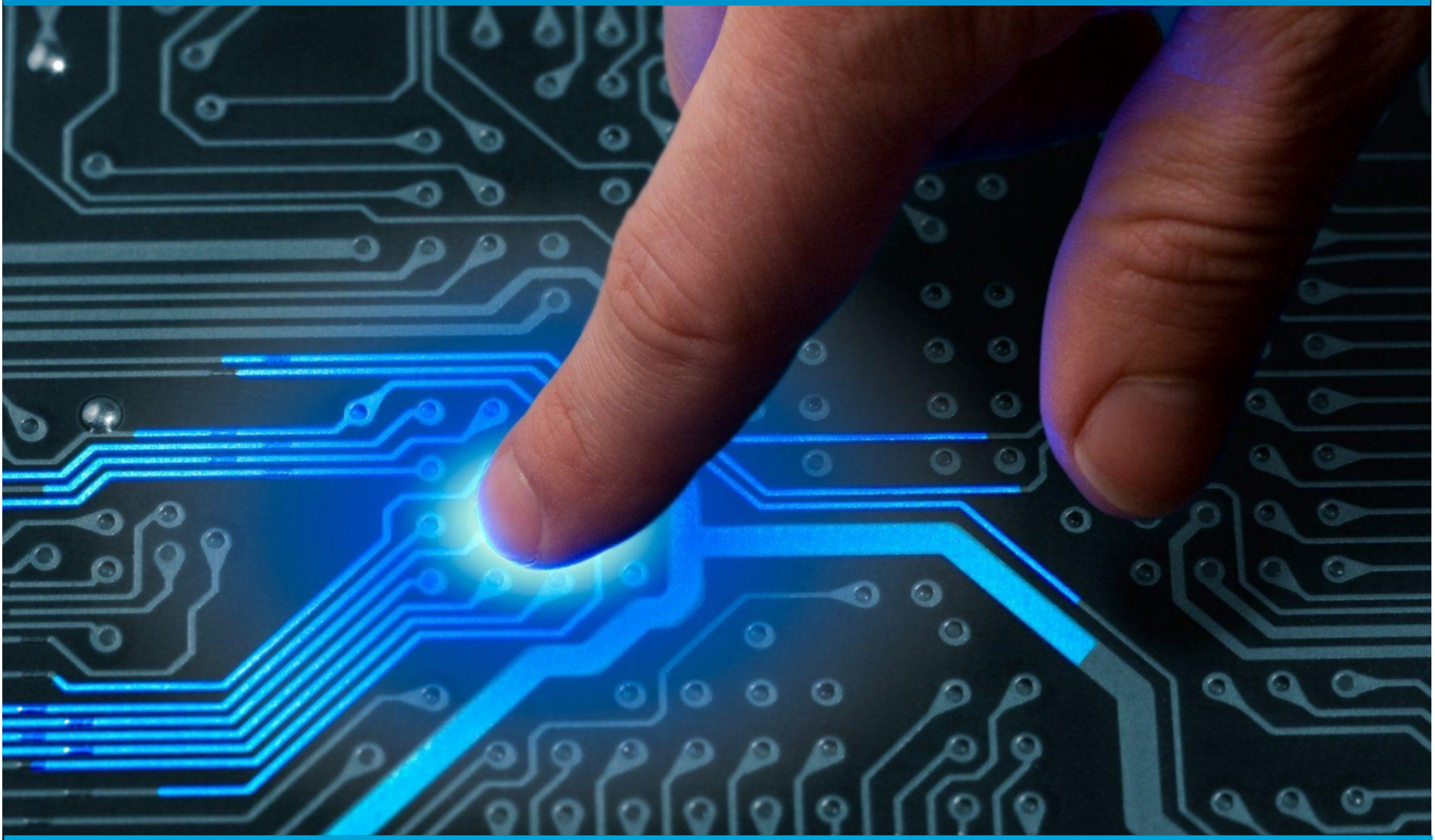
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 9, September 2020

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 9, September 2020 ||

Review on Security Attacks and Possible Solution in VANET

Parwati Ahirwar[1], Dr. Ashish Khare[2]

M.Tech Scholar, Department of CSE, Lakshmi Narain College of Technology & Science, Bhopal, India[1]

Professor & HOD, Department of CSE, Lakshmi Narain College of Technology & Science, Bhopal, India[2]

ABSTRACT: Vehicular Ad hoc Networks (VANET) is a subgroup of (Mobile Ad Hoc Networks) MANET which is using for improves traffic safety system. Vehicles movements are instructed by roads, traffic rules so it can deploy fixed infrastructure at critical locations. We focus our study on the different kind of attacks and its behavior or impact in safety system and how many challenges; we have to accept for high security. This paper presents classification of different attacks based on different layers like MAC layer, network, transport, application and multi layer and different challenges which included authentication, availability Privacy, anonymity etc.

