Novel Approach for Isolation of Sybil Attack in Vehicular Ad hoc Networks

Bharpur Singh1, Maninder Kaur2
[1]*Research Scholar,* [2]*Head of Department*
[12]*Doaba Institute of Engineering & Technology*

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, Signal Strength

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. 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 [1]. 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. The areas where highly dynamic topologies and less coverage areas are to be considered, there are various design issues which need to be taken care of [3]. A network in which all the vehicles are represented as the nodes of the network is known as the vehicular ad hoc network. These network communications are built to ensure the network safety and comfort for the driver. An intelligent transport system is provided for the purpose of establishing a vehicular ad hoc network which is anyhow a subset of the mobile ad hoc networks [4]. The vehicles find it very beneficial and so for the purpose of ensuring safety all the vehicles must be provided with this facility. The vehicles and the elements present on the roadside are provided with a wireless communication network. 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 [5]. 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. 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. However, due to the network partitioning, routing link failures as well as the rapid topology changes, the network faces many challenges. The access points are deployed along the road in the network as a solution to the problems notified. In networks where there is no issue regarding the energy consumption also, this solution is opted [6]. In the case of hybrid communication, there is a centralized architecture based cellular network in which the traffic information is gathered from the road with the help of access points. The acquired information is processed by the access points and is used by the drivers as per the requirement. VANETs security is violated by various types of attacks. 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. There is a chance that all the illegal, fake ID's and the authority are claimed. The collision within the network starts beginning which results in causing Sybil attack in the network [7]. 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.

II. LITERATURE REVIEW

Lee, B., et.al (2013) proposed a Detection Technique is for the Sybil Attack which is the DTSA protocol. The session key based certificate (SKC) is used for validations of the inter-vehicle Ids in vehicular ad hoc networks. The Ids of the vehicles are verified by the SKC and the generation of anonymous ID of the vehicle is also done here. The creation of a session key, the expiration date as well as the local server certification is also done for identifying the Sybil attack along with the verification time of the ID. The detection time of the Sybil attack is reduced with the help of this method. The reduction of verification time is also done here using the hash function and the XOR operation. The anonymous ID can be used for the purpose of protecting the privacy of the driver. The drivers can thus drive safely and reliable information can be provided for VANETs and this can result in reducing the traffic accidents [8].

Li, M., et.al (2013) studied the detection of replicated attacks in wireless sensor networks (WSNs). The variants of replication attacks are spawned. One of them is the Sybil attack. A regional statistics detection scheme (RSDS) is proposed in this paper. This scheme provides solutions to three main problems. The first is the addressing of the Sybil attack by the RSSI-based distributed detection mechanism. The second is the prevention of the network with the help of the protocol from various node failures caused due to the Sybil attacks. Third is, the verification of the RSDs which can maintain the high detection probability along with low system overhead using the imposed experiments. At the final stage, the protocol is run in a prototype detection system along with the 32 nodes. The results show that the experiment conducted here has high efficiency [9].

Gañán, C., et.al (2014) discussed a critical security issue of VANETs is discussed which is the cause of malicious vehicles. The potentially sensitive information can be leaked by the system. The vehicles that need any kind of information can be provided by the Road Side Units (RSUs) which receive the authorized status queries. There is a loss of privacy results by the RSUs which holds the checking vehicles with the query's target. A Privacy Preserving Revocation Mechanism (PPREM) is proposed in this paper. This scheme is based on the universal one-way accumulator and provides explicit, concise, authentication and unforgettable information regarding the revocation status of each certificate. Along with all this, the privacy of the user is ensured throughout. The service status checking process is replaced by the time-consuming CRL. A one way accumulator is applied here which holds a fast revocation checking process. The security and privacy of the VANETs are ensured by the PPREM. It also ensures the reduction of revocation cost [10].

Balamahalakshmi D., et.al (2014) proposed a compromised RSU detection mechanism for the purpose of detecting the Sybil attack. The trajectory information is used in this method which generates multiple RSUs. However, the location of the vehicle is hidden and not exposed. The location as well as the timing information will be generated by the RSU for the vehicle. This is done when the vehicle passes through the RSU. The verification is done through this message. For the purpose of reducing the size of the message, the number of adjacent RSUs is eliminated. The length of the trajectory information is reduced and there is no loss of information. Through the method, the bandwidth overhead of the network is also reduced [11].

Chang, S., et.al (2011) proposed a novel approach for the purpose of Sybil attack detection. The technique known as Footprint is used along with the trajectories of the vehicles in order to identify the Sybil attack. This mechanism however, preserves the location privacy of the vehicle. Whenever a vehicle comes towards the Road-Side Unit (RSU), the authorized message from the RSU is asked as a proof for the appearance time at RSU. A location hidden authorized message is created in this scheme. It has two aims. A location hidden trajectory is generated in the vehicles. It is used for the location-privacy-preserved identification. This is done by gathering consecutive series of the authorized messages. The communities of Sybil trajectories can be recognized as well as dismissed by the Footprint with the help of social relationships with accordance with the similarity definition of two trajectories used [12].

