# *VANET security -Analysis and survey*

Nice Mathew,V.Uma
Department of Computer Science, School of Engineering and Technology, Pondicherry University

***Abstract*— the vehicular communication is the most promising wireless communication technology in the computer network scenario, the inception of which has marked momentous change in the range of safety application for the passengers. With the advancements in vehicular communication, the attacks and vulnerabilities have also increased. Though research in this field is found to be narrow, yet it is a widely expanding and promising arena. This paper highlights security characteristics and challenges of VANET. It also attempts a structured and comprehensive analysis of the breaches in securities associated with VANET. It brings into limelight the various solutions in line with each security attack and tries to compare the different solutions for each attack in order to track out the significance of each solution.**

***Keywords*— *VANET ; attacks; malicious nodes;security***

## I. Introduction

Research in the field of vehicular communication has gained tremendous significance in the present times. Vehicles which have become a part and parcel of our everyday lives have been further advanced with the incorporation of communication technologies that promotes communication between vehicles and possibly with its side units. Further, with the increased flow of vehicles on the roads, the probability of accidents in line with it has also rose to alarming rates. At this context, the development of road safety measures have become the need of the hour and is of intensive interest and research. To improve road safety, one of the possible ways is to install safety applications that communicate through wireless networks. Recent advances in wireless networks and short range communications have introduced new networks like Mobile Ad-hoc Networks (MANETs) and many more. MANET comprises of self-organizing mobile nodes that lack a network infrastructure, such as base stations [20]. MANET has been extended for vehicular communications and it is called as Vehicular Ad-hoc Networks (VANETs). VANETs are a special case of mobile ad hoc networks where the vehicles form the mobile nodes of the network. For this, a network is formed between vehicles in case of Vehicle-to-Vehicle (V2V) communication or between a vehicle and an infrastructure with Vehicle-to-Infrastructure (V2I) communication. VANET has several properties like node mobility, dynamic topology formation, geographical structure based restricted motions and openness to power accessibility.

VANET technology has certain advantages, such as it improves the road safety by reducing the number of road accidents, simplifies the payment procedures at the tolls, petrol pumps etc.

In spite of its advantages, it has different security challenges. Therefore, the security of a network is an important concern in the digitalized world. In VANET, security is an important challenge. For instance, the message informations like emergency message distribution, traffic incidents and road condition warnings etc., that are exchanged between nodes should not be inserted or modified. A modification in the information may lead to an impact on the drivers behavior, change in network topology and the security may be threatened if malicious user alters the message. Some possible attacks could cause traffic jams, spread bogus information, cheat the positioning information, disclose IDs, replay duplicate messages, masquerade or forge data, violate privacy or cause wormholes, Denial-of-Service(DoS) attacks, traffic tampering, impersonation as well as hardware tampering.

The other security challenges include the bulk size of the network, the high mobility and dynamic topology of the vehicles which might result in frequent disconnections and short connection durations, discrepancies in key distribution in VANET, number of packets routed after finding good route and user privacy while tracking the vehicles etc. calls for the necessity of research in this field.

These security challenges must be overcome by VANET security protocol. These security protocols must guarantee the fundamental security requirements (such as authentication, nonrepudiation, and availability) and privacy of the driver which means location and identity should not be accessed, traced or profiled by unauthorized entities. Otherwise, it will be very difficult to attract people to use these type of technologies.

To satisfy the security and privacy needs, a well-defined suite of privileged mechanism must be devised. It should ensure security and privacy preservation in the practical design of the VANET and thereby preserve the passengers from the major security attacks like Sybil attacks, black hole attacks, DoS attacks, timing attacks etc. Moreover, due to the high mobility nature, the resource constraints and high application requirement VANET has certain critical difference from MANETs, as a result of which most of the MANET security works cannot be applied to VANET .

As such, this paper gives a structured overview of the recent research advances in VANET security services by specifying the basis of VANET security, classifying various attacks and surveying various papers that have designed security mechanism to overcome these threats, vulnerabilities and security breaches.

978-1-5386-0796-1/18/$31.00 ©2018 IEEE

## II. SECURITY REQUIRMENTS IN VANET

A. Authentication

Authentication ensures the genuineness of the message which properly identifies its sender. In certain cases , the receiver might confirm the sender using ID authentication and might be interested in knowing the property of the sender ( for instance whether it is a vehicle or not or what location it belongs to)

B. Integrity

Integrity implies the originality of the message; that it is tampered in an unauthorized manner from the time of its incipience. It could be possible by the intrusion of a malicious node that modifies the original information that may cause technical inconvenience in the machine.