KEYWORDS: VANET, DOS, DDOS, MANET, MAC, CAN.

I. INTRODUCTION

Vehicular Ad-hoc Network (VANET) is a significant part of keen transportation framework, which encourages vehicles to impart delicate data and corporate to other people. Be that as it may, because of its remarkable attributes, for example, transparency, dynamic topology and high versatility, VANET experiences different attacks. [1] Wellbeing of human lives in the road is the significant concern nowadays, in light of the fact that consistently a huge number of people groups passed on in road mishaps over the world. Vehicular Ad hoc Network (VANET) is unique sort of network that means to diminish demise rate and improves traffic security framework. Vehicular Ad-hoc Networks (VANET), the promising strategy, is getting consideration for dealing with the traffic proficiently and making the road safe. The geographies and its tremendous applications shifting from road security, to the traffic the executives, installment service to infotainment. VANETs are portrayed as a self-composed, dispersed, exceptionally versatile, unique topology, unconstrained force, computational and capacity networks. The correspondence in VANET is acted in open-get to condition which requests the security issues must be manage articulate significance. Security necessities incorporates validation, accessibility, message secrecy, message trustworthiness, information accessibility, get to control, protection, message non-renouncement and continuous guarantees of message delivery.[2]

Vehicular Ad hoc Networks (VANET) is a piece of Portable Ad Hoc Networks (MANET), this implies each node can move unreservedly inside the network inclusion and remain associated. In VANET, moving vehicles as nodes can send and get security messages to one another on the road to guarantee wellbeing of human life [1]. The essential objective of VANET is to give road security estimates where data about vehicle's present speed, area facilitates are passed with or without the arrangement of Framework. Aside from wellbeing measures, VANET additionally offers some benefit added services like email, sound/video sharing and so forth.

Committed Short Range Correspondence (DSRC) is the recurrence band that is utilized as a DSRC conveys wellbeing and non security messages in whole network by utilizing its wellbeing and non security channels. Non wellbeing applications are identified with solace of the travelers and to improve the traffic framework. Stopping accessibility and cost assortment services are instances of these applications.

Security is an important issue particularly right now network where one adjusted message can makes issue for the clients from numerous points of view. Attackers make issue straightforwardly and in a roundabout way by propelling diverse sort of attacks.

A vehicular correspondences framework includes various associating substances that we characterize broadly as: Clients, Network nodes, and Authorities.

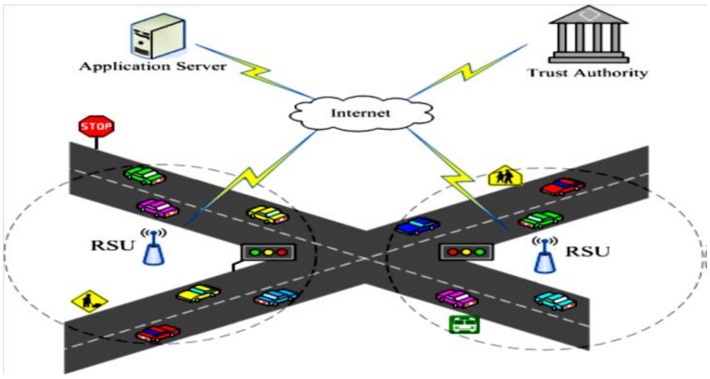


Figure 1: Architecture of VANET

Communication pattern of vehicles are following- (i) Inter-vehicle communication
(ii)Vehicle-to-road side communication
(iii)Inter-road side communication

