Implementation and Analysis of Detection of Wormhole Attack in VANET

Parteek Kumar
M-Tech Student , Kurukshetra University, India.

Dr.Sahil Verma
Lovely Professional University, Phagwara, India

Kavita
Lovely Professional University, Phagwara, India

Ranbir Singh Batth
Lovely Professional University , Phagwara, India

Abstract – To reduce the road accidents, one possible way is to exchange the information among vehicles on time which helps them to analyse the traffic environment. The information can be exchanged between vehicles in a vehicular ad-hoc n/w known as VANETs. VANETs are appearing as encouraging field in wireless technology which aims to create a mobile network in which vehicles communicate with each other in the absence of centralized architecture that helps to improve the road safety by exchanging the messages among vehicles or by providing new convenient services to the road users.

Index Terms – VANET, Intelligent Transport System (ITS), Wormhole Attack, Security and Detection.

1. INTRODUCTION

The new age of vehicles is network of sensors. The vehicles are also known as computers running on road. As mentioned above that there has been huge amount of life being lost on roads. So with increase in road traffic, there needs to be increase in road safety as well. We need to have a mechanism by virtue of which the vehicles can be made smart enough so that they are able to handle the road safety at their own.

This concept was the laid under VANETs. The vehicles communicate with each other through VANET & come to know about if there is any diversion ahead or any other information required. So VANETs support communication among the vehicle. Actually VANETs support four types of communication [7]:

Vehicle to vehicle (V2V):

With the help of intercommunication the vehicles interact with each other to ensure safety on road. The communication could be information exchange about some accident ahead or diversion.

Vehicle to Infrastructure (V2I):

Vehicles and road side units interact with each other through this communication. The communication could be data swap like information from road side garage or filling station.

Hybrid communication:

This communication is heuristic communication of above communications. It includes inter vehicle and vehicle and infrastructure communication.

Intra-vehicular communication:

This communication is vital for the vehicle as it comes to know the information about itself like fatigue detection of driver, GPS navigation etc.

VANETs have certain advantages such as providing frequent information to the drivers, reduction of road accidents etc. It also provides security and insecurity applications. The eventual objective of VANETs for transfers the messages among vehicles efficiently. The transferred messages have a great impact on the driver's behaviour if the unauthorised user alters the messages which results to change the network topology. In VANETs, attackers create a problem by launching numerous attacks which lead to disturb the network condition and security may be threatened by disclosing Ids, sending bogus information, forging data, jamming the traffic, violating privacy etc. So, security is still an open issue in the ad-hoc network.

1.1 VANET Characteristics

As MANETs and VANETs both have some trivial characteristics such as no centralization node, self management, short bandwidth but VANETs have some

exclusive characteristics that make it more challenging which are discussed below:

High Flexibility:

Vehicular Advanced Developers Hands-On Conference (Ad-Hoc) n/w is highly flexible because of the fast speed for vehicles which makes harder to predict the node's position in VANETs.

Quickly change in the n/w topology:

High flexibility and the irregular speed of vehicles are the reasons, that the vehicles may leave or join the network in very short duration. This leads to change the network topology frequently.

Indefinite n/w size:

The n/w size for VANETs is geopolitically indefinite reason being VANETs are be carried out for one big city, distinct cities or for countries.

Time constraint:

To make the decisions accurate, the report in VANETs need to be conveyed towards the nodes within a specific time. Otherwise the system becomes worthless.

Frequent change of information:

Due to the Advanced Developers Hands-On Conference (Ad-Hoc) personality of VANETs, the nodes get report from neighbour vehicles and RSUs. This result frequently changes of information among vehicles.

Improved physical security:

As the VANET nodes are physically secured which makes harder to compromise the nodes physically and lowers the consequences of infrastructure attack.

2. RELATED WORK

Otero et al. implemented two procedures which are based on range-free localization methods for the detection of wormhole. In the proposed work, First procedure performed the detection process simultaneously by using the localization procedure to find the node's position and the second procedure followed the post-localization detection approach to validate the estimate node position and detected the malicious nodes.

Fatehpuria et al. presented wormhole attack prevention by verification of digital signatures. The proposed work has identified two types of wormhole attacks: hidden and exposed attacks by using a mechanism delay per hop indication that detects the pinpoint location of wormhole and prevent it. It has followed two phases to identify the attacks. In the first phase, verification of digital signature is done to depict the presence of wormhole or not and in the second phase, delay/hop is analyzed using RTT mechanism.

