International Journal of Advance Research in Science and Engineering
Vol. No. 5, Issue No. 08 , August 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

A MONITOR BASED TECHNIQUE FOR THE DETECTION OF SYBIL ATTACK IN VANET IN NS2

Kavita khatkar[1], Richa Garg[2]

Assistant Professor (CSE), JCDM College of Engineering, Sirsa, (India)
M.Tech (CSE), JCDM College of Engineering, Sirsa, (India)

ABSTRACT

Keywords: **VANET, *Sybil Attack, Malicious Node, Malicious Nodedetection, Isolation***

I. INTRODUCTION

- **MANET** stands for Mobile Ad hoc Network. It is a robust infrastructure less wireless network. It can be formed either by mobile nodes or by both fixed and mobile nodes. Nodes are randomly connected with each other and forming arbitrary topology. They can act as both routers and hosts. Their ability to self-configure makes this technology suitable for provisioning communication, for example disaster-hit areas where there is no communication infrastructure or in emergency search. In MANET routing protocols for both static and dynamic topology are used.An ad hoc network is a wireless network describe by the nonexistence of a centralized and fixed infrastructure. The absence of an infrastructure in ad hoc networks poses great challenges in the functionality of these networks [1]

- **Types of MANET**

1. **Vehicular Ad Hoc Networks (VANETs**): These are used for the communication among the mobile vehicles. The communication being carries on even if the vehicles are moving in the different direction with in a particular area.
2. **Intelligent vehicular ad hoc networks (InVANETs):** It is used in case like collision of the vehicles or any other types of mobility problems. It is uses the scheme intelligently and the flow less communications goes on.
3. **Internet Based Mobile Ad hoc Networks (iMANET):** Itis an ad hoc networks that connection mobile nodes and fixed nodes of Internet-gateway. Ad hoc routing algorithms don't apply directly in such type of networks.

- **VANET**: 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). This kind of networks are self-configuring networks composed of a collection of

vehicles and elements of roadside structurelinked 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. 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 (*NP-problems*). It is especially difficult (e.g., for a network designer) when considering multiple design issues, such as highly dynamic topologies and reduced coverage.

Application and uses for VANET

- **Safety applications:** Safety applications are most important factor to decrease the road accident and loss of life of the occupants of vehicles. There are so many accident happened due to the collision of vehicles. The class of application provide active road safety to avoid collisions by assisting the drivers with timely information.
- **Car speed warning:** With help of these protocols use a combination of GPS and digital maps are used to judge threat level for driver approaching a curve quickly.
- **Traffic signal violation warning:** It is also designed to send a warning message when driver detects the vehicle is in risk of running the traffic signal. The decision to send a message is made on the basis of traffic signal status and timing the vehicle position and speed.
- **Collision risk warning:** 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.
- **Lane change warning:** In this application vehicle monitor the position of vehicle within a roadway lane and warn a driver if it is unsafe to change lanes.

Attacks in VANET: There are different types of attacks in Vanet. One is as follow:

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 [21]. 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.

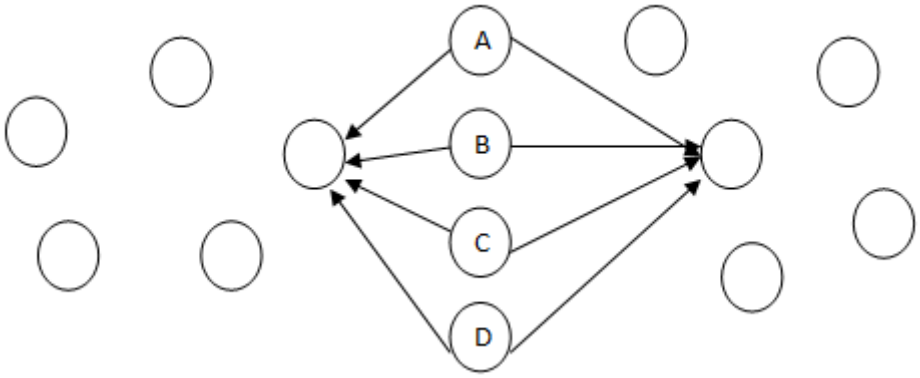

Fig. 1.4: Sybil Attack

A, B,C,D nodes are Sybil nodes which create fake or similar identity in the network and collapse the network. Sybil attack is a critical attack. In this type of attack attackers generate multiple messages from different ids to other vehicles. Other vehicles are thinking in this way that messages are coming from different vehicles with different ids, so there is condition of jam occurs. In this way attacker produce illusion of other vehicle and force them to choose another path and leave the road for the benefit of the attacker. Overall it is concluded that Sybil attack is performed or launched by sending multiple messages from different ids. In fig. 1.6 red colours cars have same id that is A which are responsible for trigger Sybil attack in the network. It is of two types delay sensitive and throughput sensitive**.**

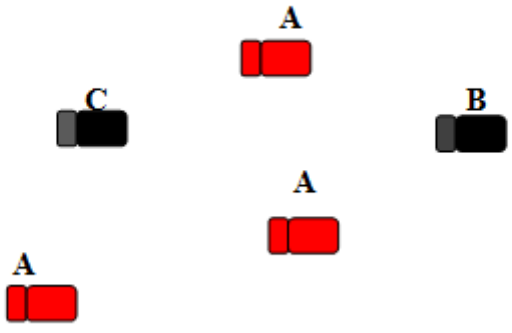

Fig 1.5 Sybil attack in the network

AODV: AODV 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. In this process a RRE,Q packed is forwarded to all the neighbours of the source node by source node itself and this forwarding of packets to the neighbours & their neighbours 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. 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. The route maintenance procedure works after selecting & establishing the route is completed. This route maintenance goes on till the destination is available with it's 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.

