A Review on Security Attacks in Vehicular Ad hoc Network

R.Priya
Research Scholar
Department of Computer Science and Engineering
Pondicherry Engineering College
Puducherry, India
priyakrish@pec.edu

Dr. N. Sivakumar
Assistant Professor
Department of Computer Science and Engineering
Pondicherry Engineering College
Puducherry, India
sivakumar11@pec.edu

Dr. M. Thirumaran
Assistant Professor
Department of Computer Science and Engineering
Pondicherry Engineering College
Puducherry, India
thirumaran@pec.edu

Abstract**—**Whenever a communication takes place between two or more vehicles there has been a need for protection. The attacker can gain access to the network by compromising either the vehicle or road side unit or the communication medium that transfers the messages between vehicles. Vehicular Ad hoc Network (VANET) have motivated the interest towards the passenger comfort and secure driving environment. However, the open-wide communication becomes a tedious challenge for VANET organization. Because of the wireless self-structured background, VANET are prone to many attackers. In this paper, we are focusing on security issues like DoS, Sybil, DDoS, jamming and flooding attacks as well as techniques like TESLA which causes harm to VANET and also security countermeasures like digital signature which are used to prevent the mentioned security issues that alleviate VANET.

Keywords*-VANET; Vehicular communication; Security attacks; DoS; DDoS; Sybil; TESLA*

*****

I. Introduction

Nowadays, ad hoc network have induced their comforts in both industrial and defense sector since, it does not demanding any pre-planned structure. Moreover, it has the prominent trait that it has the ability to form a network even though moving from one location to another.

Most of the people are died around the sphere due to road accidents either by slackness of driver, traffic jamming, inadequate road information. To overcome the road accident the proper information about the roads can be given to the driver earlier. For this, a new emerging and booming technology called Vehicular Ad hoc Network (VANET) which has no stable infrastructure with high speed vehicles. The major objective of the VANET is indemnify a secure drive by enhancing the traffic flow and shrinks traffic collisions.

VANET is a distinctive sub class of Mobile Ad hoc Network (MANET). VANET and MANET have some close resemblances with each other such as varying bandwidth, short range connectivity, and unfixed infrastructure. Intelligent Transportation System is a sub structure of VANET that provides smart communication to the vehicles with the usage of transport network. But VANET has its individual distinct features like high mobility, unreliable channels. These features paves way for number of research issues in the areas of routing, message broadcasting, security issues.

The VANET architecture is depicted in Figure.1 VANET offers a direct communication between inside and outside environment of the vehicle through wireless interfaces. Each and every nodes present in the VANET will act as a router as well host due to its decentralized organisation.

The structural design of the VANET is divided into three types. They are cellular network, pure ad hoc network and hybrid network. There exists two different types of communication in VANET Vehicle to Vehicle (V2V) and Vehicle to infrastructure (V2I) for these technical components are used to communicate among V2V or V2I it needs some technical components integrated [1] with hardware and software they are OBU and RSU. On-board Unit (OBU) is mounted in the vehicle through which it can communicates with other vehicle or with RSU. The road side unit (RSU) is placed at the road side to record the traffic patterns. Tamper Proof Module (TPM) it buffers the information that are related to the security. Electronic License Plate (ELP) it is used for vehicles electronic identity. Event Data Record (EDR) the event that takes place in the vehicle atmosphere are recorded.

The VANET uses Dedicated Short Range Communication (DSRC) protocol to communicate with RSU and other vehicles.

A. *Features of VANET*

The resemblances of VANET and MANET seems to be alike but VANET has its own distinct features. They are

1) *High Mobility*

Due to the vehicle's random speed it makes a tedious task in predicting the vehicles location.

2) *Dynamic Topology*

Due to fast random movement of the vehicle, topology of the VANET varies repeatedly. Thus, the routing path also differs rapidly.

TABLE I. FEATURES OF VANET AND MANET

S. No	**Characteristics of VANET and MANET**		
	Parameter	***VANET***	***MANET***
1	Cost	High cost	Low compared to VANET
2	Varaiation in network topology	Repeated	Gentle
3	Mobility	High	Low
4	Node density	Thick	Thin
5	Reliability	High	Low
6	Lifetime of the node	Depends on lifeime of the vehicle	Depends on power source
7	Nodes moving patterns	Regular	Random

3) Random disconnection

The fast moving of the vehicle makes the short range of communication with its neighbour causing frequent disconnection.