Harikishan et al. proposed a unique approach called IDS with use of Fuzzy inference system to encounter to the intrusion behaviour within the network. Using Sugeno Fuzzy Inference approach and ANFIS editor, an accurate attack was detected. In proposed work, MATLAB and ANFIS editor is used for experimentation and KDD CUP dataset is used for detecting the anomaly based intrusion with the use of fuzzy inference approach.

Upadhay. Described WPAODV technology for identify and prevent any wormhole. The WPAODV is depending on the hybrid model that encapsulates the proper area, neighbour node and hop count approach. In the planned scheme, WPAODV extends the AODV by adding one extra feature in it i.e. after detection; WPAODV will bypass the path that is having a wormhole. To detect whether the route is having a wormhole or not, the WPAODV used divide and conquer mechanism over the route recommended by AODV. The main objective of the planned scheme is to detect the wormhole in the route recommended by AODV.

Shamaei et al. presented a two-phase detection mechanism to detect and prevent the wormhole attacks. In the first phase, it checks whether tunnel exists or not on the selected path by calculating the average delay per hop. If the average delay per hop is higher than the predefined threshold than the wormhole existence can be imagined and in the second phase it depicts the existence of wormhole attacks and discovers the malicious node. The proposed scheme has the capability to detect in band and out band attacks without need of any addition H/W.

Biswas implemented WADP i.e. Wormhole attack detects and prevents approach by altering the AODV routing protocol. The modification in AODV is done by doing addition of two extra fields in the route reply packet that is the IP of intermediate node and the unique number assigned to it. Assumption is made in the proposed work i.e. only authentic nodes know the information. If the node does not able to specify the right IP and number then it will be considered as malicious node. WADP is an enhancement of WAP algorithm. False positives are removed in the WADP algorithm by using the node authentication process and it also helps to know the exact location of wormhole node. Thus this process is considered as a double verification for the detection of wormhole attack.

Karthiga et al. proposed a state traversal mechanism incorporate with finite state machine (FSM) to identify network intrusion with the use of optimized pattern matching algorithm and are also responsible for reduction of memory space required during the implementation of FSM. To achieve this goal, longest common substring algorithm is used and then the outcomes are correlated with the AC algorithm and the bit split algorithm. By following this approach, proposed algorithm has achieved the goal of reduction of 26% memory compared with the AC algorithm for total string patterns.

Panja et al. implemented IDS using neuro fuzzy classifiers to classify the network activities. They have also merged the Genetic Algorithm along with the Artificial Neural Fuzzy Inference System (ANFIS) to optimize data classification. In this research work, the neuro-fuzzy classifiers are used for the classification of initial network traffic. Fuzzy inference system determines he behavior of activity whether it is normal or malicious. It creates the fuzzy rule by using the human knowledge. The main aim of the defined system for trim the number of false positives in IDS.

Aggarwal et al. proposed a beacon node mechanism with neighbour node discovery for the identify and counter of wormhole attack. Defined technique detects any wormhole by the use of deviation in routing information among neighbours and it does not require any location information and additional hardware. The main goal of the defined method is to detect the wormhole in the route recommended for the AODV with the use of divide and conquer technique that will make all possible combinations of nodes. If any combination comes out to be suspicious, it will be considered as malicious.

3. SECURITY REQUIREMENTS

Security is indispensable aspect in any area especially in VANETS. In previous section we discussed about the loopholes that exist. These loopholes can be exploited by an intruder or a malicious driver. So the security is absolute necessary in VANETS. The most important security requirement comprises of CIA triad. The CIA triad stands for Confidentiality, Integrity and Availability. Apart from these requirements there are two more requirements namely authentication and non-repudiation.

Confidentiality:

It aims to provide the guarantee that no malicious driver or vehicle is able to access the private information of any other vehicle or driver. The private information could be number plate details, license information or the vehicle status etc. This security requirement is established by using encryption and keys which have expiry time as well

Integrity:

This security requirement guarantees that the message is not changed from source to destination. Whatever the type or format of message is sent by sender the same message is being received by the receiver. There is not even a single minute change in message. This requirement is indispensable as it may lead to wrong or incomplete information. In some life saving applications this is very necessary requirement. The group signature enables this requirement.