II. LITERATURE REVIEW

It represents the review of work done by various researchers which give a useful insight in route maintainence, route establishment and awareness to the other nodes. Literature review is a body of text that aims to review the current knowledge including findings, as well as theoretical and practical contributions of a particular topic. Literature review focuses on a research question, trying to identify, select and combine all high-quality research evidence and arguments.

[1]Chang, S., Qi, Y., Zhu, H., Zhao, J., & Shen, X. (2011) 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**].

[2] Tong Zhou, Romit Roy Choudhury, Peng Ning, and KrishnenduChakrabarty (2011) In this paper theyproposed 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). The detection of Sybil attacks in this manner does not require any vehicle in the network to disclose its identity; hence privacy is preserved at all times. he results also quantify the inherent trade-off between securities, i.e., the detection of Sybil attacks and detection latency, and the privacy provided to the vehicles in the network. 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). The detection of Sybil attacks in this manner does not require any vehicle in the network to explore its identity; hence privacy is preserved at all times [**6**].

[3] Lee, B., Jeong, E., & Jung, I (2013) In this paper theyproposed a DetectionTechnique Against a Sybil Attack (DTSA) protocol usingSession Key based Certificate (SKC) to validate inter-vehicleIDs in VANETs. In DTSA, the SKC (Session Key basedCertificate) used to verify the IDs among vehicles, and alsogenerates a vehicle's anonymous ID, a session Key, theexpiration date and a local server's certificate for the detectionof 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**].

[4] Li, M., Xiong, Y., Wu, X., Zhou, X., Sun, Y., Chen, S., & Zhu (2013) In this paper they proposed 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, they proposed a regional statistics detection scheme (RSDs) against sybil attacks, 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 [**8**].

[5] Gañán, C., Muñoz, J. L., Esparza, O., Mata-Díaz, J., &Alins, J(2014) In this Paper represents one of the critical security issues of Vehicular Ad Hoc Networks(VANETs) is the revocation of misbehaving vehicles. While essential, revocation checking can leak potentially sensitive information. Road Side Units (RSUs) receiving the certificate status queries could infer the identity of the vehicles posing the query. An important loss of privacy results from the RSUs ability to tie the checking vehicle with the query's target. They propose a Privacy Preserving Revocation mechanism (PPREM) based on a universal one-way accumulator. PPREM provide explicit, concise, authenticated and unforgettable informationabout 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 [9].

III.OBJECTIVES

Research objectives declare what is the aim of research and for what purpose it is carried out. Main Objectives are:

1. To analyze and study various type of routing protocols and attack in VANETs.

2. Toanalyze the performance of MANET protocol (OLSR protocol) when Sybil attack will be triggered by the malicious node in the network.
3. To propose enhancement in OLSR protocol to detect malicious vehicle and isolate Sybil attack from the network.
4. To implement existing and proposed protocols under simulated environment and analyze network performance in terms of throughput, delay and fuel emission.

IV. PROPOSED 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 neighbour node information to RSU's
4. The RSU's can maintain the neighbour 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 itself 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 neighbouring 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 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.

V. CONCLUSION AND FUTURE WORK

The vehicular adhoc network is the self configuring type of network in which vehicles can move freely on the roads. The vehicular adhocnetwork 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 are responsible to trigger various type 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. In future proposed technique will be applied for the detection of wormhole attack in the network.

REFERNCES

[1] Hugo Conceicao "Large-Scale Simulation of V2V Environments", SAC'08 March 16-20, 2008, Fortaleza,Cear´ a, Brazil, pp 28-33

[2] Stephan Olariu"An Architecture for Traffic Incident Detection ", MoMM2009, December 14–16, 2009, Kuala Lumpur, Malaysia.

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

[4] Maxim and jean-Pierre Hubaux "The security of vehicular ad hoc networks",ACM,2005

[5] SumaiyaIqbal"Vehicular Communication: Protocol Design, Testbed Implementation and Performance Analysis", IWCMC'09, June 21-24, 2009, Leipzig, Germany, pp 410-415

A. AHMAD "Hybrid Multi-Channel Multi-hop MAC in VANETs ", MoMM2010, 8–10 November, 2010, Paris, France, pp 353-357

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

[7] JosianeNzouonta et al " Routing on City Roads using Real-Time Vehicular Traffic information 2008, p-18.