C. Availability

It is the property by which all the communication set up must be made vivid and functioning. This property deals with the availability of certain resources manipulated by the protocol. Many applications require faster responses from the sensors since delays make certain messages meaningless or result in devastating consequences.

D. Confidentiality

It is the process by which a message is encrypted for protection from intrusions by unauthorized users. It prevents unauthorized nodes from accessing the content of the messages.

F. Non –Repudiation

It is the method by which the sender and receiver could trace the transaction of the message as if it was sent and received by the corresponding entities.

## III. CLASSFICATION VANET ATTACKS

This section classifies VANET attacks based on the security requirements. The classification based on [19] is shown in Fig.1.

### *A. Attacks on availability*

- Denial-of-Service: In this attack, several duplicate messages are sent to other vehicles and Road Side Units(RSU) to jam communication between the vehicle and RSU and to reduce efficiency of the VANET
- Jamming: It is same as DoS attack or it is the physical level of DoS attack. It jams the communication channel using strong interfering signals.
- Greedy behavior: This attack happens at physical layer in the OSI model, mainly on MAC layer. Its main purpose is to restrict the other nodes from using support and services.
- Broadcast tampering: In this attack, false traffic messages are generated in VANET. This may cause large problems in VANET
- Malware: This kind of attack is executed by insider attackers wherein some false updates are incorporated into the VANET services.
- Spamming: This attack happens through the flooding of packets in VANET. It may result in reduced performance of VANET.
- Black hole attack: It is a serious attack on VANET. In this attack, the malicious node refuses to receive packets which may result in the loss of data packet in VANET.

### *B. Attacks on authenticity*

- Sybil attack: In [12], it says that Sybil attacks are those in which a malicious node behaves as if they are multiple nodes.
- Replay attack: As per this attack the attacker intercepts and creates replica copies of the Replay message which may be used for malicious activity in VANET
- GPS spoofing: In VANET, location is of great importance. In this, the attacker changes the location of the vehicle by spoofing of the GPS (Global Positioning System).
- Position faking: It is similar to GPS spoofing wherein fake location messages are send in VANET.
- Tunneling : This is identical to wormhole attack, where the attacker uses the same network to establish a private connection [18]
- Key/certificate replication: In this attack, the attacker replicates secret security key or certificate.
- Message tampering/suppression/fabrication/alteration: In this attack, the attacker changes or modifies or deletes some part of the message. It also an attack against the integrity.

### *C. Attacks on confidentiality*

- Eavesdropping attack: In this attack, the attacker listening to the communication channel uses the information to quite easily attack the system. Through this attack, several types of useful information can be collected such as location data that can be used for tracking vehicles.
- Traffic analysis attack: In this mode of attack, the attacker listening on the traffic in VANET employs the information to attack any system readily.

### *D. Attacks on integrity*

- Masquerading: In this attack, the attacker personates some other vehicles by providing false ID. It may cause man-in-middle attack and other attacks. It is also an attack on authenticity.

### E. Attacks on non-repudiation

- Loss of events traceability: This attack takes place during security auditing of the computer network. It erases action-traces and creates confusion on auditors.

### F. Other attacks

- Bogus information attack: In this attack, the attacker sends false information to other nodes for their benefits.
- Malicious node attack: In this attack, a node misbehaves during the communication, like they could ride beyond the normal speed or abstain from responding at the proper time.
- Selective forwarding: In this attack, the attacker changes the route of selected packets as per his interest.
- Flooding of RREQ message: In this attack, flooding of Route Request message takes place in case the node receiving the request is a malicious node. It is another type of DoS attack