Availability:

This security requirement means the network must be available all the time. As VANETS have time critical applications, the first most important requirement is the full time availability of ad hoc network. Sometimes the application requires VANETS to reply as early as possible. This lag in reply for particular request could make the service useless. To solve the availability problem group signature technique is proposed. The DOS and DDOS attack could affect if this security requirement is not established.

Non-Repudiation:

The non-repudiation means that the sender or receiver cannot say no to the messages being sent or received by them. The non repudiation means auditing. There could be information regarding accident or information regarding car parking. The sender later cannot decline the message. The bogus information attack could be launched if there would have been no security requirement like this. This requirement gives the guarantee that intruder could be caught even after the attack is launched. In some cases non-repudiation is also known as auditability. This security requirement allows us to identify the attacker even after the attack has been launched.

Authentication:

This is utmost important requirement as it ensures the sender to prove that it is a legal sender. This is accomplished by public or private keys and CA. The sender sends the message with the key and certificate which is checked by the receiver. However signing the information makes the system complex. To make this task simple an efficient Elliptical Curve Cryptography is used.

4. ATTACKS IN VANETs

There are various security attacks to which the VANET networks are vulnerable to. These attacks have huge impact not only on the network but this could also lead to loss of life as well [13]. Fig 1.1 shows attacks on various security requirements.

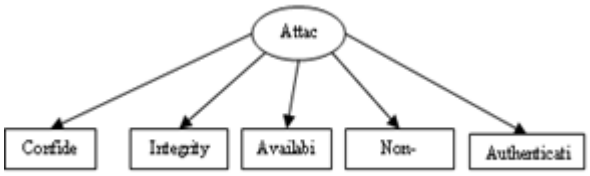

Fig. 1.1: Classification of attacks

Following are the some of the security attacks which can be launched on VANETs.

Denial of Service Attack:

The Denial of Service (DoS) attack is the attack by virtue of which an ad-hoc network is unavailable. It can be launched either by flooding the network with unusual and useless request so that the resources of the network are kept in use and the legitimate request will not be able to have access to that

particular resource. The other way of launching this attack is by crashing the communication channel [10].

Distributed Denial of Service:

This is a variant to the above attack in which more than one attacker tries to launch the Denial of Service attack on the victim node. In this attack the attack is launched with the usage of multiple computers and resources are acquired by multiple computers located at multiple positions as well. The main objective of this attack is to deny the availability as a security requirement.

Replay Attacks:

In this type of attack, the intruder replays the transmission of previous messages and tries to gain the access of the system and other resources available at the time of sending the message [8].

Sybil Attack [12]:

Sybil attack allows an attacker to create multiple false identities known as Sybil nodes which will behave as a normal node. It provides false belief to other vehicles by sending erroneous messages such as traffic jam etc and each message contains the formulated id. The main objective of an attacker is to disturb the whole network for their personal benefits.

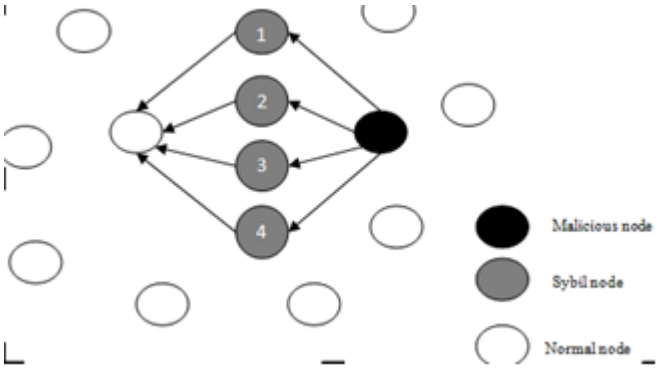

Fig. 1.2: Sybil attack

In Fig 1.2, node 1, node 2, node 3 and node 4 are the Sybil nodes that use the identity of others while communicating with the other nodes to confuse and collapse the network.

Alteration Attack:

This attack is launched when an intruder changes the existing data. This changed data is then forwarded to the network. The other way to launch this attack is delaying the information that has to be sent in the network [11].

