ISSN: 0974-5823 Vol. 6 No. 2 September, 2021

International Journal of Mechanical Engineering

A Systematic Review on Security of Wireless Network: Smart Vehicle Perspective

Syed Mohd Faisal, Dr. Taskeen Zaidi
Shri Ramswarrop Memorial University, Barabanki, India
smfaisalcse@gmail.com, taskeenzaidi867@gmail.com

Abstract **- Wireless Ad-Hoc Network is vulnerable to secure data transmission because of its open nature. This paper reviews state of art security goals, challenges, routing protocol, and attacks over the wireless network. Vehicular Ad-Hoc Network (VANET) is the most prominent technology to implement Intelligent Transport System (ITS). VANET provides ITS support, umpteen applications and features for the drivers and passengers' safety; therefore, it is necessary to understand machine ethics and make a network prone to attackers. This paper reviews some possible attacks over VANET and provide an in-depth study of Sybil attack also analyzed various detection and elimination techniques to reduce the risk of Sybil attacks.**

Index Terms - WSN, VANET, OBU, IEEE, ITS, ZOR, FCC, ETSI.

1. INTRODUCTION

Wireless Ad-hoc Network delivers applications like target tracking, environmental monitoring, health monitoring, and many more. Dependently protocol management, equipment management and topology deployment are significant areas for modern-day researchers. The performance of ad-hoc wireless networks in different domains/applications is crucial concerning security. Thus, it is necessary to detect and prevent attacks at different levels of wireless sensor network implementation. Attacks like Denial-of-Service attack, Distributed Denial of Service attack, Black-hole attack, Wormhole attack, Illusion attack, Timing attack, Man in the middle attack, social attack, and Sybil attack are still observed. [1].

Many researchers have proposed infrastructure which adds some portable devices in the network to detect an attack and trace their geographical location. However, this strategy was helpful to detect the number of attacks. Still, it failed to detect Sybil attacks where Sybil nodes mislead other legitimate network nodes by revealing wrong, stolen/duplicate identities. In the current scenario, attacker nodes disguise the identities of legitimate nodes and act as legitimate nodes. Since there is no master node in VANET to monitor communication among nodes, detecting inappropriate communication is one of the tedious tasks in the wireless sensor network. In the peer-to-peer paradigm, the system is typically divided into structured and unstructured forms where a structured system performs peers' deterministic mechanisms to manage data and cater to peer discovery. In contrast, an unstructured system generates random peer graphs and control peers to manage data using flooding. Many peer networks are decentralized where the central authority does not operate, which exposes the network to attacks. [2] [3] [4].

Let us understand the concept of the Wireless Ad-hoc network before discussing more Sybil attacks. Security is an essential concern regarding wireless networks. A harmful attack against a wireless network is a Sybil attack, where a node creates multiple illegitimate identities. Illegitimate nodes mislead the system by creating multiple identities; a Sybil node disrupts network services. These vulnerable identities insert wrong information into the system and affect the functioning of the system.

2. BACKGROUND

2.1. Wireless Ad-Hoc Network (WANET): A Wireless Ad-hoc Network (WANET) is a form of Local Area Network (LAN) that spontaneously establishes communication among multiple wireless devices without fixed infrastructure.

Devices are randomly deployed across the Wireless Ad-hoc Network; the intended device needs to discover the destination device and path through transmitting messages over the wireless communication channel. Devices can communicate directly with other devices lying in their transmission range; otherwise, devices use intermediary nodes to reach the destination. [5]. Broadly Wireless Ad Hoc Network is categorized into three categories, i.e., Mobile Ad-hoc Networks (MANETs), Wireless Sensor Networks (WSNs), and Wireless Mesh Networks (WMNs) [6] [7].

2.1.1. Mobile Ad-hoc Network (MANET): MANET is also referred to as a wireless ad-hoc network/ad-hoc wireless network. In 1996, an Internet Engineering Task Force (IETF) developed MANET to standardize the wireless IP routing protocol features. MANET consists of multiple mobile nodes that are wirelessly connected and configured via a self-

configured/self-healing mechanism in the infrastructure-less domain. MANET nodes are free to move arbitrary, which cause rapid connection establishment and connection break; consequently, topology changes frequently. MANET works on a very complex topology, where multiple transceivers are present between nodes, as represented in Figure 1. Primary challenge in MANET is that every node stores its data, manages it, and at the same time node has to work as a router to route traffic properly. MANET consists of self-forming, self-healing, peer-to-peer networks that communicate at 30MHz–5Ghz radio frequency band. This state-of-the-art formulates MANET for home use, disaster relief operations, defence, robots, road safety applications, etc. [8] [9] [10].

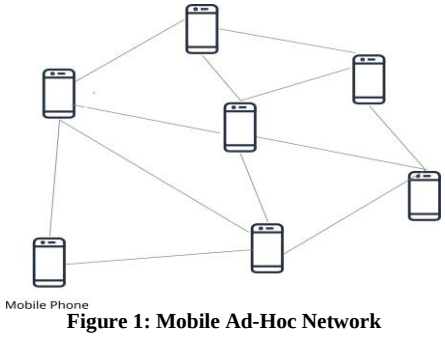

Figure 1: Mobile Ad-Hoc Network

2.1.2. Wireless Sensor Network (WSN): Wireless Sensor Networks (WSNs) interconnects disjoined distributed sensors and gather a vast amount of information such as system condition, physical condition, environmental condition, pollution, and others. A wireless sensor network is a self-organized infrastructure-less network where communication is feasible via sensors only. Sensors communicate with others via radio signals, as represented in figure 2. Devices on a wireless sensor network are equipped with time, location, speed, pressure, acceleration, air-condition, communication, and environmental sensors. After deployment, mobile devices construct self-organizing infrastructure, preferably a multi-hop network. In addition, on-board sensors capture device information, information of interest and update the user concerning this communication may be continuous or event-driven. [11] [12]. Actuators are equipped with devices to act on certain conditions. Meanwhile, the Global Positioning System (GPS) or Local Positioning System (LPS) senses track vehicles' precise positions.

As we know, devices are mobile and power limited; nevertheless, it is imperative to design protocols requiring low device complexity and less power consumption to preserve the balance among communication and signal processing capacity. Sensors in WSNs are equipped over on-board unit to track the physical/ environmental condition and relay essential information to devices. Devices are connected with base stations to interchange information from the outer world. A base station is a central component for gathering data from mobile devices in case of an adversary [13].

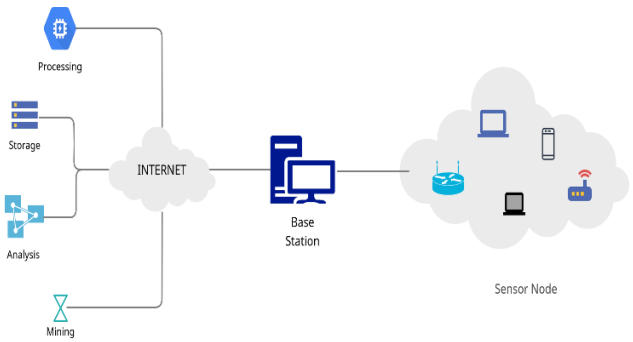

Figure 2: Wireless Sensor Network

2.1.3. Wireless Mesh Network: Wireless Mesh Networks consist of separate wireless nodes linked to the access point. WMN is a completely autonomous network, so nodes perform their internal functions simultaneously and also act as a router. Because of the absence of fixed infrastructure nodes transmit data via neighbor nodes and vice- versa [14] as represented in figure 3.

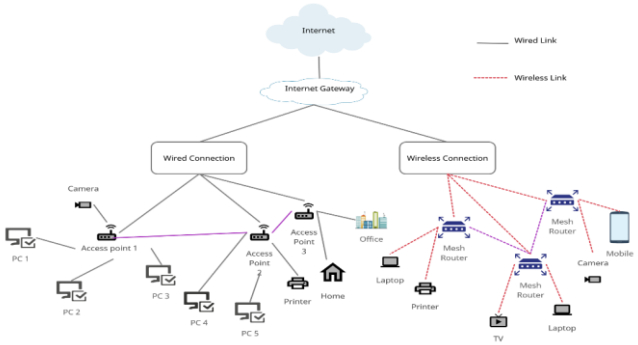

Figure 3: Wireless Mesh Network

Nodes in WMNs are small transmitters that work similarly as a wireless router. The communication with users and nodes are achieved by IEEE 802.11a, b, and g standards (Wi-Fi). Nodes are programmed in such a way that they find the shortest and safest path to travel. Only one node in WMN is physically connected with the model/router, and other nodes wirelessly share the internet connection with that one node. Similarly, connected nodes share connection with nodes in that range. This creates a "cloud of connected nodes" which can serve schools, universities, offices, cities, etc. [15] [16].

2.1.4. Others: Apart from traditional wireless ad-hoc networks, i.e., Mobile Ad-hoc Network, Wireless Sensor Network, Wireless Mesh Network many modern-day Ad-Hoc networks have arisen, some of them are Flying Ad Hoc Network (FANET), Ad Hoc UAV-Ground Network (AUGNet), Under- water Ad Hoc Network (UANET), Underwater Sensor Network (UWSN), Underwater Acoustic Sensor Network (UW-ASN), Autonomous Mobile Mesh Network (AMMNET), Unmanned Air/Aerial Vehicles Network (UAVNet).

With the widespread use of handheld and mobile devices, ad-hoc wireless networks became active and dynamic networks to transmit data. Portable devices over Wireless Sensor Networks expand WSN usage in education, business, health, emergency,

disaster management, environmental monitoring, personal area network, military surveillance, smart vehicles, and so on.
The easy connection and open nature of WANET attract users and attackers. Researchers are continually focusing on creating a secure WANET even now; many issues need to be encountered, such as finite transmission bandwidth, dynamic link establishment, abusive broadcasting message, hardware/software processing capacity, reliable data delivery, and security problems.