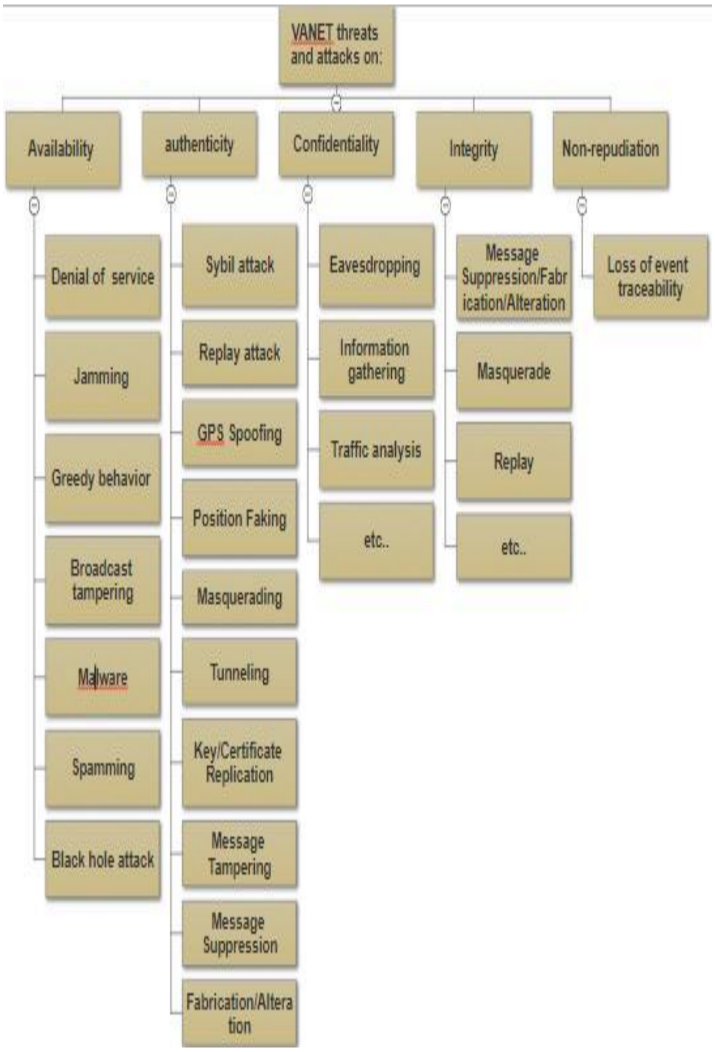

Fig.1. Classification of VANET attacks

## IV. .CONCLUSION

This paper intends to give a well-defined overview of recent advances in VANET security and threats and vulnerabilities of VANET in different scenarios. We have tried to classify the attacks and threats based on the security requirements in VANET. We have also attempted to describe20 types of attacks in VANET. Further a brief and sequential discussion is made on several security mechanisms proposed to each and every attack.

## REFERENCES

[1] Ameneh Daeinabi,Akbar Ghaffarpour Rahbar "Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks"in Multimed Tools Appl 2013 66:325–338

[2] Shan Chang, Yong Qi , Hongzi Zhu , Jizhong Zhao, Xuemin (Sherman) Shen "Footprint: Detecting Sybil Attacks in Urban Vehicular Networks" in parallel and distributed systems, VOL. 23, no. 6, june 2012

[3] Rasheed Hussain , HeekuckOh "On Secure and Privacy-Aware Sybil Attack Detection in Vehicular Communications" in Wireless Pers Commun 2014 77:2649–2673

[4] Omar Abdel Wahab , Hadi Otrok ,Azzam Mourad "A cooperative watchdog model based on Dempster–Shafer for detectingmisbehaving vehicles" in Computer Communications VOL 41 ,2014, 43–54

[5] . Karan Verma, Halabi Hasbullah"IP-CHOCK (filter)-Based Detection Scheme for Denial of Service (DoS) attacks in VANET" in Computer and Information Sciences (ICCOINS) ,2014

[6] Hichem Sedjelmac, Sidi Mohammed Senouci "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks" in Computers and Electrical EngineeringVOL 43,2015, 33-47

[7] RaghadBaiad, OmarAlhussein, HadiOtrok, SamiMuhaidat "Novel cross layer detection schemes to detect blackhole attack against QoS-OLSR protocol in VANET" in Vehicular Communications VOL 5 ,2016, 9–17

[8] Parul Tyagi , Deepak Dembla "Performance analysis and implementation of proposed mechanism fordetection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET)" in Egyptian Informatics Journal VOL 18 ,2017, 133–139

[9] Kamran Zaidi, Milos B. Milojevic, Veselin Rakocevic, Arumugam Nallanathan,and Muttukrishnan Rajarajan "Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection" in vehicular technology, VOL. 65, no. 8, august 2016

[10] Mohammad Javad, Faghihniya, Seyed Mojtaba Hosseini, Maryam Tahmasebi, "Security upgrade against RREQ flooding attack by using balance index on vehicular ad hoc network" in Wireless Netw ,2017, VOL 23,1863–1874