Fabrication Attack:

In fabrication attack the attacker sends the untrue information into the network. The information could be wrong or the transmitter could claim it to be someone else.

Masquerading attack:

In this type of attack the attacker actively participates in the network. The attacker tries to pretend like other vehicles using false identity. Message fabrication, replay attack and alteration attacks could be used towards masquerading.

Tunneling attack:

The intruder tries to establish a network between two distant ad hoc networks using an extra channel between them. This channel is known as tunnel. The nodes in two distant networks have an impression of being neighbors and send the data through the tunnel. The attacker has an access to tunnel can misuse the data then.

ID Disclosure Attack:

In this attack, the ability of the node to let know its identity is exploited and as a result its location also becomes transparent to the whole network. The intruder sends malware to the neighbors of the target node. These malwares are replicating in nature and hence targets its neighbors. When the malware reaches the neighbor of the intruder, it notes the location of target node as well as its identity is noted. One of the solutions proposed is to encrypt the confidential information of vehicle like number plate and location and later uses Public Key Infrastructure.

Node Impersonation Attack:

It is an attack in which a node sends fabricated message and gives an impression that it came from the originator. It can be launched in 2 ways either in form of Sybil attack or in form of false attribute possession. One of the methods to combat this attack by using trust value. The identity of vehicle is noticed by CA based on trust value threshold.

Flooding Attack:

In this type of attack, the attacker tries to flood the network with request for resources to the node which does not even exist, thus making the channel unavailable to be used by legitimate node. This type of attack can be launched in various ways. The control packet flooding and data flooding are one of the common methods to launch flooding attack. It is a subset of Denial of Service attack. One of the way of control flooding is RREQ Flooding. According to RREQ Flooding attack, the attacker broadcast multiple number of RREQ messages to the node which does not exist in the network.

Bogus Information Attack:

In this type of attack, the intruder sends the untrue on invalid or non existing information in the network. This leads to disturbance in the network and inconsistent data. This intruder can be either inside the network or outside the network. The intruder might act as a legitimate node by sending false identity

as bogus information. The intruder could also launch this attack for personal benefit.

Rushing attack:

In this attack, every node before broadcasting the data, first established an authentic way to the destination node using a routing protocol such as AODV, DSR etc. The attacker set a fast transmission path by exploiting the duplicate suppression mechanism to forward the packets. With this process the destination node accepting the packets those are propagated faster than the multi-hop normal route and start dropping the original packets. This forms the rushing attack.

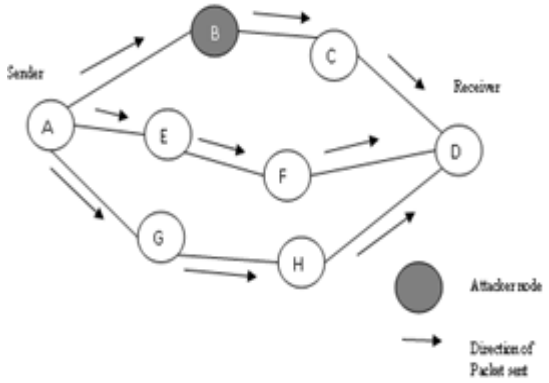

Fig. 1.3: Rushing attack

In Fig 1.3, A is the sender node and D is the receiver node. When node A forwards packet to receiver node, if there is an attacker present then he will accept the packet and forward it with the high transmission speed as compared to the other nodes. In this way, receiver found this path as a valid route and discards the packets that came from other routes.

Blackhole attack:

In this attack, an attacker introduces a malicious node in the network which attracts all other nodes and pretending as the original one. When all other nodes make a false belief on the malicious node and start sending packets through the malicious node then it selectively drop the packets.

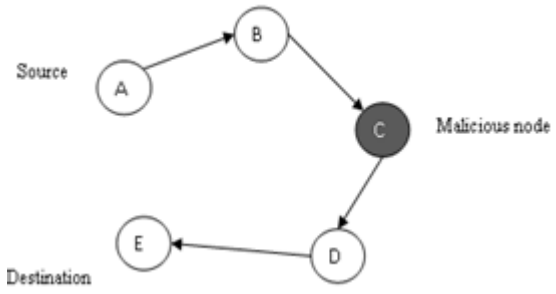

Fig. 1.4: Blackhole attack

In Fig 1.4, Node A is the source node and Node E is the destination node. The attacker node introduces the malicious node i.e. Node c which pretends as an original node. When source node sends packet to the destination node, then the malicious node selectively drop the packets in the network which degrades the communication among nodes.