Tong Zhou, et.al (2011) proposed a Privacy Preserving Detection of Abuses of Pseudonyms protocol. This is used for the detection of Sybil attacks in VANETs. Here, a malicious user is detected which pretends to be multiple vehicles. A distributive approach is used with the help of passive overhearing of set of fixed nodes which are known as road-side boxes (RSBs). The parameters which make sure about this are the detection latency and the privacy of the vehicles. This proposed scheme is able to detect the Sybil attacks at low overhead and delay along with the privacy preservation of the vehicles. The numerous vehicles that are affected by the malicious user are also highlighted by using this approach. A passive listener is used in the distributive manner which sets the fixed nodes which are also known as the road side boxes. There is no need to distinguish the identity of any vehicle which helps in preserving the privacy of the network at all times and is of great helps [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.

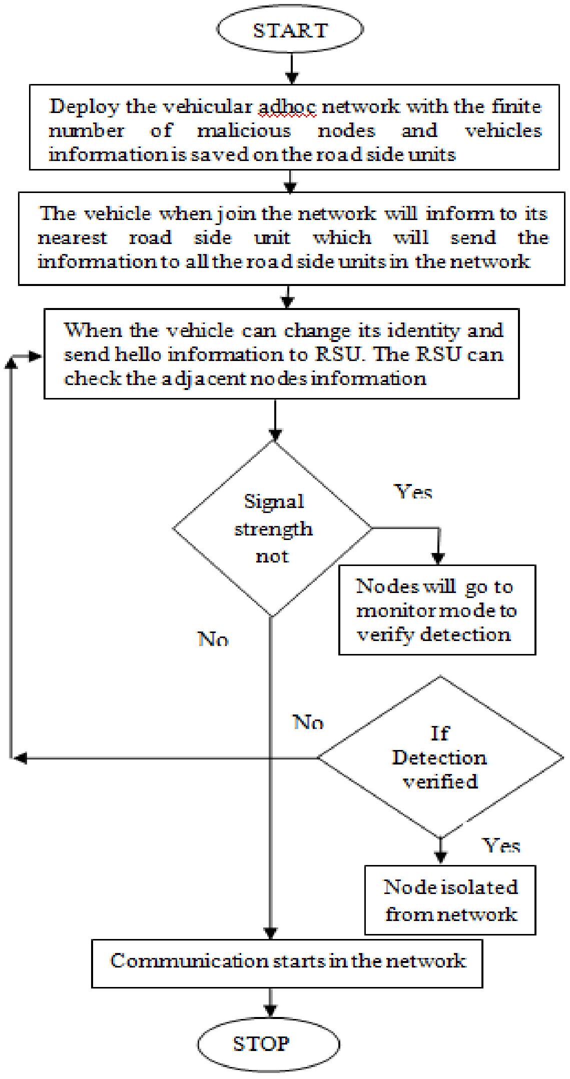
START
Deploy the vehicular adhoc network with the finite number of malicious nodes and vehicles information is saved on the road side units
The vehicle when join the network will inform to its nearest road side unit which will send the information to all the road side units in the network
When the vehicle can change its identity and send hello information to RSU. The RSU can check the adjacent nodes information
Signal strength not
Yes
Nodes will go to monitor mode to verify detection
No
No
If Detection verified
Yes
Node isolated from network
Communication starts in the network
STOP

Fig.1: Flowchart of Proposed Technique

IV. EXPERIMENTAL RESULTS

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

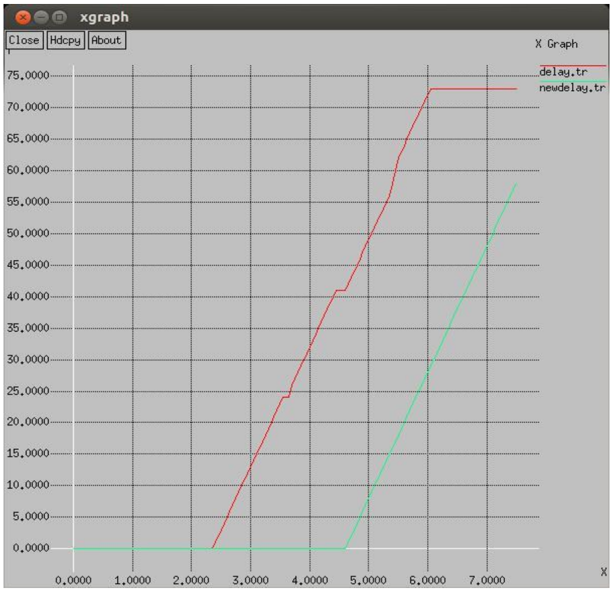

Fig.2: Delay Comparison

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.