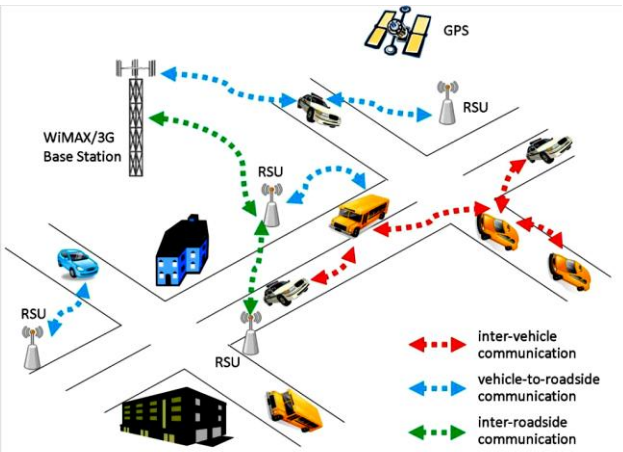

GPS
RSU
WiMAX/3G
Base Station
RSU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

Figure 2: Communication pattern of vehicles.

II. LITERATURE SURVEY

Most J. Zhang, et al., proposes AATMS, vehicles in VANET can maintain a strategic distance from malevolent vehicles and help out confided in vehicles. The possibility of AATMS is for the most part motivated by TrustRank calculation, which is utilized to battle web spams [1]

A. K. Goyal et al., proposed a safe and productive VANET framework, a broad outline of attributes, challenges, security attacks and necessities must be managed. The prime goal of this paper is to give a grouping of security prerequisites, security attributes and difficulties. [2]

D. P. Choudhari et al., breaking down the packet delivery ratio (PDR) for the network under Spying and DDoS attacks and after expulsion of these attacks the packet delivery ratio (PDR) is expanded for the network. The Packet Delivery Ratio for example PDR is the quantity of packets got and the packets created as recorded in follow document. So we characterize Packet Delivery Ratio as the absolute quantities of packets got at the goal to the all out number of packets send structure the source. [3]

R. Kolandaisamy, et al., proposed a novel plan attack location utilizing vehicle mode investigation in Exploratory Based Ant Colony Approach (EBACA) for VANET is proposed. The hidden supposition that will be that a mode investigation of vehicles determines unwavering quality and trickiness of messages they drive. With mode, all apparent data on a vehicle is submitted to give past, current and even possibility exercises and its transmission exercises. [4]

B. Luo, et al., propose a blockchain empowered trust-based area security insurance conspire in VANET. In particular, by breaking down the various prerequisites of the solicitation vehicle and the helpful vehicle during the way toward building the unknown shrouding locale, just as joining the attributes of these two jobs, we devise the trust the executives technique dependent on Dirichlet conveyance, to such an extent that both the requester and the cooperator will just help out the vehicles they trust.[5]

A. Deshpande, et al., presents the work which is performed in divided into two stages. In the first stage data is normalized using mean normalization. In second stage genetic algorithm is used to reduce number of features and further multilevel ensemble classifier is used for classification of data into different attack groups. From result analysis it is analysed that with reduced feature intrusion can be classified more efficiently.[6]

W. Li et al., proposes a Sybil nodes discovery strategy dependent on RSSI arrangement and vehicle driving framework RSDM. RSDM assesses the distinction between the RSSI succession and the driving framework by unique separation coordinating to distinguish Sybil nodes. Also, RSDM doesn't depend on VANET foundation, neighbor nodes or explicit equipment. The test results show that RSDM performs well with a higher identification rate and a lower mistake rate. [7]

Y. Gao et al., proposed identification framework comprises of two fundamental segments: ongoing network traffic assortment module and network traffic location module. To assemble our proposed framework, we go through Sparkle to speed information preparing and use HDFS to store enormous suspicious attacks. In the network assortment module, small scale group information preparing model is utilized to improve the continuous exhibition of traffic include assortment. In the rush hour gridlock location module, the order calculation dependent on Arbitrary Woods (RF) is adopted. So as to assess the precision of discovery, the calculation was assessed and thought about in the datasets, containing NSL-KDD and UNSW-NB15. The test results show that the proposed discovery calculation arrived at the precision pace of 99.95% and 98.75%, and the bogus alert rate (FAR) of 0.05% and 1.08%, separately, in two datasets. [8]

J. R. et al., essentially centers around recognizing the malignant node that professes to be a genuine vehicle all through the session capturing attack in VANETs and furthermore examines on the throughput, delay at end focuses, complete checks of packet produced, traded and dropped utilizing the Network Test system 2 (NS2) instrument and fitting induction gave. [9]

