Innovative Techniques for Malicious Node Detection and Isolation in VANETs: A Focus on Sybil Attack Mitigation

Gurleen Kaur*[1] & Eng. Prabhjot Singh[2]

*[1]Research Scholar, Universal Group of Institutes Lalru, Punjab, India

[2]Assistant Professor, Universal Group of Institutes Lalru, Punjab, India

ABSTRACT

Vehicular Ad-hoc network are wireless networks where all the vehicles from the nodes of the network. It is for the driver comfort and road safety, the inter-vehicle communication provide them. 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. This communication in the two forms is unidirectional or bidirectional fixed infrastructure. 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, AODV, LAR, NS2. DDOS

I. INTRODUCTION

VANET's is a subset of MANET and best example of VANET is Bus System of any University which is connected together. These buses are moving in different parts of city to pick or drop students if they are connected together, make an Ad hoc Network. One of the most capable areas of research is the study of the communications among vehicles called Vehicular Ad-hoc Networks (VANETs) [1]. This kind of networks are self-configuring networks composed of a collection of vehicles and elements of roadside structure linked with each other without requiring any infrastructure, sending and receiving information of current traffic situation. Nowadays, Wi-Fi (IEEE 802.11 based) technologies are the most commonly used for the initialization of VANETs. Currently, DSRC (Dedicated Short-Range Communication) has been proposed as the communications standard specifically for VANETs, it is a short medium range communications service that offers very low latency and high data rate [2]. This is especially true in certain VANETs scenarios in which buildings and distances discontinue communication channels frequently, and where the available time for connecting to vehicles could be really short. The efficient protocol configuration for VANETs without using automatic intelligent design tools is practically impossible because of the enormous number of possibilities [3]. It is especially difficult when considering multiple design issues, such as highly dynamic topologies and reduced coverage. There are different types of attacks in VANET. Sybil Attack in VANET consists of sending multiple messages from one node with multiple identities. Sybil attack is always possible except the extreme conditions and assumptions of the possibility of resource parity and coordination among entities [4]. In DOS attack the main objective is to prevent legitimate user from accessing resources and services. This attack can be trigger by jamming the whole channel and network so that no authorized vehicle can access the network. It is serious problem in which user is unable to communicate with the user due to DOS attack. DDOS is more harmful than DOS attack because it is in distributed manner. Different types of locations are used by the attacker to launch the attack [5]. It might be possible that they use different time slots for sending messages. The nature of the message and time slot varied from vehicle to vehicle. DDOS is possible at V2V and V2 I. Its main objective is to slow down the network and jam the network. In Blackhole Attack the requests is listen by an attacker for the routers in a flooding based protocol [6]. When a request is received by the attacker to the destination node for a route, it creates a reply for the short route and enters into the passageway to do something with the packets passing between them. Ad-hoc on Demand Vector (AODV) routing protocol can be described as a reactive routing protocol which is a significant on-demand routing protocol, whenever the source node needs a route to a specific destination then only it starts route establishment by initializing a route discovery process [7]. In this process a RREQ packed is forwarded to all the neighbors of the source node by source node itself and this forwarding of packets to the neighbors & their neighbors goes on until the destination node is reached or an intermediate node is reached which is having a fresh enough route to the desired destination [8]. When an intermediate node has an adequate fresh route to the destination then only it sends a reply by unicasting a RREP packet to the node from which it received the RREQ packet [9]. The route maintenance procedure works after selecting & establishing the route is completed. This route maintenance goes on till the destination is available with its every possible passage from the source node or the established route is no more needed. When the route link is lost or faded then a RERR message is used as a notification to make other nodes aware of the loss of the route link [10].

II. LITERATURE REVIEW

Chang, S. et.al (2011) propose in this paper a novel Sybil attack detection mechanism, Footprint, using the trajectories of vehicles for identification while still preserving their location privacy. More specifically, when a vehicle approaches a road-side unit (RSU), it actively demands an authorized message from the RSU as the proof of the appearance time at this RSU. With this scheme, vehicles can generate a location-hidden trajectory for location-privacy-preserved identification by collecting a consecutive series of authorized messages [11].

