Wireless Personal Communications
https://doi.org/10.1007/s11277-023-10643-6

Classification of Distributed Denial of Service Attacks in VANET: A Survey

K. Vamshi Krishna[1] · **K. Ganesh Reddy**[1]

Accepted: 13 July 2023

Abstract
Vehicular ad hoc network (VANET) is a self-organizing network established to provide wireless communication between vehicles where information plays an important role in aspects such as collision detection, re-routing, traffic monitoring, information related to gas stations, hospitals, hotels, entertainment, and more. The main challenges that VANET faces are security and privacy of information, which lead to a variety of attacks. Numerous types of attacks can be carried out on VANET, with distributed denial of service (DDOS) being one of the most common and dangerous. DDOS attacks on VANET result in the lack of availability of information for vehicles to communicate. Many methods were developed to counteract DDOS, however the efficacy of most of these existing systems was limited to some degree, and attackers exploited these weaknesses to conduct network attacks. Here we provide a full explanation of numerous DDOS attacks as well as a layer-by-layer classification of DDOS attacks that are specialized to specific layers or multi-layers. The goal of this survey is to provide useful information to fellow researchers on VANET attacks, in particular DDOS attacks, their layer-wise classification, the impact DDOS has on the network, and existing DDOS countermeasures, their limitations, and how they can be improved. We have referred to various journal papers to gather the information that can be helpful to researchers working in the field of VANET attacks.

Keywords DOS · DDOS · VANET · Layer-wise

1 Introduction

With the Internet's rapid growth and development, we now live in a world where the Internet underpins the entire human day-to-day cycle. The Internet has many advantages, but it also has many disadvantages. Security issues jeopardize data confidentiality and integrity with attacks such as DDOS attacks, Rushing attacks, wormholes, and other types of attacks. A DDOS (Distributed Denial of Service) attack is the most

✉ K. Vamshi Krishna
vamshikrishna.20phd7088@vitap.ac.in

K. Ganesh Reddy
ganesh.reddy@vitap.ac.in

[1] VIT-AP University, Amaravati, AP, India

Published online: 29 July 2023

lethal and effective attack. People generally believe that a DDOS attack is simple and does not cause much damage, but this is not the case. DDOS attacks are powerful yet simple techniques that can bring down almost anything they target. Many cutting-edge algorithms were presented to detect network vulnerabilities and improve VANET security. These models were successful to some extent, but an intruder discovered and exploited vulnerabilities in them. We analyzed these cutting-edge techniques proposed by various authors in this survey to help improve network security against DDOS assaults. The efforts in this survey will aid researchers in understanding existing solutions, limitations, and future improvements to overcome loopholes and develop new innovative models that can further improve network security against various DDOS attacks.

WANET (wireless ad hoc network) derives its name from the Latin phrase "ad hoc", which means "for this purpose." In contrast to physical connectivity, WANET does not use physical cables to connect two or more devices; in this regard [1], WANET is similar to a LAN (Local Area Network). That has significantly improved networking and communication where interaction between vehicles to vehicles (V2V), vehicles to infrastructure (V2I), and hybrid, has made waves in the automobile manufacturing industry.

The WANET hierarchical classification system is depicted below [1].

- Wireless Mesh Network (WMN)
- Mobile ad hoc Network (MANET)
- Vehicle ad hoc Network (VANET)
- Intelligent Vehicle ad hoc Network (InVANET)
- Wireless Sensor Network (WSN)

We will limit the upcoming sessions to only discussing VANET and InVANET because we are already familiar with the topics of WMN, MANET, and WSN.

2 VANET and InVANET

Since the adoption of VANET (vehicular ad-hoc network) technology by the automotive industry, methods, and applications have been drastically altered. Automotive manufacturers are developing new standards for improving driver safety as they integrate embedded components into vehicles. To meet today's expectations, VANET must rely on communication. Vehicle and roadside units communicate using wireless infrastructure and embedded components, resulting in more effective information distribution. Vehicle-to-vehicle (V2V) communication, vehicle-to-infrastructure (V2I) communication, and hybrid vehicle-to-vehicle (V2V/V2I) communication are the three types of communication used in VANET.

Intelligent Vehicle ad hoc Network (InVANET) Intelligent systems referred to as InVANET can be found under the subheading of VANETs. Intelligent Vehicular Ad Hoc networks incorporate artificial intelligence and algorithms to provide vehicles with dynamic mobility with no breaks in the conversation. For communication purposes, Vehicles in both VANET and InVANET use wired and wireless technology, where wireless uses protocols to achieve communication between vehicles, and wired uses physical devices such as "Antennas" mounted on top/side/front/rear of the vehicle [1].

2.1 Antennas and Types

Because communication in VANET and InVANET is critical, they must be used in tandem. To transport and receive information about vehicles, vendors must use both protocols and physical equipment such as antennas. An antenna is classified into two types:

1. *Directional Antennas:* For the antenna's focus of available energy to be transmitted, a specific direction must be specified. A Directional Antenna is what we'd call it here. Usually, in a very narrow, tightly focused beam, directional antennas are available in a wide range of shapes, sizes, and designs, depending on their intended use. Yagi antennas, panel antennas, parabolic or "dish" antennas, sector antennas, and grid antennas are common directional antenna types [2].
2. *Omni Directional Antennas:* The term Omni-Directional Antenna is used to describe an antenna that emits and receives energy in all horizontal directions in an equal and balanced manner. These antennas are perfect for general coverage applications. Antennas with 360-degree beam width can pick up signals regardless of their location. Our Omni-Directional Antennas, for example, include the ECO, DOD, OD, PSKN, MOD, and base stations [2].

3 DDOS Attack

A distributed denial-of-service (DDOS) attack sends malicious traffic through a large number of attack machines and attempts to overload the victim's resources through brute force. A successful distributed denial-of-service attack requires no special knowledge or skill [3]. Although there are numerous scanning scripts and tools for exploiting vulnerable systems, during the engagement phase, only a small number of DDoS attack instruments are used. To counter a large-scale distributed denial of service (DDoS) attack, systems such as Floodnet, TFN, Trin00, Stacheldraht, and TFN2K are routinely deployed. While the tools used to build botnets differ greatly, one significant difference is how master–slave communication is handled, as well as how the generated attack traffic is customized [3].

3.1 DOS and DDOS Attacks, Organized by Layers

3.1.1 Application Layer Attacks

3.1.1.1 DOS Attack When dealing with application-layer denial-of-service (DoS) attacks, the difficulty level rises. Blocking some functions or functionalities is an alternative to completely shutting down a network [4]. Financial institution attacks are fairly common, with the majority of them carried out to divert the attention of IT and security personnel away from security flaws.

Because they are more targeted and use fewer resources than traditional distributed denial of service (DDoS) attacks, these types of attacks are commonly used to disrupt transactions and databases. As a result, because they closely resemble human behavior and interface usage, these types of attacks are extremely difficult to defend against. There are several reasons why DoS attacks on the application layer are more dangerous. Resource constraints caused by unavoidable high performance across a wide range of applications Follow all traffic laws.

3.1.1.2 DDOS Attack DDoS attacks on the application layer target specific flaws or issues that can render the app unusable and prevent content from being delivered to the user's device. While web servers are the most commonly attacked, SIP phone services and BGP are also vulnerable [5]. As a result, lower-volume DDoS attacks typically follow protocol handshakes and compliance with DDoS attack chain protocols/applications. To put it another way, DDoS attacks will be launched primarily through discrete intelligent clients, specifically IoT devices, and will remain unspoofable. Attacks, by definition, oscillate up and down like a roller coaster. Hackers are constantly developing new DDoS attack methods to stay one step ahead of their victims. Because defendants are constantly devising new ways to counterattack attackers, attacks can go on indefinitely [5]. Because application layer DDoS attacks are infrequent, a behavioral or deep packet analysis is required. Identifying the precise attack vector used by virtual or physical appliances must be implemented in IDMSs to combat this emerging threat.

3.1.1.3 Data Tampering As a result, protecting this data is a top priority for V2V or V2X communication. The deliberate manipulation of data is known as data tampering (delete, manipulate, or amend) by employing unapproved channels. In terms of data, there are two possible states: transit and storage. In both cases, data can be intercepted and tampered with.

3.1.1.4 Impersonation Attack To carry out such an attack, each vehicle serves as a node, and each of those nodes has its unique identification number (id). An impersonation attack, as the name implies, involves the attacker impersonating the original node. In this attack, the attacker disguises himself as a legitimate node and receives messages from other nodes, which he/she then modifies and sends to others to pass on incorrect or fraudulent information.

3.1.1.5 Repudiation Attack A repudiation assault occurs when a user's vehicle denies doing something or starting a transaction. The user simply denies knowledge of the transaction or conversation and then claims that such a transaction or communication never occurred.

3.1.1.6 Replay Attack Delaying tactics refer to attacks in which the attacker repeatedly sends out erroneous signals or causes delays. When an attacker retransmits previously transmitted data, this is referred to as a retransmission attack.

3.1.1.7 Illusion Attack In this attack, the attacker deliberately fools his own car's sensors into reporting false sensor readings. As a result, inaccurate traffic warning messages are transmitted to nearby residents [6]. To be successful, an illusion assault requires the perpetrator to generate fictitious traffic. Before an attacker can generate a virtual traffic event, they must first fulfill two requirements. Before an attacker can do anything, they must first recognize or create a dangerous traffic situation on the road. To begin with, the enemy is capable of disseminating bogus traffic warnings [6].

3.1.1.8 False Forging Attack An attacker can launch a position-forging attack using one or more identities (IDs). An assailant can create favorable circumstances in a variety of ways. Knowing one's own vehicle's position as well as the positions of nearby vehicles can be used to pick or guess positions. An attacker can spout the position of one vehicle, and then use the spouted locations at random times. Another method for determining vehicle placement is to use digital maps. A position forging attack is defined as one that employs both ID forging

and position forging. This creates the illusion that the network contains more vehicles than it does. This simulates traffic congestion and may cause all vehicles to slow down, resulting in actual traffic jams.

3.1.1.9 Sybil Attack The SYBIL attack, for example, employs a single attacker vehicle to impersonate several real people. The Sybil attack has the potential to cause a denial-of-service attack and compromise system security. The VANET's (Velocity Detecting Programs) warning system is an excellent example of this. A hostile vehicle in Sybil can inflict damage by convincing the victim that there are more hostile vehicles nearby. Sybil causes significant damage; it consumes bandwidth, degrades network topology, and so on. Sybil is a highly dangerous program. The attack has been dubbed the Sybil attack after the novel Sybil, which examines the life of a lady with multiple personalities. VANET attacks have been classified into several subcategories by researchers.

3.1.1.10 BGP Hijacking BGP, or Border Gateway Protocol, is the Internet's routing protocol. To put it another way, it describes how to efficiently route traffic from one IP address to another. The term "BGP hijacking" refers to the malicious rerouting of Internet traffic through the use of BGP by attackers. This is accomplished by attackers pretending to own, control, or route IP prefixes that they do not own, control, or occupy. A BGP hijack is analogous to someone removing all of the road signs along a freeway and rerouting all traffic to the incorrect off-ramp.