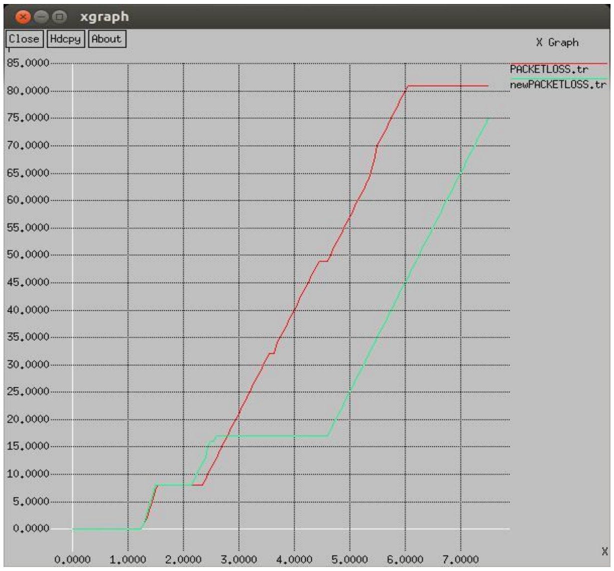

Fig.3: Packetloss comparison

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.

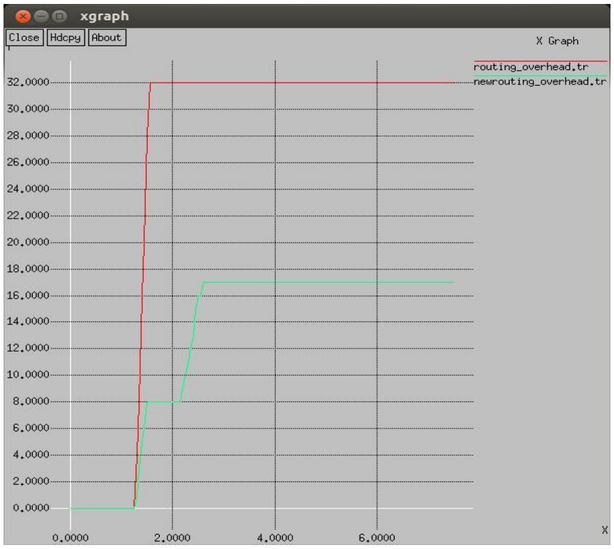

Fig.4: Routing overhead

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.

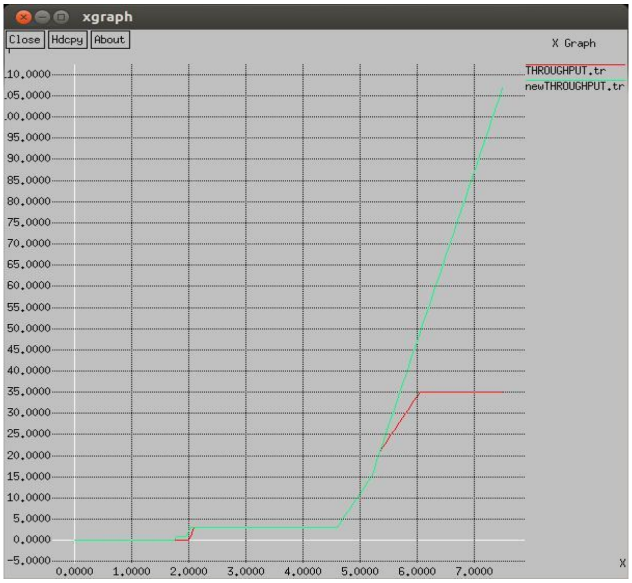

Fig.5: Throughput Comparison

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

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]. 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 Range Communications for Vehicles", IJSER September 2, 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, “Mobility Simulation of Reactive Routing Protocols for Vehicular Ad-hoc Networks”(2011) Department of MCA, Govt. College of Engineering, Ajmer, India

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

[9]. Josiane Nzouonta et al “ Routing on City Roads using Real-Time Vehicular Traffic information 2008, p-18.

[10]. Salim M.Zaki, M.A.ngadi,Maznah Kamat,” A location based routing prediction service protocol for vanet environment, IEEE, 2009

[11]. Reena Didcach “Mobility simulation of Reactive protocol for Vanet”, IEEE, 2012

[12]. Sumaiya Iqbal, “Vehicular Communication: Protocol Design, Testbed Implementation and Performance Analysis", IWCMC’09, June 21-24, 2009, Leipzig, Germany, pp 410-415

[13]. A. AHMAD, “Hybrid Multi-Channel Multi-hop MAC in VANETs”, MoMM2010, 8–10 November, 2010, Paris, France, pp 353-357