Tong Zhou, et.al (2011) proposed in this paper a lightweight and scalable protocol called Privacy Preserving Detection of Abuses of Pseudonyms protocol to detect Sybil attacks in VANET. In this protocol, a malicious user pretending to be multiple (other) vehicles can be detected in a distributed manner through passive overhearing by s set of fixed nodes called road-side boxes (RSBs). From the results, we see our scheme being able to detect Sybil attacks at low overhead and delay, while preserving privacy of vehicles. Using this protocol, the multiple vehicles which are affected by malicious user can be detected in a distributed manner through passive listener using set of fixed nodes called road-side boxes (RSBs) [12].

Lee, B., et.al (2013) proposed in this paper a Detection Technique against a Sybil Attack (DTSA) protocol using Session Key based Certificate (SKC) to validate inter-vehicle IDs in VANETs. In DTSA, the SKC (Session Key based Certificate) used to verify the IDs among vehicles, and also generates a vehicle’s anonymous ID, a session Key, the expiration date and a local server’s certificate for the detection of a Sybil Attack and the verification time for ID. Besides, a drivers’ privacy can be protected by using an anonymous ID. This DTSA helps drivers drive safely with the reliable information of VANET and reduce traffic accidents [13].

Li, M., et.al (2013) proposed in this paper the detection of replication attacks in wireless sensor networks (WSNs) has been a long-standing problem. Many variants of replication attacks were spawned such as the Sybil attack. In this paper, a regional statistics detection scheme (RSDs) against Sybil attacks is proposed, which is an effective solution to three key issues: firstly, they address the Sybil attack by a RSSI-based distributed detection mechanism, secondly, their protocol can prevented the network from a large number of nodes failure caused by Sybil attacks, Thirdly, the RSDs has been verified can maintain a high detection probability with low system overhead by implement experiments. Finally, they run our protocol in a prototype detection system with 32 nodes that the experiment result confirmed its high efficiency [14].

Gañán, C., et.al (2014) presented in this paper one of the critical security issues of Vehicular Ad Hoc Networks (VANETs) is the revocation of misbehaving vehicles. A Privacy Preserving Revocation mechanism (PPREM) based on a universal one-way accumulator is proposed on this paper. PPREM provide explicit, concise, authenticated and unforgettable information about the revocation status of each certificate while preserving the users' privacy. They have proposed PPREM for VANETs, which enhances the certificate status checking process by replacing the time-consuming CRL with a fast revocation checking process employing a one way accumulator. PPREM not only satisfies the security and privacy requirements of VANETs but can also significantly reduce the revocation cost [15].

Balamahalakshmi D., et.al (2014) they proposed a compromised RSU detection mechanism for Sybil attack detection. A footprint concept is used in proposed method to detect the Sybil attack by using the trajectory information which is generated by multiple RSUs and the location of the vehicle is preserved. The RSU will generate the location and timing information to vehicle while it passes through RSU. The result showed that the length of the trajectory information is reduced without loss of information and the bandwidth overhead is also reduced [16].

III. RESEARCH METHODOLOGY

In this work, the new scheme had been proposed which will be based on to detect malicious nodes from the network which are responsible to trigger Sybil attack in the network. The Sybil attack can harm the network throughput and delay. The throughput of the network can be reduced because network resources get wasted. The delay can be raised because packets are routed to wrong destination or long paths get followed. In this work the techniques which will be proposed are based on some assumptions. These assumptions are:

1. The speed of the mobile nodes are fixed on the defined roads
2. The RSU’s are responsible to maintain the information about all vehicles
3. The mobile nodes have to present its neighbor node information to RSU’s
4. The RSU’s can maintain the neighbor node information about all the nodes

The malicious vehicles can change its identity every time and send hello messages to RSU's for network join. The vehicles which are on the network can register it with the server. In the registered information the unique vehicle number and its identification number will be defined. This registered information can be available on all RSU's. When any join the network, is have to send hello message to RSU and then RSU ask nodes for their identification number. When the identification number will be successfully verified the RSU gather all the information about neighboring or adjacent nodes of the registered nodes. The RSU will also define the speed limit of the vehicle on the road for which it is registered. When any malicious node will can its identity can send hello message to RSU, the RSU will register the malicious node but when RSU checks the adjacent node and that are different from the legitimate node. The malicious node can be detected from the network. To verify the detection process, the RSU's will flood the monitor mode messages in the network , and adjacent nodes of the malicious nodes can start monitoring the malicious nodes and detect that it is the malicious nodes.

