Sybil attack detection in VAVET by using neighbouring vehicles in Wireless Sensor Networks

Amandeep, Naveen Dhillon

M.Tech Scholar in R.I.E.T, Phagwara

Principal in R.I.E.T, Phagwara

Abstract

Wireless Sensor Networks play a major role in revolutionizing the world by its sensing technology. Wireless Sensor Networks (WSNs) has emerged as that powerful technology which has multiple applications such as such as military operations, surveillance system and Intelligent Transport Systems (ITS). One severe attack is Sybil attack, in which a malicious node forges large number of fake identities in order to disrupt the proper functioning of VANET applications. Fake information reported by a single malicious vehicle may not be highly convincing because most of the VANET applications require several vehicles to reinforce a particular information before accepting as a truth. A Sybil attacker pretends multiple vehicles in order to reinforce false messages. . In the recent times, various techniques have been proposed for the detection of malicious node from the network. The proposed techniques is based on monitor mode and distance based techniques. 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, this is the reason that communication can be done inefficient manner through the network. Motivation behind the design of proposed approach is to locate Sybil nodes quickly without using secret information exchange and special hardware. The simulation is been performed in NS2. NS2 is an open – source simulation tool running on Unix – like operating systems. In our research, straightforwardly study the impact of parameters such as wireless communication range, vehicular densities, distance between source the destination, and minimum and maximum vehicle speeds on the end-to-end delay. The results shows that purposed technique shows good results in terms of various parameter. Here some perimeters are packet loss, throughput and routing overhead. Extensive simulation results demonstrate the accuracy of our analysis.

***Key Words*: VANET,MANET, VANET,NS2 AND UNIX** .

1.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 communication between the mobile vehicles is done using VANETs. In the range of a specific area, if the vehicles keep moving, the communication with the help of this network is still possible. The Vehicular ad hoc networks are the most prominent research area for the research purposes due to their increase in demand of usage.If there is any collision problems in the vehicles, such types of networks are used for the purpose of communication. The hybrid scheme is implemented in an intelligent manner and the communication flow is not stopped at any situation. 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.

1.1 Major Issues in VANET

The major issues which occur in VANET are enlisted below:

1. **High Mobility:** In accordance with the learn-based schemes, there is a proper learning of the behaviours of each node. It is not possible for the nodes to interact when the nodes are highly mobile.

2. **Real-time Guarantee:** For the purpose of proper message delivery, there are some strict guidelines which are to be followed. They can then be used in applications such as hazard warning, collision avoidance, and accident warning information.
3. **Privacy and Authentication:** The personal identification of each user can be exposed by others. To avoid this, there is need to identify the vehicles through the messages which can be sent only to the authenticated users through the message transmissions. A new system is set which helps in hiding the information of vehicles from the common nodes. The central authorities are however to be notified in the case of accidents or emergencies.
4. **Location Awareness**: The GPS facility is used for the purpose of handling the vehicular network's applications. There is a chance of delay to occur in situations where there is no proper system placed.

1.2 Sybil Attack in VANET

The attack occurs when a single node keeps sending multiple messages to other nodes which are pretended to be from different identities. In most of the cases, Sybil attack is possible. It can only be exempted from the extreme conditions and assumptions of chances of resource parity and coordination amongst the entities. A type of confusion occurs in the whole network when a single node starts sending multiple copies of it selves**.** The collision within the network starts beginning which results in causing Sybil attack in the network. Both internal and external attacks can be triggered in this type of attack. However, the external attacks can be avoided by providing authenticities measures. This is not possible with the internal attacks. The identity and entity within a network have one to one mapping.

2. LITERATURE SURVEY

Supinder Kaur, Anil Kumar, (2016) In this paper it is 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.

Surendra Nagar et al. (2017) In this paper, a secure routing protocol which could be applied in scenarios where DDOS attack was possible. The proposed algorithm was used to scan the infected nodes. The identified infected nodes were blocked in such a manner that they could not participate within the further activities. The intrusion prevention mechanism was used in order to protect the network. Here there were particular nodes which acted as IPS nodes and they operated within the radio range in a particular region. The neighbors were scanned by these nodes in regular manner.

Anu S Lal, Reena Nair, (2015) In this paper authors 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.

Dongxu Jin, JooSeok Song, (2014) In this paper it is presented that in traffic safety related utilization of Vehicular Ad-hoc Networks (VANETs), security is an incredible critical issue. Sybil attack is a specific kind of attack where the attacker illegitimately claims multiple identities. In the previous years, a few approaches have been hybrid for tackling this problem.

Ashritha M, Sridhar CS, (2015) In this paper, 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.