2.2 Security Goals

As we know wireless network does not inherently rely upon fixed infrastructure, this leads to address multiple challenges of their security architecture. Primarily five security measures require to be encountered to maintain a reliable and secure wireless network. [17] [18].

2.2.1. Confidentiality: Confidentiality assures the protection of information from being exposed by unauthorized access. Wireless sensor network implements confidentiality using username, password, and encryptions. Confidentiality can be achieved smoothly if the stipulation of authentication is made appropriately. [19] [20].
2.2.2. Integrity: Integrity guarantees the authenticity of the information. Integrity ensures that received information is exactly as same as it was formerly sent. Information may change or damage by system crashes or malicious users, though it is suggested to have a data backup and redundant systems to assure data integrity. [19] [20].
2.2.3. Availability: Availability is a crucial attribute of security. Availability ensures that information and service are continuously accessible even in an adversary. Availability is achieved by hardware maintenance, in-depth testing of software, and network optimization. [19] [20] [21].
2.2.4. Authentication: Authentication provides affirmation of someone as the same who is claimed to be. In Wireless Sensor Network, authentication is ensured by Message Authentication Code. (MAC). [19] [22].
2.2.5. Nonrepudiation: Non-repudiation guarantees that if a user sends a message, then, later on, it can't deny sending a message; subsequently, after receiving the message, a receiver can't deny receiving the message. [19] [23].

2.3. Challenges in Wireless Ad-Hoc Network

Wireless Ad-hoc Network is entirely different from the conventional wired network. Wireless Ad-hoc Network provides flexibility to access services on the move, and at the same time, it carries challenges to manage the network. [24].
2.3.1. Mobility: Wireless Ad-hoc Network offers flexibility to move freely in the network, also permits to join or leave network anytime. Mobility creates a center of attention for users on the move and, simultaneously, high mobility craft impediments for topologies in routing. Moreover, nodes may join or leave the network at any time; this leads to additional annoyance for topology. [25].
2.3.2. Power and Bandwidth: Wireless devices come up with limited battery power though it's necessary to route packets through a paramount path using minimum power and limited bandwidth consumption. [26].
2.3.3. Quality of Service: QoS is a parameter that renders wireless sensor networks further challenging. In contrast to a wired network, a wireless network posse far more complexities, e.g., data loss, packet delay, distortion, fluctuation in speed, active/sleep devices in the network, dynamic topology change, transmission range, transmission power; this delivers additional overhead to accord quality of services in WANs. [27] [28].
2.3.4. Security: In every form of network, security affirmation is one of the strenuous tasks, and further, it becomes more challenging when it comes to wireless networks. In the wireless network, all the transmission passes through free space, which increases an anomaly's chances to perform an active or passive attack. [29] [30].

2.4. Properties of Wireless Routing Protocols

Before we address routing protocols for Wireless Ad-hoc Networks, it is essential to be acquainted with some critical properties necessary in every routing protocol.
2.4.1. Distributed operation: Protocols are supposed to be distributed, i.e., they should not rely on a centralized node. In non-distributed protocols, messages may get into starvation, or the whole network crashes down if the centralized node's connectivity breaks down. We can't think about the centralized and non-distributed operation in ad-hoc wireless networks where nodes join or leave the system on the fly anytime, anywhere. [31].
2.4.2. Loop Free: The protocol should generate loop-free routes, which reduce the consumption and bandwidth of the network.
2.4.3. Link Support: In a wireless environment, communication must be bi-directional; this reduces the packet delay ratio and improves the network's overall performance. [32].
2.4.4. Routing Protocol: Reactive protocols establish routes on demand. The advantage of this protocol is straight, i.e., not periodically generating routes either in demand or not. This strategy certainly reduces network bandwidth consumption.
2.4.5. Multiple Routes: Concurrent multiple routes reduce the congestion, i.e., due to congestion or fault in the network; if a route gets damaged, then an alternate route must be there to serve communication. This property reduces alternate path discovery time, improves performance, and improves load balancing and fault tolerance.
2.4.6. Quality of Service: Quality of Service is to maintain end-to-end delay, bandwidth, and energy constraints. There must be some quality check parameter incorporation in the routing protocol. QoS helps to understand why this network was used and will later develop better services to serve the network. [33].

2.5. Routing Protocol in Wireless Network

Scholars suggest several routing protocols with different routing mechanisms, as represented in figure 4. At this juncture, we evaluate protocols on the ground of functionality and review some of them:
2.5.1. Proactive Routing Protocol: A Proactive routing protocol is also known as a table-driven routing protocol, where nodes periodically maintain multiple paths to a destination. All the nodes of the network periodically

broadcast a HELLO message to perceive the change in the network. [34].

2.5.2. Reactive Routing Protocol: Reactive routing is also known as an on-demand routing protocol. Node discovers routes to the destination when the source node generates demand. Route discovery is achieved by flooding a route request packet through a global broadcast in the network [35].

2.5.3. Hybrid Routing Protocol: Hybrid routing protocol blends the benefits that both proactive and reactive routing protocols provide in separate ways [36].

2.5.4. Hierarchical Routing Protocol: Hierarchical routing protocol operates on hierarchical addressing where addresses are separated into two fragments person address and host address. It's like phone books that are separated into a phone number, area code and city. Examples of hierarchical routing are HSR, CGSR [37].

2.5.5. Multipath Routing Protocol: Multi-path routing improves reliability and load balancing by detecting multiple paths between source and destination. Owing to this, the network significantly utilizes bandwidth and provides outstanding reliability. Examples of Multi-path routing are CHAMP, BMR, AOMDV, etc. [38].

2.5.6. Multicast Routing Protocol: Multicast routing is to distribute network traffic efficiently. Multicast routing allows the delivery of a message to the community of receivers in one transmission. Examples of Multicast routing are AQM, ADMR, CBM, DDM, etc. [39].

2.5.7. Location Awareness: Location-based routing makes use of the geographical position of the device. Initially, the device's geographical location is identified, and then the protocol generates a path to reach the destination. Examples of location-based routing are ALARM, DRM, LAR, GPSR, etc. [40][41].

2.5.8. Geographic Multicast Routing: The restriction of unicast routing influenced the use of multicast routing protocol in the network. The Geographical Multicast Routing identifies geographically separated destination nodes and relays a single message to reach a group of destination nodes. Examples are DGR, GAMER, GeoGRID, etc. [42][43] [44].

2.5.9. Power Awareness: Power consumption is a crucial design concern in wireless sensor networks as nodes are equipped with a limited battery. However, it is necessary to develop and deploy routing protocols that minimize energy consumption. Power awareness protocol is conscious of the state of energy of nodes and generates a path concerning that. The examples are DEAR, MEHDSR, etc. [45] [46].

2.5.10. Secure Routing: The secure routing protocol provides security checks while routing messages in a sensor network. It also provides counter-measures against some powerful attacks. Examples of secure routing are SAR, SPR [47][48].

Figure 4: Routing in Wireless Network

2.6. Attack:

In this paper, our primary focus is on attacks launched on the Wireless network. Wireless Ad-hoc Network is a collection of mobile nodes where mobile devices join and leave the network on their own, because of the open nature ad-hoc wireless environment; it is vulnerable to multiple attacks [49] [50]. Table 1 shows the types of attacks possible over the TCP/IP layer.

2.6.1. Eavesdropping: Eavesdropping is the listening of private or public communication without the users' concern. Attacker inserts malicious code in the network and starts listening communication, though eavesdropping is most effective to launch and most challenging to identify and track [51].

2.6.2. Tampering: Tampering is an act of deliberately editing, manipulating, and destroying data by an unauthorized user. First tampering was imposed in the late 1980s to sabotage and route destructive programs to modify data [52].

2.6.3. Interference: The natures of nodes in a Wireless network are mobile, so the transmitted signal of one client interferes with the transmitted signal of the other. Interference raise frame lost ratio, contraction in transmission rate, and trim down resources utilization capacity in the wireless network. To attain maximum performance, it is essential to control or remove interference [53]. Following types of interferences are possible in WAN.

2.6.3.1. Self- Interference
2.6.3.2. Multiple Access Interference
2.6.3.3. Co-channel Interference
2.6.3.4. Adjacent Channel Interference

2.6.4. Collision: A collision occurs in wireless networks when multiple users send packets at precisely exact moment. Consequences of collision are network discard all the collision packets and request for retransmission [54]. Following collisions are observed in the wireless network:

2.6.4.1. Local collision
2.6.4.2. Remote collision

2.6.5. Traffic Analysis: Traffic analysis is performed to observe, analyze, and record network traffic to detect and respond to adversaries. Without appropriate traffic analysis, it

is impractical to build a stable network [55]. Two methods are used to analyze network traffic:

2.6.5.1. Active traffic analysis

2.6.5.2. Passive traffic analysis

2.6.6. Monitoring: Monitoring is performed in real-time where active, and sleep devices are monitored and pursue necessary action to route packets through active nodes and alert modified status to neighboring devices [56].

2.6.7. Spoofing Attack: The attacker impersonates and acquires access to our private sensitive, confidential information and access privileged services that could only be restricted to legitimate users/devices. [57].

2.6.8. Sinkhole Attack: Attackers execute sinkhole attacks either by hacking a node or by inserting a fabricated node into the network. Later sinkhole node advertises (itself) as this node (sinkhole node) has the shortest path to the destination. In this way, the sinkhole attacks congregate network data transmission and can enable attacks like selective forwarding and wormhole attack [58].

2.6.9. Sybil Attack: The attacker produces as many fake identities/devices as possible and pretends it to be many different individuals all at once. The potential to produce a large number of pseudonyms depends on the attacker's capability, the bandwidth, and the processing space that the attacker has accessible. [59].