3.1.1.11 Slow Post Attack The POST attack is a major security concern for businesses today, especially given the current political climate. Most attacks begin with the attacker sending a genuine HTTP POST header to the target server, just as they would normally. The body of the message will be the exact size specified in the header. The communication's content, on the other hand, is transmitted at an uncomfortably slow rate—as little as one byte every two minutes or so. Because the entire message is technically correct and complete, it takes a long time for the targeted server to comply with all requirements. If an attacker launches hundreds or even thousands of these POST attacks at the same time, the server's resources will be quickly depleted, making valid connections difficult to maintain.

3.1.1.12 Large Payload Post A Large Payload Post-HTTP DDoS attack sends a large payload using XML encoding on web servers. This type of DDoS attack sends an XML-encoded data structure to a web server, which the server then attempts to decode but is forced to consume an excessive amount of RAM, overloading the system and crashing the service. Post-DDoS attacks with large payloads occur when web services use a DOM parser to construct an in-memory version of the SOAP message. The SOAP message size may double, and in some cases triple, as a result of this process. Users experience memory issues as a result of the increased document size. This attack can use oversized content in the SOAP message header, SOAP body, or SOAP envelope, but not in the SOAP header and SOAP body.

3.1.1.13 Mimicked User Browsing Mimicked User Browsing is a type of DDoS attack that employs botnets that pose as real people attempting to access a website. When a large enough number of these bots are deployed, the target website will either crash or become inaccessible to legitimate traffic. The motivation for distributed denial-of-service attacks is frequently financial or political gain. Mimicked User Surfing is nearly impossible to detect because it is designed to mimic the behavior of a real human browsing. As bots outnumber

human users, the website will quickly become overburdened to handle legitimate requests. They are difficult to identify because the attackers pose as legitimate users.

3.1.2 Transport Layer Attacks

3.1.2.1 DOS and DDOS Attack Because of its vulnerability, it is especially simple to launch a DoS or DDOS attack against the transport layer (Layer 4 in the OSI model). The two most widely used transport layer protocols are TCP and UDP. The major security risks associated with TCP and UDP at the Transport Layer are as follows:

3.1.2.2 TCP SYN Attack Another term for what is happening is SYN port flooding. To gain access. Most hosts' implementation of the TCP three-way handshake is flawed, making this vulnerability exploitable. Host B must maintain a "listen queue" for at least 75 s after receiving an SYN request from A. Several methods exist for storing a limited number of connections in memory, but they are not all equally efficient. By sending numerous SYN requests to a host and never responding to the SYN&ACK returned by the other server, a malicious host can take advantage of the listen-to queue's limited size. It will quickly fill up, and the other server will stop accepting new connections until a partially open connection in the listen queue completes or time out. Because it disconnects a host from the network for up to 75 s, it can be used as a denial-of-service attack or a tool for other attacks like IP spoofing.

3.1.2.3 Land Attack An attacker sends TCP SYN packets with identical source and target IP addresses and TCP port numbers. This results in the creation of a bogus stream. The affected system will either crash or reboot as a result of this confusion. Filters on edge router ingress ports can inspect all incoming packets for source IP addresses and prevent LAND attacks that originate behind aggregation points. Packets are only routed if the destination address falls within the prefix range advertised.

3.1.2.4 MITM Attack The term "man in the middle attack" refers to a listening attack in which the attacker listens in on the victim's conversations, and intercepts an ongoing conversation or data transfer. After positioning themselves in the "middle," or between the sender and receiver, the intruders pose as both valid participants in the transfer. While also providing malicious links or other content to the other legitimate participants in a way that may go unnoticed until it is too late, an attacker gains the ability to intercept data and information from both parties. This attack can be compared to a game of telephone where the words of one person are passed along from one player to another until they have changed by the time they reach the final recipient. An attacker can perform a man-in-the-middle (MITM) attack to steal confidential information or do other harm by interfering with a conversation without the knowledge of either the attacker or the intended target.

3.1.2.5 Teardrop Attack In a teardrop attack, fragmented packets are sent to a target machine as part of a denial-of-service (DoS) attack. Since TCP/IP fragmentation reassembly bugs prevent machines receiving these packets from reassembling them, the packets overlap and crash the target network device.

3.1.2.6 Session Hijacking Hijacking a session means that an attacker can take over a portion of a chat (typically over the network) and pose as one of the other participants. Session hijacking is, in most cases, an extension of sniffing; with the difference being that sniffing is passive

and hijacking is active. The fact that information is transmitted in the open makes network and unprotected protocol hijacking possible. Sniffing makes use of the same flaw. In addition to monitoring the traffic, a hacker could send a packet or frame pretending to be one of the other hosts. This is similar to spoofing, but there is no guesswork involved—the attacker has complete access to all critical information.

3.1.2.7 Sink Hole Attack A link can be made between the Sink hole and Wormhole assaults. This attack creates a sinkhole in the network that serves as a data collection hub for all redirected traffic [7]. The attacker vehicle persuades all neighboring vehicles to send traffic to it, creating a sinkhole. With all packets from nearby vehicles in hand, an attacker can alter them or drop some/all of them and relay them back. The network's lifespan is reduced as a result of the sinkhole attack.

3.1.2.8 Secure Socket Layer (SSL) Almost all online transactions are now encrypted with SSL. As a result, the assailants' focus has shifted. Messages are exchanged as part of an SSL handshake to verify the authenticity of both communicating parties. As a result of their efforts, a cryptographic key and secure communication options have been established. A variety of attacks use the SSL handshake to deplete a server's resources and cause it to crash [4] The Push do botnet can compromise a target's security and send arbitrary data to an SSL server in an attempt to gain access to sensitive data.

SSL denial-of-service attacks are classified into one of two types:

1. Protocol misuse attacks are attacks that take advantage of the protocol's vulnerabilities. In this manner, a denial-of-service attack can be carried out without a fully established secure connection. These devices do not require any sort of secret key to function.
2. Floods of SSL Traffic: This type of attack uses bandwidth and/or other system resources to send a large amount of data through the newly established secure channel. Without additional information, these incredible technologies can't distinguish between legitimate and malicious connections. They can't even issue a web challenge to determine the source's credibility [4]. As a result, your options are limited to doing nothing or employing rate-limited protection, which is susceptible to misleading actions.

3.1.2.9 Telnet Attack Telnet is a program that allows terminals to communicate with one another over a network. To send and receive data over IP networks, port 23 is used. These three types of Telnet attacks can be divided into three categories:

- The Telnet protocol lacks encryption, making it vulnerable to sniffers. Every message sent across the network is delivered in plain text between the parties involved. Frame sniffing is possible due to a flaw in the protocol that attackers are exploiting. An attacker can easily sniff plaintext data passing over the network
- Telnet protocol brute force attack Password brute-force attacks begin with a dictionary of often-used words and a program designed to establish Telnet sessions with each word on the dictionary provided by the attacker.

3.1.3 Network Layer Attacks

3.1.3.1 Location Attack Attack a malicious node learns about the node and the route it is taking by processing and monitoring traffic. Malicious nodes may thus launch additional attacks on the system.

3.1.3.2 Packet Dropping Attack Despite the absence of infected vehicles, wireless ad hoc networks may experience packet loss due to congestion. Packet loss is frequently associated with the following conditions: I. Network Congestion II. Channel conditions III. Resource constraints [8].

The Disposal of a Careless Packet a packet-dropping attack typically begins with a hostile node interfering with route construction. This can be done more efficiently by exploiting flaws in well-known ad hoc routing protocols used in wireless networks because they are predicated on the assumption that network nodes are trustworthy. A rogue vehicle has complete freedom to do whatever it wants because it is inside the route [8]. A malicious intermediate vehicle dropping a packet may cause communication between the source and destination to be suspended or incorrect information to be generated, both of which are undesirable outcomes.

3.1.3.3 Flooding Attack The attacker sends several packets to the vehicle until it becomes overloaded and can no longer receive packets from other nodes, resulting in a denial-of-service attack, preventing the attacked vehicle from processing valid traffic. It is dangerous to have these types of attackers on your network because they consume all available bandwidth and deny it to legitimate users; the flooding attack occurs in all secure on-demand routing protocols, including SRP and SAODV. A flooding attack can be classified into two types based on the packets used: Data flow attack with RREQ and RRQ.

3.1.3.4 Replay Attack Using this attack type, attackers continuously deliver error messages or cause a delay. A replay attack involves retransmitting a previous transmission to the target computer.

3.1.3.5 DOS Attack The Dos assault is the most well-known of the attacks identified thus far. DOS attacks use packet flooding and jamming to disrupt the network for anyone who is connected to it [9]. To launch a denial-of-service attack, the attacker uses the following techniques: jamming the communication channel, overloading the network, and discarding packets. Attackers will primarily target network bandwidth, the operating system, data structures, or the node/processing network's power.

3.1.3.6 DDOS Attack DDOS can cause far more damage when used in conjunction with DoS attacks. In a DDOS attack, the attacker selects targets in the network and launches an attack against them, converting those nodes into attackers. Zombies are valid nodes that have turned into attacker nodes [10]. A denial of service attack is what this type of zombie attack is called (DDOS attack) according to a Kaspersky study, 79 countries were targeted by DDoS attacks in the first quarter of 2018. 95.14 percent of the attacks were carried out in the top ten countries. A DDoS attack lasted nearly 12 days or 297 h. DDOS attacks are difficult to detect because they are only active for a short period and cause significant damage. To launch a DDOS attack, either V2V or V2I can be used.

3.1.3.7 Message Tampering Data that has been passed between the source and the destination during the transmission process is included in a message tampering attack. In the event of a message tampering attack, message transmission activity will be jeopardized because the message was changed by an unauthorized third party, making it difficult to determine whether or not the message was altered.

3.1.3.8 Sybil Attack With the SYBIL attack, it is possible to be attacked using multiple false identities at the same time, which is very damaging. The Sybil attack has the potential to start a DOS attack and compromise the system's security. Consider the VANET warning system (Speed detection app). A hostile node in Sybil dupes an attacked node into thinking there are several nodes nearby. Sybil causes severe damage; it consumes bandwidth, degrades network topology, and so on. The Sybil attack is named after the book Sybil, which is a case study of a woman with multiple personality disorder. According to experts, the VANET has been the target of numerous attacks.

3.1.3.9 Wormhole Attack The colluding nodes create the illusion [11] that two geographically dispersed (remote) nodes are directly connected and appear to be neighbors. However, they are not the same thing. The wormhole attack's goals are man-in-the-middle attacks and packet drops. When a rogue node connects to a network, it can intercept data packets and send them through a tunnel to another malicious node [11]. The tunnel can be built using either a wired or a long-range high-bandwidth wireless link operating in a different frequency band.

3.1.3.10 Black Hole Attack The black hole attack is an important type of VANET attack. In a Black Hole attack, the attacker employs the routing protocol to appear to have the shortest path to the target node. A Black Hole attack redirects all traffic intended for a specific node [12]. VANET makes extensive use of AODV, also known as the demand-driven protocol because it only identifies a route when one is required. The software uses four different message types to communicate with AODV. Routing requests are represented by RREQ, routing responses by RREP, and routing errors by RERR.

3.1.3.11 Routing Attack The attacker is using network layer routing methods to cause havoc. The attacker either releases the packet or disrupts the network's routing mechanism in this attack method. There are three types of routing assaults to consider: black hole, grey hole, and wormhole.