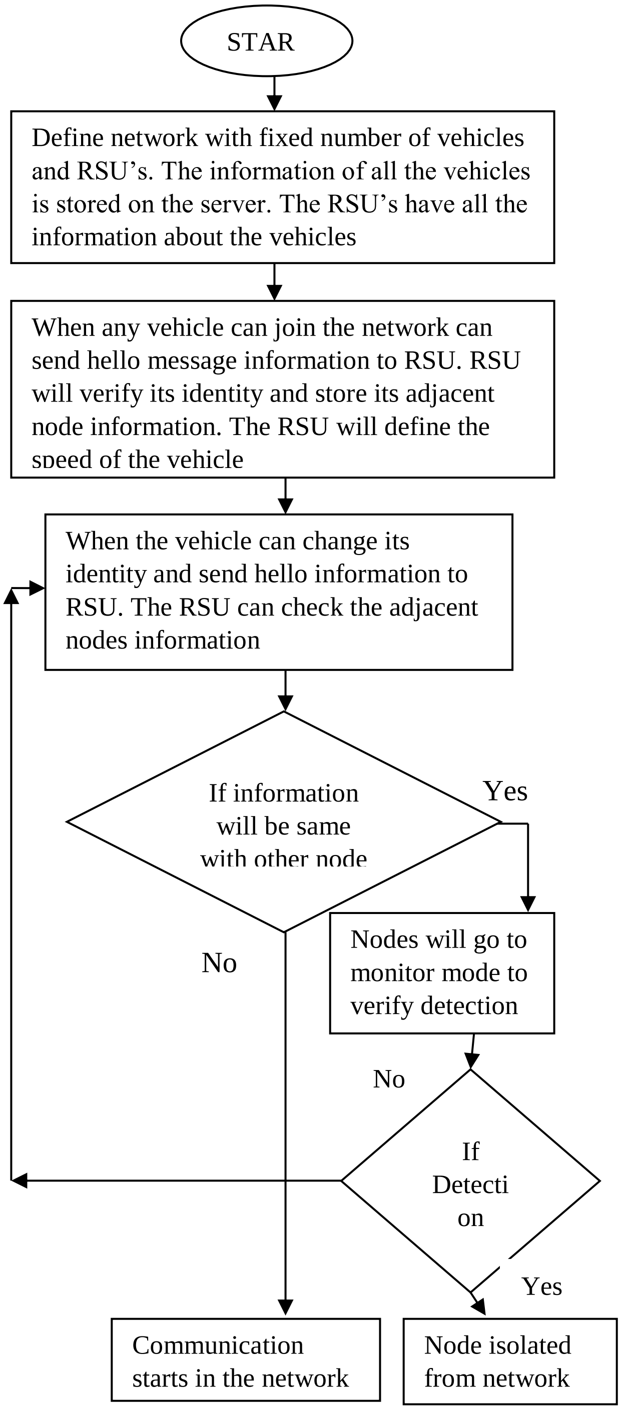
STAR
Define network with fixed number of vehicles and RSU's. The information of all the vehicles is stored on the server. The RSU's have all the information about the vehicles
When any vehicle can join the network can send hello message information to RSU. RSU will verify its identity and store its adjacent node information. The RSU will define the speed of the vehicle
When the vehicle can change its identity and send hello information to RSU. The RSU can check the adjacent nodes information
If information will be same with other node
Yes
No
Nodes will go to monitor mode to verify detection
No
If Detecti on
Yes
Communication starts in the network
Node isolated from network

Fig 1:- Flowchart of Proposed Technique

IV. EXPERIMENTAL RESULTS

The proposed technique is implemented in NS2 and the results are analysed in terms of various parameters such as Fuel emission, Packetloss and Throughput.