2.6.10. Wormhole Attack: A malicious node creates a tunnel to another malicious node at a long-range. The idea is to perturb the selection of shortest path, since malicious nodes are directly connected via tunnel so legitimate node forwards data through the malicious node (as it seems that malicious node has the shortest path), this leads malicious nodes to modify or damage transmitted data. Wormhole attacks are of the following type:

2.6.10.1. Open Wormhole

2.6.10.2. Half-open Wormhole

2.6.10.3. Closed Wormhole

2.6.11. Black-hole Attack: Mostly reactive routing protocols are used in an ad-hoc wireless network, so there is no predefined route. In a black-hole attack, when nodes initiate to send data, it broadcasts a route request packet in the network; here malicious node generates a false shortest route and replies for the route request packet. Legitimate node trust on the received route and forwards data; later, the malicious node can drop all the messages or collect all the data for their benefit and sell [60].

2.6.12. Desynchronization Attack: Attackers maintain a meaningful archive to store original packets in their database and forward tampered packets, insert frames in packets, remove the frame from packets, and change the sequence of frames in packets. This attack is performed to collect confidential information from the network [61].

2.6.13. Session Hacking: Session hacking usually attempts to extract session tokens. A session hacking attack is usually launched to manage session tokens. Attacker surreptitiously attains authenticated user session ID and pretends as an authenticated user. Once the attacker has authenticated user's session ID, it masquerades as an authenticated user and access services granted to the authenticated user. This attack is applied chiefly to web applications and browser sessions [62]. Session hacking is of two types:

2.6.13.1. Active

2.6.13.2. Passive

2.6.14. Flooding Attack: The attacker floods a vast number of bogus messages on a device or server in an attempt to push services or servers down.

2.6.15. Repudiation Attack: A repudiation attack occurs when a user sends a message or initiates communication, and later it (user) denies the transmission or communication.

2.6.16. Malicious Code: Malicious code arrives in the form of java applets, browser plug-ins, popup messages, and others. Protection from malicious code is one of the onerous tasks as none of the antivirus, firewalls, IDS, and others give complete assurance of prevention from the malicious code [63].

Table 1: Attacks in Wireless Network

Layers	Attacks
Physical layer	Jamming, Eavesdropping, Interference, Tampering
Data link layer	Collision, Traffic Analysis, Monitoring, Exhaustion
Network layer	Spoofing, Sinkhole, Sybil, Wormhole, Black hole, Selective forward, Resource compromise
Transport layer	Desynchronization, Session hacking, SYN flooding, flooding
Application layer	Data corruption, Repudiation, Malicious code, Overwhelm

3. VEHICULAR AD-HOC NETWORK (VANET)

Wireless Sensor Network has provided significant traits that have affected various areas of everyday life, e.g., defence, health, industry, entertainment, commercial, and many others. The wireless sensor network is a combination of nodes used to observe the environment, such as position, sound, pressure, temperature, humidity, etc. The information guided by WSN is utilized to perform multiple tasks, i.e., detection of the neighbor nodes, data store, data collection, data processing, node location detection, route discovery, data monitoring controlling, and synchronizing [64].

Wireless Sensor Network comprises several tiny embedded devices, which share details anonymously about their position, operational parameters, and service status.

Vehicular Ad-hoc Network is a subdomain of Wireless Sensor Network (WSN). VANET aims to create communication among a group of vehicles without the aid of a central controlling unit. Majorly VANET helps in a critical emergency with no infrastructure to pass information and save human lives.

Revolution in Automobile industry drives advancement in communication system and monitoring, receipt development and deployment of Intelligent Transport System (ITS). VANET emerged as a significant motivation in the implementation of Intelligent Transport System (ITS) [65].

VANET is a highly dynamic, self-organizing network uses Direct Short-Range Communication (DSRC) to communicate with vehicles on the road and roadside units (RSUs). Vehicles equipped with On-Board Units (OBUs) and RSUs are placed on the green, which provides a gateway to access the Internet. Communication between vehicles and RSUs is accomplished

via DSRC using IEEE 802.11p. IEEE 802.11p works on a 5.9 GHz frequency band, connecting vehicles and RSUs under 100 to 500 meters.

3.1. IEEE 802.11p: IEEE 802.11p is also known as Wireless Access for Vehicular Environment (WAVE) Protocol. WAVE protocol is devoted to offer an Intelligent Transport System (ITS). Application of WAVE is to establish communication between Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) using frequency band 5.9 GHz. US Federal Communications Commission (FCC) & European Telecommunications Standards Institute (ETSI) allocate 30 and 75 MHz spectrum in 5.9 GHz frequency band for Direct Short-Range Communication (DSRC) [66]. Vehicle to Vehicle and Vehicle to Infrastructure Communication adapt DSRC protocol, which probably trims down the possibilities of accidents on the road by assisting drivers regarding real-time traffic. In addition to non-safety applications, DSRC protocol is crucial for passenger safety, which renders safety applications more important than other applications.

Table 2 is the data frame of IEEE 802.11 where Frame Control (FC) indicates the type of frame, DUR is the Duration of the frame, SA defines the Source Address, DA is Destination Address, TA defines Transmission station Address, SEQ is the Sequence number to indicate each frame uniquely, RA is Receiving station Address and FCS is Frame Check Sequence to check the error in the frame during transmission.

Table 2: IEEE 802.11 DATA FRAME

FC	DUR	SA	DA	TA	SEQ	RA	DATA	FCS

WAVE standard is defined for the Physical layer as well as the MAC layer of DSRC as represented in table 3 and figure 6. Presently IEEE proposes IEEE 1609.2 standard, which is an advanced standard of IEEE 802.11p. IEEE 1609.2 standard in VANET ensures safety criteria via protecting messages from leakage and unauthorized access of information. As WAVE protocol runs over Vehicle Multi-technology Communication Device (VMCD) owing to messages and services are protected from various attacks (spoofing, masquerading, eavesdropping, and others) by IEEE 1609.2 [67].

- WME-Wave Management Entity
- PLME-Physical Layer Management Entity
- PLCP- Physical Layer Control Entity
- MLME-Media access control Layer Management Entity
- PLME-Physical Layer Management Entity
- U-MLME- Upper Media access control Layer Management Entity
- L-MLME Lower Media access control Layer Management Entity

Table 3: OSI vs WAVE layer protocol

Application	IEEE 1609.1	Upper Layers
Presentation		
Session		
Transport	IEEE 1609.3	Networking Services
Network		
Data link	IEEE 1609.4	LLC Sublayer
	IEEE 802.11	MAC Sublayer
Physical	IEEE 802.11p	Physical

3.1.1. IEEE 1609 Standard: Organization of WAVE IEEE 1609 standard is categorized as shown in figure 5, 6:

3.1.1.1. IEEE P1609.0 (Draft Standard for WAVE): IEEE P1609.0 standard guides necessary services for multichannel DSRC/WAVE devices to communicate with high mobile devices.

3.1.1.2. IEEE 1609.1 (Trail Standard for WAVE) (Resource management): It defines the services and interfaces of WAVE applications. It also describes data and management services, communication message format, storage format, status, and request message format to communicate with its component and other wireless devices.

3.1.1.3. IEEE 1609.2 (Trail use of the standard for WAVE) (Security Services): IEEE 1609.2 standard defines security services, message format, and processing methods for devices using WAVE/DSRC standard. This standard also defines the situation where secure message exchange is called and authenticate to process those messages.

3.1.1.4. IEEE 1609.3 (Trail use of the standard for WAVE) (Network Services): Network layer and transport layer resources are specified by IEEE 1609.3, including addressing and routing through WAVE data exchange support. It also offers a data stream through WAVE data exchange, which acts as an alternative to IPv6. [68].

3.1.1.5. IEEE 1609.4 (Trail use of the standard for WAVE) (Multi-channel operation): IEEE 1609.4 describes routing, management, and switching services. It is an enhancement of IEEE 802.11 to support WAVE standard.

3.1.1.6. IEEE 1609.11 (Over the air data exchange for ITS): IEEE 1609.11 ensures service and secure message transmission, which is necessary for electronic payment.

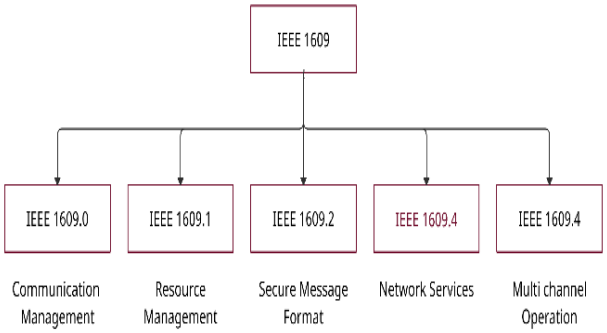

Figure 5: IEEE 1609 Structure

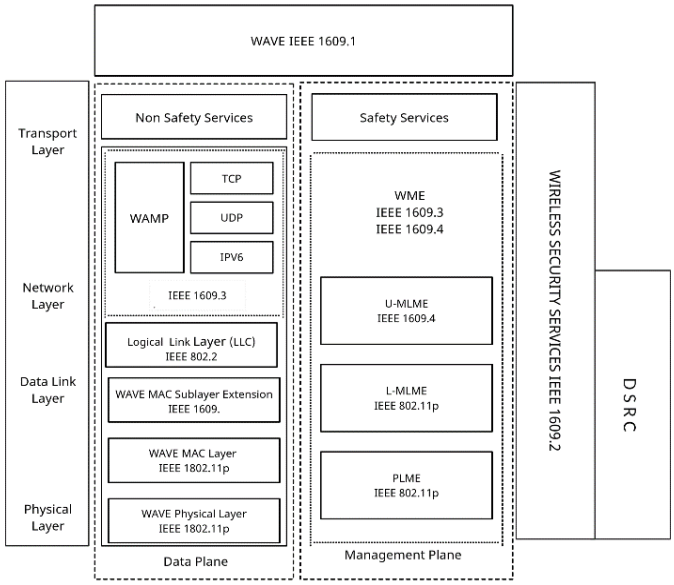

Figure 6: Wireless Access for Vehicular Environment (WAVE) Architecture

3.2. The VANET Architecture: VANET is a self-organizing infrastructure-less network where each vehicle connects with other vehicles or stable Road Side Units (RSUs). The vehicle on the network moves independently, considering any reason, vehicle applies the brake and connects with new neighbors.