[11] Tarek Bouali ,Sidi-Mohammed Senouci and Hichem Sedjelmac"A distributed detection and prevention scheme from malicious nodes in vehicular networks" in Int. J. Commun. Syst. 2016,VOL 29,1683–1704

[12] Thiago Bruno M. de Sales , Angelo Perkusich , Leandro Melo de Sales , Hyggo Oliveira de Almeida , Gustavo Soares , Marcello de Sales "ASAP -V: A privacy-preserving authentication and sybil detection protocol for VANETs" in Information Sciences VOL 372 ,2016, 208–224

[13] OmarAbdelWahab,AzzamMourad,HadiOtrok,JamalBentahar"CEAP:SVMbased intelligent detection model for clustered vehicularadhocnetworks"in Expert Systems With Applications50,2016,40–54

[14] HichemSedjelmaci, Sidi Mohammed Senouci, TarekBouali "Predict and prevent from misbehaving intruders in heterogeneous vehicular networks" in Vehicular Communications VOL 10, October 2017, Pages 74-83

[15] Roshan Jahan , Preetam Suman "Detection of malicious node and development of routing strategy in VANET" in 3rd International Conference on Signal Processing and Integrated Networks (SPIN) ,2016

[16] Xia Feng and Jin Tang "Obfuscated RSUs Vector Based Signature Scheme for Detecting Conspiracy Sybil Attack in VANETs" in Hindawi Mobile Information Systems Volume 2017, Article ID 4682538

[17] Mohamed Nidhal Mejri , Jalel Ben-Othman " GDVAN: A New Greedy Behavior Attack Detection Algorithm for VANETs" in mobile computing, VOL. 16, no. 3, march 2017

[18] A. Rawat, S. Sharma, R. Sushil, "VANET: security attacks and its possible solutions" , J. Inform. Oper. Manag. 3 (1) (2012) 301–304.

[19] Richard Gilles Engoulou, Martine Bellaïche , Samuel Pierre, Alejandro Quintero, "VANET security surveys", in Computer Communications VOL 44 ,2014, 1–13

[20] G. Jyoti, M.S. Gaur, in S. Auerbach (Ed.), "Security of Self-organizing NetworksMANET, WSN, WMN, VANET", in 1st Auerbach Publications Boston, MA, USA 2010

TABLE 1: COMPARISON OF SURVEY WORKS BASED ON SECURITY MECHANISMS

| **Author and publication year** | **Title** | **Detection attacks** | **Technique/Algorithm** | **Evaluation** | **Merits/Demerits** |
|---|---|---|---|---|---|
| [1]Ameneh Daeinabi and Akbar Ghaffarpour Rahbar[2011] | Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks | To detect malicious vehicles | This involves a misbehave detection method at the application layer using DMV algorithm that detects malicious node and sends warning message. | The number of packets that are dropped/duplicated by the malicious node based on time | DMV has improved .Better Performance even at high speeds |
| [2]Shan Chang, Yong Qi, Hongzi Zhu,Jizhong Zhao, Xuemin (Sherman) Shen[2012] | Footprint: Detecting Sybil Attacks in Urban Vehicular Networks | Sybil attack | It uses a linkable ring signature which is signer ambiguous, to generate location-hidden authorized message. Signer ambiguous means it stores information about the location and disguises the original authorized message. | Time complexity of the signature generation, verification algorithms and the Sybil attack detection algorithm | In this paper, every road side units (RSUs) are considered to be trustworthy. If one RSU is compromised, it cannot detected. |
| [3]Rasheed Hussain, · Heekuck Oh [2014] | On Secure and Privacy-Aware Sybil Attack Detection in Vehicular Communications | Sybil attack and privacy | A tamper resistant module (TRM) is used for data analysis and sybil attacks are avoided through beacons. Road side units (RSUs) reports the attacks to the revocation authority(s) by generating event reporting message (ERM). | Computation time involved in the message generation. | It preserves the privacy in event reporting message and if vehicles travel under only one domain RSU, the Sybil attacks can be easily detected. But it requires more storage space. |
| [4]Omar Abdel Wahab, Hadi Otrok ,Azzam Mourad [2014] | A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles | It detects misbehaving vehicle | It uses Quality of Service Optimized Link State Routing (QoS-OLSR) protocol for detecting misbehaving vehicles. It contains two phases: motivation phase and a detection phase. In motivation phase, trusted MPR and cluster head are elected. In detection phase, behavior of the MPR nodes are monitored. It uses Dempster–Shafer method to make final decision. | Number of nodes, packet delivery ratio and stability of VANET. | It doesn't give any idea about dealing with mobile nature of VANET<br>It gives solution to reduce accidents due to over speed. |
| [5]Karan Verma, Halabi Hasbullah[2014] | IP-CHOCK (filter)-Based Detection Scheme for Denial-of-Service(DoS)attacks in VANET | Detection of Denial of service (DoS) in VANET | The Bloom-filter-based detection method, enhances the availability of a service by detecting and defending the IP spoofing of addresses.. | Detection time of attack and detection probability of the system | It requires fewer resources and are easily deployable. But, it does not give solution for handling mobile nodes. |