M. Poongodi et al., proposed reCAPTCHA controller instrument forestalls the robotized attacks comparatively like botnet zombies. The reCAPTCHA controller is utilized to check and restrict the vast majority of the robotized DDoS attacks. For actualizing this system, the data hypothesis based measurement is utilized to examine the deviation in clients demand regarding entropy. Recurrence and entropy are the measurements used to quantify the weakness of the attack. [10]

S. Kumar et al., proposed a packet location calculation for the anticipation of DoS attacks is proposed. This calculation will have the option to recognize the numerous malignant nodes in the network which are sending irrelevant packets to stick the network and that will in the end stop the network to send the security messages. The proposed calculation was recreated in NS-2 and the quantitative estimations of packet delivery ratio, packet misfortune ratio, network throughput demonstrates that the proposed calculation improve the security of the network by distinguishing the DoS attack well in time. [11]

A. M. Alrehan et al., center around examining the principle attacks alongside DDoS attack on VANET framework just as investigating potential arrangements with an emphasis on AI based answers for recognize such attacks right now. [12]

R. N. Nabwene et al., Trust foundation in VANET helps manage insider attacks, albeit the vast majority of the current arrangements accept the attacker will consistently show a stable deceptive conduct after some time, which isn't the situation with clever insider attackers, they display insightful practices to evade identification. Right now audit existing arrangements utilized in rowdiness identification with essential worry on shrewd attacks like the adaptive recognition limit, assessment of trust among vehicles for autonomous timeframes and reach determinations, just as give proposals on future research to alleviate astute attacks. [13]

T. Zaidi et al., Right now, it is being seen that numerous security challenges are there where research need to step-up forward for making VANET progressively secure. A basic examination is talked about broadly concerning VANET parts, security issues and difficulties, attacks and its answers. [14]

S. Hamdan et al., shows an improved calculation will be proposed, exploiting the impression and security safeguarding identification of maltreatment of nom de plumes techniques. The cross breed location plan will be actualized utilizing the ns2 test system. P2DAP acting superior to anything impression when the quantity of vehicles increments. In the other hand, the impression calculation acting better when the speed of vehicles increments. Another half and half calculation will be played out that relies upon the encoded, validation and on the direction of the vehicle. The situations will be created utilizing SUMO and MOVE instruments. [15]

A. M. R. Tolba et al., a trust-based appropriated verification (TDA) strategy that depends on a worldwide trust server and vehicle conduct for keeping away from crash attacks is proposed. In addition, a channel state steering convention (CSRP) is proposed to improve the correspondence unwavering quality among the vehicles. Solid vehicles are distinguished by the on-board unit (OBU) vitality and the channel condition of the vehicle to convey consistent correspondence. [16]

III. VANET CHARACTERSTICS

In addition to the similarities to ad hoc networks, VANETs possess unique network characteristics that distinguish it from other kinds of ad hoc networks and influence research in this area. Few important characteristics of VANETs are as follows:

(i)High Mobility
(ii)Rapidly changing network topology
(iii)Unbounded network size
(iv)Frequent exchange of information
(v)Wireless Communication
(vi)Time Critical
(vii) Sufficient Energy
(viii)Better Physical Protection

A. VANET APPLICATIONS

Significant uses of VANET incorporate giving wellbeing data, traffic the board, cost services, area based services and infotainment.

B. VANET ATTACKS

VANET experience the ill effects of different attacks; these attacks are examined in the accompanying subsections:

Greedy drivers: Selfish minded drivers attempting to boost their benefit by making accept a blocked way to their goals, and thusly stifle traffic by attacking the steering instruments.

Snoops: Drivers endeavoring to profile drivers and concentrate their recognizing data. Pernicious Snoops can even track vehicle areas and decide the personalities of drivers by relating them to the house or work locales.

Pranksters: Drivers attempting to debilitate applications or keep data from arriving at others vehicles. Such attacks are indicated by Denial of administration attacks (DoS).

Malicious attackers: Drivers purposely endeavoring to make hurt by means of the accessible applications inside the system. A few attacks center around harming traded information between vehicles, for example, message manufacture, concealment or change. Sybil attack has a place likewise with this classification.

Industrial insiders: If vehicle producers are answerable for making sure about interchanges inside VANETs, representatives can uncover secret information to pernicious elements.