The task to establish a connection is achieved by a group of communications represented in figure 7. Initially, all the vehicles must be equipped with On-board units (OBUs) (device mounted on the vehicle for communication) and WSNs to communicate with vehicles and infrastructure; afterward, vehicles may communicate among other vehicles by Vehicle to Vehicle (V2V) communicate and with RSU by Vehicle to Infrastructure (V2I) communication [69]. In this way, VANET assures guided, secure communication and ensures passenger's safety. VANET also provides listed services:

3.2.1. Information Support: Information of vehicle condition like vehicle speed, fuel, rainfall alert, road condition, etc.

3.2.2. Smart Assistance: Smart assistance guide information about navigation, collision alert, etc.

3.2.3. Warning Notice: Critical life-saving information like an emergency, accident alert, adverse traffic, unfavorable road condition, etc.

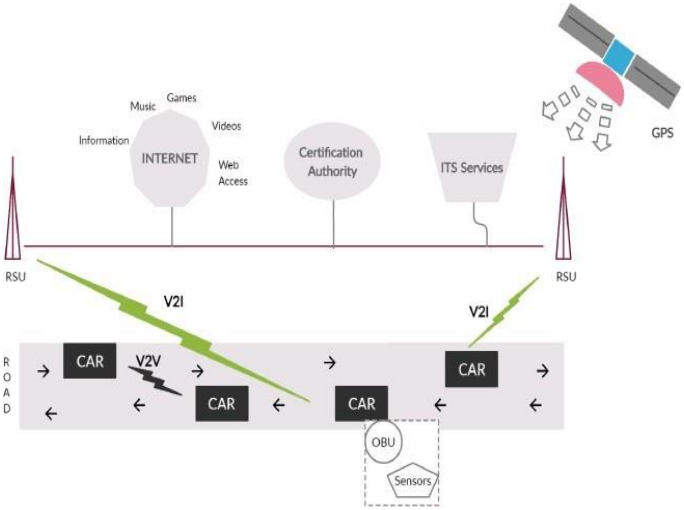

Figure 7: Architecture of VANET [74]

3.3. VANET Components: Different components are involved in the deployment of VANET; some primary components are outlined below.

3.3.1. Vehicle: The very primary component of VANET is the vehicle which is independent to move in any direction. The vehicle are equipped with On-Board Units (OBUs) having dual interfaces. The first interface is for Wi-Fi Network, and the second is for GSM Network [70], as shown in figure 8. The vehicle is equipped with number of sensors that may scare manufacturer and designers although its crucial to understand that passenger safety is more than anything else. It's necessary to design a state of art machine which guarantees passenger safety and experience.

3.3.2. Road Side Units (RSUs): RSUs are placed in the green whose hardships are to manage all vehicles in its region and maintain communication with neighbor RSUs and base station [71].

3.3.3. Dual-mode OBU: On-board units are communication devices equipped on vehicles. It allows vehicles to communicate with other vehicles on the road and with RSU. Dual-mode OBU provides dual-mode wireless communication simultaneously.

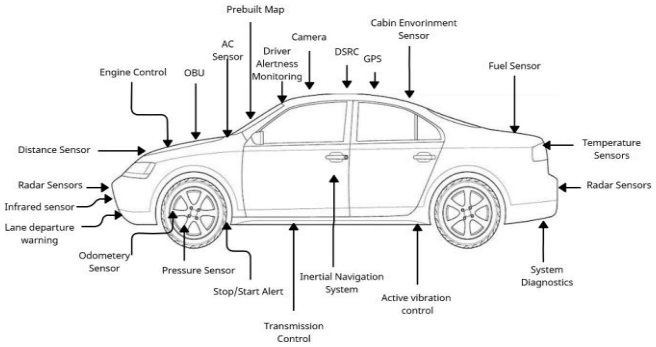

Figure 8: Smart Vehicle

3.3.4. Tamper Proof Device: A tamper-proof device is a unique device mounted on a vehicle that stores confidential information about the vehicle. Tamper-proof devices store the private key to decrypt and authenticate messages proportionally signs outgoing messages.

3.3.5. GSM Network: Global System for Mobile Communication is ETSI standard for fully optimized telephonic communication.

3.3.6. Base Station: Base stations are the central data management component that connects and communicates with multiple RSUs.

3.4. Routing Protocols: The nature of VANET is highly mobile; connectivity is a significant concern. As we know, the vehicle in a network moves with fast speed and may have different directions. Additionally, the density of vehicles in the network dynamically changes; these all-challenges spur on researchers to develop fast and robust routing protocols [72]. Some routing protocols used in VANET are shown in Table 4:

Table 4: Comparison of Routing protocols of VANET

Attributes	Protocols				
	Topology-Based Routing Protocol	Broadcast-Based Routing Protocol	Geo Cast Routing Protocol	Position-Based Routing Protocol	Cluster-Based Routing Protocol
Packet forwarding	Wireless Multi-hop Forwarding	Wireless Multi-hop Forwarding	Wireless Multi-hop Forwarding	Heuristic Method	Wireless Multi-hop Forwarding
Recovery Method	Multi hop forwarding (Proactive Protocols) and carry and forward (Reactive Protocols)	Carry and forward	Forwarding	Carry and forward	Carry and forward
Digital Map Requirement	No	No	No	No	Yes
Virtual Interface Requirement	No	No	No	No	Yes
Environment	Urban	Highway	Highway	Urban	Urban
Realistic Traffic Flow	Yes	Yes	Yes	Yes	No

3.4.1. Topology-Based Routing Protocol: Topology-based routing protocols use link information for communication. This routing protocol is divided into three categories:

3.4.1.1. Proactive routing protocol: A proactive routing protocol is continuously computing routes and maintains an updated routing table. Simultaneously uses the shortest distance to reach the destination employing Distance Vector Routing Protocol (DSDV) or Link State Routing Protocol (LSR). A network's routing table is maintained after a fixed interval irrespective of the path getting used or not. This leads to excessive bandwidth consumption as proactive routing protocol is inappropriate in a dynamic network like VANET.

3.4.1.2. Reactive Routing Protocols: Reactive routing protocols are also known as on-demand routing protocols as they search for paths when a request is generated and maintains only currently used paths. This approach saves bandwidth consumption and excessive path management in the routing table (less memory is required). Various routing protocols have been proposed. Some of them are Dynamic Source Protocol (DSR), Ad-hoc On-demand Distance Vector Routing Protocol (AODV) and, Pretty Good Protocol (PGP).

3.4.1.3. Hybrid Routing Protocols: Hybrid routing protocol adapts advantages of proactive and reactive routing protocol. A Proactive routing protocol is used for local search and reactive for global search. A Hybrid routing protocol is effective in some means, but it consumes high latency to establish a new path. Zone Routing Protocol (ZRP), Landmark Ad-hoc Routing (LANMAR), Distributed Spanning Tree (DST), Fisheye State Routing (FSR) are some Hybrid Routing Protocols.

3.4.2. Broadcast Routing Protocols: The working principle of broadcast routing protocol is to flood packets over the entire network, pretending that only legitimate receivers will accept that, and the rest will drop the packets. The broadcast routing protocol is used for announcements like transmitting climate conditions, road conditions, emergency warning messages, advertisements, etc. Some broadcast routing protocols are Distributed Vector Broadcast Protocol (DV-CAST), Density Aware Reliable Broadcasting Protocol (DECA), Position Aware Reliable Broadcasting Protocol (POCA) [73].

3.4.3. Geo Cast Routing Protocols: Geo Cast is a location-based routing protocol. This protocol divides the network into Zone of Relevance (ZOR) and Zone of Forwarding (ZOF). Zone of Relevance ensures communication between ZOR vehicles. If a vehicle wants to initiate communication with non-ZOR vehicles, it will turn out to be part of Zone of Forwarding (ZOF). The vehicle that becomes a part of ZOF has the liability for transmitting information to ZORs. Some Geo Cast Routing Protocols are GeoGrid, IVG, GeoNode, GeoTORA, DRG, DEG-CASTER [75].

3.4.4. Position-Based Routing Protocols: In this routing protocol, geographical information of the vehicle is utilized to determine the exact position. It provides reliable and efficient routing using the Global Positioning System (GPS) and location information of vehicles. Packets are transmitted to the destination via the geographically nearest vehicle. This type of protocol is efficient as global route discovery and maintenance is not required. Some Position-Based Routing Protocols: Distance Routing Efficient Algorithm for Mobility (DREAM), Grid Location Service (GLS), Location Aided Routing (LAR), and Greedy Perimeter Stateless Routing (GPSR) [76].

3.4.5. Cluster-Based Routing Protocols: These protocols work on clusters. Vehicles with identical characteristics like vehicle speed and trajectory are coupled in a cluster; each cluster has its cluster head, which coordinates with vehicles on the same cluster. Cluster is in coordination with cluster gateway to communicate with other clusters. Every cluster is allocated with two cluster heads and two cluster gateways, whereas a single cluster head and cluster gateway actives for a time being. When a cluster head disjoints, another cluster head becomes the main cluster head. Some Cluster Based Routing Protocols: Cluster for Open Inter Vehicular Communication Network (COIN), Low Energy Adaptive, Cluster Hierarchy (LEACH), Hybrid Energy Efficient Distributed (HEAD), Base Station Controlled Dynamic Clustering Protocol (BCDCP) [77].