3. PROBLEM FORMULATION AND OBJECTIVE

3.1. PROBLEM FORMULATION

The vehicular ad hoc network is the network which has high mobility and decentralized in nature. Due to such type of network malicious nodes enters the network which triggers various types of attacks. The security attacks can be categorized as active and passive attacks. The active attacks are those which affect network performance. The Sybil attack is the active type of attack in which malicious nodes spoof identification of the normal nodes. The normal nodes will start communicating with the malicious node instead of normal node. The Sybil attack reduces network performance in terms of certain parameters. The techniques which are proposed so far for the detection of malicious nodes have two major issues which are require extra hardware and software, accuracy of malicious node detection is low. The technique is required for the detection of malicious node which detects malicious nodes without any hardware or software and also detects malicious nodes accurately.

3.2. OBJECTIVES

Following are the various objectives of this research work:-

1. To study and analyze various malicious node detection techniques in vehicular ad hoc network

2. To propose novel approach for the detection of malicious nodes in vehicular ad hoc network

3. Implement proposed approach and compare with existing in terms of throughput, packet loss and delay.

4. RESULTS

There are a number of quantitative metrics that can be used for evaluating the performance of a routing protocol for mobile wireless ad-hoc networks. In this thesis, we follow the general ideas described in RFC 2501, and we use four quantitative metrics. The packet delivery ratio and average end-to-end delay are most important for best-effort traffic. The other two qualitative metrics used in this thesis are and throughput.

4.1Throughput

The throughput is defined as the fraction of all the received data packets at the destinations over the number of data packets sent by the sources. This is an important metric in networks. If the application uses TCP as the layer 2 protocol, high packet loss at the intermediate nodes will result in retransmissions by the sources that will result in network congestion. The Ids of the vehicles are verified by the GSR and the generation of anonymous ID of the vehicle is also donehere.

$$Throughput = \frac{Total\ data\ packets\ recieved}{Total\ data\ packets\ sent}$$

4.2Routing Overhead

Ad hoc networks are designed to be scalable. As the network grows, various routing protocols perform differently. The amount of routing traffic increases as the network grows. An important measure of the scalability of the protocol, and thus the network, is its routing overhead. It is defined as the total number of routing packets transmitted over the network, expressed in bits per second or packets per second. The causes of routing overhead are network congestion and route error packets. The Vehicular ad hoc networks are the most prominent research area for the research purposes due to their increase in demand of usage.

4.3Packet loss

The packet loss is the parameter which counts the number of packets which get lost in the network.

$$Packet\ loss =\ number\ of\ packewts\ sent - number\ of\ packets\ recieved$$

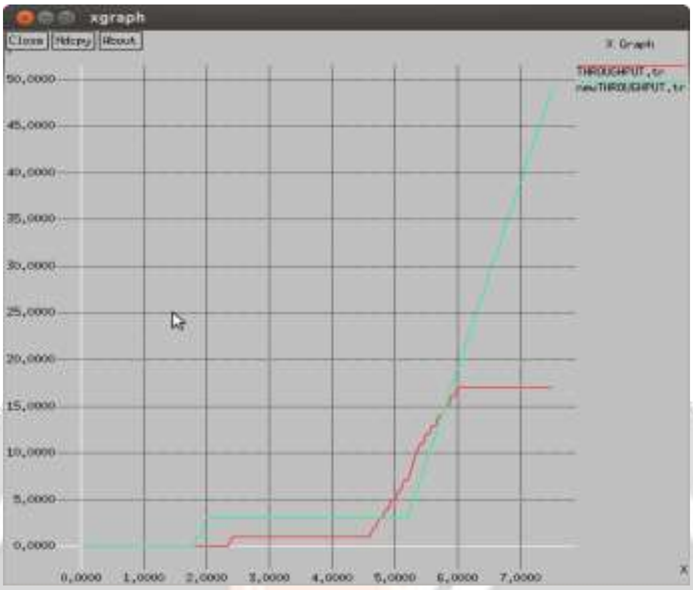

Figure -1: Throughput

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. When used in the context of communication networks, such as Ethernet or packet radio, throughput or network throughput is the rate of successful message delivery over a communication channel.

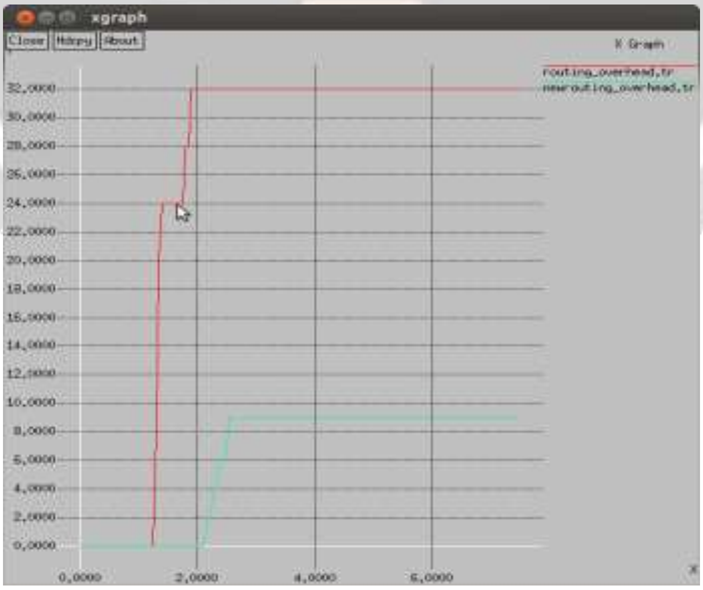

Figure -2: Routing overhead

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.

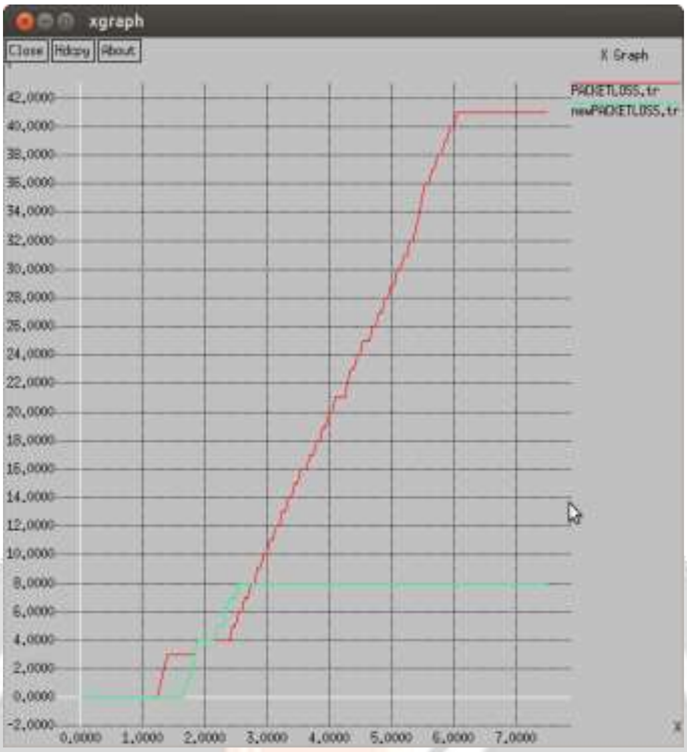

Figure -3: Packet loss

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is either caused by errors in data transmission, typically across wireless networks or network congestion.

5. CONCLUSIONS

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, sometime 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 hybrid technique is been done in Ns2 and results shows that performance is increased in the network.

The hybrid technique can be compared with the other secure techniques which are applied to isolate malicious nodes from the network. The reactive routing protocols has high performance in terms of certain parameters like throughput, routing overhead and packetloss. The reactive routing protocols do not have any parameters for the detection of malicious nodes. The secure channel establishment is the scheme techniques for the vehicular ad hoc networks. In future the technique of secure channel establishment will be applied to remove the chances of information spoofing in the network.

REFERENCES

[1] Yuan Yao, *Member, IEEE,* Bin Xiao," Multi-channel based Sybil Attack Detection in Vehicular Ad Hoc Networks using RSSI". 10.1109/TMC.2018.2833849, IEEE Transactions on Mobile Computing

[2] Surendra Nagar, Shyam Singh Rajput, Avadesh Kumar Gupta, Munesh Chandra Trivedi, "Secure Routing Against DDoS Attack in Wireless Sensor Network", 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" volume 3, issue 9, 2017.

[3] Supinder Kaur, Anil Kumar, "Techniques to Isolate Sybil Attack in VANET-A Review", 2016, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Volume 14, issue 6

[4] 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), Volume 8, issue 5

[5] 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), Volume 43, issue 88

[6] Dongxu Jin, JooSeok Song, "A Traffic Flow Theory Aided Physical Measurement- Based Sybil Nodes Detection Mechanism in Vehicular Ad-hoc Networks", 2014, IEEE/ACIS 13th International Conference on Computer and Information Science (ICIS), volume 10, issue 23

[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, issue 22

[8] 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, Volume 13, Issue 4

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