahimi, "Detection and identification of attacks in vehicular Ad Hoc network," in *Proceedings of the 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, pp. 58–62, IEEE, Fez, Morocco, October 2016.

[88] S. RoselinMary, M. Maheshwari, and M. Thamaraiselvan, "Early detection of dos attacks in VANET using attacked packet detection algorithm (apda)," in *Proceedings of the 2013 International Conference on Information Communication and Embedded Systems (ICICES)*, pp. 237–240, IEEE, Chennai, India, February 2013.

[89] A. Singh and P. Sharma, "A novel mechanism for detecting dos attack in VANET using enhanced attacked packet detection algorithm (eapda)," in *Proceedings of the 2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS)*, pp. 1–5, IEEE, Chandigarh, India, December 2015.

[90] G. A. Issac and A. J. Mary, "Validation scheme for VANET," in *Proceedings of the 2019 2nd International Conference on Signal Processing and Communication (ICSPC)*, pp. 11–15, IEEE, Coimbatore, India, March 2019.

[91] M. Sohail, R. Ali, M. Kashif et al., "Trustwalker: an efficient trust assessment in vehicular internet of things (viot) with security consideration," *Sensors*, vol. 20, no. 14, Article ID 3945, 2020.

[92] A. Wasef and X. Shen, "EMAP: expedite message authentication protocol for vehicular ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 1, pp. 78–89, 2013.