4) Limited bandwidth

The range of bandwidth limited for automotive application is 5.850-5.925 provided by the Dedicated Short Range Communication (DSRC).

B. Applications of VANET

The applications of the VANET are typically grouped into safety related applications, transport efficiency, infotainment applications.

1) Safety related applications

It contains flair applications that are admitted by Vehicle Safety Consortium (VSC) they are warning of traffic violation, arc speed, changing of lane, stop sign assistance for movement, sensing of vehicle pre-crashing.

2) Transport efficiency

It provides application that are admitted by Car to Car Communication Consortium (C2C- CC) it includes guidance and navigation of routes, merging assistance of lane.

3) Infotainmnet

It provides information such as online services, nearest gas station, restaurants, gaming application, news updates, weather reports etc.

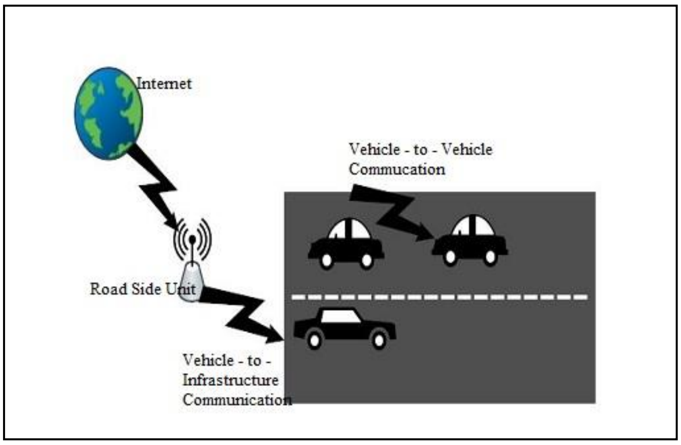
Internet
Vehicle - to - Vehicle Commucation
Road Side Unit
Vehicle - to - Infrastructure Communication

Figure 1. VANET Architecture.

II. SECURITY IN VANET

The VANET are exposed to various types of attacks, vulnerabilities due to its unfixed infrastructural environment. For instance broadcasting of fraudulent threatening messages and clampdown of genuine cautioning messages thus it leads to misfortunes of survival and time.

A. Security Requirements in VANET

Due to the open-wide communication of the VANET, some of the security requirements are found and they are as follows:

1) Authentication

Authentication is a method by which confidentiality of the message transferred is maintained. Before a message is used by a vehicle or RSU it makes sure that the message is received from an authentic sender. In other words, it makes sure that the sender is an impersonator or not.

2) Authorization

After the vehicle has been authenticated the next step is known as Authorization. This authorization is a technique in which the administrator will make sure that the vehicles have the appropriate rights to view or access or modify the data.

3) Trusted Third Party Authentication

The trusted third party (TTP) is sometimes known as trusted authority as its entity are trusted by all other entity in that environment. In some scenario, TTP must protect the resources as long term secrets. The compromising of such secrets may leads to render an insecure communications.

4) Confidentiality

Confidentiality is a technique that makes sure the vehicles privacy is maintained at all times. There are different techniques in VANET that allows the vehicle to maintain privacy. It also makes sure that the vehicles details are not revealed to other vehicles who are not allowed to hear it. Confidentiality of vehicles data has to been maintained in case of V2R and V2V communications. Confidentiality can be identified using encryption and authentication techniques.

5) Integrity

The message send by the sender to the receiver via the network the integrity of the message should be maintained. That is there should not be any modification or tampering of messages.