3.1.3.12 IPV4 and IPV6nAttacks Some types of attacks haven't changed much since the introduction of the IPv6 protocol. Security enhancements in the new IPv6 protocol have not made IPv6 networks any more secure. If IPv6 is not patched, a variety of attacks could bring the network down. As a result, some attacks that were previously known to work on IPv4 networks would no longer work on IPv6 networks. As a result, both IPv4 and IPv6 networks are at risk [13].

1. *The Sniffing Attacks*: Sniffing attacks are common in both IPv4 and IPv6 networks. Sniffing is a network attack that captures data as it passes through the system. An attacker can use a sniffing attack to gain access to confidential data transmitted via an unencrypted protocol. The IPsec security architecture, which is optional in IPv4 but required in IPv6, can protect against sniffing attacks.

2. *Flooding Attacks*: Flooding is the most common type of attack against IPv4 networks. As a result, network devices such as routers and hosts are bombarded with network traffic. When a device is targeted, it is unable to handle the volume of network traffic and becomes inoperable. DoS attacks, in which the targeted network device is bombarded with network traffic from multiple hosts at the same time, can be local or spread. Because the fundamental concepts of a flooding attack are the same regardless of whether it targets IPv4 or IPv6, it can also cause damage to IPv6 networks. There could be new ways to exploit IPv6's extension headers, new ICMPv6 message formats, and IPv6's reliance on multicast addresses (for example, all routers must have site-specific multicast addresses).
3. *Reconnaissance Attacks*: When launching a larger attack, reconnaissance attacks are frequently used as the first salvo. Reconnaissance attacks are carried out by an intruder to gather information about the victim network that will be useful in future attacks. An intruder can conduct a reconnaissance attack by using active or passive tactics such as scanning techniques. The intruder first determines the IP addresses of the victim network using ping probes. An intruder will use the port scan process once he or she has discovered an accessible system. As a result, IPv6 subnets are significantly larger than IPv4 subnets (the default subnet size in IPv6 networks is 64 bits). An attacker would need 264 probes to scan the entire subnet, making it impossible. Reconnaissance attacks against IPv6 networks are significantly more difficult to launch as a result.
4. *Security Threats*: All IPv6 nodes must be able to process routing headers by the IPv6 protocol specification. Unfortunately, access restrictions based on destination addresses can be bypassed using routing headers [13]. Such behavior may result in several security issues. The hacker could send a packet to a publicly accessible address, but the routing header would contain a "forbidden" address (address on the victim network). Despite being filtered on destination addresses, the publicly available host will still send it to the routing header's "forbidden" address. An intruder on your computer can easily launch a denial-of-service attack by impersonating packet source addresses and exploiting any publicly available host to redirect attack packets.
5. *Fragmentation-Related Security Threats*: IPv6 packets cannot be fragmented by intermediary nodes, as specified in the protocol standard. When using the IPv6 path MTU discovery method, packets can only be fragmented at the source node (based on ICMPv6 messages). IPv6 networks should have an MTU of at least 1280 octets. Because the packet in question is the last of its kind to arrive, any fragments with less than 1280 octets should be discarded for security reasons. An attacker can use fragmentation to ensure that port numbers are not found in the first fragment, thereby avoiding security monitoring systems (which do not reassemble fragments) that expect to find transport layer protocol data in the first fragment. Overloading the target system's reconstruction buffers with numerous tiny pieces can lead to system failure a type of (denial of service attack). This can be avoided by limiting the total number of fragments as well as the rate at which they arrive.

3.1.3.13 ICMP Flooding Attack Ping flood attacks make use of the Internet Control Message Protocol (ICMP), which is a type of denial-of-service attack (ICMP). A large number of ICMP echo queries are sent to the target device in an attempt to disable or completely disable the device (pings). They are frequently used in pinging network devices to check their health and connectivity, as well as the link between sender and receiver. A flood of request packets forces the network to send an equal number of reply packets. As a result,

traffic cannot reach the destination. ICMP flood DDoS attacks necessitate the attacker to know the target's IP address. Attacks can be classified into three types based on the victim's IP address and how it is resolved: Attacks employing ICMP flood DDoS tactics flood the targeted device's network connections with unwanted traffic, preventing legitimate requests from passing through. In this situation, a Denial of Service attack is possible (DoS).

3.1.3.14 Ping of Death Attack A distributed denial-of-service attack has been launched. The attacker's goal is to freeze or crash the targeted machine by sending a large packet that exceeds the operating system's maximum size limit.

3.1.3.15 Rushing Attack It is a type of attack that targets the network/transport layer. The source vehicle sends the RREQ to the destination vehicle. If an attacker vehicle forwards RREQs, all RREQs forwarded by the attacker arrive at the destination before any other RREQs forwarded by other vehicles [14]. All legitimate RREQs are discarded at the destination because it has already received RREQ from the attacker's vehicle. As a result, security threats will increase.

3.1.4 Data Link Layer Attacks (LLC and MAC)

3.1.4.1 DOS Attack Denial-of-service attacks on the MAC layer include masquerading attacks, resource depletion attacks, and media access assaults. Masquerading attacks are so-called because the attacker pretends to be another network or access point to gain access to a specific client. The term "Resource Depletion Attack" refers to an attack in which an adversary sends out a large number of requests from random MAC addresses in an attempt to deplete the available resources on a system [15]. When we talk about Media Access attacks, we're referring to those that target the Distributed Coordinated Function of the 802.11 networks (DCF).

3.1.4.2 DDOS Attack The term "denial of service" refers to an attack in which the attacker uses a reasonable service request as a pretext to consume excessive service resources, reducing or eliminating the availability of the resources for legitimate users. Several attackers flood the targeted system's bandwidth or resources (To maximize the power of a denial of service attack, more than one server is sometimes targeted) [16].

In this article, we'll look at various methods for launching Denial-of-Service (DoS) attacks using the MAC protocol. To fully occupy the channel, the majority of these attack techniques require a change to the MAC protocol. This type of attack is vulnerable because some MAC protocol implementations are hard-coded in firmware. They include sending RTS/DATA packets with only one RTS/CTS and then dropping them, as well as sending RTS/CTS packets with two RTS/DATA packets and then dropping them. Because the MAC layer in some stack implementations is hard-coded into the firmware, these attacking methods may not be applicable.

3.1.4.3 Jamming Attack Wireless communications can be hampered by intentionally interfering with radio signals. When a transmitter detects that the wireless channel is congested or distorted signals are received by receivers, it will turn off [17]. Jamming is typically used to defend against physical layer attacks, but cross-layer attacks are also possible. Jammers were classified into four types.

A. Constant Jammer: In this design, the jammer continuously sends out RF signals, which the channel receives and decodes. It does not follow any MAC-layer standards. Because the transfer is continuous, it does not wait for the channel to become idle before beginning.
B. Deceptive Jammer: In this paradigm, the jammer continuously injects a series of packets into the channel, with no interruption in transmission. It also transmits and responds to fabricated messages from the past. The jammer will send out preambles, which it will check and then ignore to jam the network.
C. Random Jammer: The jammer in this model has a period of continuous jamming followed by a period of no jamming. While jamming for t1 units of time, it turns off all radio signals and goes to sleep. The jammer awakens from a t2-unit slumber and resumes normal jamming operations. Time t1 and time t2 are deterministic or stochastic, respectively.
D. Reactive Jammer: The jammer will remain silent when the channel is not in use. When it detects activity on a channel, it starts sending a signal to that channel right away. It should not use any power to determine whether or not a channel jammer is in use.

3.1.4.4 Sybil Attack In this type of attack, a vehicle impersonates many other vehicles. These identities can be used to carry out a wide range of attacks [12]. These forged identities also give the impression that there are more automobiles on the road. Because this attack can spoof the positions or identities of other network nodes, it opens the door to any type of attack.

3.1.4.5 Collision Attack A compromised sensor node can easily launch a malicious collision attack [18]. During a collision attack, one of the malicious nodes disregards the MAC protocol requirements and sends a brief noise packet to cause collisions with other nodes' transmissions. This attack consumes very little of the attacker's energy, but it has the potential to cause significant network disruptions. Because wireless networks are broadcast, detection is difficult.

3.1.4.6 Sleep Deprivation Attack Stajano was the first to propose the sleep deprivation attack. One of the goals is to have a battery-powered computer that can stay in low-power sleep mode without interfering with the operations of any of the nodes. The attacker launches a sleep deprivation attack by legitimately interacting with the victim; however, the interaction's goal is to prevent the victim node from entering its power-saving sleep mode. As a result of this attack, the victim's life expectancy will be drastically reduced. Furthermore, because it primarily employs exchanges that appear innocent, this assault is difficult to detect.

3.1.4.7 Channel Access Deny Vehicles seeking slot time must wait for confirmation from all of their neighbors before indicating that their request has been granted. If a single car occupies a slot, all of its neighbors must state this in their FIS. The attacker could intervene to stop the procedure [19] in progress by providing a signal in its FI that the space is not reserved for this vehicle. The assailant's goal is to disrupt and obstruct the slot reservation procedure. Because vehicles may be denied time slots even for sending security notifications, this security flaw may result in denial of service (DoS) attacks.

3.1.4.8 Slot Reservation Attack Due to the DTMAC scheduling system, only one slot per frame can be reserved by the same vehicle at any given time. A selfish vehicle, on the other hand, may request multiple slots in the same frame [19].

3.1.4.9 Frame Information Poisoning While Frame Information is sent in clearly, there is no way to verify its integrity. This means that it is very easy to forget. Malicious vehicles, for example, may falsely indicate that a free slot is occupied to prevent cars from obtaining it [19].

3.1.5 Physical Layer Attacks

3.1.5.1 DOS Attack The physical layer is only concerned with things as simple as a cable transmitting bits from one location to another. Hubs, patch panels, and R45 jacks are all part of the componentry for both the 100 Base-T and 100 Base-X base layers. Physical layer attacks include things like breaking, obstructing, or manipulating physical media to cause a malfunction [20]. These attacks prevent legitimate network users from accessing network data. Repairing physical media resources is necessary for availability.

3.1.5.2 DDOS Attack DDoS attacks on network infrastructure are becoming more common as wireless network usage and relevance grow [21]. There is always the risk of interference with wireless transmissions. Because they share the same 2.4 GHz frequency spectrum, 802.11n networks can be disrupted by Microsoft's Xbox.

3.1.5.3 GPS Spoofing The detection of spoofing attacks is a major focus of research into the physical layer of security against spoofing attacks. A few studies also look at ways to prevent the problem from occurring in the first place. Installing a countermeasure against spoofing attacks is also critical [22]. To avoid detection, the spoofer can exploit detection algorithms' flaws to deceive the victim in future communications.

3.1.5.4 Jamming Attack JAMMING is the term used to describe when interference from the sender or receiver objects jeopardizes the integrity of the network flow. By putting a jammer between the sender and the receiver, the sender can disrupt the communication medium and commit hostile acts such as integrity and accessibility violations. One of the most significant attack tactics is jamming, which can severely impede IoT network connectivity and data movement between IoT devices connected by wireless links.

3.1.5.5 Tampering Tampering is a type of IoT attack in which the attacker physically or electronically modifies the hardware or software components of the target device. Recent and widespread physical layer attacks give hackers access to the privacy, availability, and integrity of all IoT items by granting them complete control of the device [23]. By tampering with Internet of Things (IoT) systems, the security of those systems may be jeopardized.

