UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 6, June 2017

Segregation of Sybil Attack using Neighbouring Information in VANET

Anu Panchal[1], Dr. Dinesh Singh[2]

M.Tech Student, Computer Science Engineering Department, Deenbandhu Chhotu Ram University of Science and Technology, Murthal, Sonepat[1]

Assistant Professor, Computer Science Engineering Department, Deenbandhu Chhotu Ram University of Science and Technology, Murthal, Sonepat[2]

Abstract: Sybil attack bogus traffic scenario by sending fake message with multiple ID which often cause jam and accident in VANET. It is very hard to defend and establish when it is eject by devise attackers using their real ID. In this paper, we present Neighbor based information (NBH) in which trust value is to be calculated by their neighbor node which restrain to spread false message. NBH can detect Sybil attack with stolen ID. Simulation results show that proposed technique increases the detection and reduces the percentage of Sybil attack.

Keywords: VANET, Sybil Attack, NBH, Simulation, NS-2.

I. INTRODUCTION

In 20 century, there were two researchers named as Alexander Propov also Gugliemo Marconi, worked freely on the radio framework. Previously, 1990, he introduced setup in Russian naval force for two best approach correspondence for area. This will be start up of vehicular correspondence. Those evolvement technologies promote vehicle will interface with neighbor vehicles and flourish into enlarged transport system(ITS) should furnish diverse administrations by using transmission media. On July 2010, on conveyance transmission and data automation endorse on the road conveying, movability, transportation administration, climatic mode, electronic symbol plate disclosure to administrative different operations. [1]. Intelligent Transport System treated as communication automation. Radio Modem transmission on UHF and VHF commonness are extensively used in precise and high area transmission with ITS. Short range correspondence of 350m get by utilizing 802.11 protocol uniquely WAVE(Wireless Access in Vehicular Environment) or Dedicated Short Range Communication(DSRC) affirm by US Department of transportation. Long Range correspondence suggest by utilizing framework data, for example, Wi-Max, GSM, 3G. It is one way or two way short range wireless transmission intended for car. It is utilized for street wellbeing, cautioning, crash shirking, stopping installment and so on.[2]
VANET has been growing up most recent twenty years. In VANET there are two kind of communication i.e. Vehicle to Vehicle communication (V2V) and Vehicle to Infrastructure communication(V2I) as shown in fig 1

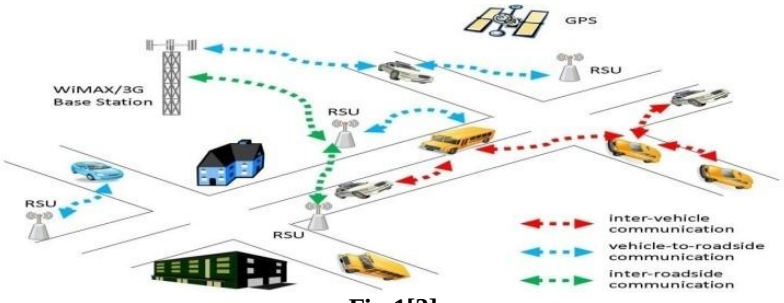


Fig 1[3]

VANET has numerous application, for example, Weather Forecasting, Collision Avoidance, Lane change cautioning, Emergency brake and so on. With these application it convey numerous security danger to VANET, for example, Black opening assault, Wormhole assault, Sybil assault. For preclude with these danger, every vehicle gave his one of a kind personality. A genuine character gives a permit to act vehicle as inner node however personality based security is open in Sybil assault [4]. Sybil assault is a deliberate peril to VANET. In Sybil assault it make numerous personalities to steal or demolish security controls by the method for swindle, constraint or complication sharing. Bluffing of nodes with different nodes dignitary is called malignant node/Sybil assailant and the nodes whose

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 6, June 2017

character is farce is called Sybil nodes. For eg. Ravenous driver can fabricated adjoining number of moving vehicles, which make a hallucination of movement blockage. By then, unique vehicles will pick a support approach to go and cleared the street for insatiable driver. Since the spawn vehicle are control of one vindictive node, the noxious node have furthermore control of other framework, for example, if vehicle reduce its speed superlatively, it will communicate a notice to taking after vehicles. Beneficiaries will hand-off the message to further vehicles. This sending method can be arranging vast number of insidious vehicles. In this assailant can make an enormous accident on expressway, possibly bringing on an unprecedented loss of life. In this paper detail as takes after. Section 2 displays the related work of Sybil assault. Section 3 speaks to the proposed work. Section 4 approach in points of interest of identifies potential Sybil nodes. Section 5 clarifies the technique utilized for reproduction demonstrates and displays come about. Finally, Section 6 conclusion of paper.