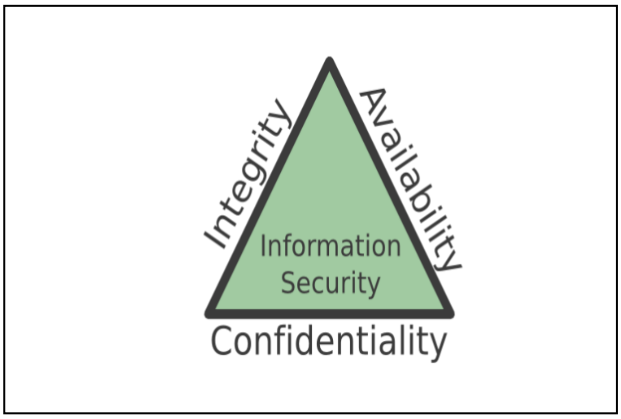

Figure 2. CIA Triangle.

6) Access Control

Access control is a security technique that can be used to legalize who or what can view or use resources in a computing environment.

7) Non repudiation

It prevents either sender or receiver in the network from disagreeing a transferred message. Thus, when a message is sent, the receiver can prove that the unproven sender in fact the message. Similarly, when a message is received, the sender can prove that the unproven received in fact received the message.

8) Privacy

The passenger's profile or driver information should be preserved against from the malicious attackers.

9) Availability

Ensuring that legitimated parties are able to access the information when needed. Information only has value if the right people can access it at the right times. Denying access to information has become a very common attack nowadays.

B. Types of Attackers

The attacker is a person who wants to destroy or control the entire network. The classification of attackers are as follows:

1) Insider

In a network, they perform the attack by communicating other members in a network. They have some additional advantages when compare to other type of attackers because the insider may have some authorized access to the network moreover they know the target's network architecture.

2) Outsider attacker

In a network, they perform the attack by indirectly communicating with other members in a network. Insider have direct communication with network by which they can perform more attacks in the network. Whereas, the outsider performs less number of attacks as they have restricted to access the resources in the network.

3) Malicious

They perform the attack towards the targeted network with the lack of their own profits. They attack the network not for their individual benefits.

4) Rational

They are opposite to the malicious attackers. They perform the attack towards the targeted network with the surplus profits of their own.

5) Active attacker

When a network receives a packet the attacker captures and modifies the message that are present in the packet and retransmits the message.

6) Passive attacker

When a network receives a packet the attacker captures and sniffs the messages in the packet and retransmits the packet without any modification. Passive attacker is less harmful when compared to active attacker. But passive attacker is difficult to identify.

C. Security Threats in VANET

VANET faces many security threats along with the attacks. They are as follows:

1) Bogus Information

In this, the attacker broadcast the falsified information to the vehicles that are present in the network. This is done for the attacker's own profit.

2) Masquerade

A vehicle frauds its characteristics and mislead to act as other vehicle for its individual gain.

3) Malware and spam

The insider causes the interception in the network by spreading viruses, spam. They are typically performed when updating the software's of road side unit and on-board units thereby, the effect of the attack gets increased.

4) Intentional Attack

It is very tough to protect the intentional attack. Because it is created by the trustworthy insider. A real node can hold the entire network by rejecting the messages to nearby nodes, attaching false information, not using the bandwidth properly.

5) Man in the Middle Attack

A spurious car may eavesdrop the communication that are exchanged between the vehicles. By which the attacker sends some fake information to the vehicles.

D. Security Issues in VANET

There are various attacks that affects the VANET's performance and are as follows:

1) Denial of Service Attack

The malicious attackers broadcast the fraudulent messages to block the entire communication medium. By which the network performance can be degraded and the efficiency becomes low. The Figure 3 depicts the DoS attack in that the authentic cars are name as A, B, C in which the malicious attackers sends the fraudulent messages like accident ahead, lane ahead.