3.5. Characteristic of VANET: VANET is a subset of MANET, as we know; VANET is equipped with all the characteristics of MANET and is also uniquely fitted with many characteristics. Listed below are some characteristics of VANET:

3.5.1. High Mobility: The fast-moving world of vehicles increased the difficulties in tracking and distributing emergency Information Systems (EIS).

3.5.2. Network Topology: Generally, vehicles move at a breakneck speed on highways and change direction randomly

because of this topology changes rapidly, which causes intermittent communication links [78].

3.5.3. Location Information: Global Positioning System (GPS) is installed in all Smart vehicles, which accredit the network to transfer information accurately. GPS also incorporate to reduce latency and increase throughput [79].

3.5.4. Network Size: Practically there is no boundary for VANET; it can be as small as a city and as big as a country or beyond. So, there is no geographical limitation for VANET [80].

3.5.5. Energy Efficient: Compared to other wireless ad-hoc network wings, VANET vehicles (nodes) have an unlimited power supply.

3.6. Application of VANET: A momentary communication in the network between vehicles allows real-time applications to offer services on the go. The VANET classifies application into three categories:

3.6.1. Safety Applications: Safety applications reserve foremost priority among others as these applications aimed to reduce road accidents and save human lives by exchanging safety messages with nearby vehicles and RSUs. These applications inform drivers about surrounding vehicles, road conditions, weather conditions, fatigues in the vehicle, and others [81]. Listed below are some safety applications:

3.6.1.1. Slow or stop vehicle alert
3.6.1.2. Emergency brake light
3.6.1.3. Post-crash notification
3.6.1.4. Cooperative collision warning
3.6.1.5. Lane change warning

3.6.2. Convenience Applications: Convenience application ensures all the applications to make a trip genuinely complete with minimum effort and time. Below are some convenience applications:

3.6.2.1. Congested road notification
3.6.2.2. Tool booth collections
3.6.2.3. Parking availability notification

3.6.3. Commercial Applications: Commercial applications inform the driver about the vehicle's status and offer amusement through online advertising services. [82].

3.6.3.1. Vehicle Diagnostic
3.6.3.2. Service announcement
3.6.3.3. Real-time video on demand

3.7. Challenges in VANET: Due to the diverse nature of VANETS, its security and communication system are incredibly diverse, and inconsequence VANET faces unusual tribulations. Broadly these challenges are categorized into Technical and Social challenges. Listed are some security challenges that need to be encountered to implement a safe and secure network [83]:

3.7.1. Mobility: High mobility invites frequent link connectivity and dis-connectivity among fast-moving vehicles, which makes communication highly unreliable. Therefore, VANET requires less complicated algorithms that can sustain high mobility and miscellaneous volume of vehicles.

3.7.2. Volatility: As we know, the vehicle in VANET moves with high velocity; therefore, connections are managed and establish for a concise duration of time. This makes it challenging to authenticate vehicles and apply all the security checks.

3.7.3. Latency Control: Latency is the round-trip time between devices. It's a common practice to create a protocol that guarantees nearly zero latency. Although transmission medium, propagation, storage delay, processing delay are some factors that alter latency parameters.

3.7.4. Network Scalability: VANET is an extensive network covering countries though control of such heterogeneous networks is a big concern. Pre-stored information is insufficient to handle real-time networks, so there must be some uniform global mechanism to check protocols, services, and applications.

3.7.5. Error Tolerance: VANET relies on protocols to alert drivers for fatigue and accidents while providing services for news and entertainment. So, a mistake in protocols can crash down the whole network harshly. Consequently, protocols need to be designed to consider these issues.

3.8. Risk Factor: Probably all attacks in a wireless network are possible in VANET, although all attacks rely on various factors [84]:

3.8.1. Attacker Motivation: An attacker's motive in VANET is one of the most vital factors to achieve a triumphant attack. Significantly higher is the attackers' motivation, the risk to a network is more elevated.

3.8.2. The Target of Attack: Unless the attacker discovers any vulnerability in VANET, an attacker can't launch an attack. Initially, an attacker passively monitors vulnerabilities and afterwards launches an attack. Vulnerability, for instance, protocols, gateways, hardware, and misconfiguration in components.

3.8.3. Attacker's Budget: The budget of an attacker is an important constraint. To impose an attack, an attacker requires high-end hardware and software, i.e., bypass software, signal jammer, firewall cracker, password cracker, conqueror hardware, and others.

3.8.4. Time: Time represents the total time requires to launch a successful attack. In VANET, information gathering is a tedious task, as vehicles move fast and communicate for a short period. Hence, the attacker needs to activate and launch an attack within a specific time frame only.

3.8.5. Personal Reputation: Higher is the attacker's reputation may motivate the attacker to launch more destructive attacks. As well as reputation is also linked with the attacker's motivation, which facilitates the attacker to target a victim, find vulnerabilities, and launch an attack [85].

3.9. Attacks on VANET: Like other wired and wireless networks, VANET is also vulnerable to attacks. Attacks compromise security protocols either by manipulating the vehicular system or by negotiating network security protocols. In the subsequent section, we have explained various security attacks possible on VANET.

3.9.1. Denial of Service (DOS) Attack: Denial of service is a widespread active and malicious attack in nature. The attacker transmits dummy messages to overload the network or bring a network down. This may cause a distraction to the driver, which leads to an accident. DOS attacks can be launched in many ways by transmitting bogus information that causes

inappropriate results or by jamming communication channels [86].

3.9.2. Double Denial of Service (DDOS) Attack: A DDOS attack is somewhat similar to a DOS attack with more catastrophic damage. In a DDOS attack, attackers launch attacks on the network in different timeslots from multiple geographical locations. Since the attacker uses different time slots and multiple geographical locations thus, this attack is one of the most challenging attacks to track.

3.9.3. Black Hole Attack: Malicious node publicizes itself in the network as having an optimum path to reach the destination. Packets transmitted by legitimate vehicles will redirect to some unauthorized entity or drop by a malicious vehicle.

3.9.4. Wormhole attack: The attacker connects two remote vehicles through a communication channel, i.e., a tunnel. Thus, legitimate vehicles are deemed neighbors of legitimate vehicles and start transmitting data by virtual tunnel set up by a malicious node. The aforementioned strategy threatens the confidentiality and availability of packets.

3.9.5. Timing Attack: Information is valuable if available on time. Numerous security applications were running on VANET that require a live update of nearby vehicles, environment, and emergency services, so a slight delay may formulate a serious miss happening. A timing attack is one of the new attacks where the attacker neither alters the packet nor transmits packets to an unauthorized vehicle. In contrast, the attacker adds multiple time slots on the original message packet to fabricate delay.

3.9.6. Location Attack: This attack is in concern to privacy. The attacker tracks the vehicle to obtain driver's personal information, geographical location, and trajectory.

3.9.7. Masquerade: Every vehicle receives a unique identity in VANET, which restricts vehicle authentication legitimacy. Malicious vehicle impersonates and popularizes to be another vehicle by adapting false identity.

3.9.8. Social Attack: Primarily attacker aims to distract the driver concentration and make the driver angry. Unmoral messages, i.e., You are an Idiot Driver, are transferred to the victim's vehicle to make the driver angry, facilitating drivers to take unusual action.

3.9.9. Man in Middle Attack: Man in the middle attack is an attack on confidentiality and integrity. A malicious vehicle manages itself between communicating vehicles, where a malicious vehicle listens and injects bogus information between communicating vehicles.

3.9.10. Sybil Attack: Sybil attack is a severe threat to VANET, where intruders fabricate vehicle identities. Sybil nodes impersonate their identities by stealing the vehicle's identity or creating fake identities, as VANET is a highly dense and mobile network, which helps attackers create an illusion of the presence of multiple authenticated vehicles in the network.

4. SYBIL ATTACK

John R. Douceur first examined the Sybil attack in context to the peer-to-peer system. VANET is vulnerable to multiple attacks, although the Sybil attack is the most catastrophic attack to demolish the security and confidentiality of VANET, as shown in figure 9. In a nutshell, the Sybil attack generates multiple fabricated identities that act as multiple inimitable vehicles in the network. Generation of fabricated identities relies solely on the attacker's capabilities, i.e., an attacker may forge identities, theft, and share identities. Wireless networks are affected by Sybil attacks. The researchers have proposed an efficient method for separating valid RSSI observations of a node from malicious participants. A challenge-response defence mechanism was also proposed. The real-world scenarios were observed [87].

Sybil attacks may harm catastrophic real-time applications. For example, a malicious vehicle fabricates multiple vehicles in the network and transmits incorrect road conditions; legitimate vehicles believe that message was genuine, coming from multiple vehicles and reacting in response to the message received. In such a way, malicious vehicles get exclusive access to the road, which was impossible otherwise. In addition, the Sybil attack also influences voting base events, unfair use of shared resources, Sybil vehicle influence legitimate node to gain personal benefit, aggregation of data, routing.

Some genuine issues are explicated below:

I. *Voting:* Sybil attackers generate fabricated identities as many as they want, participating in voting and facilitating results.

II. *Shared Resources:* Resources are allocated among legitimate vehicles. In the presence of Sybil vehicles fare resource allocation is impractical.

III. *Personal Benefit:* Sybil nodes report legitimate vehicles as malicious vehicles because of which RSUs block legitimate vehicles. This issue is in concern to gain personal benefit.

IV. Aggregation of Data: Sybil nodes eagerly pass incorrect information to fabricate overall calculated data.

V. *Routing:* Communication among vehicles is possible through information received from its neighbors. A Sybil neighbor vehicle will pass incorrect routing information to access transmitted data packets.