3.1.5.6 Eavesdropping Attack Eavesdropping is a typical method of gathering and analyzing communication traffic [23]. Active and passive eavesdroppers are the two basic categories. Eavesdropper covertly watches communication to passively listen. Active

eavesdropper, on the other hand, actively seeks to intercept the data transfer by returning fake data to the sender [24].

3.2 (MAC sublayer)

3.2.1 Masquerading attack

In a masquerading attack, the MAC address of a specific station or access point is spouted. Because of the open nature of the wireless medium, an attacker can simply sniff wireless communications to determine the identity of devices on the network [25]. Wireless traffic sniffing, device driver software, and spoofing can then be used to spoof those identities.

3.2.2 Resource Depletion

Common targets for resource depletion attacks are shared resources such as the AP, which are attached to deplete the AP's processing and memory power, rendering it useless to legal stations [25]. Attacks like this can be supplemented by more sophisticated attacks like the introduction of rogue access points to take over abandoned stations that are being used.

3.2.3 PCF Attack

When in PCF (Point Coordination Function) mode, the access point serves as a network referee. It provides the devices with priority mechanisms [26]. An attacker could use false clock settings to spoof beacon frames. As a result, the stations' contention periods would be distorted, resulting in a Denial of Service (DoS).

3.3 11p (PHY)

3.3.1 Single Adversary Attack (SAA)

A single adversary enters the network and sends massive data flows to every legitimate node. As a result, energy would be depleted from both nodes and channels [27]. SAA has the potential to have a significant global impact on the network.

3.3.2 Colluding Adversary attack (CAA)

Colluding adversaries can disrupt the intended traffic flow by sending massive data flows directly to each other [27].

3.3.3 Vampire Attack

Rather than exploiting design or implementation flaws in specific routing protocols, vampire attacks make use of more general aspects of protocol classes such as link-state and distance-vector [28]. They can also use geographic and beacon-based methods to

direct traffic to their intended destinations. Furthermore, these attacks do not rely on flooding the network with a large amount of data, but instead strive to transmit the least amount of data possible to achieve the greatest energy drain, avoiding a rate-limiting method. Vampires send communications that adhere to protocol, making these attacks extremely difficult to detect and stop.

3.4 2(Logical link sub-layer)

3.4.1 Spanning Tree Protocol (STP)

In an STP attack, the attacker spoofs the topology's root bridge. A recalculation of the STP balance is attempted by broadcasting an STP configuration/topology change BPDU. The attacker system has lower priority to bridge, as announced by BPDU sent out. An array of frames transmitted from other switches will be visible to the attacker. A delay of 30 to 45 s due to STP resets can result in a denial of service attack (DoS) if the root bridge is changed frequently. To make its host the root bridge, the attacker uses STP network topology alterations (Figs. 1, 2, 3, 4, 5).

3.4.2 CDP Attack (Cisco Discovery Protocol)

Aside from information gathering, there was a vulnerability in CDP that allowed a hacker to overload and crash Cisco devices with fake CDP packets. Because CDP is not authenticated on a networked Cisco system, an attacker can send either false or legitimate CDP packets and have them immediately received by the attacker's system [29].

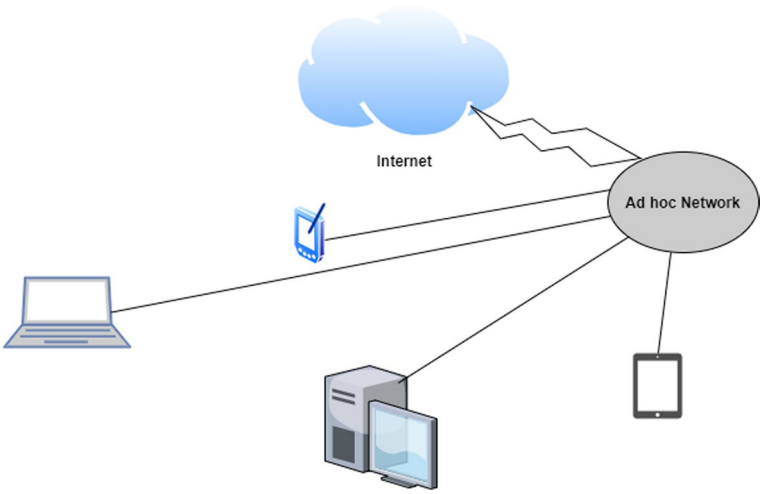

Fig. 1 WANET

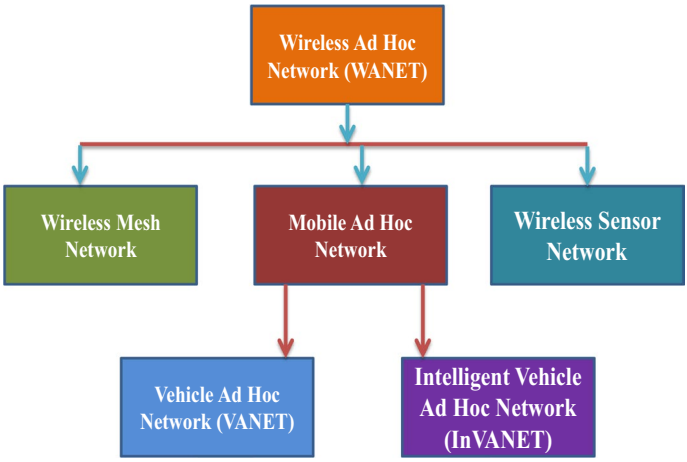

Fig. 2 Classification of WANET

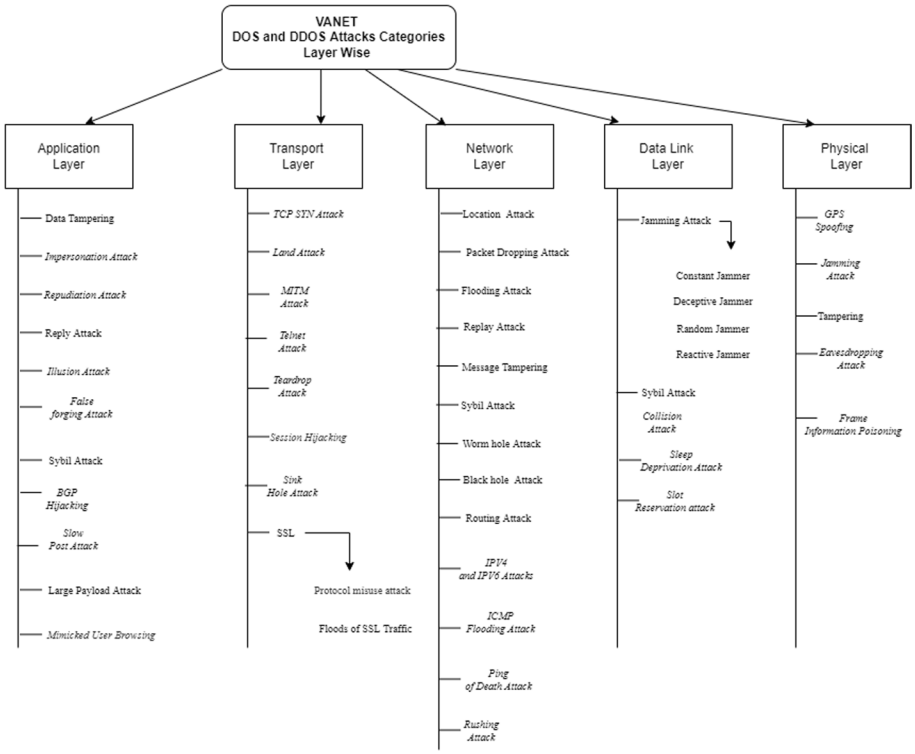

Fig. 3 Layer-wise classification of DDOS attacks

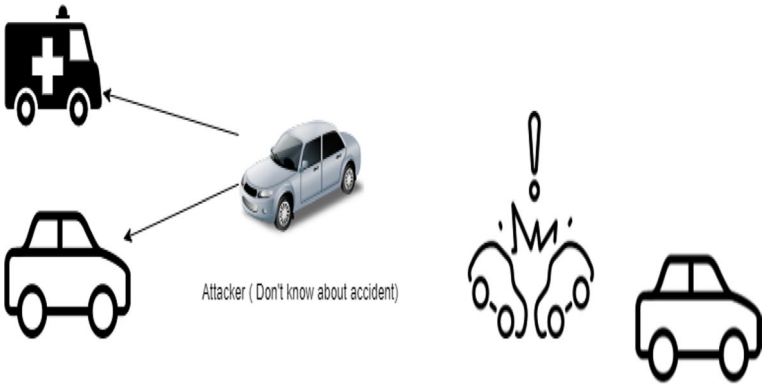

Fig. 4 Impersonation attack

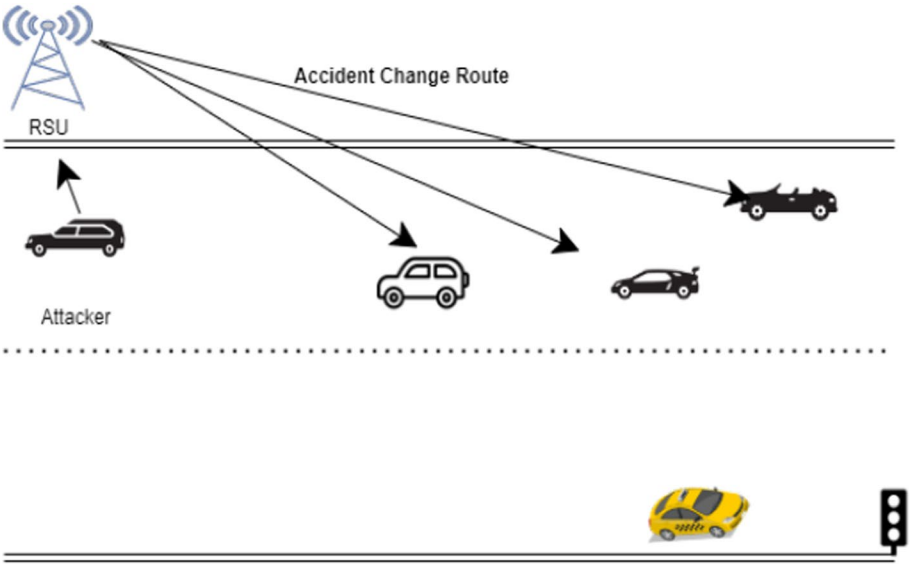

Fig. 5 Illusion attack

3.4.3 CAM Table Overflow

Since CAM overflow attacks make switches vulnerable, an attacker can use them as a hub to access every host on the network, listen in on communications, and launch MITM attacks. Attacking neighbor switches can be done using this technique [29].