| | | | | | |
|---|---|---|---|---|---|
| [6]Hichem Sedjelmai, Sidi Mohamed Senouci[2015] | An accurate and efficient collaborative intrusion detection framework to secure vehicular networks | Selective forwarding, black hole attack, packet duplication, resource exhaustion attack, wormhole attack and Sybil attack | The proposed approach applies certain number of detection agents that run at three levels i.e. cluster member, cluster-head and RSU. It contains 2 main detection systems and a decision system. It classifies nodes based on the monitoring and attacker will be stored in Blacklist. RSU broadcasts black list in order to prevent legitimate vehicles to communicate with them. | Detection rate of attacks, false positive ratio and detection time | It doesn’t give accurate rules for classification of malicious node and normal node. |
| [7]RaghadBaiad, OmarAlhussein, HadiOtrok,SamiMuhaidat[2016] | Novel cross layer detection schemes to detect black hole attack against QoS-OLSR protocol in VANET | Detection of black hole attack | Proposes cooperative cross layer based intrusion detection schemes (IDSs) to enhance the performance of the watchdog detection technique in black hole attack. It introduces the individual intrusion detectors for network layer, physical layer and MAC layer and then proposes two cross layers detection schemes it integrates them together to build a reliable and efficient IDS scheme. | Detection rate and false alarm rate of the scheme. | It can be useful for both dense and light number of nodes. |
| [8]Parul Tyagi, Deepak Dembla [2016] | Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET) | Detection of black hole attack | Algorithm is proposed to enhance the security mechanism of AODV protocol and to introduce a mechanism to detect Black Hole attacks by storing all route replies in a look up table. Priority is calculated based on sequence number and the RREP (route replay) having presumably very high Destination sequence number is discarded. | Throughput, packet loss ratio and collision rate in VANET routing protocols. | It doesn’t consider the scenario in which, source node is unaware of which node receives the transmitted Request packet and sends a reply.<br>It enhances the AODV protocol for black hole detection. |
| [9]Kamran Zaidi,Mils B.Milojei, Veselin Rakocevic,Arumugam,Nallanathan and Muttukrishnan Rajarajan[2016] | Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection | To detect anomalies and identify rogue nodes | The proposed host based Intrusion Detection effectively detects a false information attack using statistical techniques and can also detect other types of attacks. The extensive data collected are analyzed using statistical techniques, and the decision to accept or reject data is based on hypothesis testing. | Density of nodes, beaconing time and the number of rouge nodes. | It is not dependent on any infrastructure. It is possible for vehicles to keep the network functioning even when up to 40% of nodes are malicious and contribute false Parameter values. |
| [10]Mohammad Javad,Faghihniya, Seyed Mojtaba Hosseini,Maryam Tahmasebi[2016] | Security upgrade against RREQ(Route Request) flooding attack by using balance index on vehicular ad hoc network | DoS attack happening due to flooding of RREQ | The proposed protocol is B-AODV. Balance index is a measure to accept or reject the RREQ packets. When RREQ reaches to the node, receiver node increases RREQ source IP counter value. Each node after receiving the RREQ, will compute the balance index. If number of source node RREQ is more than balance index, then receiver node drops RREQ. The balance index is calculated by mean and standard deviation of the number of RREQ packets | Routing overhead, end to end delay, packet Delivery ratio (PDR) and throughput. | It doesn’t give any clarification about capturing number of RREQ packets. |