Currently, Sybil attack detection and elimination, gain the attention of research scholars and scientists to work on it. Many Sybil attack detection and elimination mechanisms have been proposed; here in this paper, we review some of them:

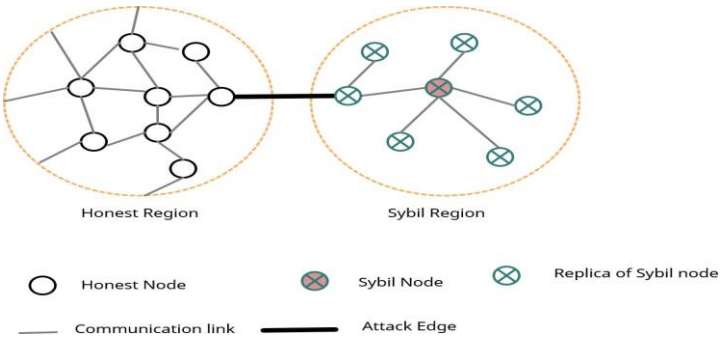

Figure 9: Sybil Attack

4.1. Trust Device: Like a trust certificate, a trust device is a physical equipment equipped in a previously coated device with certificates and keys to manage secure communication. Since every message authenticates by a trusted device, it is potentially problematic for attackers to obtain credentials. The authors proposed a new algorithm to identify Sybil nodes in a static and dynamic manner. The Sybil nodes were detected to improve the security of wireless networks [88].

4.2. Resource Testing: We can't detect Sybil attacks via message tracking solely; therefore, the author proposed a mechanism to monitor vehicle resources (computational resources, radio resources, and memory resources) and locate vehicles transmitting messages through shared resources and receiving the signal on shared sources. This mechanism is inadequate since the malicious vehicles may fabricate multiple resources [89].

4.3. Signal Strength: This mechanism calculates the signal strength captured from vehicles of the network. The illustrated scheme is a combination of three components: claimer, witness, and verifier. The claimer periodically broadcasts a beacon message encapsulated with the claimed position; the witness vehicle collects all claimers' beacon messages and calculates estimated distance using signal strength. Verifier vehicles gather all received signals and compare claimed distance with predicted distance. If the verifier found a distance disparity, mark the vehicle as Sybil vehicle [90].

4.4. Domain-Specific: Domain-specific information is required to detect the Sybil node. It is assumed that if the Sybil node attacks the network, all Sybil vehicles move in the same direction with the same speed in a specific domain. Moreover, network trackers track vehicles moving in specific domains with identical trajectories, driving patterns, and alert RSUs concerning Sybil nodes. The various other techniques for detecting Sybil attacks in Wireless Sensor Networks were studied and analyzed [91].

4.5. Neighbor List Method: This method is one of the fresh approaches to detect Sybil vehicles. After specific intervals vehicles in the network transmit HELLO messages to their adjacent neighbors, all the vehicles are bound to respond to HELLO messages; the HELLO messages generator vehicle constructs a list of adjacent vehicles. According to this method, if a specific vehicle is a neighbor for a longer duration, then mark the vehicle as a suspected vehicle and generate an alert signal to inform legitimate nodes about the presence of the suspected vehicle [92].

5. CONCLUSION

The Wireless Sensor Network (WSN) is vulnerable to attacks. There are different kinds of attacks possible in VANET. The communication may be between multiple wireless nodes, and it is infrastructure less. The devices may be connected randomly and connected directly to one another using an intermediate node. Communication in Wireless Sensor Network (WSN) is possible through sensors only. The wireless sensor network is decentralized, and one node in WSN will be connected to the router, and other nodes may be connected with the neighbor node. Various security challenges in WSN like confidentiality, integrity, availability, authentication, non-repudiation, etc. The issues like mobility, quality of service, bandwidth, and security is also a problem. Various routing protocols are helpful for data communication between source to the destination like proactive, reactive, and hybrid.

The VANET is a part of a wireless network that communicates among groups of vehicles in the absence of central authority. The VANET is a self-organized network used for Direct Short-Range Communication (DSRC) to communicate with vehicles and Roadside Units (RSU). The VANET offers high mobility, efficient communication, dynamic network topology, etc. The challenges in VANETs are random change in topology, latency, scalability, fault-tolerant network, attacks, etc. A brief overview of security challenges in VANETs and various attacks was also discussed in the presented work.

REFERENCES

[1] Nguyen Tran, Jinyang Li, Lakshminarayanan Subramanian, and Sherman S.M. Chow. "Optimal sybil-resilient node admission control" In The 30th IEEE International Conference on Computer Communications (INFOCOM 2011), Shanghai, P.R. China, 2011.

[2] Dai Nguyen, H.P. Zolt a'n, R., "The Current Security Challenges of Vehicle Communication in the Future Transportation System" In Proceedings of the 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), Subotica, Serbia, 13–15 September 2018; pp. 000161–000166.

[3] M. Faizan, R. A. Khan, A. Agrawal, "Ranking potentially harmful Tor hidden services: Illicit drugs perspective." Applied Computing and Informatics, 2020.

[4] M.S. Abdalzaher et. al, "Game theory meets wireless sensor networks security requirements and threats mitigation: a survey," Sensors, vol. 16, no. 7, pp. 1003, 2016.

[5] S. K. Shah, S. S. Panchal and D. Vishwakarma," Study of the Effect of Change in Power on Parameters of Reactive Protocol Implemented Using MATLAB Based True Time Network Simulator for WANET," 2010 International Conference on Computational Intelligence and Communication Networks, Bhopal, 2010, pp. 183-187, doi: 10.1109/CICN.2010.46.

[6] Z. Ismail and R. Hassan," A performance study of various mobility speed on AODV routing protocol in homogeneous and heterogeneous MANET," The 17th Asia Pacific Conference on Communications, Sabah, 2011, pp. 637-642, doi: 10.1109/APCC.2011.6152886.

[7] Leslie D. Fife and Le Gruenwald. 2003. Research issues for data communication in mobile ad-hoc network database systems. SIGMOD Rec. 32, 2 (June 2003), 42–47. DOI: https://doi.org/10.1145/776985.776991.

[8] H. Su and X. Zhang, "Cross-layer based opportunistic MAC protocols for QoS provisioning's over cognitive radio wireless networks," IEEE J. Select. Areas Commun., vol. 26, no. 1, pp. 118–129, Jan. 2008.

[9] Kumar, N., Iqbal, R., Misra, S., & Rodrigues, J. J. "An intelligent approach for building a secure decentralized public

key infrastructure in VANET" Journal of Computer and System Sciences, 81(6), 1042-1058.

[10] Ankit Agrawal and A. K. Verma. 2016. A review & impact of Trust Schemes in MANET. In Proceedings of the International Conference on Advances in Information Communication Technology & Computing (AICTC' 16). Association for Computing Machinery, New York, NY, USA, Article 26,1–7.

[11] M. Razfar et al.," Wireless network design and analysis for real time control of launch vehicles," IEEE International Conference on Wireless for Space and Extreme Environments, Baltimore, MD, 2013, pp. 1-2, doi: 10.1109/WiSEE.2013.6737574.

[12] P. Li, C. Xu, H. Xu, L. Dong and R. Wang," Research on data privacy protection algorithm with homomorphism mechanism based on redundant slice technology in wireless sensor networks," in China Communications, vol. 16, no. 5, pp. 158-170, May 2019.

[13] Adrian Perrig, John Stankovic, and David Wagner. 2004. Security in wireless sensor networks. Commun. ACM 47, 6 (June 2004), 53–57. DOI: https://doi.org/10.1145/990680.990707

[14] Lili Qiu, Paramvir Bahl, Ananth Rao, and Lidong Zhou. 2006.Troubleshootingwireless mesh networks. SIGCOMM Computer. Communication, Rev.36, 5 (October2006),17–28. DOI: https://doi.org/10.1145/1163593.1163597

[15] N. Tatebe, K. Hattori, T. Kagawa, Y. Owada and K. Hamaguchi," Energy-efficient construction algorithm for mobile mesh networks," The 20th Asia-Pacific Conference on Communication (APCC2014), Pattaya, 2014, pp. 73-77, doi: 10.1109/APCC.2014.7091608.

[16] S. Pandi, S. Wunderlich and F. H. P. Fitzek," Reliable low latency wireless mesh networks — From Myth to reality," 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, 2018, pp. 1-2, doi: 10.1109/CCNC.2018.8319326.

[17] C. Chen, Z. Huang, Q. Wen and Y. Fan," A novel dynamic key management scheme for wireless sensor networks," 2011 4th IEEE Inter- national Conference on Broadband Network and Multimedia Technology, Shenzhen, 2011, pp. 549-552, doi: 10.1109/ICBNMT.2011.6155995.

[18] M. W. Khan and M. Faisal, “Security Attributes prioritization using Fuzzy Analytic Network Process” Journal of Critical Reviews, Vol. 7, Issue 11, pp.2080-2096, 2020.

[19] M. W. Khan, D. Pandey and S. A. Khan, “Critical Review on Software Testing: Security Perspective”, Smart Trends in Information Technology and Computer Communications in Springer CCIS series, pp.714-713, Jaipur, India, 2016.

[20] M. W. Khan, D. Pandey and S. A. Khan, “Test Plan Specification using Security Attributes”, in ICIC Express Letters, An International Journal of Research and Surveys, Volume- 12, No. 9, 2018.

[21] M. W. Khan, D. Pandey and S. A. Khan, “Measuring the Security Testing Attributes through Fuzzy Analytic Network Process: A Design Perspective”, Journal of Advanced Research in Dynamical and Control Systems (JARDCS), special issue12, pp.1514-1523, 2018.

[22] M. W. Khan and D. Pandey, “Revisiting Software Security Models: A Design Perspective”, International refereed research journal, Academic Social Research, Volume-2, Issue-1, January to March 2016.

[23] M. W. Khan, S. Sankhwar and V. Singh, “Security Testing Profile: An Introduction”, National conference on Information Security Challenges (NCISC-2016), 24th Feb 2016, Lucknow.