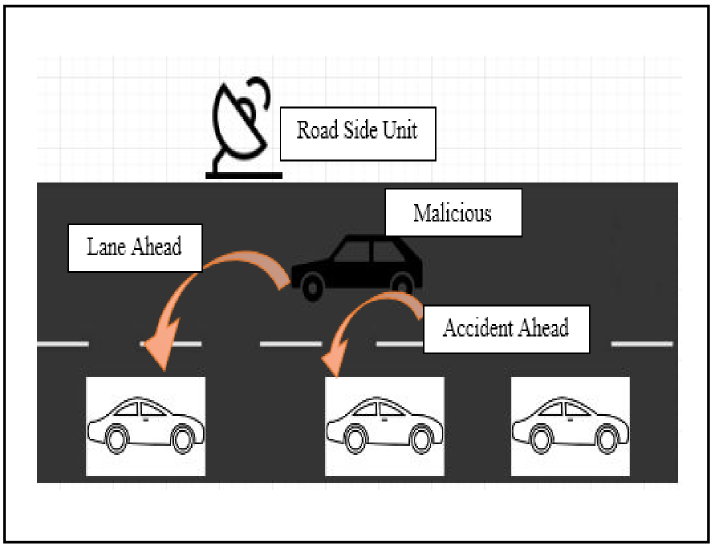

Figure 3. Denial of Service Attack.

2) Sybil Attack

In this type of attack, a node sends numerous message packet to other nodes and every message has a bogus identity in it. The main motivate is to create a vehicle and placing it to the different locations at a same time.

3) Distributed Denial of Service Attack

When compared with DoS attack, DDoS attack has a severe effect. In this type of attack many number of malevolent vehicle attacks the authentic vehicle with a bogus messages in a scattered manner from various locations at various timeslots. The Figure 4 depicts the DDoS attack in which the malicious attackers M1, M2, M3 sends fraudulent messages to the authentic vehicle A so that A can't communicate with other vehicle.

4) Jamming Attack

It intentionally transfers radio signals to falsify the entire communication by reducing the signal to noise ratio. The jammers continuously send frequent signals to interfere with the communication between nodes in the network. The victim feels that the channel is busy. The overall motive of this attack is to degrade the overall QoS services.

5) Flooding Attack

It is a form of denial of service attack in which the attacker brings the network down by flooding continuous services.

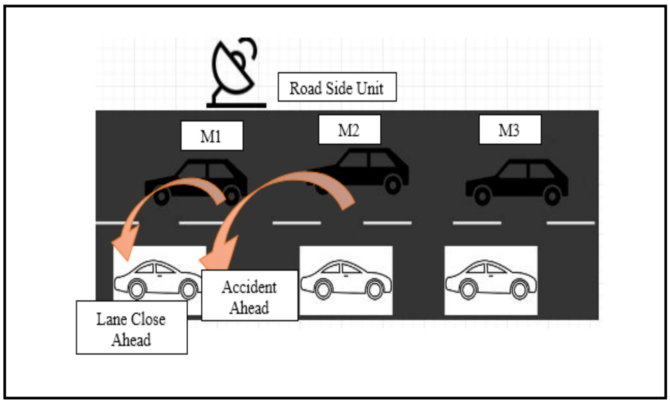

Figure 4. Distributed Denial of Service Attack.

E. *Security Countermeasures in VANET*

The security countermeasures used are VANET are as follows:

1) *Public Key Approaches*

Each and every node has two keys secret and public keys. They are handled by the Public Key Infrastructure (PKI). PKI system is used in addition with the in-built two components of the VANET they are Event Data Recorder (EDR) and Tamper proof Module (TPM).

2) *Symmetric and Hybrid Approaches*

In this scheme the vehicle communicates with each other by sharing the agreeing secret key for communication. In VANET based communication the normal security scheme used are public or symmetric key but new a hybrid system uses both symmetric and public keys for two types of communications they are pair-wise and group communication. When two vehicle communicates with one another pair-wise communication can be used. When more than two vehicle communicates with each other group communication is used.

3) *Certificate Revocation Approaches*

To provide security in VANET Public Key Infrastructure (PKI) is used which contains certification revocation system. It has the ability to dismiss the membership of the vehicle. It can be done in two ways centralized and decentralized. In centralized approach, the revocation decision is taken by the central authority. In decentralized approach, the revocation decision is based on the neighbor vehicles of the group.

4) *ID based cryptography*

ID-based online/offline signature (IBOOS) scheme is used for verification purposes. Offline process is first done in RSU or first in the vehicles. During vehicle to vehicle communication online process is used.

5) *Digital Signatures*

The nodes present in the network transfers the message while sending messages there is a necessity to maintain the security. For this purpose digital signature can be used. By using the public key cryptosystem the sender sign the data with digital signature. At the other end the receiver the hash code to decrypt the data.