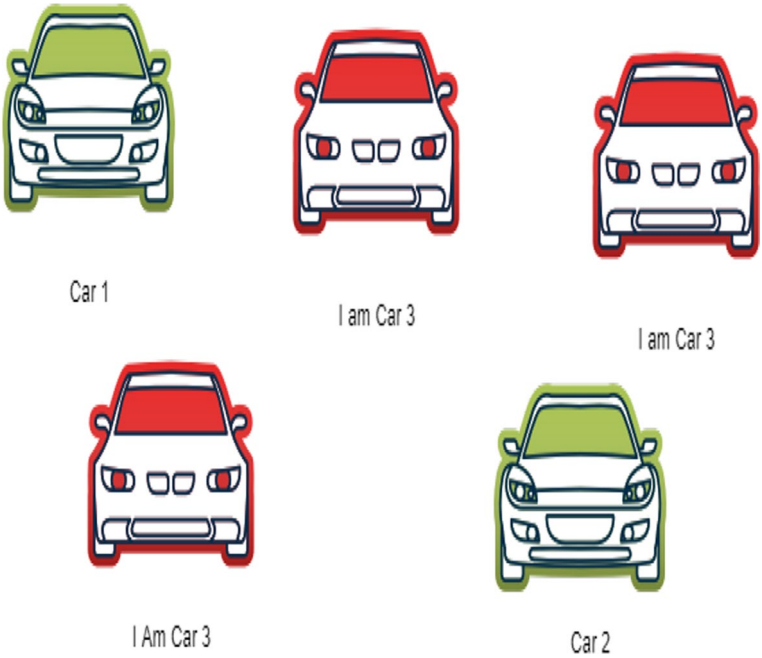

Fig. 6 Sybil attack

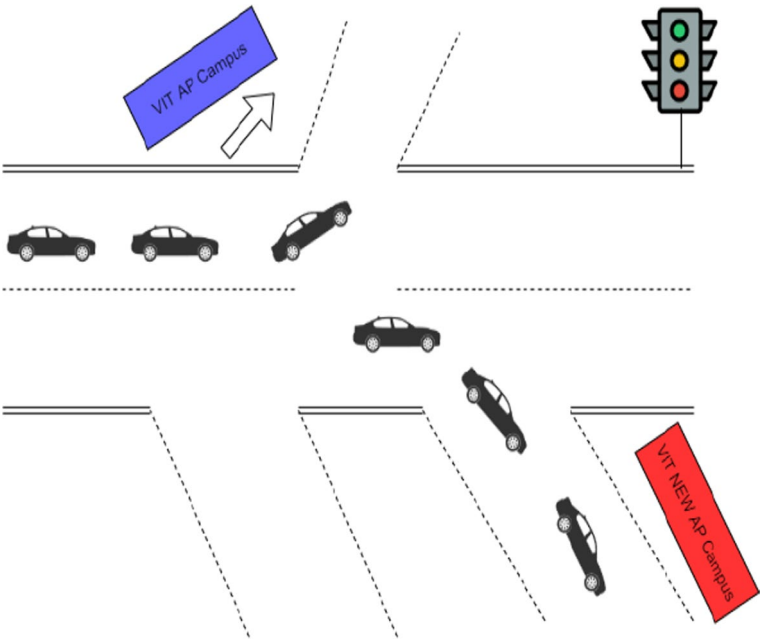

Fig. 7 BGP hijacking

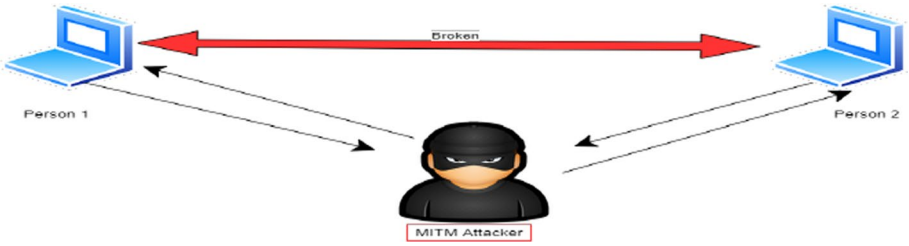

Fig. 8 MITM attack

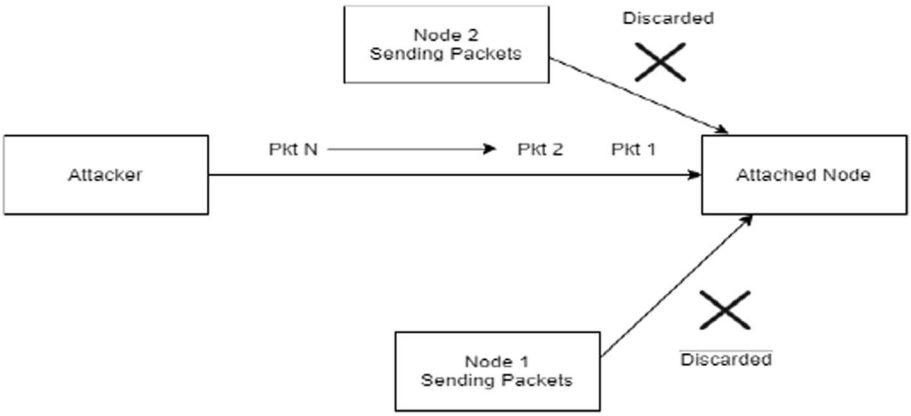

Fig. 9 Flooding attack

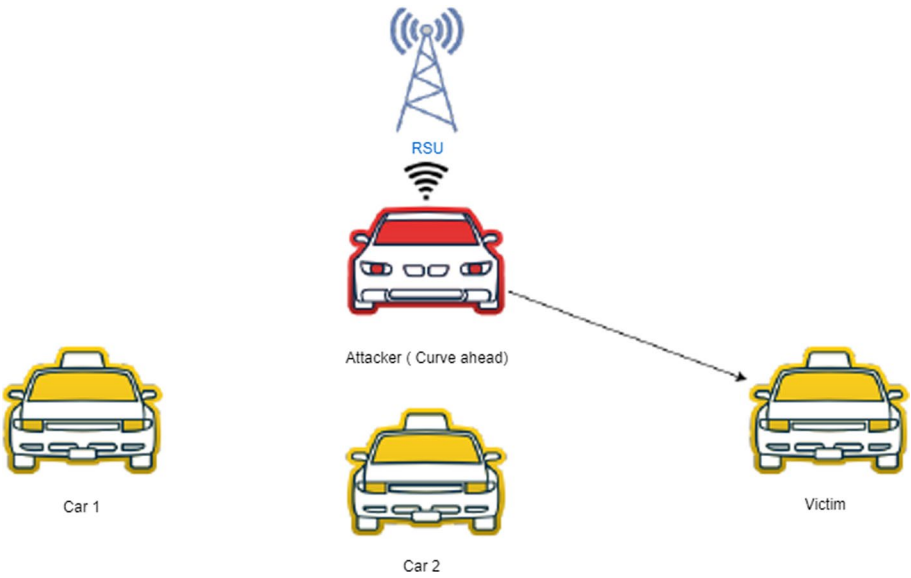

Fig. 10 DOS attack

3.4.4 DHCP Starvation

Using a bogus wireless card, the attacker sends a large number of requests to the DHCP server. If enough queries are dumped onto it, the attacker can exhaust all of the DHCP addresses on the network. The DHCP resource is then depleted for clients on the victim network [29]. When a Rogue DHCP Server is installed on the network, the attacker can respond to changing IP settings by using it as a DHCP Server. The unfortunate people are victims (Figs. 6, 7, 8, 9, 10).

4 Existing Counter Measures to DDOS Attack

Authors [30] proposed a countermeasure to flooding attack in VANET; authors used Q learning algorithms that fall under the reinforcement leering to build a proposed model that handles the flooding attack effectively. Authors [31] presented a novel method known as a Homogeneous Discrete-Time Markov Chain that counters the data tampering attack which leads to the modification of actual with failed data. Authors [32] proposed a Machine Learning (ML) technique to overcome the security issues known as "Routing and reply" attacks, the ML algorithm used is SVM (Support Vector Machine) along with a cross-layer selection method. Author [33] suggested a countermeasure to jamming attack which can block all the communication channels leading to unavailability of information. To solve these issues an ML algorithm "SVM classifier" was proposed that detected intruders by classifying normal and abnormal patterns. Author [34] provided a solution to Sybil's attack on VANET by using the Signal Strength Index, Fitness Function, and Throughput. The throughput was achieved by the use of signal strength and the fitness function was used to fix issues countered while using the proposed method. Author [35] presented a novel method called DPBHA to solve the black hole attack where authors used a dynamic threshold and generated forged RREQ for the development of the model. Authors [36] proposed a novel method of SBGM and Dynamic wrapping threshold for countering the attacks such as a gray hole and black hole issues. Authors [37] proposed a method that is used to countermeasure the VANET attack known as the "Sinkhole" with the use of the CL-MLSP method and AODV protocol. Authors [38] presented a method that overcame the limitations of the existing methods in the form of performance increase using new features along with the data-driven methodology to overcome spoofing attacks in VANET, they achieved 99.1% accuracy in the detection of attacks. Authors [39] suggested the NOMA simulator for 5G wireless communication, this proposed method is applied for dropping attacks that drop packets and disturb the flow of information. This method used ML and DL techniques such as RF, KNN, and Neural networks. Authors [40] presented CR—VANET using the DL method that predicted collision attack that is caused by modifying the communication data between vehicles leading to false data circulating. Authors [41] to counter the MITM attack presented a novel method using the Xerosploit toolkit for testing purposes and auditing fluxion tools that provided a primitive measure in protecting credentials. Authors [42] proposed IPS for protecting Road Side Unit (RSU) from intruders launching black hole and wormhole attacks. The IPS algorithm with swam approach provides the required security from attacks and safeguards RSU which is one of the sources of communication between vehicles. Authors [43] presented a countermeasure to sleep deprivation attack that leads to DDOS attacks disputing the flow of information, the solution is developed using ML's

BayesNet technique using different datasets to find the performance of every and finding the optimal. Authors [44] proposed an IDS for detecting GPS spoofing which monitors the behavior of the system to identify if any attacker is present or not. The proposed IDS is developed using DL techniques to improve the accuracy of the system. Authors [45] presented a novel method SAMA that protects the vehicles from location attacks, this method is implemented using triangulation concept with RSSI and programming language C++ and multimap. Authors [46] proposed a management system known as MOVE that secures the vehicles information from Frame Information Poisoning attack, MOVE uses simulator OMNET++ for simulation and monitoring. Authors [47] presented a framework to design IDS for detecting TCP SYN Attacks for which the authors used the ML approach using the VDOS-LRS dataset that leads to detecting DOS and DDOS attacks. Authors [48] proposed a DL technique for identifying the DDOS attack SIP networks using failover addressing and load balancing to migrate the attacks and achieved accuracy and increase in performance. Authors [49] presented an IDS IEC104 honeypot that can overcome the drawbacks of signature and anomaly IDS, the proposed IEC104 honeypot is mainly used to protect IIoT from telnet attacks and provides encryption, authentication, and integrity features. Authors [50] presented a detection model that counters false messages communicated by an intruder into the network that can lead to land and teardrop attacks, the concept of Fuzzy-based context-aware is used by the authors to design the detection model. Authors [51] proposed a Novel embedding algorithm using an adapted distance metric that was a success in overcoming the attacks encountered by SPT attacks. Authors [52] presented an optimal replacement for existing IDS, the proposed IDS SDN-guard uses sampling methods and a linear integer program to determine the CAM Table Overflow attacks that fall under the DDOS attack category. Authors [53] proposed a model that combines ARP and ICMP protocols to find the intruder and countermeasure the DHCP Starvation. Authors [54] proposed a neural network method to counter SAA attacks; authors used multimodal fusion models and features for the design state-of-art model that improves the detection and performance rate. Authors [55] present a prevention method known as LEACH protocol that is deployed during communication between V2V, V2I, and V2X to counter Vampire attack which drains the battery of vehicles during communication and can cause devastation to the path. Authors [56] proposed IDS that works online and offline to validate the RSU and vehicles, TDES, dynamic keys sharing, and CPA methods are used for the development of IBOOS to protect the vehicles from SAA attacks. Authors [57] proposed IDS using PML-CIDS with an alternating direction method that counters Eavesdropping Attacks and differentiates between intruder or non-intruder vehicles. Authors [58] proposed IDS that countermeasures the rushing attack using hybrid ML, advantages of RF, Corsets, and cluster algorithms (Figs. 11, 12, 13, 14, 15).