II. RELATED WORK

Yo[9] portrayed the Sybil assault, location and proposed the position check to identify Sybil assault. Claimers Estimated Position is utilized for relating signal quality circulation show and proposed two techniques into gathered estimation, which can at last acquired evaluated position of claimer. In radio model utilized radio engendering model, shadowing model comprise two sections. Initial segment is as way model and second part as shadowing reflection demonstrates for variety of energy at certain separation. For assessed node position RSSI is utilized to identify Sybil node. On the off chance that two message have same evaluated position to be set apart as Sybil node.. Shikha[10]proposed a time stamp for Sybil assault, if any vehicle contain numerous timestamp in system of last RSU, it check as Sybil node or if any message contain same timestamp it check as Sybil assault. In this, it give private and computerized mark to timestamp. Along these lines, vehicles not have the capacity to utilize timestamp which is acquired from different vehicles. Azita [11] proposed a fluffy rationale is utilized to find the fake character of foe vehicle by examine neighbor data. Fluffy rationale is utilized to manage inexact as opposed to exact. Esteem lies in the vicinity of 0 and 1. It contain two part named neighborhood administrator module and fluffy leader. Parameter to passed neighbor data than fluffy chief to be passed. In this way, Fuzzy principles and enrollment work is utilized to ascertain enemy level of node. Enemy is contrasted and their limit an incentive in confirmation model to check the conduct of model. Every node send and refresh message table to decide new level of malevolent neighbor node. Park[12] expected CA proposed an accumulation of timestamp for dynamic directions of vehicle for Sybil assault identification. Two timestamp is issued for each activity message send by vehicle and last two RSU vehicles must be passed. Issuing Digital marked timestamp by issuing RSU to diminish overhead. RSU confirm given timestamp than substantial timestamp to make conglomeration timestamp for both present and past. Chen[13] proposed Robust detection(RobSAD) is utilized for Sybil assault in view of typical movement directions and unusual. Approved framework give alter free computerized Signature. In this algo, does not have to bolster other vehicle nodes, Sybil nodes will be meddled or protected by other. Every node should store wrote foundation signature. It is more doable when there is restricted framework assets. Shan[14] proposed endorser equivocal signature, mean the RSU ought not utilize a committed personality to sign message. Impermanent linkable property require two approved message perceived if and just in the event that they created same RSU at given timeframe. Area concealed approved message era plot utilized linkable ring mark. Both are linkable to each other. Back to back approved message acquire by mysterious vehicle from RSU frame a direction to character comparing vehicle. Xin[15] proposed an occasion based notoriety strategy in which every vehicle has one of a kind notoriety esteem and one of a kind trust esteem, Unique ID, mystery key and hash work. At the point when the updating of notoriety and limit esteem inform the driver through UI(User Interface) in OBU. Occasion notoriety can't achieve its limit esteem. Sybil assault stolen ID despite the fact that Sybil assailant can send fake message with genuine id. Neighbor node data accepted that dominant part of neighbors as ordinary nodes.

III. PROPOSED WORK

The real issue of the Vehicular Ad hoc systems is identified with the security for the best possible routing of information. As nodes in the system are exceptionally vehicular and allowed to move anyplace there are high prospect of security dangers. We need such parameters by which we can guarantee that nodes in the system don't act greedy or carry on viciousness. Nodes take a shot at the basis of cooperation for a communication. Hence it is important to give a protected, vigorous, vitality productive, less perplexing and less overheads convention that guarantees secure correspondence and legitimate steering. With the investigation of existing work in the field of Vehicular spontaneous systems it is certain that the fundamental concentration of research is to enhance the enduring quality of system by enhancing the correspondence among the nodes and the directing conventions with the utilization of trust parameter. Trust framework guarantees secure directing and dependable way choice by considering the conduct of nodes as reliable nodes or dishonest and distinguish the acting mischievously nodes. In the event that we need to enhance the execution of system as far as high bundle conveyance proportion, decreased

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

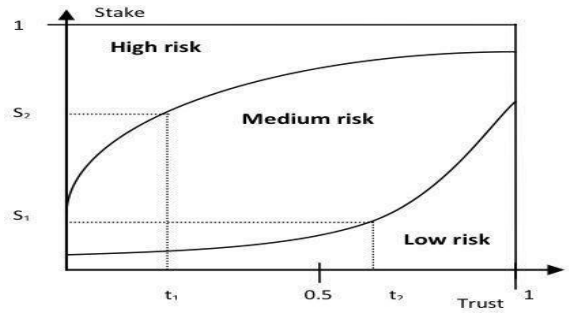
ISO 3297:2007 Certified

Vol. 4, Issue 6, June 2017

message overhead, high throughput and less packet loss, we need such conventions which depend on trust and concept trust. In the meantime it ought to have the capacity to manage traffic jam in the system as and when require emerges. We need to enhance the above said parameters and furthermore keep our architecture straightforward, less unpredictable operations and vitality moderating, we have to join trust and in existing ordinary AODV convention. Trust is dynamic in nature; it continues advancing with area, time and different variables. Trust can be clarified as the stages through which the trust passes or basically we would say be able to the advancement of trust. Trust incorporates Trust Computation, Trust Propagation, Trust Aggregation and Trust Prediction. These are new territories of research in dispersed Adhoc systems.

Trust propagation: It is accessible in sharing the trust esteems among the nodes in the system accordingly lessening overheads.
Trust aggregation: It is utilized to appraise the last estimation of trust. As trust esteems are proliferated in the system, in this manner for single node there are distinctive estimations of trust from various nodes. At that point to get the last trust esteem total is finished. The many-sided quality of conglomeration operations ought to be low.
Trust Prediction: Trust Prediction is utilized to anticipate the estimations of trust on the premise of present and past practices. So there is a need to break down the trust in Vehicular directing conventions and comprehend its effect on its execution. The idea of trust ought to be basic in usage and without complicated adaption packet structure or new increments.

Calculation of Trust
Every node has its trust esteem related with it in the steering table; the esteem can be refreshed just by alternate nodes. Trust esteem is Ti is characterized in the vicinity of 0 and 1, as appeared in figure below, it depends on hazard we will take. A trust esteem Ti of node i more like 1 implies node is trusted more by the associates and A trust esteem Ti of node i more like 0 implies node is not trusted by the companions. Henceforth we have to setup an threshold θ such that



On the off chance that Ti > θ we confide in the node, and scrutinize transmission
On the off chance that Ti < θ we don't confide in the node.
We should accept there are 16 nodes

Step 1: firstly allocate arbitrary Trust an incentive to every node between medium trust an incentive close θ
This is done through rand() work in NS-2.
Step 2: On runtime the two nodes are chosen as Source and Destination,
Step 3: Utilizing AODV path way is chosen with some transitional nodes, trust updation is done through these nodes as these nodes sees the source and destination taking after parameters most brief way S (Dijkastra's), Energy of Node E (E0 beginning and last Ef) , No of bundles (packets)effectively Sent P.
Step 4: Monitor parameters S, E and P for time of communication
Step 5: Update path trust using $T_i = \frac{E_0 - E_f}{S} * p/k$

Case 1
For example initial energy is 1J and final Energy is 0.8 Joules for 2000 packets with path with 3 hops. K is normalizing factor usually K = 1e4 to 1e7, here 1e4 depending upon duration. Trust value to be updated is 0.13 to source and destination

Case 2: Large Path or Hops (ie no shortest path Sybil attack)
For example initial energy is 1J and final Energy is 0.8 Joules for 2000 packets with path with 20 hops. K is normalizing factor usually K = 1e4 to 1e7, here 1e4 depending upon duration. Trust value to be updated is 0.02 to source and destination

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 6, June 2017

B. FLOWCHART

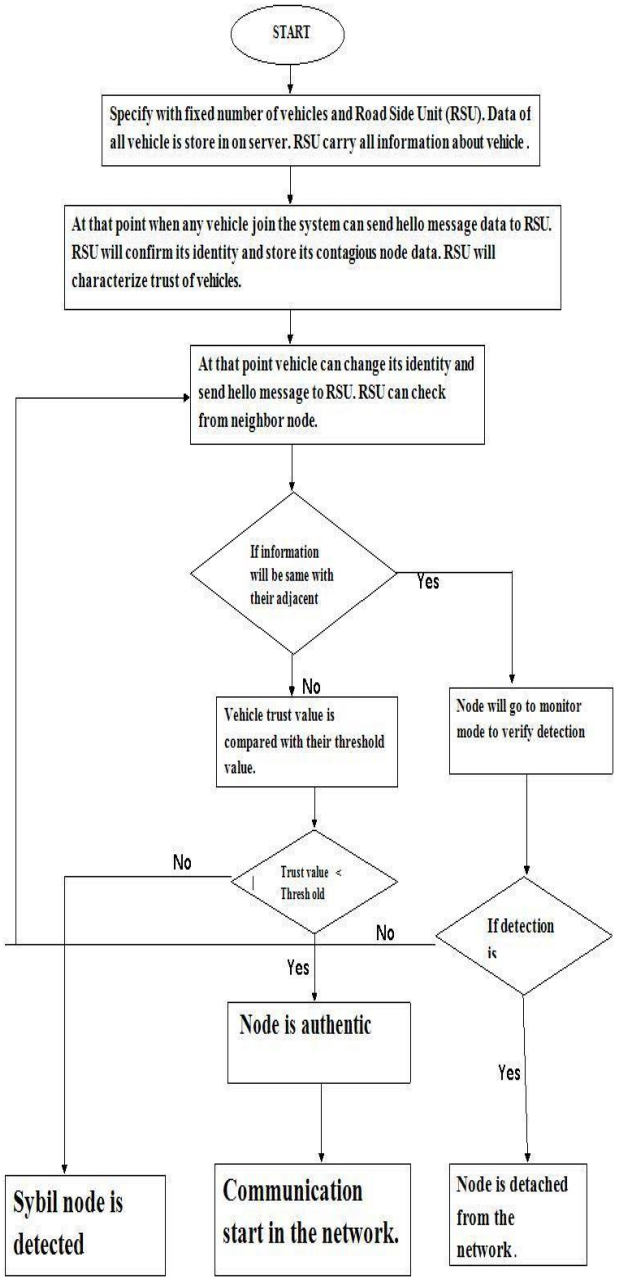


Fig 2

Step1. Establish system of connection with establish number of vehicles and Road Side Unit. Vehicle particular symbol and their ID symbol will be certified. That certified data accessible for all RSU. Server saved all vehicle data. RSU saved all data regarding vehicles.

Step2 If different vehicle unite the network, they transmit "HELLO" information to RSU. RSU reveal the node that they authenticate their identification symbol..

Step3 If ID is validated by RSU and then accumulate its nearby-neighbor node data.

Step4 favorably validated its ID signal. RSU collect all data about certified nearby-neighbor node. RSU disclose the vehicle trust value on road which is to be certified.

Step5 When attacker node send "HELLO" message to RSU. RSU certified vengeful node but when RSU inquiry the nearby-neighbor node and desperate establish as real node. It can be discover from system. RSU will barrage the counselor mode messages in the system and adjacent node of the attacker node start find out attacker node and notice that it is the attacker node.

Step 6. Stop

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 6, June 2017

C. ALGORITHM

As we know Sybil attack introduce to malicious node wrongfully taking on various identities. SO, detect Sybil nodes by real nodes. In this system, a trust value is given to vehicles. Threshold value is to be fixed. Vehicles whose trust value is less than their threshold value to be marked as real vehicles. Generally If trust value is more than threshold value, it is to be marked as Sybil node.

DISCLOSURE AND SEGREGATION ALGORITHM

N:- Node in the network
Tr:- Trust value of node
Th:- Threshold value of node
Ngh:- Neighbor vehicle of node
RSU:- Road Side Unit
n:- Number of new node enter in the network

Step 1:- Start
Step 2:- Node(N) transmit "HELLO" message to Rsu
Step 3:- if Info[authorized] = Info[RSU]
then
RSU assign ID to that Node[Ni] to N
else
Repeat step 1
Step 4:- If info[Ni] = info[N]
then
Tr value[Ni] > Th value[Ni]
then
Node marked as adversary node else
Node marked as real node and start communicate with other node.
Step 5:- RSU store Info[Ngh[Ni]] to RSU
Step 6:- If new node enter in the network and send "HELLO" message. RSU collect all information of Ngh[V] [Neighbor vehicle] of new node.
Step 7:- If Info[n [Ngh[V]]] == Info [R[Ngh[V]]]
then
no adversary node is detected
Step 8 :- If adversary node == detected then
Malicious node is detached with their ID
else
Repeat Step 8
Endif

IV. RESULTS AND SIMULATION

The simulation is based on SUMO and NS2. SUMO is the Simulation of Urban mobility software that enables to simulate the road traffic. SUMO is used to generate simple nodes mobility in NS2. NS2 which is an object oriented, time discrete network simulation tool. It can present many well developed low layer protocol with easy programming interfaces.[6]. NS2 is used with configured area 1000 X 1000 m. Some node act as RSU and some node act as vehicles. For simulation purpose we take 18 nodes. RSU are to be fixed where as other nodes moving with their speed 20 to 40 m/s. For the disclosure of node one node act as Sybil node. AODV protocol is used for communication.

Table 1 Simulation Table

Parameters	Values
Simulator Area	1000 X 80
Number of nodes	18
Vehicle Speed	10 m/s – 40 m/s
Communication range	250m/s
Routing Protocol	AODV
MAC protocol	802.11

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 6, June 2017

A. Experimental Results

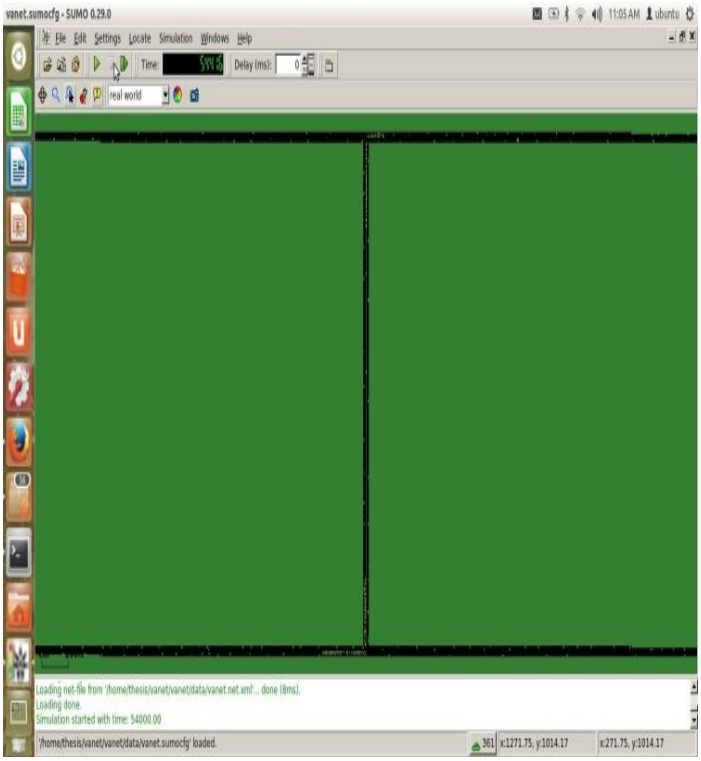


Fig 2(SUMO-GUI)

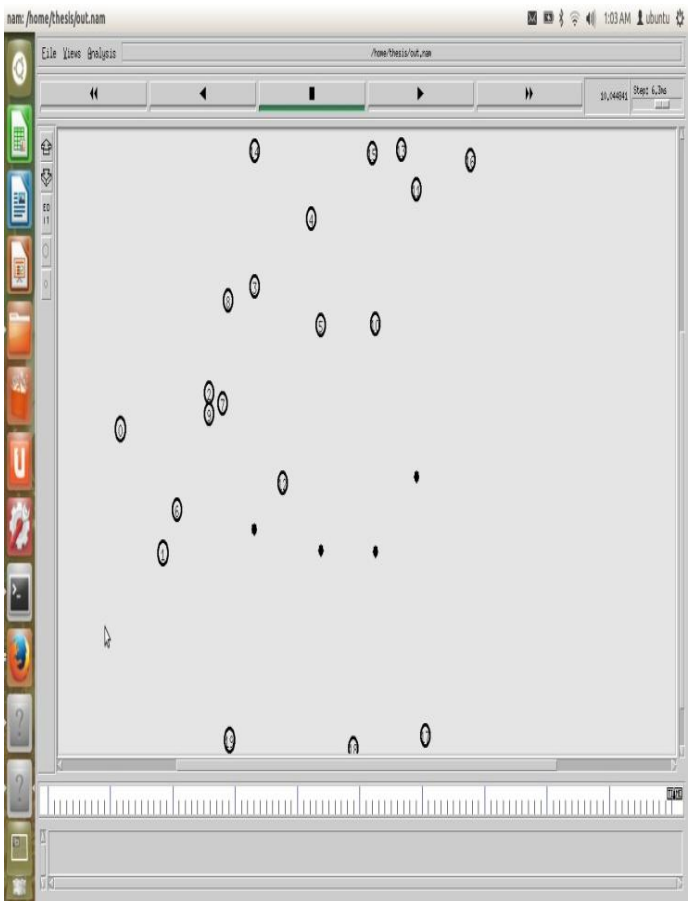


Fig 4 (Number of nodes moving and import to NS2)

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 6, June 2017

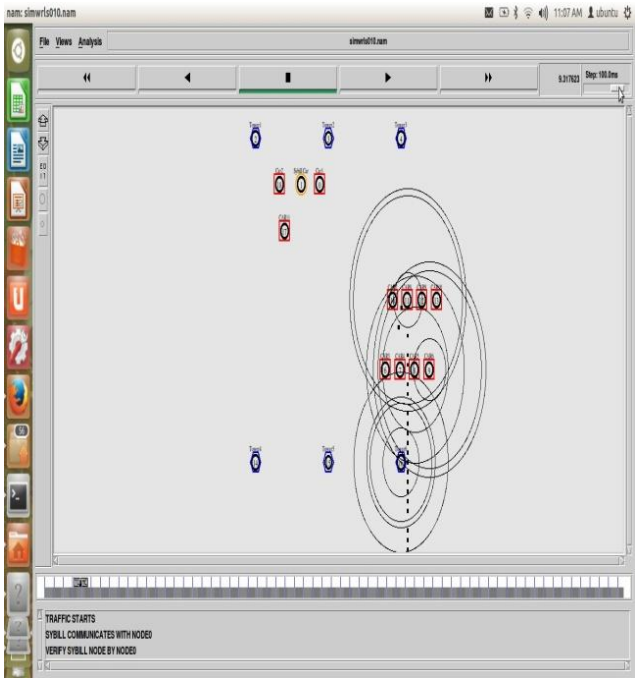


Fig 5 (Disclosure of adversary node)

A. X-Graph Results

In this section we analyze and evaluate the performance of NBH.

1. **Throughput:-** Network throughput refers to the average data rate of successful data or message delivery over a specific communications link. Network throughput is measured in bits per second (bps)[7] .We calculate throughput of EBRS and NHB. Form that point it show throughput of NBH is better than EBRS as shown in fig 6.

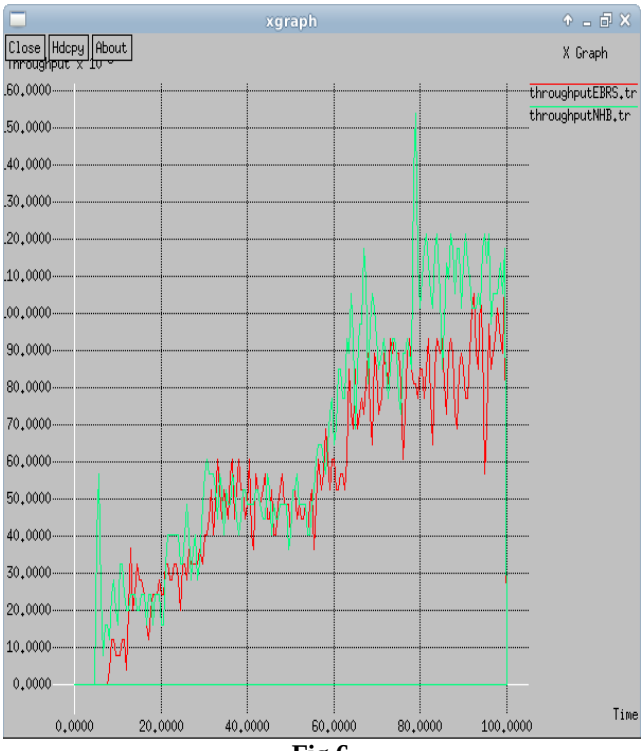


Fig 6

2. **Delivery Ratio**:- As we can see that our method produced better effect to reduce Sybil attack impact.

UGC Approved Journal

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 6, June 2017

Delivery ratio of EBRS and NBH as shown in fig 7. It indicate when the density of vehicle is small, delivery ratio of vehicle is small. When the number of vehicles on the road is little, distance between Vehicle will be too away to receive message. But if vehicle num is more than 100, delivery ratio will be decreased. Sybil attack can be defended by the process of Disclosure and Detection.

Fig 7

3. Delay:- Communication delay of EBRS and NBH with different packet size. In this we conclude delay of NBH is less than EBRS. Increase of vehicle density will increase the communication delay. So many vehicles on road cause intense competition of wireless channel in the process of communication. Bigger the packet higher the communication delay as shown in fig 8.

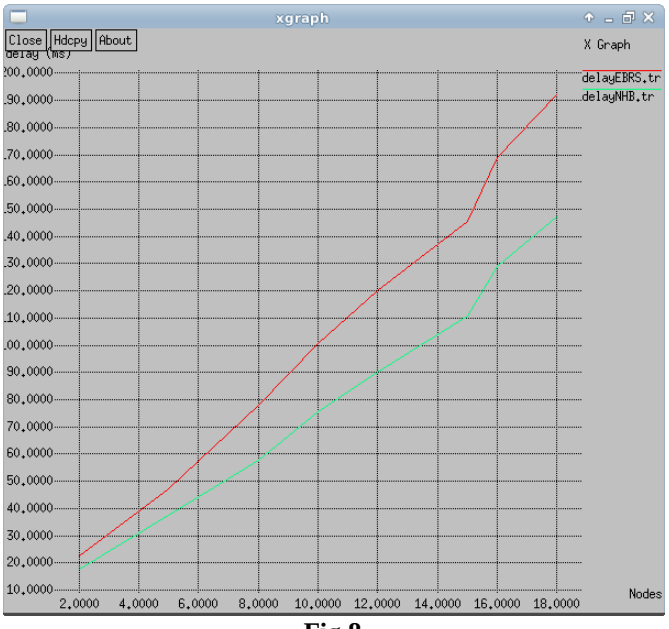


Fig.8

4 Packet Sent:- Packet Sent tells the number of times a task went into a send sleep state while waiting for the network to send each packet to the client. The network model determines that there can be only one outstanding packet per connection at any one point in time. This means that the task sleeps after each packet it sends. If there is a lot of data to send, and the task is sending many small packets (512 bytes per packet), the task could end up sleeping a number of times[8]. Packet sent by NBH is much better than EBRS as shown infig9