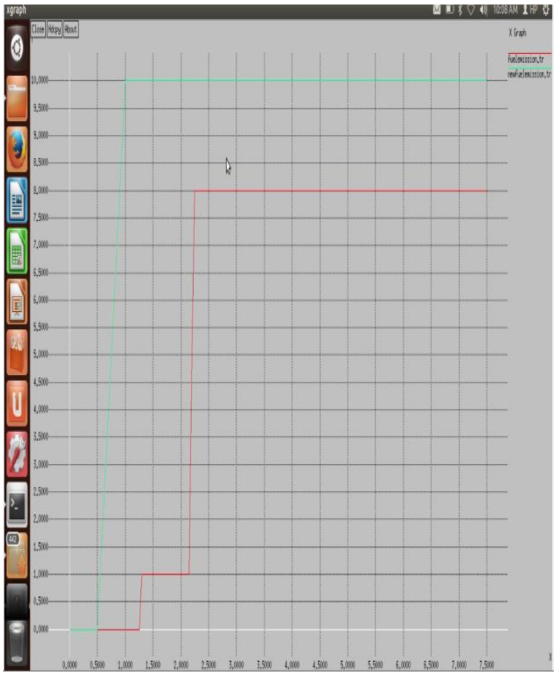

Fig 2: Fuel emission

As shown in figure 2, fuel emission graph is shown of previous and proposed scenario and it is clearly shown that fuel emission of existing scenario is more due to Sybil attack and it is 35. In the proposed scenario as Sybil attack is detected and isolated due to which fuel emission is reduced to 10.

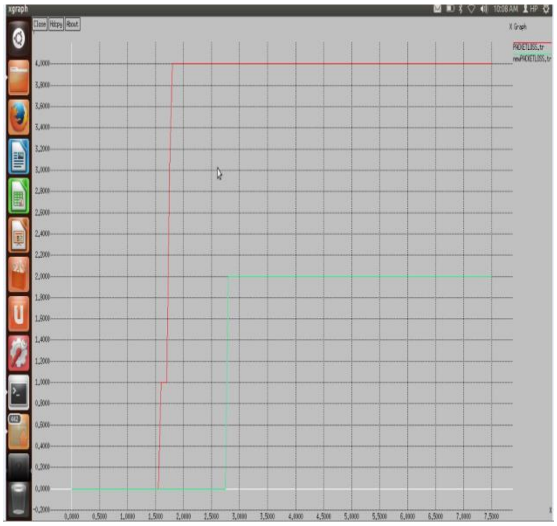

Fig 3: Packetloss

As shown in figure 3, packetloss graph is shown in which packetloss in existing and proposed scenario is shown and it is analyzed that packetloss of existing scenario is more due to Sybil attack, as network traffic is redirected to malicious node which leads to packetloss and in the proposed scenario packetloss is reduce to isolation of malicious nodes. The packetloss in the existing scenario is 4 packets and in proposed scenario it is 2 packets.

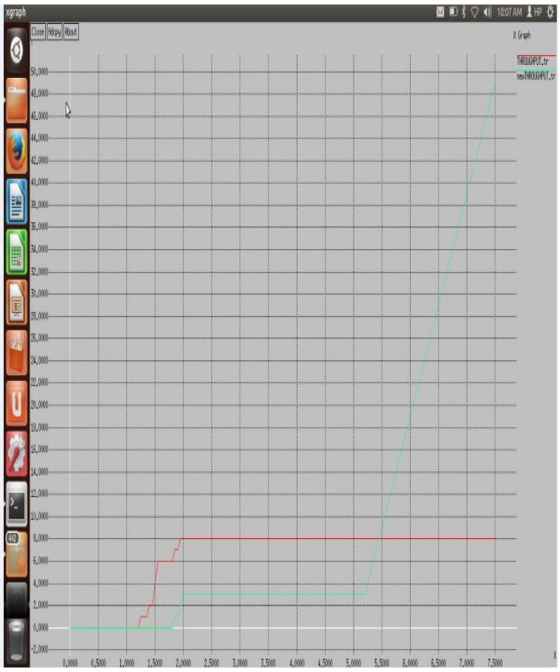

Fig 4: Throughput

As shown in figure 4, throughput graph of proposed and existing schemes are shown with red and green line. Due to isolation of Sybil attack from the network throughput is increased to 50 packets and due to Sybil attack in the network throughput will be 28 packets**.**

V. CONCLUSION

The vehicular adhoc network is the self-configuring type of network in which vehicles can move freely on the roads. The vehicle adhoc network is the decentralized type of network in which vehicles can join or leave the network when they want. Due to such type of network nature many malicious nodes may join the network which is responsible to trigger various types of security attacks. The Sybil attack is most common type of attack in which malicious nodes can change its identification time to time. In this work, it is been concluded that Sybil attack reduced network performance in terms of throughput, delay and packeltoss. In this work, technique will be proposed which will be based on network information and monitor mode technique. The simulation is performed in NS2 and it has been analyzed that proposed technique will detect malicious nodes from the network in minimum amount of time.