In the preceding section, a literature survey on existing models was conducted, in which various researchers presented their ideas on understanding the various forms of DOS and DDOS attacks and developed solutions to countermeasure the attacks using Computational Intelligence Techniques (CIT) such as Artificial Intelligence (AI), Deep Learning (DL), Machine Learning (ML), and new novel methods. We have correlated the details of the existing models such as techniques/algorithms used in developing the system, different types of attacks to which these existing systems can be applied to countermeasure and reduce the severity of these attacks, the limitations of the existing system along with suggestions to overcome them and finally further enhancements to improve the performance of a system in Table 1 below.

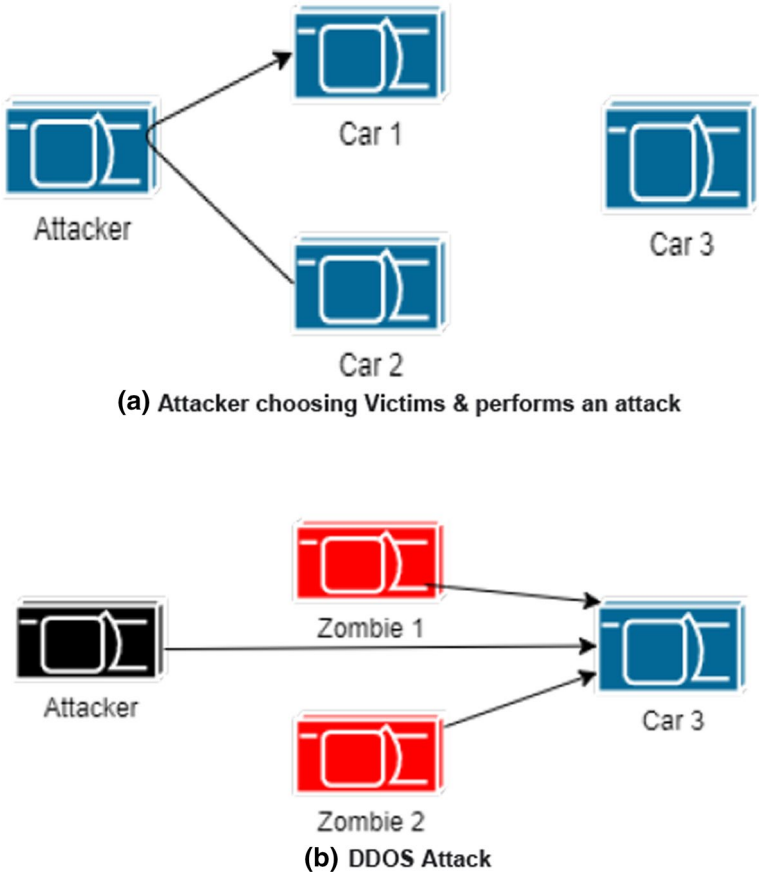

Fig. 11 **a** Attacker choosing Victims and performs an attack. **b** DDOS attack

4.1 Future Research Work

According to our survey, there has been a lot of research done in the field of VANT to solve difficulties such as vehicular network privacy and security. Given its wireless form of communication and vehicle mobility, VANET faces numerous security challenges. Researchers in the field of VANET have devised numerous solutions to all of the attacks that occur from time to time, but the intruder finds some vulnerability in the solution and exploits it. As per our survey, we discovered a few issues that might be considered to improve security and privacy, as well as established targets for future research work.

1. The majority of the solutions were aimed at overcoming security challenges associated with V2V, V2I, or V2X; however, not all of them were collated. As an outcome of future studies, a single framework that can address the difficulties raised by the mentioned modes of transportation can be developed.
2. A great deal of effort was put into securing the RSU, which is safer than vehicles. Additional research ideas for safeguarding vehicles that can be easier targets for intruders must be proposed.

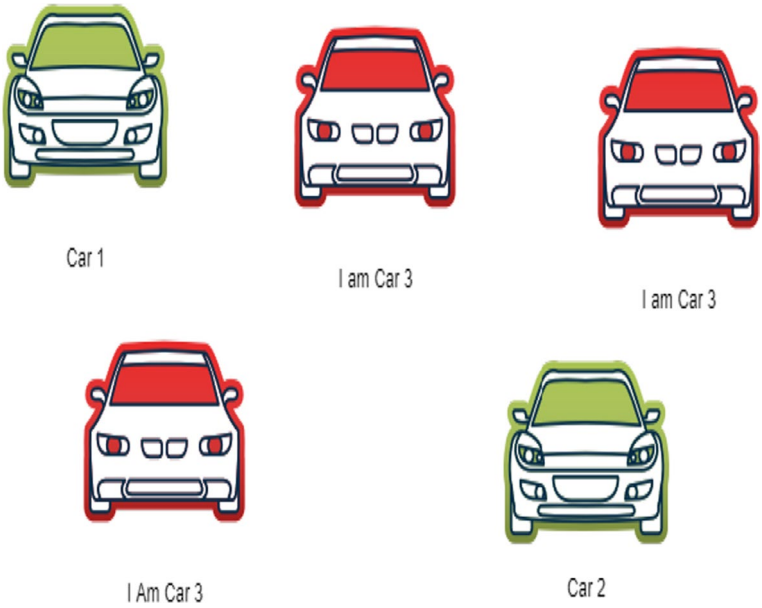

Fig. 12 Network layer sybil attack

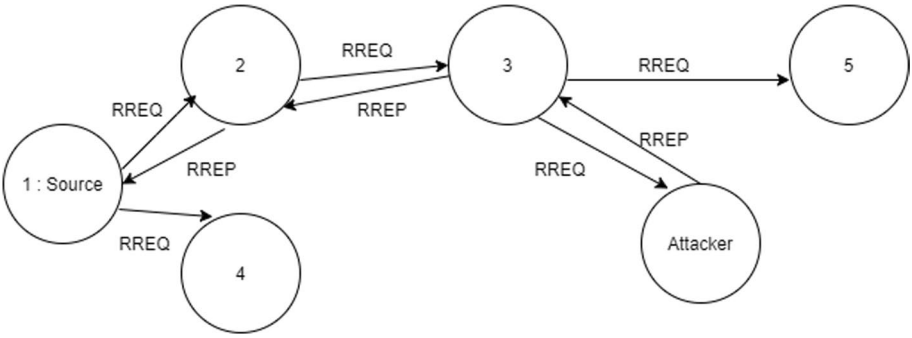

Fig. 13 Black hole attack

3. Exiting solutions were largely built using ML algorithms, with minimal room for Artificial Intelligence (AI), Deep Learning (DL), and Neural Networks (NN) solutions. In future research, new solutions must be developed to solve ML disadvantages such as performance drops with large datasets, continuous learning, decision-making, and learning from previous jobs.
4. Existing intrusion detection systems (IDS) were designed only for the detection or prevention of assaults; previous IDS were unable to conduct both techniques in a single framework using modern CIT algorithms. As part of future work for researchers, an IDS framework that performs dual roles utilizing CIT such as AI, NN, and DL can be proposed.

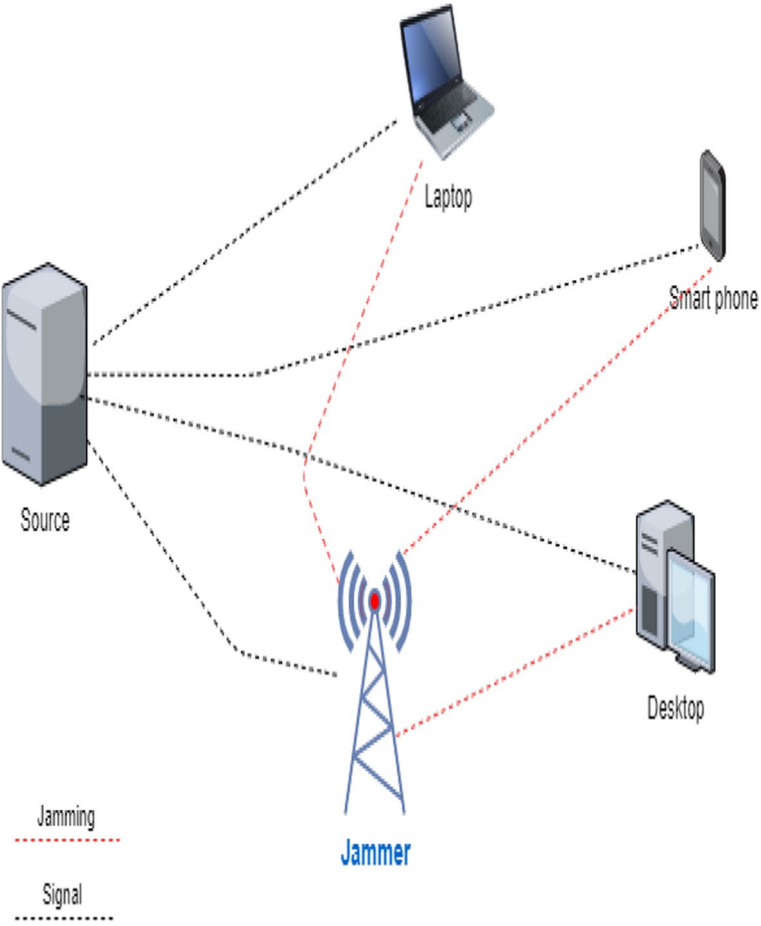

Fig. 14 Jamming attack

5 What Makes this Survey Differ from Other Existing Surveys?

The majority of existing surveys provided helpful information about various vehicular network attacks, existing countermeasures, and others. These surveys dealt with a particular type of attack and the subcategories of that attack. In this survey, we provide in detail one of the most severe attacks that can completely bring down the network; DOS and DDOS attacks impact the availability of network resources, leading to various problems. These attacks are launched in various forms and can affect any layer, causing a malfunction in the flow of information. The highlights of our survey and how it differs from existing surveys are mentioned below:

1. Regressive work has been done in detecting several attacks that lead to DOS and DDOS attacks.

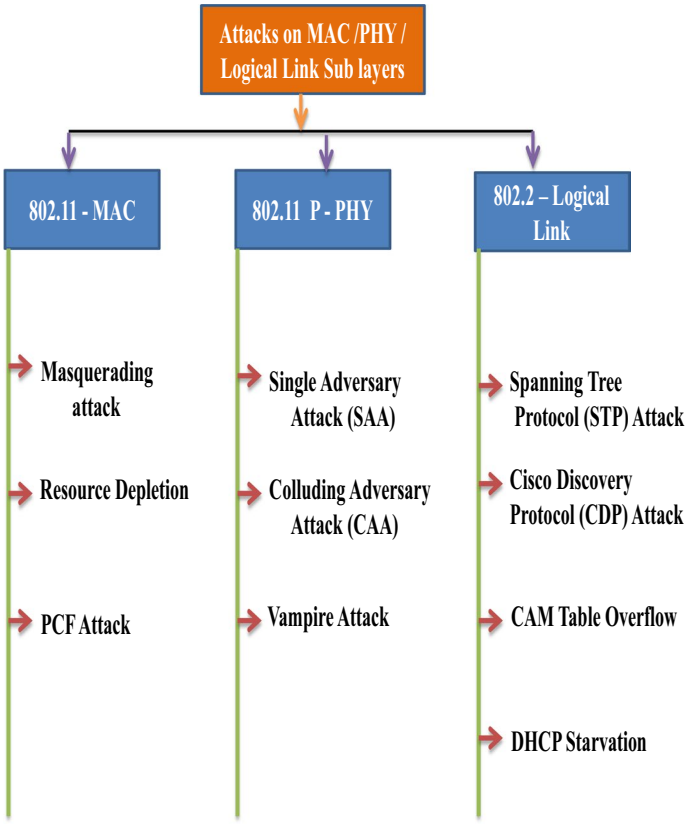

Fig. 15 MAC/PHY/logical link sub-layer attacks

2. We carefully investigated each attack after discovering it and classified it layer by layer. Additional research was conducted to uncover assaults that affect a specific layer as well as attacks that can occur across multiple layers.
3. We reviewed recent publications to compile a list of existing methods, strategies, and algorithms for each assault that can provide countermeasures.
4. The existing solutions were examined to determine how these strategies were used to provide solutions to a specific attack or group of attacks.
5. A deeper analysis was conducted to evaluate the limitations and weaknesses of existing approaches in terms of accuracy, performance, and other factors.
6. The study of existing methods gives us a clear picture of their drawbacks and we have suggested how these drawbacks can be overcome and the existing research work can be further enhanced.

Table 1 Correlation of existing countermeasures, their limitations, and future work

Citation	Method/technique used	Counter measure to	Limitations/future work
[30]	RF-based Q Learning	DDOS flooding attack	Fog and AI-related attacks
[31]	Homogeneous Discrete-Time Markov Chain	Data Tampering	Reduce computing cost
[32]	Cross-Layer selection using SVM	Routing / Reply Attack	Can obtain better results using more features
[33]	SVM Classifier	Jamming Attack	Improved and advanced jamming attacks must be considered
[34]	Signal Strength Index, Fitness Function, and Throughput	Sybil Attack	Network Optimizing and performance
[35]	Novel solution—DPBHA using dynamic threshold and generating forged RREQ	Black hole	Various security issues and gray hole detection and prevention
[36]	Novel—SBGM and Dynamic wrapping threshold	Gray hole and Black hole	Modifications in hop count and sequence number
[37]	CL-MLSP using AODV	Sinkhole	ML and Multicast routing protocols
[38]	Data-driven methodology using new features	Spoofing Attack	VAE—profiling-based detection
[39]	NOMA using ML and DL algorithms	Dropping Attacks	Extending simulation run time and use of large datasets
[40]	CR-VANETs using the DL method	Collision Attack	Production of new datasets and applying DL methods to new ones
[41]	Use of Xerosploit and Fluxion tools	MITM Attack	Improve the accuracy of encryption and more DL algorithms for performance
[42]	IPS and PSO algorithms	Wormhole and Blackhole Attacks	V2V detection and accuracy
[43]	Bayes Net Classifier using different datasets	Sleep Deprivation Attack	Run time verification of attacks
[44]	Deep Learning Technique	GPS Spoofing	To extend the idea to handle internal and external attacks
[45]	Novel—SAMA using RSSI	Location Attack	Use of other languages and data sets
[46]	MOVE Management System	Frame Information Poisoning	Increase performance and further decrease travel time of vehicle
[47]	Novel Framework using ML approaches	TCP SYN Attack	Use of DL methods to improve performance
[48]	Deep Learning Techniques using failover, load balancing, and higher availability	BGP Hijacking	Another type of attack can be detected by improving the training model
[49]	IEC104 honeypot	Telnet attack	Durability and Speed to be improved
[50]	Fuzzy-based context-aware detection model	Land and teardrop attacks	Addressing false alarms and use of AI methods
[51]	Novel embedding algorithm using an adapted distance metric	Spanning Tree Protocol	Leakage of Information
[52]	SDN Guard using a sampling technique	CAM Table Overflow	The use of ML methods can improve performance

Table 1 (continued)

Citation	Method/technique used	Counter measure to	Limitations/future work
[53]	ARP with a conjunction of ICMP	DHCP Starvation	Use various other protocol combination
[54]	Adversarially robust fusion using neural networks	Single Adversary Attack (SAA)	Extend to multiple attacks
[55]	LEACH protocol	Vampire Attack	Improve performance of cluster head
[56]	IBOOS	Colluding Adversary Attack (CAA)	Improvement of delay and false drop
[57]	PML-CIDS using alternating direction method	Eavesdropping Attack	Use of ML algorithms
[58]	ML—RF, Corsets, and cluster algorithms	Rushing Attack	Use of real-world scenarios

6 Conclusion

The primary concern of the drivers is safety. VANET has the capability of meeting safety requirements by providing road information to its users. VANET, on the other hand, is not immune to vulnerabilities and threats. Vehicle applications must be safeguarded; if an attacker modifies the content of safety applications, users will be directly impacted. We hope to better understand attackers and their tactics by employing the proposed layer-wise attacks. Keeping an eye on attackers is difficult, but in the future, we will develop a system that can identify network attacks based on a specific attack type.

Author Contributions Self.

Funding My research is non-funding, no organization, person(s) or any others are funding.

Availability of Data and Materials None.

Code Availability It's a Review paper, so no code is implemented or available.

Data Availability There is no dataset(s) available for my research work as it is a review paper.

Declarations

Conflict of interest None.

References

1. Kaur, R., & Jagdev, G. (2018). A study on working of prominent routing protocols in WANETs. *International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)*, *5*(1), 26–33. ISSN 2349-4859 (online). ISSN 2349–4840 (Print). https://doi.org/10.20431/2349-4859.0501004
2. Li, H., Xu, Z. (2018). Routing protocol in VANETs equipped with directional antennas: Topology-based neighbor discovery and routing analysis. *Wireless Communications and MobileComputing*, vol. 2018, ArticleD 7635143, 13 pages, https://doi.org/10.1155/2018/7635143
3. Poongothai, M., & Sathyakala, M. (2012). Simulation and analysis of DDoS attacks. In *International conference on emerging trends in science, engineering, and technology (INCOSET)*, pp. 78–85. https://doi.org/10.1109/INCOSET.2012.6513885.
4. Kumar, G. (2016). Denial of service attacks: An updated perspective. *Systems Science & Control Engineering*. https://doi.org/10.1080/21642583.2016.1241193
5. Zeebaree, S. R. M., Sharif, K. H., Mohammed Amin, R. M. (2018). Application layer distributed denial of service attacks defense techniques: A review. *Academic Journal of Nawroz University, 7*(4), 113–117. https://doi.org/10.25007/ajnu.v7n4a279
6. Lo, N., & Tsai, H. (2007). Illusion attack on VANET applications: A message plausibility problem. *IEEE Globecom Workshops, 2007*, 1–8. https://doi.org/10.1109/GLOCOMW.2007.4437823
7. Malhi, A., & Batra, S. (2019). Security of vehicular ad-hoc networks: A comprehensive survey. *Computers & Security 89*(1):101664. https://doi.org/10.1016/j.cose.2019.101664
8. Edemacu, K., et al. (2014). Packet drop attack detection techniques in wireless ad hoc networks: A review. *6*(5).
9. Rathod, A., Patel, S. (2017). A survey on black hole & gray hole attacks detection scheme for vehicular ad-hoc network. *International Research Journal of Engineering and Technology (IRJET)*, *04*(11).
10. Suresh Babu, G. N. K., Srivatsa, S. K. (2013). Distributed denial of service: attack at application and transport layers and precautions. *IJERTV2IS2462*, *02*(02).

11. Gupta, C., Singh, P., Tiwari, R. (2017). Network and transport layer attacks in ad-hoc network. *International Journal of Advanced Research in Computer and Communication Engineering*, 6(2), ISSN (Online) 2278-1021 ISSN (Print) 2319-5940.
12. Rahbari, M., & Jamali, M. A. J. (2011) Efficient detection of Sybil attack based on cryptography in VANET. *International Journal of Network Security & Its Applications (IJNSA)*, 3(6).
13. Durda, E., & Ali Buldub, A. (2000). IPV4/IPV6 security and threat comparisons. *Procedia - Social and Behavioral, Sciences, 2*(2), 5285–5291. https://doi.org/10.1016/j.sbspro.2010.03.862
14. Al Shahrani, A. S. (2011). Rushing attack in mobile ad hoc networks. In *Third international conference on intelligent networking and collaborative systems*, pp. 752–758. https://doi.org/10.1109/INCoS.2011.145.
15. Kaur, J. (2016). Mac layer management frame denial of service attacks. In *International conference on micro-electronics and telecommunication engineering (ICMETE), Ghaziabad, India*, pp. 155–160. https://doi.org/10.1109/ICMETE.2016.83.
16. Xu, R., Zhao, Z., He, F. (2010). DDoS attacks at MAC layer in tactical mobile ad hoc networks. In *International conference on communications and intelligence information security*, pp. 100–104. https://doi.org/10.1109/ICCIIS.2010.11.
17. Kiran Varma, K. S., & Satyanarayana, B. P. (2014). Jamming attacks: An approach for prevention. *International Journal of Computer Science And Technology (IJCST)*.
18. Pawar, P. M., Nielsen, R. H., Prasad, N. R., Ohmori, S., Prasad, R. (2012). Behavioural modelling of WSN MAC layer security attacks: A sequential UML approach. *Journal of Cyber Security and Mobility*, pp. 65–82.
19. Baccari, S., Touati, H., Haddad, M., Muhlethaler, P. (2020). Performance impact analysis of security attacks on cross-layer routing protocols in vehicular ad hoc networks. In *SoftCom - international conference on software, telecommunications and computer networks*, Hvar / Virtual, Croatia. final-02996797.
20. Kumar, G. (2104). Understanding denial of service (Dos) attacks using OSI reference model. *International Journal of Education and Science Research Review*, *1*(5). ISSN 2348–6457.
21. Obaid, H. S., & Abeed, E. H. (2020). DoS and DDoS attacks at OSI layers. *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, *2*(8).
22. Yılmaz, M. H., & Arslan, H. (2105). A survey: Spoofing attacks in physical layer security. In *IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops)*, pp. 812–817. https://doi.org/10.1109/LCNW.2015.7365932.
23. Aydos, M., Vural, Y., & Tekerek, A. (2019). Assessing risks and threats with layered approach to Internet of Things security. *Measurement and Control*. https://doi.org/10.1177/0020294019837991
24. Lei, H., Gao, C., Ansari, I. S., Guo, Y., Pan, G., & Qaraqe, K. A. (2016). On physical-layer security over SIMO generalized-KK fading channels. *IEEE Transactions on Vehicular Technology, 65*(9), 7780–7785. https://doi.org/10.1109/TVT.2015.2496353
25. Farooq, T., Llewellyn-Jones, D., & Merabti, M. (2010). Mac layer dos attacks in IEEE 802.11 networks. In *The 11th annual conference on the convergence of telecommunications, networking, and broadcasting (PGNet 2010)*, Liverpool, UK.
26. Martínez, A., & Zurutuza, U. (2008). Beacon frame spoofing attack detection in IEEE 802.11 networks. In *Third international conference on availability, reliability, and security.*
27. Zhou, Y., Wu, D., Nettles, S. M. (2004). Analyzing and preventing MAClayer denial of service attacks for stock 802.11 systems. In *Workshop on broadband wireless services and applications (BROADNETS)*.
28. Vasserman, E. Y., & Hopper, N. (2013). Vampire attacks: Draining life from wireless ad hoc sensor networks. *IEEE Transactions on Mobile Computing, 12*(2), 318–332. https://doi.org/10.1109/TMC.2011.274.
29. Singh, R., Kaur, A., Sethi, S. (2015). Attacks at data link layer of OSI model: An overview. *International Journal of Advanced Technology in Engineering and Science*, Volume No.03, Special Issue No. 02.
30. Karthikeyan, H., & Usha, G. (2022). Real-time DDoS flooding attack detection in intelligent transportation systems. *Computers and Electrical Engineering*. https://doi.org/10.1016/j.compeleceng.2022.107995
31. Poongodi, M., Bourouis, S., Ahmed, A. N., Vijayaragavan, M., Venkatesan, K. G. S., Alhakami, W., Hamdi, M. (2022). A novel secured multi-access edge computing based VANET with neuro-fuzzy systems based blockchain framework. *Computer Communications* https://doi.org/10.1016/j.comcom.2022.05.014.