UGC Approved Journal

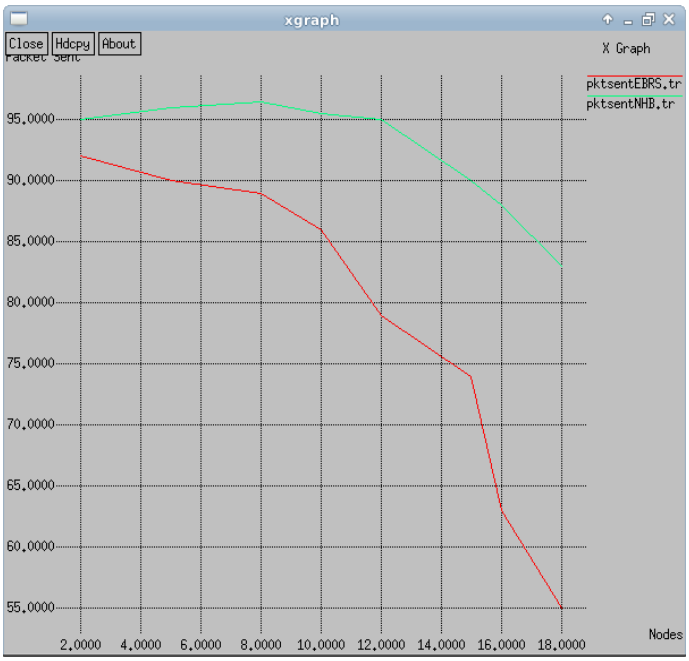
IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 6, June 2017



V. CONCLUSION

By comparing methods, NBH can defend against Sybil attack In VANET, it ensure privacy, authenticity and integrity of vehicles. By establish trust and threshold value for message, the false message is eliminated. In NBH, RSU issue identification to vehicle. Our further work to strong the security assumption of RSu and true relationship between vehicles.

REFERENCES

[1] https://en.wikipedia.org/wiki/ITS
[2] https://en.wikipedia.org/wiki/Dedicated_short-range_communications
[3] https://www.google.co.in/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&ved=0ahUKEwirpLjj1p7UAhVKt48KHWP4BFwQjBwIBA&url=https%3A%2F%2Fwww.researchgate.net%2Fprofile%2FVinita_Jindal2%2Fpublication%2F266148960%2Ffigure%2Ffig1%2FAS%3A392345674633216%401470553906234%2FFig-1-VANET-Architecture-8.ppm&psig=AFQjCNGHxTVYgxoe_Ukdmy_RlrSzG4dTJA&ust=1496476261224241&cad=rjt
[4] Feng, X., Li, C. Y., Chen, D. X., & Tang, J. (2016). A method for defensing against multi-source Sybil attacks inVANET. Peer-to-Peer Networking and Applications, 1-10.
[5] http://www.nsnam.com/2016/06/sumo-open-street-maps-and-ns2-real.html
[6] Feng, X., Li, C. Y., Chen, D. X., & Tang, J. (2016). A method for defensing against multi-source Sybil attacks inVANET. Peer-to-Peer Networking and Applications, 1-10.
[7] https://www.techwalla.com/articles/how-to-calculate-network-throughput
[8] http://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.dc20022_1251/html/monitoring/X40994.htm
[9] Yu, B., Xu, C. Z., & Xiao, B. (2013). Detecting sybil attacks in VANETs. Journal of Parallel and Distributed Computing, 73(6), 746-756.
[10] Sharma, S., & Sharma, S. (2016, December). A defensive timestamp approach to detect and mitigate the Sybil attack in vanet. In Contemporary Computing and Informatics (IC3I), 2016 2nd International Conference on (pp.386-389). IEEE.
[11] Bojnord, A. S., & Bojnord, H. S. (2017). A Secure Model for Prevention of Sybil Attack in Vehicular Ad HocNetworks. International Journal of Computer Science and Network Security (IJCSNS), 17(1), 30.
[12] Park, S., Aslam, B., Turgut, D., & Zou, C. C. (2009, October). Defense against sybil attack in vehicular ad hoc network based on roadside unit support. In Military Communications Conference, 2009. MILCOM 2009. IEEE (pp.1-7). IEEE.
[13] Chen, C., Wang, X., Han, W., & Zang, B. (2009, June). A robust detection of the sybil attack in urban vanets. In Distributed Computing Systems Workshops, 2009. ICDCS Workshops' 09. 29th IEEE International Conference on (pp. 270-276). IEEE.
[14] Chang, S., Qi, Y., Zhu, H., Zhao, J., & Shen, X. (2012). Footprint: Detecting sybil attacks in urban vehicular networks. IEEE Transactions on Parallel and Distributed Systems, 23(6), 1103-1114.
[15] Feng, X., Li, C. Y., Chen, D. X., & Tang, J. (2016). A method for defensing against multi-source Sybil attacks in VANET. Peer-to-Peer Networking and Applications, 1-10.