Evaluation of Hybrid framework for Detection of Sybil Attack in VANET

Pallvi Minhas[1], Pallavi Jindal[2]

Research Scholar, Assistance Professor& Department of computer science, Baddi university of Emerging Sciences&Technology, Baddi Solan H.P-173205, India

***Abstract**: MANET stands for Mobile Ad hoc Network. It is a robust infrastructure less wireless network. Malicious vehicles can degrade the network performance by triggering some security attack. VANET 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. These are used for the communication among the mobile vehicles. It has some security issues like attacks, authentication etc. In this work, a novel technique has been proposed to detect malicious vehicles and isolate Sybil attack from the network. This will help to improve network performance.*

Keywords: *MANET, VANET, Malicious node, Sybil Attack. Collision, V2V communication*

I. INTRODUCTION

Vehicular adhoc networks (VANETs) are classified as an application of mobile adhoc network (MANET) the main benefits of VANETs are the potential in providing travellers comfort & they enhance road safety and vehicle security while protecting drivers' privacy from attacks perpetrated by adversaries. Recently VANETs have emerged to turn the attention of researchers in the field of wireless and mobile communications. Vehicular adhoc 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. Vehicular ad-hoc network is subclass of mobile ad hoc networks which provides a distinguished approach for intelligent transport system. It is autonomous and self-organizing wireless communication network, where all the nodes in VANET involve themselves as servers or client for exchanging and sharing information. The network architecture of VANET can be classified into three categories pure cellular, pure ad-hoc and hybrid.

A. *V2V Communication*: Possible Deployment regarding the C2C-CC reference architecture together with the advances in heterogeneous communication technologies, vehicular networks potentially have two main types of communication scenarios: car-to-car (C2C) communication scenario and car-to-infrastructure (C2I) communication scenario [5].These types of communication scenarios allow a number of deployment options for vehicular networks. Vehicular network deployment can be integrated into wireless hot spots along the road. Such hot spots can be operated individually at home or at office, or by wireless Internet service providers or an integrated operator. Vehicles can even communicate with other vehicles directly without a communication infrastructure, where vehicles can cooperate and forward information on behalf of each other [5].Based on their specific characteristics, the technologies for vehicular communication can be categorized in the following three categories [5].

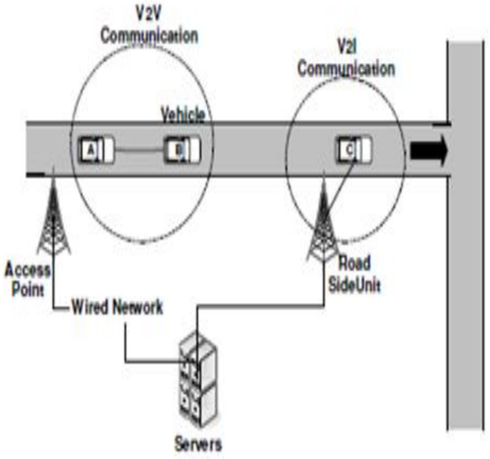


Fig.1.1 V2V Communication

B. ***Major Issues in VANET*:** There are some issues in VANET. These are as follow:

a. *High Mobility*: Due to high mobility all the nodes are not interacted properly with each other because they have to learn about others behaviour first according to learn based scheme. It also decreases efficiency of the system.

b. *Real-time Guarantee*: VANET applications are used for hazard warning, collision avoidance, and accident warning information, so applications involve strict deadlines for proper message delivery.

c. *Privacy and Authentication*: It is required to follow the vehicles for the identification of vehicles from the message they send for authentication of all message transmission, which most consumers will not like others to know about their personal identification. Therefore a system wants to be introduced which enables message to be unknown to the common nodes but also recognition by central authorities in cases like accidents.

d. *Location Awareness*: For the proper location awareness GPS system is required to handle the VANET application. If there is no Proper system for location identification, delay is there automatically.

e. *Delay in VANET*: In a VANET delay issue should be minimum for the new path identification. In this system vehicle and RSU detect chances of collision between multiple vehicles are not able to communicate amongst themselves. The system will collect data about vehicles that are coming in opposite direction and are approaching towards the destination. For this, there are many safety applications are present in VANET to decrease the road accident and loss of life of the occupants of vehicles. Collision leads the jam problem. To overcome this problem delay should be minimum.