[24] Yi Yang and Rajive Bagrodia. 2009. Evaluation of VANET-based advanced intelligent transportation systems. In Proceedings of the sixth ACM international workshop on VehiculAr InterNETworking (VANET' 09). Association for Computing Machinery, New York, NY, USA, 3–12. DOI: https://doi.org/10.1145/1614269.1614273

[25] A. K. Goyal, A. Kumar Tripathi and G. Agarwal," Security At- tacks, Requirements and Authentication Schemes in VANET," 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), GHAZIABAD, India, 2019, pp. 1-5, doi: 10.1109/ICICT46931.2019.8977656.

[26] V. Hemamalini, G. Zayaraz, V. Susmitha and V. Saranya," An Efficient Probabilistic Authentication Scheme for Converging VANETs," 2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM), Tindivanam, 2017, pp. 147-152, doi: 10.1109/ICRTCCM.2017.40.

[27] R. Krishnan P. and A. R. Kumar P.," Security and Privacy in VANET: Concepts, Solutions and Challenges," 2020 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2020, pp. 789-794, doi: 10.1109/ICICT48043.2020.9112535.

[28] S. Hayat, X. Liu, Y. Li and Y. Zhou," Comparative Analysis of VANET's Routing Protocol Classes: An Overview of Existing Routing Protocol Classes and Futuristic Challenges," 2019 IEEE 2nd International Conference on Electronics Technology (ICET), Chengdu, China, 2019, pp. 1-7, doi: 10.1109/ELTECH.2019.8839402.

[29] S. A. Khan, M. W. Khan and D. Pandey, “A Fuzzy Multi-Criteria Decision-Making for Managing Network Security Risk Perspective”, Cloud-Based Data Analytics in Vehicular Ad-Hoc Networks, IGI Global, pp.115-140, 2020

[30] Syed A. Khayam and Hayder Radha. 2004. Analyzing the spread of active worms over VANET. In Proceedings of the 1st ACM international workshop on Vehicular Ad Hoc networks (VANET' 04). Association for Computing Machinery, New York, NY, USA, 86–87. DOI: https://doi.org/10.1145/1023875.1023889

[31] Muhammad Noman Javed, Hammad Shafiq, Khubaib Amjad Alam, Abid Jamil, and Muhammad Umar Sattar. 2019. VANET's Security Con- cerns and Solutions: A Systematic Literature Review. In Proceedings of the 3rd International

Conference on Future Networks and Distributed Systems (ICFNDS' 19). Association for Computing Machinery, New York, NY, USA, Article 40, 1–12. DOI: https://doi.org/10.1145/3341325.3342028

[32] Alan Said, Domonkos Tikk, and Andreas Hotho. 2012. The challenge of recommender systems challenges. In Proceedings of the sixth ACM conference on Recommender systems (RecSys' 12). As- sociation for Computing Machinery, New York, NY, USA, 9–10. DOI: https://doi.org/10.1145/2365952.2365959

[33] Piotr Szczurek, Bo Xu, Ouri Wolfson, and Jie Lin. 2012. A method- ology for the development of novel VANET safety applications. In Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications (VANET' 12). Association for Computing Machinery, New York, NY, USA, 119–122.DOI: https://doi.org/10.1145/2307888.2307911

[34] W. A. Hussein, B. M. Ali, M. F. A. Rasid and F. Hashim," Design and performance analysis of high reliability-optimal routing protocol for mobile wireless multimedia sensor networks," 2017 IEEE 13th Malaysia International Conference on Communications (MICC), Johor Bahru, 2017, pp. 136-140, doi: 10.1109/MICC.2017.8311747.

[35] S.M. Faisal, A.K. Vajpayee, "Extended Zone Routing Protocol", International Journal of Computer Sciences and Engineering (IJCSE), Volume-5, Issue-5, May 2017.

[36] J. Hao, G. Duan, B. Zhang and C. Li," An energy-efficient on-demand multicast routing protocol for wireless Ad Hoc and sensor networks," 2013 IEEE Global Communications Conference (GLOBECOM), Atlanta, GA, 2013, pp. 4650-4655, doi: 10.1109/GLOCOMW.2013.6855685.

[37] L. Hu, Y. Li, Q. Chen, J. Liu and K. Long," A New Energy-Aware Routing Protocol for Wireless Sensor Networks," 2007 International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, 2007, pp. 2444-2447, doi: 10.1109/WICOM.2007.609.

[38] P. Goswami and A. D. Jadhav," Evaluating the performance of routing protocols in Wireless Sensor Networks," 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12), Coimbatore, 2012, pp. 1-4, doi: 10.1109/ICC-CNT.2012.6396097.

[39] M. Piechowiak, P. Zwierzykowski, P. Owczarek and M. Wasłowicz," Comparative analysis of routing protocols for wireless mesh networks," 2016 10th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), Prague, 2016, pp. 1-5, doi: 10.1109/CSNDSP.2016.7573902.

[40] M. Sana and L. Noureddine," Multi-hop energy-efficient routing proto- col based on Minimum Spanning Tree for anisotropic Wireless Sensor Networks," 2019 International Conference on Advanced Systems and Emergent Technologies (IC ASET), Hammamet, Tunisia, 2019, pp. 209-214, doi: 10.1109/ASET.2019.8871032.

[41] C. Jiang, Y. Ren, Y. Zhou and H. Zhang," Low-Energy Consumption Uneven Clustering Routing Protocol for Wireless Sensor Networks," 2016 8th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC), Hangzhou, 2016, pp. 187-190, doi: 10.1109/IHMSC.2016.214.

[42] M. M. E. A. Mahmoud, X. Lin and X. Shen," Secure and reliable routing protocols for heterogeneous multi-hop wireless networks," in IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 4, pp. 1140- 1153, April 2015, doi: 10.1109/TPDS.2013.138.

[43] H. Ben Fradj, R. Anane, M. Bouallegue and R. Bouallegue," A range-based opportunistic routing protocol for Wireless Sensor net- works," 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, 2017, pp. 770-774, doi: 10.1109/IWCMC.2017.7986382.

[44] A. Solanki and N. B. Patel," LEACH-SCH: An innovative routing protocol for wireless sensor network," 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, 2013, pp. 1-5, doi: 10.1109/ICCCNT.2013.6726641.

[45] Sheetalkumar Doshi, Shweta Bhandare, and Timothy X Brown. 2002. An on-demand minimum energy routing protocol for a wireless Ad Hoc network. SIGMOBILE Mob. Comput. Commun. Rev. 6, 3 (July 2002), 50–66. DOI: https://doi.org/10.1145/581291.581300.

[46] Nguyen Thi Thu Hang and Nguyen Tien Ban. 2017. Hybrid Routng Protocol and Dynamic Delivering Scheme for Multi Event Wireless Sensor Network. In Proceedings of the Eighth International Symposium on Information and Communication Technology (SoICT 2017). Association for Computing Machinery, New York, NY, USA, 286–292. DOI: https://doi.org/10.1145/3155133.3155192.

[47] T. Zaidi and S. Faisal," An overview: Various attacks in VANET," The 4th International Conference on Computing Communication and Automation (IC-CCA'18), pp. 1-6, 2018.

[48] H. Shen and X. Ye," Research on the Location Attack Based on Multiple Counterfeit Identities Technology in Sensor Networks," 2014 International Conference on Wireless Communication and Sensor Network, Wuhan, 2014, pp. 193-197, doi: 10.1109/WCSN.2014.46.

[49] D. Kim and S. An," PKC-Based DoS Attacks-Resistant Scheme in Wireless Sensor Networks," in IEEE Sensors Journal, vol. 16, no. 8, pp. 2217-2218, April15, 2016, doi: 10.1109/JSEN.2016.2519539.

[50] H. Wang, G. Yang, J. Xu, Z. Chen, L. Chen and Z. Yang," A noval data collection approach for Wirelsee Sensor Networks," 2011 International Conference on Electrical and Control Engineering, Yichang, 2011, pp. 4287-4290, doi: 10.1109/ICECENG.2011.6057687.

[51] Sunghyuck Hong and Sunho Lim," Analysis of attack models via Unified Modeling Language in Wireless Sensor Networks: A survey study," 2010 IEEE International Conference on Wireless Communications, Networking and

Information Security, Beijing, 2010, pp. 692-696, doi: 10.1109/WCINS.2010.5541868.

[52] B. Tian, Y. Yao, L. Shi, S. Shao, Z. Liu and C. Xu," A novel sybil attack detection scheme for wireless sensor network," 2013 5th IEEE International Conference on Broadband Network & Multimedia Technology, Guilin, 2013, pp. 294-297, doi: 10.1109/ICBNMT.2013.6823960.

[53] N. Siasi, A. Aldalbahi and M. A. Jasim," Reliable Transmission Scheme Against Security Attacks in Wireless Sensor Networks," 2019 International Symposium on Networks, Computers and Communications (ISNCC), Istanbul, Turkey, 2019, pp. 1-6, doi: 10.1109/ISNCC.2019.8909123.

[54] C. Tumrongwittayapak and R. Varakulsiripunth," Detecting sinkhole at- tack and selective forwarding attack in wireless sensor networks," 2009 7th International Conference on Information, Communications and Signal Processing (ICICS), Macau, 2009, pp. 1-5, doi:10.1109/ICICS.2009.5397594.

[55] M. Kaur and A. Singh," Detection and Mitigation of Sinkhole Attack in Wireless Sensor Network," 2016 International Conference on Micro- Electronics and Telecommunication Engineering (ICMETE), Ghaziabad, 2016, pp. 217-221, doi: 10.1109/ICMETE.2016.117.

[56] D. S. Patil and S. C. Patil," A Novel Algorithm for Detecting Node Clone Attack in Wireless Sensor Networks," 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, 2017, pp. 1-4, doi: 10.1109/ICCUBEA.2017.8463789.

