The Authentication Approach for Detection of Malicious node in VANET

Akanksha kumari[1], Yogesh Kumar[2]
[1]*Mtech Scholar,* [2]*Assistant Professor*
[12]*Ganga Technical Campus, Soldha Bahadurgarh*

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.

I. INTRODUCTION

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. The buses have the facility of picking as well as dropping the students from different areas in a region. 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 [1]. 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. 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 [2]. 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 [3]. 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. The affect of the traffic lights is measured with the help of the delay-bounded routing protocol [4]. During the crossing of a vehicle through an intersection, the information about the traffic lights is gathered, Along with this, the information related to the traffic load of the road present in the next section is provided. This helps in providing a more accurate assumption regarding the vehicles and the message deliverance in a strategic manner. There is a better usage of the time and a reduction in use of the radio resources which are needed to deliver the message within the time according to the simulation results achieved. For the purpose of assuming the available time and the distance travelled, the linear regression technique is used by the protocol. At a certain moment, there can be switching provided to the delivery strategy which will help in reducing the number of relays by radio [5]. There are various routing protocols in VANET. The vehicular communications are made to be more challenging due to the fact that there are various characteristics of the location based routing protocols. The networks are divided into three broad categories which are cellular, ad hoc and hybrid. Infotainment which includes latest new, or the information of the locality, is supported by the cellular network. The vehicle to infrastructure model is the basis of this category. A wide range of vehicular applications are supported by the present infrastructure. There is however, still a need of a fixed infrastructure deployment due eliminate the drawbacks found [6]. The ad hoc networks which do not require any prior infrastructure help in reducing the drawbacks identified. This is more prominent in the vehicle to vehicle communication. DGR (Directional Greedy Routing) is another

protocol in which the hop count is reduced by selecting the node which moves towards the destination. The Predictive Directional Greedy Routing (PDGr) enhances the Directional Greedy Routing protocol which predicts the mobility of the vehicle. The mobility information is achieved from the traffic pattern as well as the street layout. In GSR (Geographic Source Routing), the Dijkastra's shortest path algorithm is used by the GPS system on the map. This method helps is calculating the shortest path on each junction. The AODV is an on-demand routing protocol, which is described as a reactive routing protocol. When in a network, there is a need for the source node to route to particular destination the routing establishment is initialized by the route discovery process [7]. All the neighbors forward the RREQ packet to the neighbors of the source node on its own. The forwarding of packets to their neighbors and further to the next neighbors keeps going until the destination is reached. The process can also stop on an intermediate node which has a fresh route to the required destination.

II. LITERATURE REVIEW

Supinder Kaur, Anil Kumar, (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. Sybil attack and its impacts on the networks have been discussed. In VANET many attacks has been trigger by the malicious node. In this manner keeping in view above challenges there is a need to improve the efficiency of VCWC protocol with the goal that it might have the capacity to control both, the factors which make wireless communication unreliable and furthermore support the above application challenges to a vast extent. In this we have reviewed different papers which depict influences of attacks in VANET. The primary focus on Sybil attacks and its consequences has been discussed [8].

Anu S Lal, Reena Nair, (2015) discussed that Vehicular specially appointed networks (VANETs) are progressively used for traffic control, accident avoidance, and management of toll stations and public areas. They proposed 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 [9].

Ashritha M, Sridhar CS, (2015) discussed that the security and privacy are the two major concerns in VANETs. 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. It additionally gives privacy to the clients by making utilization of pseudo-id. As the transmission range increases the number of authenticated vehicle additionally increases. In the second scenario the speed of vehicles increases the rate of authenticated vehicle diminishes. In future work we intend to develop faster authentication mechanism and secure routing protocol to enhance the system security [10].

Mahdiyeh Alimohammadi and Ali A. Pouyan, (2015) presented that security issues are the testing problems in this system. Sybil attack is one of the serious security threats that attacker tries to forge a few identities. 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 [11].

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 system 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. In this way, an analysis of the attack potential on vehicular impromptu system (VANET) realizations as to spoofed time information is provided in this work. 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 [12].

Khaled Rabieh, et.al, (2015) proposed 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. We likewise discuss a few Sybil attack alarming methods. 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 has 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.

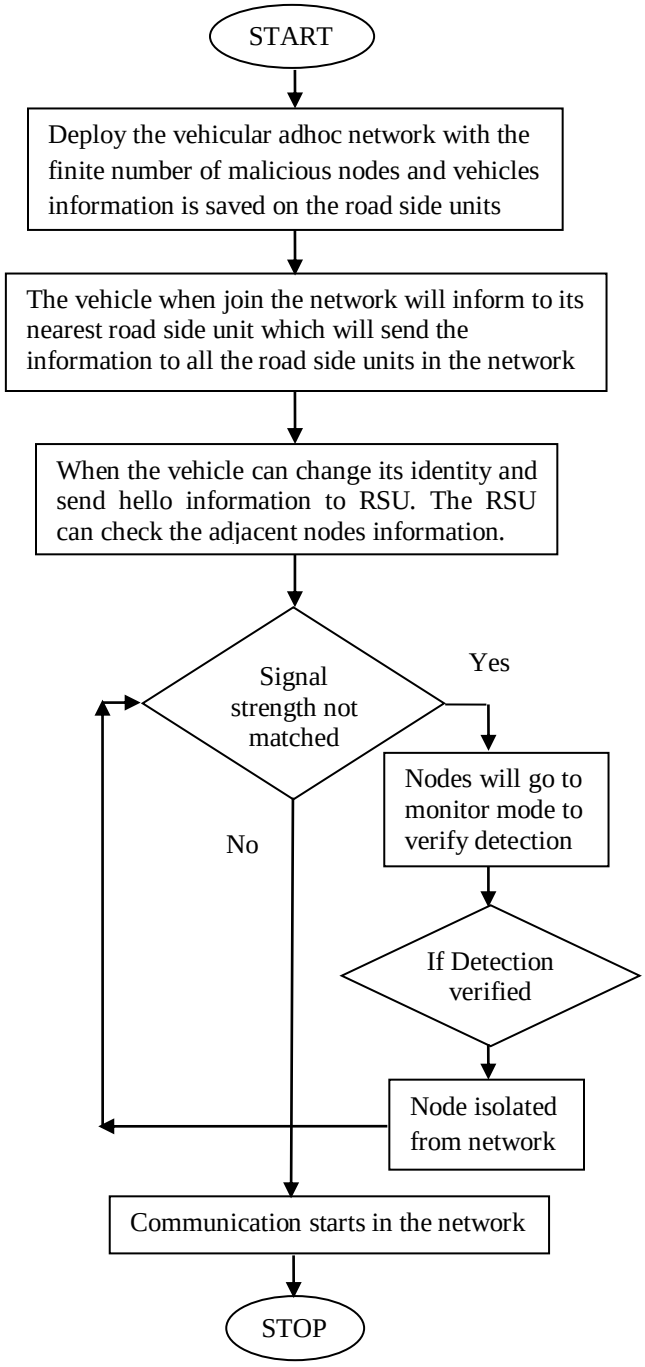

Fig.1: Flowchart of Proposed technique

IV. EXPERIMENTAL RESULTS

The proposed technique is implemented in NS2 and the results are evaluated by making comparisons against proposed and existing techniques in terms of several parameters.

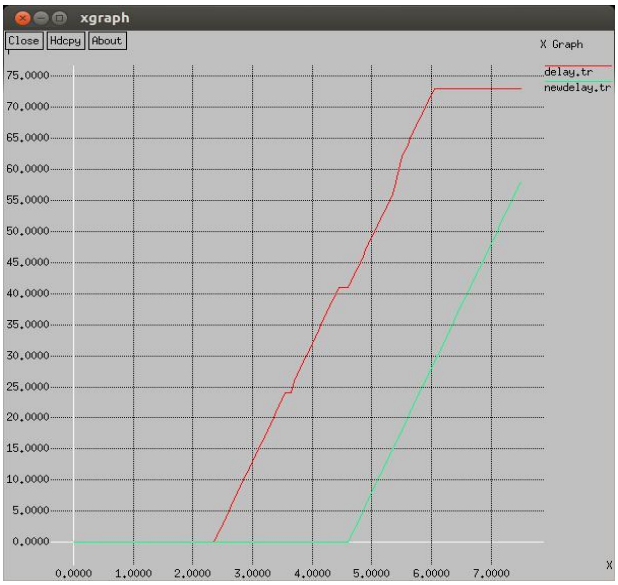

Fig.2: Delay Comparison

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.

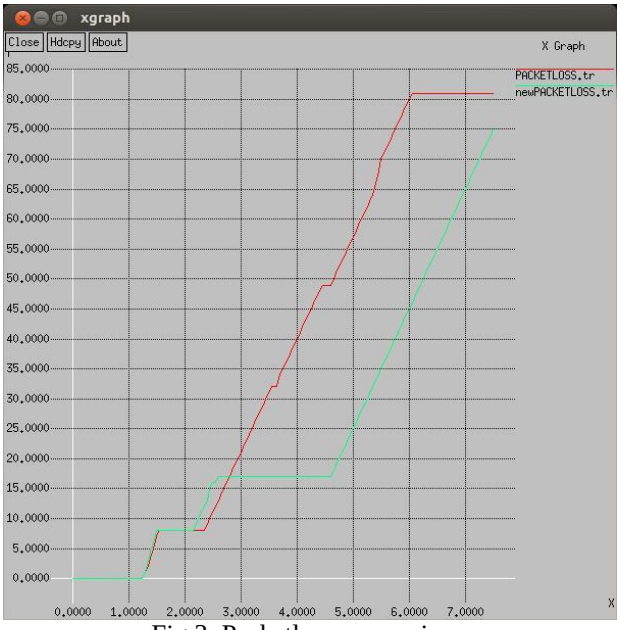

Fig.3: Packetloss comparison

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 from the network.

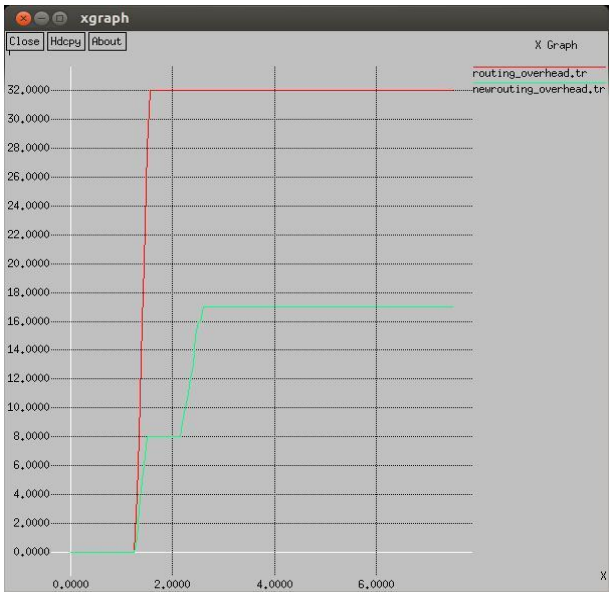

Fig.4: Routing overhead

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.

V. CONCLUSION

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. 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.

VI. REFERENCES

[1]. Adil Mudasir Mala and Ravi kant sahu, "Security Attack with an Effective Solution for DOS attack in VANET", International Journal of Computer Applications (0975 – 8887), Volume 66– No.22, March 2013

[2]. Ajay Rawat, Santosh Sharma, Rama Sushil, "VANET: Security Attack and its Possible Solutions", Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, 2012, pp-301-304

[3]. Jeong-Ah Jang, "A Fixed Sensor-Based Intersection Collision Warning System in Vulnerable Line-of-Sight and/or Traffic-Violation-Prone Environment", 2012, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, pp 1-11

[4]. Rakesh Kumar, Mayank, "A Comparative Study of Various Routing Protocols in VANET", 2012 pp 1-12

[5]. Reena Didcach, "Mobility simulation of Reactive protocol for VANET", IEEE, 2012

[6]. Parastoo Kafil, Mahmoud Fathy, Mina Zolfy Lighvan, "Modeling Sybil Attacker Behavior in VANETs", 2012 9th International ISC Conference on Information Security and Cryptology

[7]. Hao Wu, "An Empirical Study of Short Range Communications for Vehicles", IJSER September 2, 2011, Cologne, Germany, pp 83-84

[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]. 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)

[10]. 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)

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

[12]. 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)

[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