II. REVIEW OF LITERATURE

In this paper, they present a lightweight security scheme for detecting and localizing Sybil nodes in VANETs, based on statistical analysis of signal strength distribution. Their scheme is a distributed and localized approach, in which each vehicle on a road can perform the detection of potential Sybil vehicles nearby by verifying their claimed positions. They first introduce a basic signal-strength-based position verification scheme. In this technique, traffic patterns and support from roadside base stations are used to their advantage then, propose two statistic algorithms to enhance the accuracy of position verification. The statistic nature of our algorithms significantly reduces the verification error rate. InGPS and RSSI signal measurements are used for detecting Sybil nodes. The proposed scheme uses Vehicle-to-Vehicle (V2V) communications to confirm reported positions of vehicles by referencing the RSSI measurements. To correct inaccuracies arising from RSSI measurement, caused by vehicle mobility, traffic patterns and support from roadside base stations are used [**3**].

In this paper, they propose a security protocol to detect Sybil attacks for position based applications in privacy preserved vehicular ad hoc networks (VANETs). Vehicles in our protocol identify Sybil attacks locally in a cooperative way by examining the rationality of vehicles' positions to their own neighbours. The attack detection utilizes the characteristics of communication and vehicles' GPS positions which are included in the periodically broadcasted safety related messages. No extra hardware and little communication and computation overhead will be introduced to vehicles. Therefore, their protocol is very light weighted and suitable for real applications. Moreover, a smart attacker scenario in which a malicious vehicle may adjust its communication range to avoid detection and the malicious vehicles' collisionscenario are also considered. Simulation results based on NS2 are presented to demonstrate the performance of the proposed protocol [**4**].

In this paper, they propose 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. They design a location-hidden authorized message generation scheme for two objectives: first, RSU signatures on messages are signer ambiguous so that the RSU location information is concealed from the resulted authorized message; second, two authorized messages signed by the same RSU within the same given period of time (temporarily linkable) are recognizable so that they can be used for identification. With this scheme, vehicles can generate a location-hidden trajectory for location-privacy-preserved identification by collecting a consecutive series of authorized messages. Utilizing social relationship among trajectories according to the similarity definition of two trajectories, Footprint can recognize and therefore dismiss “communities” of Sybil trajectories [**5**].

In this paper proposed 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. this DTSA reduces not only the detection time against a Sybil attack but also the verification time for ID by using a hash function and an XOR operation. 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 [7].

III. SYBIL ATTACK IN VANET

It 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. When any node creates multiple copies of itself then it creates confusion in the network. Claim all the illegal and fake ID's and Authority. It can create collision in the network. This type of situation is known as Sybil attack in the network. This system can attack both internally and externally in which external attacks can be restricted by authentication but not internal attacks. As there is one to one mapping between identity and entity in the network.

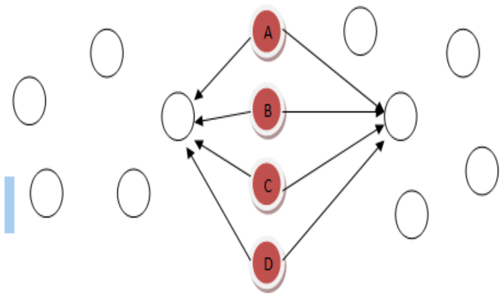
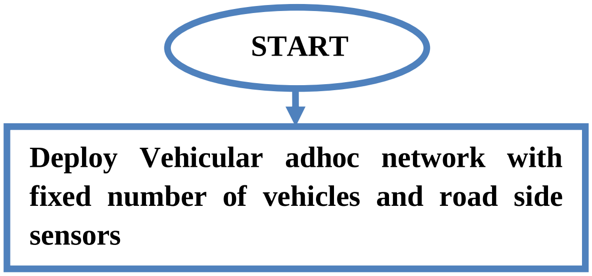


Fig.3.1 Sybil Attack

A, B, C ,D nodes are Sybil nodes which create fake or similar identity in the network and collapse the network.