III. DETECTION OF DENIAL OF SERVICE ATTACKS

A. *Extended Three Party Password Based Authenticated Key Exchange (E-3PAKE)*

R. Muthumeenakshi et. al [2] proposed an Extended Three Party Password based Authenticated Key Exchange (E-3PAKE) to defend against Denial of Service (DoS) attack. VANET affords value added services such as internet access, gaming, content sharing, business, infotainment etc. which are termed as non-safety application. The proposed scheme is based on authentication model to improve the security in value added services. The previous existing works also based on value added services but it prone many security issues DoS is one among them. This scheme aims to provide authentication in value added services. For this, it uses batch message dispatch it customizes the roles of the user based on the type of the user category such as primary, secondary, premium. Of these, the primary category are given as the highest priority because it comes under the crisis request such as hospital service etc. The incoming messages are signed by the on board unit along with their keys for authentication purposes and the message are interchanged with road side unit inorder to provide data integrity of the requesting services.

B. *Bloom Filter based IP-CHOCK*

Karan Verma et. al proposed a method [3] permits the valid service from the authorized vehicle in VANET environment. The abnormal traffic of the vehicle in VANET has been examined by the IP-CHOCK detection algorithm which is divided into three phases. The traffic information of the vehicle that are entering in the VANET are collected and checked by the phase1detection engine. The non-fraudulent, non-malicious IP address of the vehicles' information are stored in the database and the fraudulent, malicious information are stored in decision engine. The final phase is the bloom filter with hash which sends an alert to all the connected vehicle in VANET about the malicious IP address; otherwise it updates the legitimate IP address.

C. *VAST (VANET Authentication using signature and TESLA++)*

Ahren Studer et. al [4] proposed a framework VAST is deployed as the combination of ECSDA and TESLA++ which is used to verify the each message packet. The role of TESLA++ is to verify the valid incoming messages and filters the fraudulent message and ECSDA uses digital signature. Inorder to ensure the secure message, every message is generated with digital signature, message authentication code and the receiver authenticates the packet by verifying them. This framework thwarts from flooding and computational DoS attacks.

D. *TESLA ++ (Time Efficient Stream Loss Torrelant Authentication)*

Ahren Studer et. al [4] proposed TESLA++ which is considered to be a small enhancement of TESLA as it overcomes the memory based DoS attacks. In this, the sender transmits the message authentication code before transmitting the message and key. The receiver buffers the message authentication code inorder to reduce the memory overhead. The pitfall of TESLA ++ in lossy network are non- reputation, multi- hop functionality.

E. TESLA (Time Efficient Stream Loss Torrelant Authentication)

The broadcast message in TESLA [4] are authenticated by using symmetric cryptography along with delayed key disclosure. To validate the source message, the sender transmits the packet along with the message authentication code by using sender's key for an interval of time (K_i). At the other end, the receiver buffers the received message and message authentication code until the key is broadcasted by the sender. After a period of time the receiver, receives the key and checks the message and message authentication code with that key. The pitfall of TESLA is it suffers from memory based DoS attack.

IV. DETECTION OF SYBIL ATTACKS

A. Radio Resource Testing

Salam Hamdan et. al proposed [5] a mechanism used for the detection of Sybil attack. It is in supposition that each node is restricted to have number of resources. The resources present in the node are compared with usual nodes if it results less number of resources it is detected as the Sybil node otherwise it is a legitimate node.

B. Sensor based on Position Verification

The techniques proposed by Tim Leinmuller et. al [6] are

1) Acceptance Range Threshold

The maximum acceptance range of the threshold is fixed based on the channel radio of the information. It discards the beacon message that are larger than the current position of the receiver's nodes.

2) Mobility Grade Threshold

The mobility of the supposition nodes is described with a maximum speed. Every node issues a timestamp upon receiving the beacon message. The average speed of the node is computed if there is a variation in the position of the beacon message, MGT discards the node.

3) Maximum Density Threshol (MDT)

The threshold determines the number of nodes that can reside in an area. The sensors predefines the maximum density of the threshold. The threshold restrains the number of nodes that can reside in an intended area. If the entirety of the node exceeds the defined threshold the beacon from that position are discarded.