[57] S. Ahmad Salehi, M. A. Razzaque, P. Naraei and A. Farrokhtala," Detection of sinkhole attack in wireless sensor networks," 2013 IEEE International Conference on Space Science and Communication (IconSpace), Melaka, 2013, pp. 361-365, doi: 10.1109/IconSpace.2013.6599496.

[58] R. Sathish and D. R. Kumar," Dynamic Detection of Clone Attack in Wireless Sensor Networks," 2013 International Conference on Communication Systems and Network Technologies, Gwalior, 2013, pp. 501-505, doi: 10.1109/CSNT.2013.110.

[59] C. Chen, L. Hui, Q. Pei, L. Ning and P. Qingquan," An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks," 2009 Fifth International Conference on Information Assurance and Security, Xi'an, 2009, pp. 446-449, doi: 10.1109/IAS.2009.33.

[60] V. C. Manju and K. M. Sasi," Detection of jamming style DoS attack in Wireless Sensor Network," 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, Solan, 2012, pp. 563-567, doi:10.1109/PDGC.2012.6449882.

[61] V. Shakhov," On a new type of attack in wireless sensor networks: Depletion of battery," 2016 11th International Forum on Strategic Technology (IFOST), Novosibirsk, 2016, pp. 491-494, doi: 10.1109/IFOST.2016.7884162.

[62] D. Bharti, N. Nainta and H. Monga," Performance Analysis of Wireless Sensor Networks Under Adverse Scenario of Attack," 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 2019, pp. 826-828, doi: 10.1109/SPIN.2019.8711688.

[63] B. Shimpi and S. Shrivastava," A modified algorithm and protocol for Replication attack and Prevention for Wireless sensor Networks," 2016 International Conference on ICT in Business Industry & Government (ICTBIG), Indore, 2016, pp. 1-5, doi: 10.1109/ICTBIG.2016.7892694.

[64] A. Bhatia, K. Haribabu, K. Gupta and A. Sahu," Realization of flexible and scalable VANETs through SDN and virtualization," 2018 International Conference on Information Networking (ICOIN), Chiang Mai, 2018, pp. 280-282, doi: 10.1109/ICOIN.2018.8343125.

[65] S. Hu, Y. Jia and C. She," Performance Analysis of VANET Routing Protocols and Implementation of a VANET Terminal," 2017 International Conference on Computer Technology, Electronics and Communication (ICCTEC), Dalian, China, 2017, pp. 1248-1252, doi: 10.1109/IC-CTEC.2017.00272.

[66] Deeksha, A. Kumar and M. Bansal," A review on VANET security attacks and their counter-measure",2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, 2017, pp. 580- 585, doi: 10.1109/ISPCC.2017.8269745.

[67] R. Kaur, T. P. Singh and V. Khajuria," Security Issues in Vehicular Ad- Hoc Network (VANET)," 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, 2018, pp. 884-889, doi: 10.1109/ICOEI.2018.8553852.

[68] Muhammad Sameer Sheikh, Jun Liang," A Comprehensive Survey on VANET Security Services in Traffic Management System", Wireless Communications and Mobile Computing, vol. 2019, Article ID 2423915, 23 pages, 2019. https://doi.org/10.1155/2019/2423915

[69] A. A. Celes and N. E. Elizabeth, Verification "Based Authentication Scheme for Bogus Attacks in VANETs for Secure Communication," 2018 International Conference on Communication and Signal Processing (ICCSP), Chennai, 2018, pp. 0388-0392, doi: 10.1109/ICCSP.2018.8524540.

[70] Ashley and Steven, “Smart Cars and Automated Highways”, vol. 120, pp 58-62, year 1998. https://doi.org/10.1115/1.1998-May-1

[71] Mohamed Nidhal Mejri, Jalel Ben-Othman, Mohamed Hamdi, "Survey on VANET security challenges and possible cryptographic solutions", Vehicular Communications, Volume 1, Issue 2, 2014, Pages 53-66, ISSN 2214-2096, https://doi.org/10.1016/j.vehcom.2014.05.001.

[72] Mohammad S.A., Rasheed A., Qayyum A. (2011) VANET Architectures and Protocol Stacks: A Survey. In: Strang T., Festag A., Vinel A., Mehmood R., Rico Garcia C., Ro¨ckl M. (eds) Communication Technologies for Vehicles. Nets4Cars/Nets4Trains 2011. Lecture Notes in Computer Science, vol 6596. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-19786-4 9

[73] M. S. Al-kahtani," Survey on security attacks in Vehicular Ad Hoc Networks (VANETs)," 2012 6th International Conference on Signal Pro- cessing and

communication Systems, Gold Coast, QLD, 2012, pp. 1-9, doi: 10.1109/ICSPCS.2012.6507953.

[74] Syed Mohd Faisal and Taskeen Zaidi, "Timestamp Based Detection of Sybil Attack in VANET" International Journal of Network Security, Vol.22, No.3, PP.399-410, May 2020 (DOI: 10.6633/IJNS.202005 22(3).05)

[75] Bagloee, S.A., Tavana, M., Asadi, M. *et al.* Autonomous vehicles: challenges, opportunities, and future implications for transportation policies. *J. Mod. Transport.* 24, 284–303 (2016). https://doi.org/10.1007/s40534-016-0117-3

[76] Sheikh MS, Liang J, Wang W, "A Survey of Security Ser- vices, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs)". Sensors (Basel). 2019;19(16):3589. Published 2019 Aug 17. doi:10.3390/s19163589

[77] Changjiang Jiang, Min Xiang and Weiren Shi," Overview of cluster- based routing protocols in wireless sensor networks," 2011 International Conference on Electric Information and Control Engineering, Wuhan, 2011, pp. 3414-3417, doi: 10.1109/ICEICE.2011.5777573.

[78] Gillani S., Shahzad F., Qayyum A., Mehmood R. (2013), "A Survey on Security in Vehicular Ad Hoc Networks" In: Berbineau M. et.al. (eds) Communication Technologies for Vehicles.ets4Cars/Nets4Trains 2013. Lecture Notes in Computer Science, vol 7865. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-37974-1 5.

[79] Quyoom Abdul, Mir Aftab Ahmad, Sarwar Dr. Abid, "Security Attacks and Challenges of VANETs: A Literature Survey", Journal of Multimedia and Information System, J Multimed Inf Syst 2020;7(1):45-54.

[80] Mahmood A. Al-shareeda, Mohammed Anbar, Selvakumar Manickam, and Iznan H. Hasbullah, "Review of Prevention Schemes for Man-In-The- Middle (MITM) Attack in Vehicular Ad Hoc Networks", Int. j. eng manag. res., vol. 10, no. 3, pp. 153-158, Jun. 2020.

[81] Kumar, R.P., Shanmugam, M. (2019). " A detailed case study on VANET security requirements, attacks and challenges". Advances in Modelling and Analysis B, Vol. 62, No. 2-4, pp. 48-52. https://doi.org/10.18280/ama b.622-403

[82] Saini, Garima and Tripathi, R.C. and Tyagi, Priyanka and Kaushik, Preeti and Aggarwal, Archit," Approach for Detection of Malicious Nodes in VANET (March 15, 2019)". International Conference on Advances in Engineering Science Management & Technology (ICAESMT) - 2019, Uttaranchal University, Dehradun, India, Available at SSRN: https://ssrn.com/abstract=3403953 or http://dx.doi.org/10.2139/ssrn.3403953

[83] Ahmad Yusri Dak, Saadiah Yahya,and Murizah Kassim," A Literature Survey on Security Challenges in VANETs", International Journal of Computer Theory and Engineering, Vol. 4, No. 6, December 2012

[84] S. A. Ansar, S. P. Srivastava, J. Yadav, M. W. Khan, A. Yadav and R. A. Khan, "Estimation of Software Risks through CVSS: A Design Phase Perspective", Turkish Online Journal of Qualitative Inquiry, Vol.12, No.4, 2021.

[85] Jenis Shah, Deven Gol," Survey of Detection Techniques for DOS Attack in VANET", International Journal of Science and Research (IJSR), Volume 6 Issue 3, March 2017, 810 – 812

[86] Vinh Hoa La, Ana Rosa Cavalli. " Security attacks and solutions in Vehicular Ad Hoc Networks: a survey", International journal on AdHoc networking systems (IJANS), 2014, 4 (2), pp.1 - 20.

[87] Y. Liu, D. R. Bild, R. P. Dick, Z. M. Mao and D. S. Wallach, "The Mason Test: A Defense Against Sybil Attacks in Wireless Networks Without Trusted Authorities," in IEEE Transactions on Mobile Computing, vol. 14, no. 11, pp. 2376-2391, 1 Nov. 2015, doi: 10.1109/TMC.2015.2398425.

[88] Wang, C.; Zhu, L.; Gong, L.; Zhao, Z.; Yang, L.; Liu, Z.; Cheng, X. Accurate Sybil Attack Detection Based on Fine-Grained Physical Channel Information. Sensors 2018, 18, 878. https://doi.org/10.3390/s18030878

[89] Mina Rahbari and Mohammad Ali Jabreil Jamali, EFFICIENT DETEC- TION OF SYBIL ATTACK BASED ON CRYPTOGRAPHY IN VANET, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 20.

[90] N. Singh, D. Pandey, V. Pandey and M. W. Khan, "Effective Requirement Engineering Process by incorporating Risk Management Approach", Solid State Technology, Vol.63, No.5, pp.814-822, 2020.

[91] S. T. Patel and N. H. Mistry, "A review: Sybil attack detection techniques in WSN," 2017 4th International Conference on Electronics and Communication Systems (ICECS), 2017, pp. 184-188, doi: 10.1109/ECS.2017.8067865.

[92] Grover J, Gaur MS, Prajapati VLNK. A Sybil attack detection approach using neighboring vehicles in VANET. SIN'11, Sydney, Australia; 2011.