IV. PROPOSED METHODOLOGY

The vehicular adhoc network is the self configuring network in which the vehicles can join or leave the network when they want, and no central controller is present in VANET. Due to decentralized type of network much of the security issues raised in the network. The malicious node can join the network and it may trigger Sybil attack in the network. In this work, algorithm will be proposed which isolate Sybil attack in the network. An algorithm will be proposed which isolate Sybil attack in the network.


START
Deploy Vehicular adhoc network with fixed number of vehicles and road side sensors

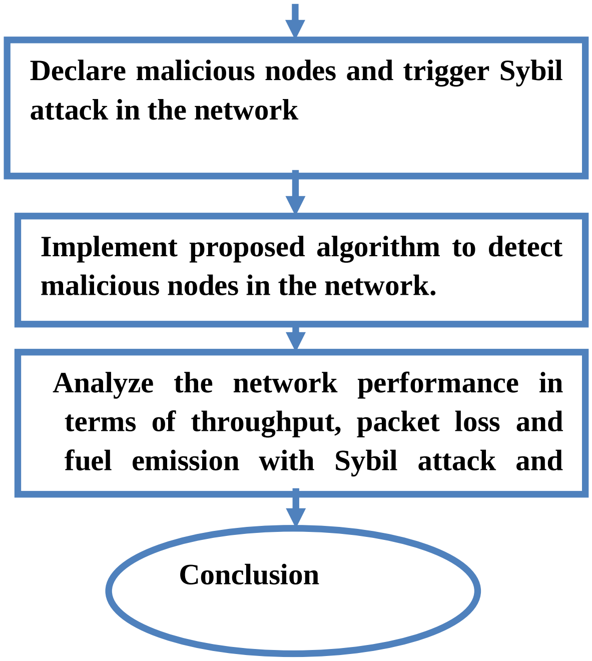

Declare malicious nodes and trigger Sybil attack in the network
Implement proposed algorithm to detect malicious nodes in the network.
Analyze the network performance in terms of throughput, packet loss and fuel emission with Sybil attack and
Conclusion

Fig.5.1. Flowchart of Methodology

```
Algorithm: Input: Road side units, smart cars, malicious car
Output: Detection of Malicious car
Set registration process
{
Car send its credentials to road side units
If ( stored credentials == send credentials )
{
Assign identification number;
Else
{
Repeat step of registration


}

If( Identification== assigned)

{

Communication starts between cars

Road side units start gathering information about neighbours

If (Neighbour information on each road side units == same)
{
No malicious node exits in the network;
Else
{
Road side units flood ICMP messages in the network
```

```
Monitoring process= true
If ( malicious car== detected)
{
Isolate malicious car with identification number
Else
Repeat process of monitoring
}
End
```

V. EXPERIMENTAL RESULTS

The whole scenario has been implemented in NS2.

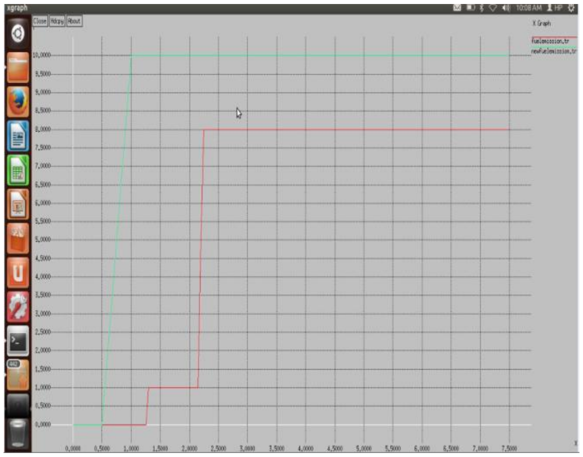


Fig.5.1 Fuel Emission

As shown in figure 5.1, 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.

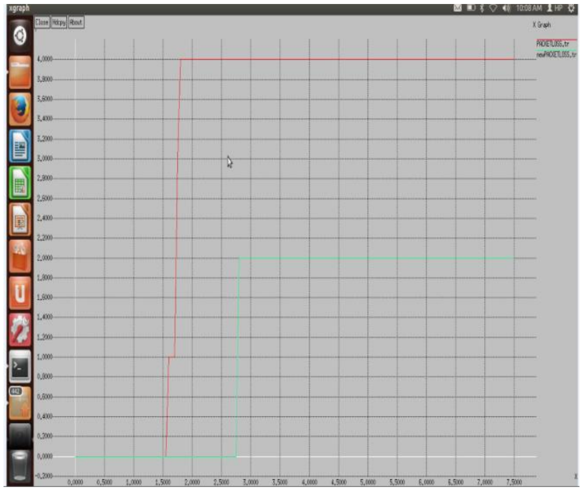


Fig. 5.2 Packetloss

As shown in figure 5.2, packet loss graph is shown in which packet loss in existing and proposed scenario is shown and it is analysed that packet loss of existing scenario is more due to Sybil attack, as network traffic is redirected to malicious node which leads to packet loss and in the proposed scenario packet loss is reduce to isolation of malicious nodes. The packet loss in the existing scenario is 4 packets and in proposed scenario it is 2 packets.

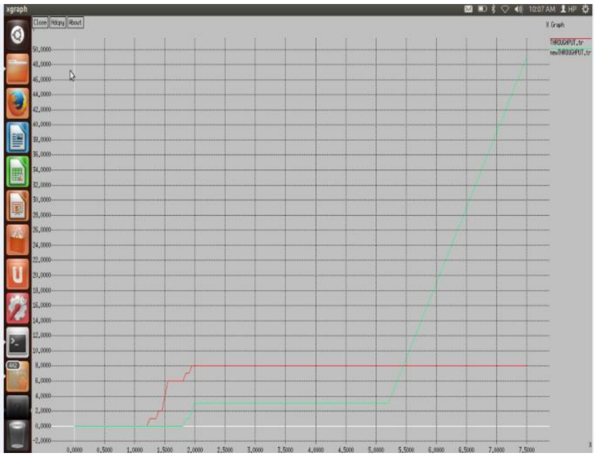


Fig.5.3 Throughput

As shown in figure 5, 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**.**

VI. CONCLUSION

In VANET many attacks has been trigger by the malicious node. Therefore keeping in view above challenges there is a need to improve the efficiency of VCWC protocol so that it may be able to control both, the factors which make wireless communication unreliable and also support the above application challenges to a large extent. All the problems discussed in this paper can be raised if some of the wrong information can be flooding in the network. The wrong information can be flooding in the network by malicious vehicles. These malicious vehicles can degrade the network performance by triggering some security attack. In this work, a novel technique has been proposed to detect malicious vehicles and isolate Sybil attack from the network. This will help to improve network performance.

VII. REFERENCES

[1] Raya, M., & Hubaux, J. P. "Securing vehicular ad hoc networks", Journal of Computer Security, 15(1), pp.39-68, 2007.

[2] Iqbal, S., Chowdhury, S. R., Hyder, C. S., Vasilakos, A. V., & Wang, C. X. " Vehicular communication: protocol design, test bed implementation and performance analysis", In Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly , pp. 410-415, 2009.

[3] Xiao, B., Yu, B., & Gao, C. "Detection and localization of sybil nodes in VANETs", In Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks pp. 1-8,2006.

[4] 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.

[5] 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.

[6]. 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.

[7]. 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.

[8]. 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.

[9]. 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.

[10]. 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.

[11] M. Raya, J. Pierre, Hubaux,"Securing vehicular ad hoc Networks" Journal of Computer Security,vol.15, january 2007, pp: 39-68

[12] Jason J. Haas and Yih-Chun Hu University of Illinois at Urbana-Champaign Urbana, Illinois, U.S.A," Real-World VANET Security Protocol Performance" (2007) p1-7.