4) Map based verification

Street maps are used to navigate the position of the vehicle. Also, it can verify whether the vehicle are physically present or not.

V. DETECTION OF DISTRIBUTED DENIAL OF SERVICE ATTACK

A. Genetic Algorithm

The framework proposed by Avleen Kaur Malhi et. al [7] manipulates the genetic algorithm against DDoS attack. Inorder to overcome the problem of ID based cryptography and public key infrastructure the framework calculates the vehicle's fitness. The sender broadcast the signed message and the receiver validates the message. The sender transmits the signed message and the receiver validates the message. If the authentication of the message were provided then it ensures that the message was from the secured sender. To maintain the message integrity digital signature were used and to preserve the privacy pseudonyms were assigned by the road side to the vehicles.

B. Firecol

François Jérôme et. al proposed a new collaboration [8] Firecol that detects flooding DDoS attack. It encompass on intrusion prevention system which is installed at the service provider. It act as a service through which the customers may subscribe. It develops a virtual protection guard against flooding DDoS attack for the enrolled customers. The framework is composed of selection manager which computes the present profile traffic flow from the saved one it chooses one profile and then it forwards to score manager. The role of the score manager is to allocate score for the adopted rule based on the entropy, frequency. The level of the attack are categorized as high, low based on the threshold

C. IP Traceback based Intelligent Filtering

Minho Sung et. al [9] proposed a scheme to defense against DDoS attack using packet filtering. It contains three modules. The Enhanced probabilistic marking module runs in router background where the presence of DDoS attack exist or not. In attack mitigation decision making module, it constructs the attack path with the help of the IP traceback next based on the probability of the decision the packet may be dropped. In preferential packet filtering module based on the collected packet information it filters the packet if it is detected as the attack packet.

D. Traffic Congestion

Ayonija Pathre et. al [10] proposed a new scheme for traffic congestion. The communication that takes place in the network were monitored by the road side unit. The attacker misguides the fraudulent message endlessly to other vehicles thereby causing congestion in the network. The vehicles that causes the transmission of fraudulent message are identified and discarded.

VI. DETECTION OF JAMMING ATTACK

A. Fuzzy Logic

S.K. Bhavithra et. al [11] identifies the jamming attack by using fuzzy logic. The aim of this paper is to send information in an alternative path if it detects the jamming attack in the network. Fuzzy logic is employed for the detection of the jamming attack. To provide an alternative path Localizability Aided Localization approach is used for sending an information to the receiver.

B. Threshold Technique

Gagandeep Kaur et. al [12] proposed threshold based technique [12] for the detection of jamming attack. In a vehicular environment malicious and non-malicious nodes are exist due to the decentralized architecture of the VANET. The threshold values of the data are allocated, if the malicious nodes are identified based on the data packet that are sent in the network. If the value exceeds the allocated threshold it is identified as the malicious jamming node.

C. DJAVAN (Detecting Jmming Attack in Vehicle Ad hoc Network)

Lynda Mokdad et. al [13] proposed an algorithm that uses packet delivery ratio for the identification of jamming attack. The solution computes the packet delivery ratio and it may have a drop in a time slot. If the variation drop has a vast difference, then it recognises the existence of jamming attack.

VII. DETECTION OF FLOODING ATTACK

A. FDER (Flooding Detection based on Encounter Record)

Thi Ngoc Diep Pham et. al [14], the flooding attack is detected based on the defined time interval, rate limit of the message that are allocated to the nodes. If the traffic pattern of the normal nodes exceeds the allocated limit it is detected as the attacking node. Moreover, encounter record is used for tracking the nodes behavior.

B. Slow Detection, Fast Recovery

Ding Pengfule et. al [15] proposed a mechanism based on Adaptive threshold detection algorithm is employed. It records the present traffic of the network and changes the threshold value. The value of the threshold are computed based on the current change in the network. If the computed value exceeds the threshold value it is detected as the existence of flooding attack.

VIII. CONCLUSION

VANET is an infrastructure less network which is used for communication between two or more vehicles with the help of On-board unit, Road side unit. Due to the contrasting features of VANET there are different vulnerabilities which causes the network crash down. Over the past decade various researchers have concentrated on different security vulnerabilities and its countermeasures in VANET. So, this paper provides a detailed survey of the latest security related detection techniques in VANET. Based on the survey our research is based on the attacks in the VANET and its countermeasures.