| | | | | | |
|---|---|---|---|---|---|
| [11]Tarek Bouali,Sidi-Mohamed Senouci and Hichem Sedjelmac[2016] | A distributed detection and prevention scheme from malicious nodes in vehicular networks | To detect the malicious nodes | Proposed a new distributed proactive Intrusion Detection System (IPDS) based on Kalman Filter, which is able to predict the trustworthiness of network members, detect suspected. Attackers using a classification process, and inform the nodes rest of the network. It uses a clustered architecture where a cluster-head is responsible for monitoring and categorization into appropriate list (White, Gray and Black). The white list contains identities of the most trustworthy vehicles, the gray list holds nodes that are not malicious but have low trust values and the black list is used to store malicious identities. | Packet delivery ratio , end to end delay and detection rate of malicious node | It predicts the future behavior of vehicle |
| [12]Thiago Bruno M.deSales ,Angelo Perkusich ,LeandroMelo de Sales,HyggoOliveira deAlmeida, Gustavo Soares, Marcello deSales[2016] | ASAP-V:A privacy-preserving authentication and Sybil detection protocol for VANETs | Sybil attack | The proposed ASAP -V protocol is divided into four phases:<br>Registration phase: a certifying authority register the details of vehicle like signing key, digital certificate temporary key.<br>Assignment phase: Is responsible for managing pseudonym assignments to vehicles.<br>Detection phase: Detects the Sybil attacked vehicle<br>Prosecution phase: Once a misbehaved vehicle v is detected, all other vehicles store v's messages as a set of sample n suspected messages. | Management, storage, computation, communication overheads, detection time and false positive rate for Sybil attack | It has good false-negative and false-positive detections without a centralized infrastructure during detection time. |
| [13]OmarAbdel Wahab,Azzam Mourad,HadiOtrok,JamalBentahar[2016] | CEAP:SVM(Support Vector Machine)-basedintelligentdetectionmodelforclusteredvehicularadhocnetworks | Detection of malicious vehicles | CEAP (Collection,Exchange,Analysis,and Propagation). Detects malicious vehicles in the clustered VANET. The model has four phases:<br>Data collection phase: The cluster members, including the cluster head, are appointed as watchdogs to continuously monitor and analyze the behavior of the MPR nodes.<br>Data exchange: the watchdogs located in the same cluster share their collected evidences<br>Data analysis phase: It consists of analyzing the training set using SVM and classifying the MPRs accordingly. Data propagation phase: The cluster-head propagates the classes determined within its cluster to the other clusters whenever a contact between them takes place in order to mitigate the detection time and overhead. | Accuracy rate, attack detection rate, false positive rate and packet delivery ratio. | It doesn't consider condition that the cluster-heads may also be malicious themselves by propagating falsified data. |
| [14]HichemSedjelmaci, Sidi Mohammed,Senouci, TarekBouali[2016] | Predict and prevent from misbehaving intruders in heterogeneous vehicular networks | Detection of misbehaving vehicle | An efficient attack detection and prediction scheme is proposed detect and especially predict the future misbehavior of a vehicle. This scheme is based on game theory concept to predict the misbehavior of an attacker. The attack–defense problem is formulated as a game between two players: the Attacker (i.e. misbehavior vehicle) and the Services Centre (SC). Based on Nash Equilibrium (NE) concept it predicts the future behavior of monitored vehicles. | Accuracy Prediction Rate (APR), which is false positive rate, Detection Time. | It can detect and predict the future misbehavior of a malicious vehicle. |
| [15]Roshan Jahan and | Detection of | Detection of | This paper presents a routing | Node speed, | It doesn't give |

| | | | | | |
|---|---|---|---|---|---|
| Preetam Suman[2016] | malicious node and development of routing-strategy in VANET | malicious node | strategy to prevent from attack and identify the malicious node. It identifies malicious node by double acknowledgement of packet. | throughput, packet drop and packet delivery ratio. | solution for handling mobile nature of nodes. |
| [16]Xia Feng and Jin Tang [2017] | Obfuscated RSUs Vector-Based Signature Scheme for Detecting Conspiracy Sybil Attack in VANETs | Sybil attack | It is based on the idea of vehicle's identity certificates. It uses ring based identification scheme and replaces vehicles' identities with their trajectory for the purpose of anonymity. | Computation time and Privacy Protection | It is assumed that information synchronization of all RSUs are stored in signature verification module |
| [17]Mohamed Nidhal Mejri and Jalel Ben-Othman[2017] | GDVAN: A New Greedy Behavior Attack Detection Algorithm for VANETs | DoS attacks | If a greedy behavior is suspected, the watchdog software determines the responsible nodes using the packet delivery ratio, the queue length, the throughput and the back off supervision. | Connection duration time and number detected nodes. | It considers the greedy behavior detection scheme in VANET. |