Jamming: The jammer purposely creates meddling transmissions that forestall correspondence inside their gathering range. In the VANET situation, an attacker can generally effectively segment the system, without bargaining cryptographic components and with restricted transmission power.

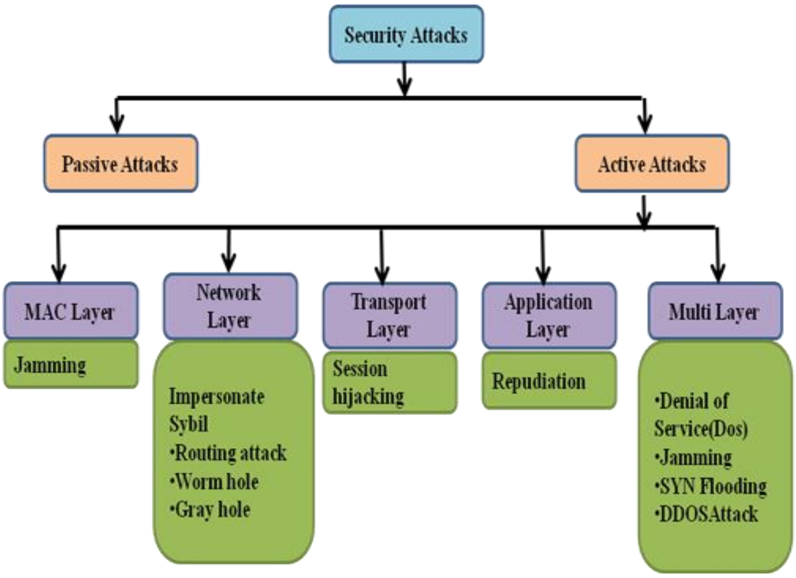


Figure 3: Classification of attacks based on Layers

• Node Impersonation Attack

Every vehicle has a remarkable identifier in VANET and it is utilized to check the message at whatever point a mishap occurs by sending incorrectly messages to different vehicles [4, 9, and 10]. Fig clarifies this situation where vehicle an includes in the mishap at area Z. At the point when police distinguish the driver as it is connected with driver's personality, attacker changes his/her character and just declines it.

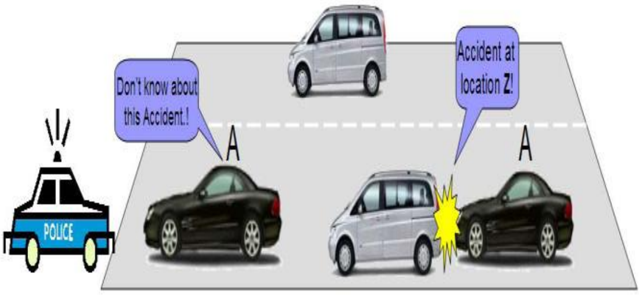


Figure 4: Node Impersonation Attack

• Sybil Attack

Sybil attack [10] so has a place with the top of the line. In Sybil attack, the attacker sends various messages to different vehicles and each message contains distinctive manufactured source personality (ID). It gives fantasy to other vehicle by sending some off-base messages like road turned parking lot message [3, 4]. Figure 5 clarifies Sybil attack in which the attacker makes different vehicles on the road with same personality. The goal is to uphold different vehicles on the road to leave the road for the advantages of the attacker.

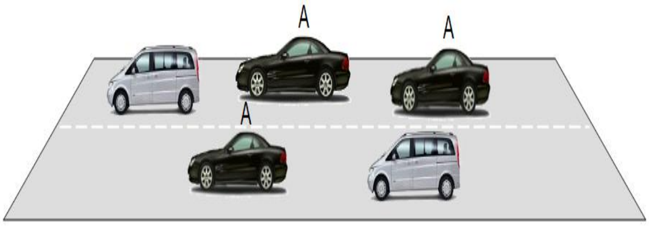


Figure 5: Sybil Attack

• Routing attack

Directing attacks re the attacks which misuses the weakness of system layer steering conventions. Right now attack the attacker either drops the parcel or upsets the directing procedure of the system. Following are the most widely recognized directing attacks in the VANET.

a) Black Hole attack:
Right now attack, the attacker initially draws in the nodes to transmit the bundle through itself. It tends to be finished by ceaseless sending the malignant course answer with new course and low bounce tally. In the wake of pulling in the node, when the parcel is sent through this node, it quietly drops the bundle.