Wormhole attack:

This is the attack in which attacker joins the two faraway parts of ad-hoc network using an additional communication channel as tunnel. The tunnel records the ongoing communication at one network position and transmits the recorded communication at other network position. This process is also known as tunnelling [5]. To launch this attack, attacker introduces two malicious nodes which are assumed as neighbour nodes that help to transfer the data using tunnel. The malicious nodes attract the other nodes by advertising the shortest path among them so that they can be able to transfer the packets from one network to another network. The path introduced to transfer the packets is harder to predict because it is not a part of real network. Fig 1.5 below shows the wormhole attack where node P (Source) wants to transmit packets to node T (Destination). M1 and M2 are the attacker nodes which are neighbours of node P and T and tunnel is created between them which records the ongoing communication, tampering the data and forward it to the destination.

Classification of wormhole attacks

Wormhole attacks can be categorized into two ways: Wormhole attacks based on implementation process and Wormhole attacks based on the communication medium

Wormhole attacks based on implementation process [10]: Wormhole attacks can be launched using various modes.

Wormhole attack based on packet encapsulation:

In this mode, when the source node broadcast the packets, the malicious node encapsulates the packet and forwards it to the colliding node that decapsulates the packet and again rebroadcast the packet to second colliding node. This results that wormhole is created between two colliding nodes by creating the virtual tunnel in the network.

Wormhole attack based on out of band:

In this mode, two malicious nodes are introduced that uses the direct wireless link or long range directional wireless link to forward the route request. This mode is hard to launch because it requires special hardware.

Wormhole attack using high power transmission:

In this mode, when the malicious node gets RREQ then it forwards the route request with a high power and the other nodes do not have that capability in the network. The node

which listens high power broadcast must be malicious node that receives it and further rebroadcast to the destination.

Wormhole attack using packet relay:

In this mode, malicious node relay packets among two nodes that are far apart to convince them that they are neighbours.

Wormhole attack using protocol deviation:

In this mode, malicious node does not comply with the protocol rules and broadcast the packets without backing off to launch wormhole attack. The main purpose of broadcasting the packets without backing off is to be the first at the destination so that no legitimate request is received by the destination.

Wormhole attacks based on the communication medium

Wormhole attack can be categorized into two ways based on the communication medium: Out of band wormhole attack and in band wormhole attack.

Out of band wormhole attack:

Here, the attackers create a direct link to transfer the data among two endpoints and it requires external communication medium between two end points

In band wormhole attack:

Here, the attacker makes an overlay tunnel over the actual wireless medium and it does not use any external communication medium between two end points.

Simulation Environment and its Parameters

In this section, the proposed work is implemented using ns2 simulator. A dynamic set of mobile nodes is considered in order to set up a vehicular environment. The simulation results are discussed. Performance metrics such as throughput, packet delivery ratio and end to end delay are computed. The initial parameters taken during the simulation are represented in the following table:

Table 1.1: Parameters taken during simulation

Parameters	Values
Simulation Time	400s
Number of mobile nodes	5, 10, 15, 20
Traffic Type	UDP
Topology	Random
Ad-hoc routing protocol	AODV
Size of Packet	1000 bits
Antenna type	Omni
Channel type	Wireless
Network interface type	Physical/ Wireless physical
Radio Propagation Model	Two ray ground
Interface Queue Type	Drop Tail
MAC Protocol	IEEE 802.11
Speed	20

Performance Metrics

Packet Delivery Ratio (PDR):

PDR is the ratio of the total number of packets received by the destination to the total number of packets delivered by the source. Mathematically, it can be defined as:

PDR = (Total number of received packets/ Total number of delivered packets)*100

Throughput:

When the number of packets is transmitted from one node to another node within a specified time interval, then it is known as throughput of the network. It is usually measured in bytes/sec or kilobytes/sec.

End to End delay (E2E delay):

The data transmitted during the average time period from one end to another end.

4.1 Simulation Results

Following is the screenshot of NS2 simulator utilizing NAM.

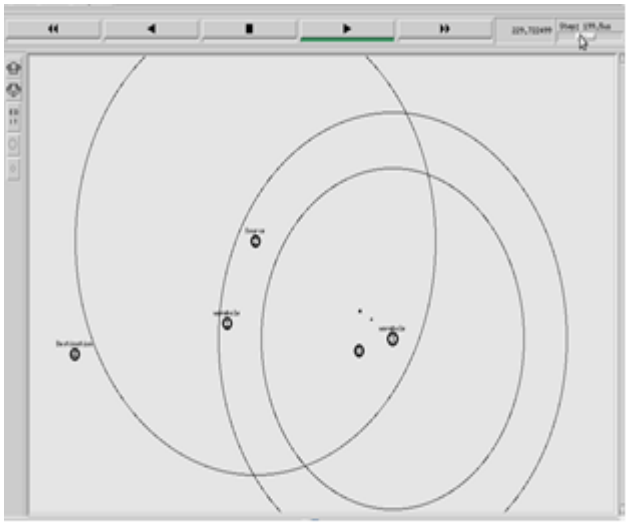

Fig. 1.7 (a) Source node broadcast packets to wormhole nodes

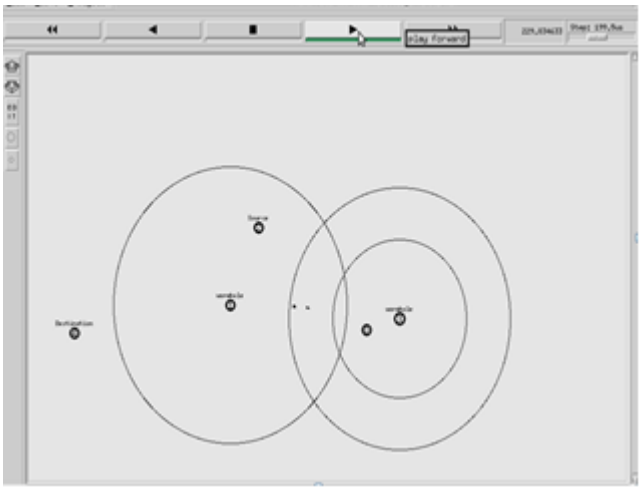

Fig. 1.7 (b) Wormhole node broadcasts packet to another wormhole node

4.1.1 Effect on PDR, Throughput, and E2E delay with varying number of nodes and two wormhole nodes

Packet Delivery ratio is evaluated for the routing protocol AODV, after the wormhole attack and after the proposed scheme deletes the wormhole node. It is seen as shown in Fig 1.7 the packet delivery ratio is very less in case of wormhole attack as wormhole nodes drops the packet and is considerably improved when the proposed scheme deletes the wormhole node. It is analyzed that the normally the packet loss is nearly 8.74% (91.26 ratio of packets sent to packets received) with 15 number of nodes which is highly increased by two wormhole nodes to nearly 49.5% (50.43 ratio of packets sent to packets received) by dropping the packets. The proposed scheme reduces this packet loss to nearly 15% (84.97). Results depict that PDR is highly dropped by wormhole attack of AODV which is then improved by proposed detection scheme.

Throughput analysis of the network is made for the routing protocol AODV, after the network affected by wormhole attack and after the proposed scheme deletes the wormhole node by varying the node density in the network. It is clearly seen that how the degraded throughput of network is improved by our proposed scheme. It is analyzed that throughput for the wormhole affected network is reduced to nearly 63 kbps from 88 kbps with 5 number of nodes which depicts that how these wormhole nodes degrades the network performance. The proposed scheme improves the throughput value after detection of wormhole nodes i.e. from 88 kbps to 73.22 kbps. It is depicted from the results that wormhole attack greatly drops the value of normal AODV protocol which is then improved by proposed detection scheme.

5. CONCLUSION

Security is the considerable problem to implement in VANETs because it is inherently vulnerable to mischievous attacks. Each node is an independent unit in VANETs, thus each node without sufficient security is prone to be compromised. One of the most dangerous attacks is the wormhole attack that disturbs the whole network and degrades the performance of the network. In this thesis, the scheme is proposed which includes the RTT, usage level of links and count of neighbors to detect the wormhole nodes in VANET. The proposed scheme is assessed and simulated against AODV protocol on NS-2 simulator. The efficiency of the proposed scheme is validated through results as the degraded throughput from 17% is raised by proposed scheme to 75%, packet loss rate is reduced to 10 % from 85% after the removal of wormhole nodes. The main advantage of the proposed algorithm is that it is simple and cost effective because it does not require any- additional hardware, clock synchronization and position information. Similarly, the throughput as well as the end to end delay shows the effective results after implementing the proposed algorithm on the attack environment.

REFERENCES

[1] R.S. Raw, M.Kumar and N.Singh, "Security challenges, issues and their solutions for VANET," International journal of Network Security & Its Applications (IJNSA), vol. 5, no. 5, pp. 95-105, 2013.

[2] A.Y. Dhak, S. Yahya and M. Kassim, "A Literature Survey on Security Challenges in VANETs," International Journal of Computer Theory and Engineering, vol. 4, no. 6, pp. 1007-1010, 2012.

[3] R. G. Engoulou et al. "VANET security surveys," in Computer Communications, Canada, 2014.

[4] B. Mokhtar and M. Azab, "Survey on Security Issues in Vehicular Ad Hoc Networks," Alexandria Engineering Journal, vol. 54, no. 4, pp. 1115-1126, 2015.

[5] S. Singh and S. Agrawal, "VANET routing protocols: Issues and challenges" In: Engineering and Computational Sciences (RAECS), 2014 Recent Advances in (pp. 1-5). IEEE.

[6] A. Singh and M. Singh, "A comprehensive review on vehicular ad hoc network," International Journal of Advanced Research in Computer and Communication Engineering, vol. 4, no. 4, pp. 462-468, 2015.

[7] B. Patel and K. Shah, "A survey on vehicular ad hoc networks". IOSR Journal of Computer Engineering (IOSR-JCE) vol.15, no. 4, pp.34–42, 2013

[8] S. Dhankhar and S. Agrawal, "Vanets: A survey on routing protocols and issues", International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), vol3, No.6, pp.13427–13435, 2014.

[9] A. K. Fatehpuria and S. Raghuwanshi, "An Efficient Wormhole Prevention in MANET Through Digital Signature", International Journal of Emerging Technology and Advanced Engineering, vol. 3, no. 3, 2013.

[10] A. Harikishan and P. Srinivasulu , "Intrusion detection system using fuzzy inference system," International Journal of Computer & Organization Trends, vol. 3, no. 8, pp. 345-352, 2013.

[11] V. K. Upadhya and R. K. Shukla, "WPAODV: Wormhole Detection and Prevention Technique", International Journal of Advanced Networking and Applications, vol. 5, no. 3, p. 1922, 2013

[12] S. Shamaei and A. Movaghar, "A Two-Phase Wormhole Attack Detection Scheme in MANETs", The ISC International Journal of Information Security, vol. 6, no. 2, pp. 183-191, 2015..

[13] Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications," ASTM Standard E2213, 2003 (2010).

[14] Vehicle safety communications project task 3 _nal report," The CAMP Vehicle Safety Communications Consortium, Tech. Rep. DOT HS 809 859, Mar. 2005.
[15] R. Baldessari, B. Bdekker, A. Brakemeier, M. Deegener, A. Festag, W. Franz, A. Hiller, C. Kellum, T. Kosch, A. Kovacs, M. Lenardi, A. Lbke, C. Menig, T. Peichl, M. Roeckl, D. Seeberger, M. Strassberger, H. Stratil, H.-J. Vgel, B. Weyl, and W. Zhang, Car-2-car communication consortium manifesto," Tech. Rep. Version 1.1, Aug. 2007.
[16] Joe, M. Milton, and B. Ramakrishnan. "Review of vehicular ad hoc network communication models including WVANET (Web VANET) model and WVANET future research directions." *Wireless networks* 22.7 (2016): 2369-2386.
[17] Joe, M. Milton, and B. Ramakrishnan. "WVANET: Modelling a novel web based communication architecture for vehicular network." *Wireless personal communications* 85.4 (2015): 1987-2001.
[18] Ramakrishnan, B., R. S. Rajesh, and R. S. Shaji. "CBVANET: A cluster based vehicular adhoc network model for simple highway communication." *International Journal of Advanced Networking and Applications* 2.4 (2011): 755-761.