32. Fan, Q. G., Wang, L., Cai, Y. N., Li, Y. Q., Chen, J. (2006). VANET routing replay attack detection research based on SVM. In *MATEC Web Conf. Volume 63, international conference on mechatronics, manufacturing and materials engineering (MMME)*.
33. Kim, H., & Chung, J. M. (2022). VANET jamming and adversarial attack defense for autonomous vehicle safety. *Computers, Materials, and Continua*.
34. Sefati, S. S., & Tabrizi, S. G. (2022). Detecting sybil attack in vehicular ad-hoc networks (VANETs) by using fitness function, signal strength index and throughput. *Wireless Personal Communications, 123*, 2699–2719. https://doi.org/10.1007/s11277-021-09261-x
35. Malik, A., Khan, M. Z., Faisal, M., Khan, F., Seo, J.-T.. (2022). An efficient dynamic solution for the detection and prevention of black hole attack in VANETs. *Sensors*, *22*(5), 1897. https://doi.org/10.3390/s22051897.
36. Remya Krishnan, P., Arun Raj Kumar, P. (2022). Detection and mitigation of smart blackhole and gray hole attacks in VANET using dynamic time warping. *Wireless Personal Communications, 124*, 931–966 (2022). https://doi.org/10.1007/s11277-021-09390-3.
37. Sangaiah, A. K., & Javadpour, A., Ja'fari, F., Pinto, P., Ahmadi, H. R., Zhang, W. (2022). CL-MLSP: The design of a detection mechanism for sinkhole attacks in smart cities. In 2022 Microprocessors and microsystems, https://doi.org/10.1016/j.micpro.2022.104504.
38. Kim, C., Chang, S.-Y., Lee, D., Kim, J., Park, K., & Kim, J. (2023). Reliable detection of location spoofing and variation attacks. *IEEE Access, 11*, 10813–10825. https://doi.org/10.1109/ACCESS.2023.3241236
39. Mughaid, A., AlZu'bi, S., Alnajjar, A. et al. (2022). Improved dropping attacks detecting system in 5G networks using machine learning and deep learning approaches. *Multimedia Tools*. https://doi.org/10.1007/s11042-022-13914-9.
40. Bahramnejad, S., Movahhedinia, N., Naseri, A., et al. (2023). A deep learning method for automatic reliability prediction of CR-VANETs, PREPRINT (Version 1) available at Research Square, https://doi.org/10.21203/rs.3.rs-2604220/v1.
41. Kaushik, K., Singh, V., Manikandan, V. P. (2022). a novel approach for an automated advanced MITM attack on IoT networks. In Sugumaran, V., Upadhyay, D., Sharma, S. (Eds) *Advancements in Interdisciplinary Research. AIR 2022. Communications in Computer and Information Science, vol 1738*. Springer, Cham. https://doi.org/10.1007/978-3-031-23724-9_6.
42. Soni, G., Chandravanshi, K., Jhariya, M. K., Rajput, A. (2022). An IPS approach to secure V-RSU communication from Blackhole and wormhole attacks in VANET. In: H. K. D. Sarma, V. E. Balas, B. Bhuyan, N. Dutta (Eds) *Contemporary issues in communication, cloud and big data analytics. Lecture notes in networks and systems, vol. 281*. Springer, Singapore. https://doi.org/10.1007/978-981-16-4244-9_5.
43. Verma, A., & Saha, R. (2022). Analysis of BayesNet classifier for DDoS detection in vehicular networks. In *International conference on augmented intelligence and sustainable systems (ICAISS)*, Trichy, India, 2022, pp. 980–987. https://doi.org/10.1109/ICAISS55157.2022.10011115.
44. Manale, B., & Mazri, T. (2022). Intrusion detection method for GPS based on deep learning for autonomous vehicle. *International Journal of Electronic Security and Digital Forensics, 14*(1), 37–52.
45. Babaghayou, M., Labraoui, N., Ari, A. A. A., Lagraa, N., Ferrag, M. A., & Maglaras, L. (2022). SAMA: Security-aware monitoring approach for location abusing and UAV GPS-spoofing attacks on Internet of Vehicles. In *CROWNCOM 2021, WiCON 2021: Cognitive radio oriented wireless networks and wireless internet* (343–360). https://doi.org/10.1007/978-3-030-98002-3_25.
46. Pedroso, C., Gomides, T. S., Guidoni, D. L., Nogueira, M., Santos, A. L. (2022). A robust traffic information management system against data poisoning in vehicular networks. In *IEEE Latin America Transactions, 20*(12), 2421–2428. https://doi.org/10.1109/TLA.9905610.
47. Ben Rabah, N., & Idoudi, H. (2023). A machine learning framework for intrusion detection in VANET communications. In K. Daimi, A. Alsadoon, C. Peoples, N. El Madhoun (Eds) *Emerging trends in cybersecurity applications*. Springer, Cham. https://doi.org/10.1007/978-3-031-09640-2_10.
48. Mahajan, N., Chauhan, A., Kumar, H., et al. (2022). A deep learning approach to detection and mitigation of distributed denial of service attacks in high availability intelligent transport systems. *Mobile Networks*, pp. 1423–1443.
49. Grigoriou, E., et al. (2022). Protecting IEC 60870-5-104 ICS/SCADA systems with honeypots. In *2022 IEEE international conference on cyber security and resilience (CSR)*, Rhodes, Greece, pp. 345–350, https://doi.org/10.1109/CSR54599.2022.9850329.

50. Ghaleb, F. A., Saeed, F., Alkhammash, E. H., Alghamdi, N. S., & Al-rimy, B. A. S. (2022). A fuzzy-based context-aware misbehavior detecting scheme for detecting rogue nodes in vehicular ad hoc network. *Sensors*. https://doi.org/10.3390/s22072810
51. Byrenheid, M., Strufe, T., Roos, S. (2020). Secure embedding of rooted spanning trees for scalable routing in topology-restricted networks. In *International symposium on reliable distributed systems (SRDS)*, Shanghai, China, 2020, pp. 175–184. https://doi.org/10.1109/SRDS51746.2020.00025.
52. Dridi, L., & Zhani, M. F. (2018). A holistic approach to mitigating DoS attacks in SDN networks. *International Journal of Network Management*. https://doi.org/10.1002/nem.1996
53. Yaibuates, M., & Chaisricharoen, R. (2020). A combination of ICMP and ARP for DHCP malicious attack identification. In *Joint international conference on digital arts, media and technology with ECTI Northern Section conference on electrical, electronics, computer and telecommunications engineering (ECTI DAMT & NCON)*, Pattaya, Thailand, , pp. 15–19, https://doi.org/10.1109/ECTIDAMTNCON48261.2020.9090760.
54. Yang, K., Lin, W.-Y., Barman, M., Condessa, F., Kolter, Z. (2021). Defending multimodal fusion models against single-source adversaries. In *IEEE/CVF conference on computer vision and pattern recognition (CVPR)*, Nashville, TN, USA, 2021, pp. 3339–3348, https://doi.org/10.1109/CVPR46437.2021.00335.
55. Jagnade, G. A., Saudagar, S. I., Chorey, S. A. (2016). Secure VANET from vampire attack using LEACH protocol. In *International conference on signal processing, communication, power and embedded system* (SCOPES), Paralakhemundi, India, pp. 2001–2005, https://doi.org/10.1109/SCOPES.2016.7955799.
56. Hemamalini, V., Zayaraz, G., Susmitha, V., Saranya, V. (2017). An efficient probabilistic authentication scheme for converging VANETs. In *Second international conference on recent trends and challenges in computational models (ICRTCCM)*, Tindivanam, India, pp. 147–152, https://doi.org/10.1109/ICRTCCM.2017.40.
57. Zhang, T., & Zhu, Q. (2018). Distributed privacy-preserving collaborative intrusion detection systems for VANETs. *IEEE Transactions on Signal and Information Processing over Networks, 4*(1), 148–161. https://doi.org/10.1109/TSIPN.2018.2801622
58. Bangui, H., Ge, M., Buhnova, B. (2021). A hybrid data-driven model for intrusion detection in VANET. In *The 12th international conference on ambient systems, networks, and technologies (ANT)/ the 4th international conference on emerging data and industry 4.0 (EDI40)/affiliated workshops*, https://doi.org/10.1016/j.procs.2021.03.065.

Mr. K. Vamshi Krishna received his B.Tech degree in Computer Science and Engineering from Rao Bahadur Y. Mahabaleswarappa Engineering College (RYME), Bellary affiliated to Visvesvaraya Technological University (VTU) in 2009 and his M.Tech degree in CSE from the Jain University Global campus Kanakapura, Bangalore, in 2012. At present, he is pursuing his PhD under the guidance of Dr. Ganesh Reddy K at VIT-AP University. He has published two papers on network security and one IEEE conference in the area of information security in VANET. His main research areas are information security, and computer networks.

Dr. K. Ganesh Reddy received his B.Tech degree in Information Technology from Andhra University, in 2007 and his M.Tech degree in Information Security from the National Institute of Technology Rourkela (NITR), Orissa, in 2010. He was awarded the Ph.D. degree in computer science and engineering from the National Institute of Technology Karnataka (NITK) Surathkal, in 2014. At present, he is working as an associate professor at VIT-AP University. He has published twenty international conference and journal articles and two national conferences in the area of wireless and information security. He is an editorial board member of the journal of information and has reviewed IEEE, Springer international conference articles, and Wiley, Hindawi, and Oxford journal articles. His main research areas are information security, cloud computing, algorithm design, and computer networks. He is an Associate Member of the National Cyber Safety and Security Standards (NCSSS) India, and a member of the Institution of Engineers (India). He is a certified security analyst by NCSSS.