b) Worm Hole attack:
Right now, adversary gets bundles at one point in the system, burrows them to another point in the system, and afterward replays them into the system starting there. This passage between two adversaries are called wormhole. It tends to be set up through a solitary long-run remote connection or a wired connection between the two adversaries. Consequently it is straightforward for the adversary to cause the burrowed parcel to show up sooner than different bundles transmitted over an ordinary multi-jump course.

c) Gray Hole attack:
This is the expansion of black hole attack. Right now attack the noxious node carries on like the black node attack yet it drops the bundle specifically. This determination can be of two kinds:
i) A malignant node can drop the parcel of UDP though the TCP bundle will be sent.
ii) The malignant node can drop the parcel based on probabilistic appropriation.

• Session hijacking
Most verification process is done toward the beginning of the meeting. Thus it is anything but difficult to commandeer the meeting after association foundation. Right now assume responsibility for meeting between nodes.
Repudiation: The fundamental danger in renouncement is denial or endeavor to denial by a node engaged with correspondence. This is unique in relation to the imitate attack. Right now or greater element has regular personality henceforth it is anything but difficult to get undefined and subsequently they can be denied.

• Denial of Service
DoS attacks are most conspicuous attack right now. Right now forestalls the real client to utilize the administration from the injured individual node. DoS attacks can be done from multiple points of view.
a) Jamming: Right now attacker detects the physical channel and gets the data about the recurrence at which the beneficiary gets the sign. At that point he transmits the sign on the channel so channel is jam.
b) SYN Flooding: Right now no of SYN demand is sent to the injured individual node, spoofing the sender address. The injured individual node send back the SYN-ACK to the spoofed address however unfortunate casualty node doesn't receive any ACK parcel consequently. This outcome too half opens association with handle by an injured individual node's cradle. As an outcome the real solicitation is disposed.
c) Distributed DoS attack: This is another structure Dos attack. Right now, attackers attack the injured individual node and keeps authentic client from getting to the administration.

C. VANET SECURITY REQUIREMENTS

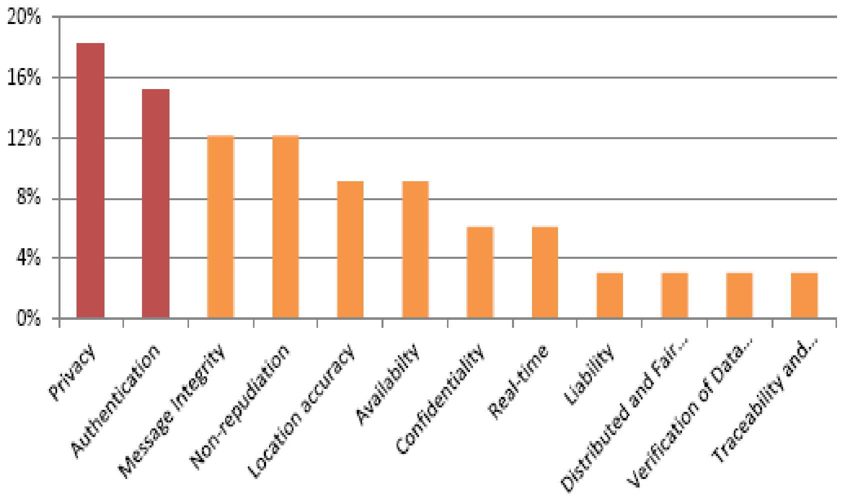


Figure 6: VANET Security requirement

1. Privacy
2- Authentication
3. Non-repudiation
4. Availability
5. Real-time constraints
6. Integrity
7. Confidentiality

IV. POSSIBLE SOLUTION FROM ATTACK

There are different kinds of attack which is talked about. Presently following table depict the conceivable arrangement of from these attacks.