VI. REFERENCES

[1] Bilal Mustafa Umar Waqas Raja, “Issues of Routing in VANET”, 2010, School of Computing Blekinge Institute of Technology Box 520, SE – 372 25 Ronneby Sweden

[2] Vasundhara Uchhula Dharamsinh, “Comparison of different Ant Colony Based Routing Algorithms”, 2006, Desai University Nadiad, Gujarat, India volume 4, issue 6, pp- 1-5

[3] [3] Caelos de morais cordeiro and dharma p.agrawal, “Mobile ad-hoc networking”, 2009, IJESE, Vol. 3, issue 2, pp- 61-63

[4] Muddassar Farooq and Gianni A. Di Caro, “Routing Protocols for Next Generation Networks Inspired by Collective Behaviors of Insect Societies: An Overview”, 2008, Next Generation Intelligent Networks Research Center National University of Computer and Emerging Sciences (NUCES) Islamabad, Pakistan, volume 1, issue 9, pp1-60

[5] Ajay Rawat, Santosh Sharma, Rama Sushil, “VANET: Security Attack and its Possible Solutions”, Journal of Information and Operations Management, Volume 3, Issue 1, 2012, pp-301-304

[6] Jason J. Haas and Yih-Chun Hu, “Real-World VANET Security Protocol Performance”, 2007 University of Illinois at Urbana-Champaign Urbana, Illinois, U.S.A, volume 19, issue 11, p1-7

[7] Adil Mudasir Mala and Ravi kant sahu, "Security Attack with an Effective Solution for DOS attack in VANET", 2013, International Journal of Computer Applications (0975 – 8887) Volume 66– No.22, pp-44-52

[8] Josiane Nzouonta, Neeraj Rajgure, Guiling Wang, Member, IEEE, and Cristian Borcea, Member IEEE," VANET Routing on City Roads using Real-Time Vehicular Traffic Information", 2008, volume 9, issue 14, pp1-18.

[9] Raya M. and Hubaux J., "Security of Ad Hoc and Sensor Networks", 2005, 3rd ACM Workshop, Alexandria, volume 5, issue 2, pp- 152-161

[10] Reena Dadhich, "Mobility Simulation of Reactive Routing Protocols for Vehicular Ad-hoc Networks", 2011, Department of MCA, Govt. College of Engineering, Ajmer, India, volume 8, issue 3, pp- 211-219

[11] Chang, S., Qi, Y., Zhu, H., Zhao, J., & Shen, X. "Footprint: Detecting sybil attacks in urban vehicular networks", IEEE sponsored Parallel and Distributed Systems, IEEE Transactions on, 23(6), pp.1103-1114, 2011.

[12] Hao, Y., Tang, J., & Cheng, Y. "Cooperative sybil attack detection for position based applications in privacy preserved VANETs" IEEE In Global Telecommunications Conference (GLOBECOM 2011), IEEE pp. 1-5,2011

[13] Lee, B., Jeong, E., & Jung, I. "A DTSA (Detection Technique against a Sybil Attack) Protocol using SKC (Session Key based Certificate) on VANET", International Journal of Security & Its Applications, 7(3), pp.1-10, 2013.

[14] Li, M., Xiong, Y., Wu, X., Zhou, X., Sun, Y., Chen, S., & Zhu, X." A Regional Statistics Detection Scheme against Sybil Attacks in WSNs", IEEE Sponsored In Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on pp. 285-291, 2013.

[15] Gañán, C., Muñoz, J. L., Esparza, O., Mata-Díaz, J., & Alins, J. "PPREM: privacy preserving revocation mechanism for vehicular ad hoc networks", Computer Standards & Interfaces, 36(3), pp-513-523, 2014

[16] Balamahalakshmi D., & Shankar M. K. V., "Sybil Attack Detection with Reduced Bandwidth Overhead in Urban Vehicular Networks", International Journal of Engine ring Trends and Technology (IJETT) – Volume 12, pp. 578 – 584, 2014