REFERENCES

[1] Fengzhong Qu, Zhihui Wu, Fei-Yue Wang, and Woong Cho, “A security and privacy review of VANETs,” Journal of IEEE Transactions on Intelligent Transportation Systems vol. 16, no. 6, Dec. 2015, pp.2985-2996.

[2] R.Muthumeenakshi, T.R. Reshmi and K. Murugan, “Extended 3PAKE authentication scheme for value-added services in VANETs,” Journal of Computers & Electrical Engineering, vol. 59, 2017, pp. 27-38.

[3] V Verma Karan, and Halabi Hasbullah, “Bloom-filter based IP-CHOCK detection scheme for denial of service attacks in VANET”, Journal of Security and Communication Networks, vol. 8, no. 5, 2015, pp.864-878.

[4] Studer Ahren, Fan Bai, Bhargav Bellur, and Adrian Perrig, “Flexible, extensible, and efficient VANET authentication,” Journal of Communications and Networks , vol. 11, no. 6, Dec. 2009, pp.574-588.

[5] Salam Hamdan, Raad Al Qassas and Sara Termori, “Comparative Study on Sybil Attack Detection Schemes,” International Journal of Computers and Technology, vol. 14, Jan. 2015, pp.5869-5876.

[6] Tim Leinmuller, Elmar Schoch, and Frank Kargl, “Position verification approaches for vehicular ad hoc networks,” Journal of IEEE Wireless Communications, vol. 13, no. 5, 2006, pp.16-21.

[7] Avleen Kaur Malhi, and Shalini Batra, “Genetic-based framework for prevention of masquerade and DDoS attacks in vehicular ad-hoc networks,” Journal of Security and Communication Networks, vol. 9, no. 15, 2016, pp.2612-2626.

[8] François Jérôme, Issam Aib, and Raouf Boutaba, “FireCol: a collaborative protection network for the detection of flooding DDoS attacks,” Journal of IEEE/ACM Transactions on Networking (TON), vol. 20, no. 6, 2012, pp.1828-1841.

[9] Minho Sung and Jun Xu, “IP traceback-based intelligent packet filtering: a novel technique for defending against Internet DDoS attacks,” Journal of IEEE Transactions on Parallel and Distributed Systems, vol. 14, no. 9, 2003, pp.861-872.

[10] Ayonija Pathre, Chetan Agrawal, and Anurag Jain., “A novel defense scheme against DDOS attack in VANET,” Wireless and Optical Communications Networks, 2013, pp.1-5,

doi: 10.1109/WOCN.2013.6616194.

[11] S.K. Bhavithra, K.P. Vijayakumar and P. Ganeshkumar, “A Robust Approach for Jamming Attack Detection in VANET,” vol. 24, 2016, pp.83-89, doi:10.5829/idosi.mejsr.2016.24.IIECS.23144.

[12] Gagandeep Kaur, Parveen Sharma, “Technique to Detect and Isolate Jamming Attack in VANET”, International Journal of Applied Engineering Research, vol. 12, no. 21, 2017, pp. 10824-10827.

[13] Lynda Mokdad, Jalel Ben-Othman and Anh Tuan Nguyen, “DJAVAN: Detecting jamming attacks in Vehicle Ad hoc Networks,” Journal of Performance Evaluation, vol. 87, May 2015, pp.47-59.

[14] Thi Ngoc Diep Pham, Chai Kiat Yeo, Naoto Yanai, and Toru Fujiwara, “Detecting Flooding Attack and Accommodating Burst Traffic in Delay Tolerant Networks,” Journal of IEEE Transactions on Vehicular Technology, 2017, doi:10.1109/TVT.2017.2748345

[15] Ding Pengfule, Tian Zhihong, Zhang Hongli, Wang Yong, Zhang Liang, and Guo Sanchuan, “Detection and Defense of SYN Flood Attacks Based on Dual Stack Network Firewall,” Data Science in Cyberspace, 2016, pp. 526-531, doi:10.1109/DSC.2016.108