Table 1: Summary of security solutions

Sr No	Attack	Solution	Technology
1	Replay attack Impersonation Eavesdropping	ARAN	Cryptographic Technique
2	DoS Routing attack Impersonation	SEAD	One way hash function technique
3	DoS Routing attack Replay attack	Ariadne	Symmetric cryptography technique, MAC
4	Routing attack Impersonation Bogus information	SAODV	Digital signature, hash function
5	Session hijacking	One Time Cookie	Random cookie generation
6	Sybil Attack	RobSAD	Motion pattern analysis
7	Impersonation	Holistic Protocol	ID Registration Technique

V. CONCLUSION

This paper shows the various aspect of VANET like its architecture, application, attacks and difficulties have been talked about; besides different attributes of VANET have been recorded which recognized it from different systems like MANET. This paper remembers different attacks for VANET have been characterized relying upon the various layers. It has been seen that the grouping assists with managing various kinds of attack in VANET. We have been talked about security challenge and security prerequisites. We have found after overview that attacks in multilayer like denial of services (DOS) and DDOS are hurtful for security framework just as confirmation and Protection are enormous difficulties. In future we examine vehicular system utilizing half breed anticipation technique.

REFERENCES

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

[2] A. K. Goyal, A. Kumar Tripathi and G. Agarwal, "Security Attacks, Requirements and Authentication Schemes in VANET," *2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, GHAZIABAD, India, 2019, pp. 1-5.

[3] D. P. Choudhari and S. S. Dorle, "Maximization of packet delivery ratio for DADCQ protocol after removal of Eavesdropping and DDoS attacks in VANET," *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Kanpur, India, 2019, pp. 1-8.

[4] R. Kolandaisamy, R. M. Noor, M. R. Zaba, I. Ahmedy and I. Kolandaisamy, "Markov Chain Based Ant Colony Approach for Mitigating DDoS Attacks Using Integrated Vehicle Mode Analysis in VANET," *2019 IEEE 1st International Conference on Energy, Systems and Information Processing (ICESIP)*, Chennai, India, 2019, pp. 1-5.

[5] B. Luo, X. Li, J. Weng, J. Guo and J. Ma, "Blockchain Enabled Trust-based Location Privacy Protection Scheme in VANET," in *IEEE Transactions on Vehicular Technology*.

[6] *A. Deshpande and R. Sharma, "Anomaly Detection using Optimized Features using Genetic Algorithm and MultiEnsemble Classifier", IJOSTHE, vol. 5, no. 6, p. 7, Dec. 2018. https://doi.org/10.24113/ojssports.v5i6.79*

[7] W. Li and D. Zhang, "RSSI Sequence and Vehicle Driving Matrix Based Sybil Nodes Detection in VANET," *2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN)*, Chongqing, China, 2019, pp. 763-767.

[8] Y. Gao, H. Wu, B. Song, Y. Jin, X. Luo and X. Zeng, "A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network," in *IEEE Access*, vol. 7, pp. 154560-154571, 2019.

[9] J. R. and N. S. Bhuvaneswari, "Malicious node detection in VANET Session Hijacking Attack," *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, Coimbatore, India, 2019, pp. 1-6.

[10] M. Poongodi, V. Vijayakumar, F. Al-Turjman, M. Hamdi and M. Ma, "Intrusion Prevention System for DDoS Attack on VANET With reCAPTCHA Controller Using Information Based Metrics," in *IEEE Access*, vol. 7, pp. 158481-158491, 2019.

[11] S. Kumar and K. S. Mann, "Prevention of DoS Attacks by Detection of Multiple Malicious Nodes in VANETs," *2019 International Conference on Automation, Computational and Technology Management (ICACTM)*, London, United Kingdom, 2019, pp. 89-94.

[12] A. M. Alrehan and F. A. Alhaidari, "Machine Learning Techniques to Detect DDoS Attacks on VANET System: A Survey," *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, Riyadh, Saudi Arabia, 2019, pp. 1-6.

[13] R. N. Nabwene, "Review on Intelligent Internal Attacks Detection in VANET," *2018 4th Annual International Conference on Network and Information Systems for Computers (ICNISC)*, Wuhan, China, 2018, pp. 1-6.

[14] T. Zaidi and Syed.Faisal, "An Overview: Various Attacks in VANET," *2018 4th International Conference on Computing Communication and Automation (ICCCA)*, Greater Noida, India, 2018, pp. 1-6.

[15] S. Hamdan, A. Hudaib and A. Awajan, "Hybrid Algorithm to Detect the Sybil Attacks in VANET," *2018 Fifth International Symposium on Innovation in Information and Communication Technology (ISIICT)*, Amman, 2018, pp. 1-6.

[16] A. M. R. Tolba, "Trust-Based Distributed Authentication Method for Collision Attack Avoidance in VANETs," in *IEEE Access*, vol. 6, pp. 62747-62755, 2018.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING