International Journal of Scientific Research in Computer Science and Engineering
Vol.6, Issue.5, pp.11-15, October (2018)

Research Paper

E-ISSN: 2320-7639

Evaluation of proposed technique for detection of Sybil attack in VANET

Kanwalprit Singh[1*], Harmanpreet kaur[2]

[1] Dept. CSE, Sri Sai College Of Engg & Technology Manawal, IK Gujral Punjab Technical University, Jalandhar, India
[2] Dept. CSE, Sri Sai College Of Engg & Technology Manawal, IK Gujral Punjab Technical University, Jalandhar, India

Available online at: www.isroset.org

Received: 09/Oct/ 2018, Accepted: 22/Oct/ 2018, Online: 31/Oct/2018

Abstract:- The vehicular Adhoc networks are the self configuring and de-centralized type of network in which no central controller is present. The vehicle nodes have high mobility due to which path establishment from source to destination is the major issue in the network. Sybil attack is such a critical attack where the multiple messages are created by the attacker and are sent to other vehicles with different Ids each time. This makes the other nodes get confused such that the nodes assume the messages are arriving from other nodes. Due to this a jam occurs within the network. This forces the vehicle to choose another path and leave the road which is a benefit for the attacker.In the recent times, various techniques have been proposed for the detection of malicious nodes from the network. The proposed technique is based on monitor mode and signal strength based technique. The simulation is been performed in Ns2 and results shows that purposed technique shows good results in terms of various parameters.

***Keywords*:-** VANET, Sybil, Monitor mode

I. INTRODUCTION

MANET is a mobile ad hoc network which consists of a robust infrastructure. This network is a complete wireless network which comprises of fixed or mobile nodes within it. An arbitrary topology is formed here when the nodes are connected to each other on random basis [1]. The nodes present in the network can be considered as routers or as hosts accordingly. This type of network has a property of self-configuration and this is the reason that the communication can be done in an efficient manner through this network [2]. The areas which have no possibility of direct communication, such as the disaster prone areas, the MANETs provide the facility of communicating in those areas. The static as well as the dynamic topologies are used here in this network. In an ad hoc network the centralized infrastructure is absent which results in posing many threats in the functioning of this network. VANET is a part of the mobile ad hoc networks. The example of a vehicular ad hoc network can be taken as a Bus System which is followed in universities [3]. The buses have the facility of picking as well as dropping the students from different areas in a region [4]. These buses however, are connected to each other also. This forms an ad hoc network. The Vehicular ad hoc networks are the most prominent research area for the research purposes due to their increase in demand of usage. The vehicles and the elements that are present at the roadside are connected to each other for the purpose of communication and this network is self-configuring in nature. They do not require any fixed infrastructure for them. The transferring and receiving of the information back and forth holds the current traffic conditions of the network. Wi-Fi is the new latest technology used for the purpose of initiating the implementation of vehicular ad hoc networks. For the purpose of communication in VANETs the new Dedicated Short-Range Communication (DSRC) method is proposed [5]. The low latency and high data rate is ensured with the usage of this technique as it provides the short and medium range communications within it. The organizations which are build up in a certain building with less distances, the communication channels are changed more recently, and also the time provided to connect to the vehicles is less use this kind of techniques. With the absence of an automatic intelligent design for building an efficient protocol configuration in VANETs is not possible. It is due to the fact that there are many problems (NP-problems) arising with it.When the topology of the network is changed or there are highly moving nodes or vehicles present in the system, the routing mechanism in VANET is very difficult to perform. A greedy position based routing approach known as the Edge Node Based Greedy Routing (EBGR) is used for the purpose of forwarding the packets to the nodes. These nodes are available in the edge of the transmission range of the source or the forwarding node [6]. On the basis of the potential score of the nearest node, the most appropriate next hop is appointed. There is a minimization of the end to end delay of the packet transmission in the results when compared to the current routing protocols of the VANET. A gray-hole attack is basically the extension of black-hole attack. In this, the source and monitoring systems are

handled using partial forwarding. The selective data packet dropping method is presented as a normal node and this node 2222participates in communication. A node that can behave in a complete normal manner and switch to behaving like black hole which is actually an attacker, is known as a gray hole node. This gray hole node will behave completely normal and so it is difficult to identify the attacker. The routing table which contains the information of the next hop node is updated for each node. A specific route is to be chosen by the node is the source node needs to route a packet to the destination node [7]. The routing table is used to check if the route selected by the source node is available or not. A broadcasting Route Request (RREQ) message is sent to the neighbour of the node if it initiaes a route discovery process. The intermediate nodes, after receiving the message, update the routing tables for reverse route to the source. When the RREQ query reaches top the destination node or any other node that has a route to the destination, a route reply message is sent back to the source node. There are two phases of the gray hole attack:

Phase 1: The AODV protocol is exploited by the malicious node. This is done to show that it has a valid route to the destination node which intends to interrupt the packets available in the spurious route.

Phase 2: In this phase, the malicious node drops the interrupted packets on the hold of certain probability. The packet selection is done on the base of this probabilistic method. The behaviour of the attacker node changes instantly which results in either transferring or dropping the packets. The malicious node creates an illusion of genuine nodes by forwarding some packets. This creates a level of difficulty of detect the attacks in the network.

II . LITERATURE REVIEW

Supinder Kaur, et.al (2016) presented that VANETs are self-arranging networks composed of a gathering of vehicles and elements of roadside structure linked with each other without requiring any infrastructure, sending and accepting information of current traffic situation. These are used for the communication among the mobile vehicles. It has some security issues like attacks, authentication and so forth. In this paper, we have discussed different attacks which can be trigger in VANET. Sybil attack and its impacts on the networks have been discussed. This paper has reviewed different papers which depict influences of attacks in VANET. The primary focus on Sybil attacks and its consequences has been discussed [8].

Ashritha M, et.al (2015)discussed that the security and privacy are the two major concerns in VANETs. Because of exceedingly dynamic environment in V ANETs computation time for authentication is more. In the meantime the greater part of the privacy safeguarding schemes is prone to Sybil attacks. In this paper a lightweight authentication scheme is proposed between vehicle to RSU, vehicle to vehicles and to construct a secure communication system. In this method we make utilization of timestamps approach and furthermore reduce the computation cost for authentication in exceedingly dense traffic zones. The privacy of the vehicle is preserved by not disclosing its real character. Performance results show that the computation over head cost is observed to be substantially low by making utilization of XOR and hash functions for authentication [9].

Mahdiyeh Alimohammadi et.al (2015) presented Vehicular impromptu system (VANET) has attracted the attention of numerous analysts lately. It enables value-included administrations, for example, road safety and managing traffic on the road. One of the fundamental purposes for making invalid identities is interruption in voting based systems. In this paper a secure protocol is proposed for unraveling two clashing goals privacy and Sybil attack in vehicle to vehicle (V2V) communications in VANET. The proposed protocol is based on the Boneh-Shacham (BS) short gathering signature scheme and batch verification. Experimental results demonstrate efficiency and applicability of the proposed protocol for giving the requirements of privacy and Sybil attack detection in V2V communications in VANET [10].

Sebastian Bittl, Arturo A. et.al (2015) discussed that Car2X communication is going to enter the mass market in up and coming years. So far all realization propositions intensely rely on upon the global positioning 2222system for giving location information and time synchronization. Be that as it may, examines on security impact of this kind of data input have concentrated on the possibility to spoof location information. Also, a Sybil attack can be performed and reliability of the fundamental data sets of time and position inside VANET messages is very questionable considering the outlined attacks. Mechanisms to stay away from or restrain the impact of outlined security flaws are discussed. An evaluation of the possibility to do the described attacks in practice utilizing a current Car2X hardware solution is provided [11].

Anu S Lal, et.al (2015) discussed that Vehicular specially appointed networks (VANETs) are progressively used for traffic control, accident avoidance, and management of toll stations and public areas. Security and privacy are two major concerns in VANETs. This paper proposes an improvement for the scheme CP2DAP, which detects Sybil attacks by the cooperation of a central authority and a set of fixed nodes called road-side units (RSUs). The modification proposed is a local authority based collaborative scheme for detecting Sybil attacks and a revocation method utilizing blossom channel to prevent additionally attacks from malicious vehicles. The detection of Sybil attack in this manner does

not require any vehicle to disclose its identity; subsequently privacy is preserved at all times [12].

Khaled Rabieh, et.al, (2015) presented that an attacker may launch a Sybil attack by pretending to be multiple simultaneous vehicles. In this paper, we propose a cross-layer scheme to enable the RSUs to identify such Sybil vehicles. Since Sybil vehicles don't exist in their claimed locations, our scheme is based on checking the vehicles' locations. A challenge packet is sent the vehicle's claimed location utilizing directional antenna to detect the presence of a vehicle. On the off chance that the vehicle is at the expected location, it ought to have the capacity to get the challenge and send back a valid response packet. With a specific end goal to reduce the overhead and as opposed to sending challenge packets to every one of the vehicles constantly, packets are sent just when there is a suspicion of Sybil attack. The evaluation results demonstrate that our scheme can accomplish high detection rate with low probability of false alarm. Also, the scheme requires acceptable communication and computation overhead [13].

III. RESEARCH METHODOLOGY

The vehicular adhoc networks is the decentralized type of network in which no central controller is present and nodes can change its location any times. The vehicular adhoc networks have three major issues which are security, routing and quality of service. Due to self configuring nature of the network, malicious nodes join the network which is responsible to trigger various type of active and passive attacks. The Sybil attack is the active type of attack in which malicious node spoof the identification of the legitimate node. The legitimate node is not able to get the required data which leads to reduction in network throughput. In this work, technique is been proposed which will detect and isolate malicious nodes from the network which are responsible to trigger Sybil attack in the network. The proposed techniques is based signal strength based technique and monitor mode techniques. In the proposed technique, the road side units flood the ICMP messages in the network. The vehicle nodes when receive the ICMP messages will start sending its signal strength value to its nearest road side units. The road side units will gather all the information and exchange the information with each other. The vehicle node which has multiple signal strength values will be detected as the node which may cause the intrusion in the networks. To confirm that which node is the malicious node, the road side units send the control packets in the network and vehicle nodes when receive the control packets will go to monitor mode and start watching its adjacent nodes. The node which is malicious is detected and technique is multiple path routing is applied which isolate malicious nodes from the network.

Signal strength and Monitor mode algorithm

Input: vehicles, RSU, malicious vehicle

Output: Malicious vehicle

Apply information gathering process

{

1. Node send its credentials to road side units
2. If(Matched= true)
3. Assign identification
4. Else
5. Send not verified message
6. }
7. }

If (signal strength ==not matched)

1. Send ICMP messages in the network
2. Node receive the message go to monitor node
3. If(Node change id==true)
4. Node ==Malicious node
5. Else
6. Node=Legitimate node
7. }

End

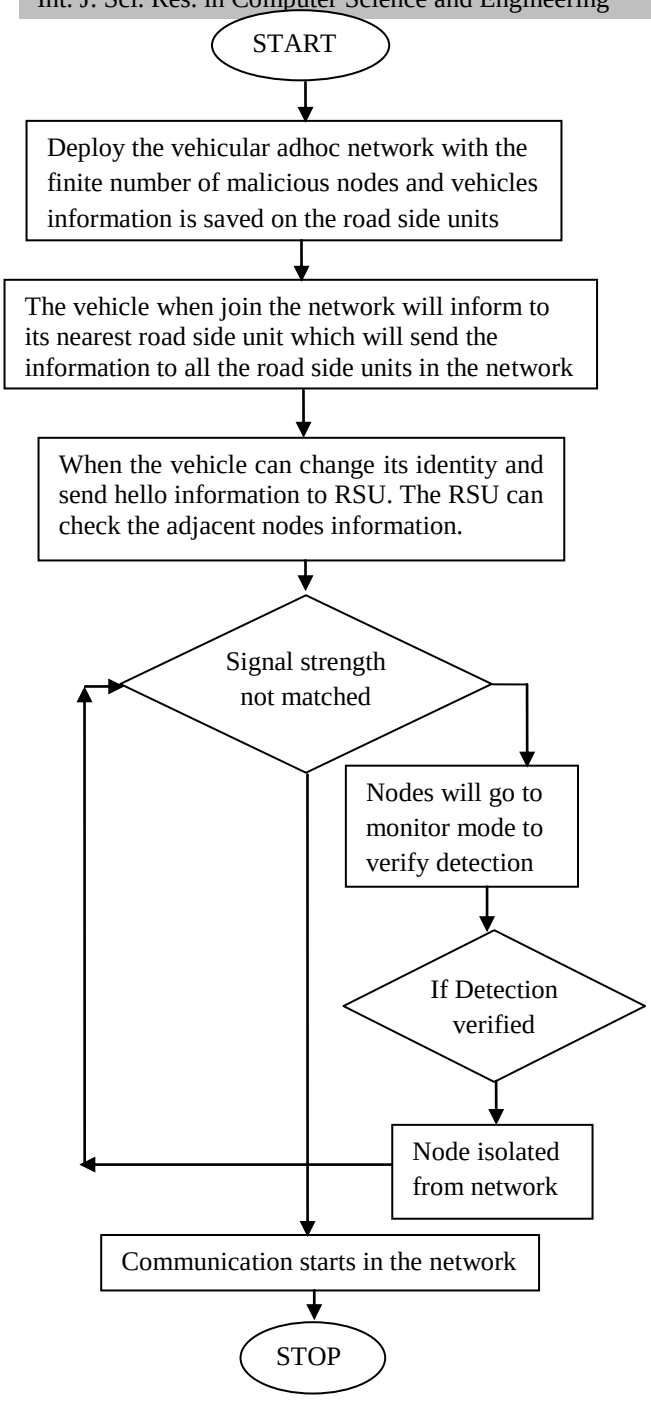

Fig 1 Proposed technique Flowchart

IV. EXPERIMENTAL RESULTS

The proposed work is implemented in MATLAB and the results are evaluated in terms of several parameters.

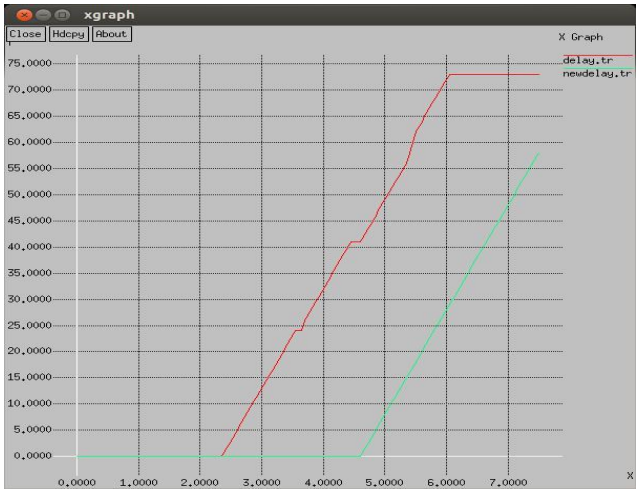

Fig 2:Delay Comparison

As shown in figure 2, the delay of the proposed and existing technique is compared and it is been analyzed delay of the proposed technique is reduced isolation of Sybil attack in the network.

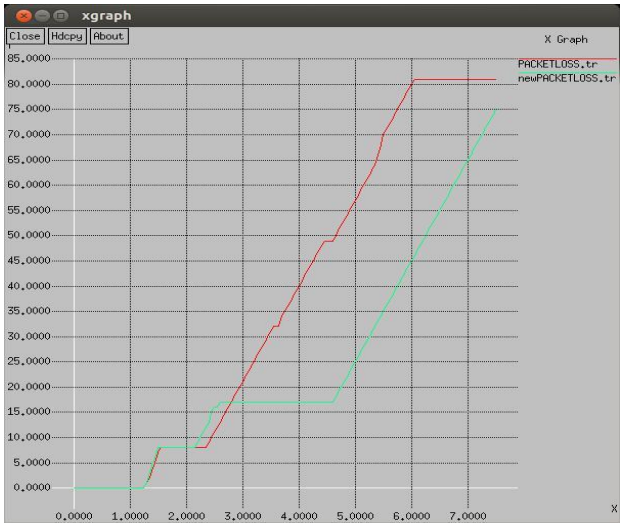

Fig 3: Packetloss comparison

As shown in figure 3, the packetloss of the proposed and existing technique is compared and it is been analyzed that network packetloss is reduced when Sybil attack is isolated

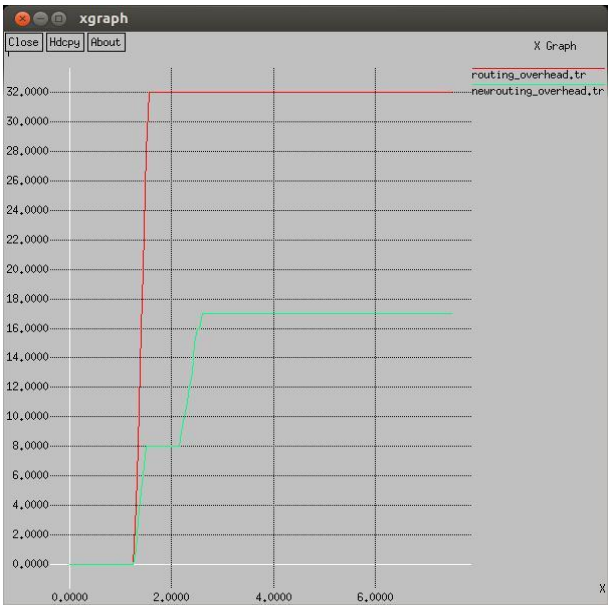

Fig 4: Routing overhead

As shown in figure 4, the routing overhead is the parameter which measures the extra number of packets which are transmitted in the network. The routing overhead in the network is reduced when attack is detected and isolated from the network.

Fig 5: Throughput Comparison

As shown in figure 5, the throughput of the proposed and existing technique is compared and it is been analyzed that after the malicious node isolation the network throughput is increased at steady rate.

IV. CONCLUSION

In this work, it is been concluded that broadcasting is the technique which is applied to select efficient path from source to destination. Due to decentralized nature of the network, some time malicious nodes join the networks which are responsible to trigger various type of active and passive attacks. This work is based on to detect malicious nodes from the network which are responsible to trigger Sybil attack in the network. The simulation of the proposed technique is been done in Ns2 and results shows that performance is increased in the network.

V. REFERENCES

[1] Rajesh Rajamani et al "On spacing policies for highway vehicle automation", American control conference chicago, Illinois June 2000

[2] Gang Liu and Han Guo, " Some aspects of road sweeping vehicle automation", IEEE lasme international conference on advanced intelligent mechatronics,2001

[3] Kung et.al "A survey of mobility models for ad hoc network research", wireless communication & mobile computing (WCMC): special issue on mobile ad hoc networking: research, trends and applications, vol. 2, no. 5, pp. 483-502, 2002.

[4] HAO Wu "An Empirical Study of Short RangZe Communications for Vehicles", IJSER September , 2011, Cologne, Germany, pp 83-84

[5] Su-Jin Kwag, "Performance Evaluation of IEEE 802.11 Ad-hoc Network in Vehicle to Vehicle Communication", Mobility 06, 1-59593-519-3

[6] Michel Hugo "Self-Organized Traffic Control", VANET'10, September 24, o, Illinois,

[7] Reena Dadhich Department of MCA, Govt. College of Engineering, Ajmer, India," Mobility Simulation of Reactive Routing Protocols for Vehicular Ad-hoc Networks"(2011)

[8] Supinder Kaur, Anil Kumar, "Techniques to Isolate Sybil Attack in VANET-A Review", 2016, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)

[9] Ashritha M, Sridhar CS, "RSU Based Efficient Vehicle Authentication Mechanism for V ANETs", 2015, IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO)

[10] Mahdiyeh Alimohammadi and Ali A. Pouyan, "Sybil Attack Detection Using a Low Cost Short Group Signature in VANET", 2015, IEEE

[11] Sebastian Bittl, Arturo A. Gonzalez, Matthias Myrtus, Hanno Beckmann, Stefan Sailer, Bernd Eissfeller, "Emerging Attacks on VANET Security based on GPS Time Spoofing", 2015 IEEE Conference on Communications and Network Security (CNS)

[12] Anu S Lal, Reena Nair, "Region Authority Based Collaborative Scheme to Detect Sybil Attacks in VANET", 2015 International Conference on Control, Communication & Computing India (ICCC)

[13] Khaled Rabieh, Mohamed M. E. A. Mahmoud, Terry N. Guo, and Mohamed Younis, "Cross-Layer Scheme for Detecting Large-scale Colluding Sybil Attack in VANETs", 2015, IEEE ICC

