International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Detecting and Avoiding Sybil Attack in OLSR Protocol

Amit Kumar[1], Varun Singla[2]

[1, 2]Lovely Faculty of Technology and Sciences, Lovely professional University, Phagwara, India

Abstract: ***The ad hoc network is an infrastructure less wireless network consisting of mobile moving nodes. VANETs is the recently developed technique to achieve traffic safety and efficiency through inter vehicle communication, where routing protocol plays a vital role. Inefficient network security brings the severe degradation in network throughput and performance. Routing throughput and performance is largely dependent on the availability and security of the wireless link which makes it a very pivotal parameter, that can't be ignored in order to obtain proper performance and throughput measurement in VANETs. Secured routing is greatly dependent on the availability, performance and stability of the wireless links, which makes it a vital parameter that shouldn't be neglected in order to obtain proper security measurement in VANET. Many malicious vehicles demean the functioning of network by actuating some attacks So this work presents a refreshing technique that has been put forward to search malicious vehicles and remove the attack i.e. Sybil attack from the OLSR routing protocol. This remotion of attack from the OLSR protocol will increase the performance and stability of the network.***

Keywords: MANET; VANET; Malicious node; Sybil Attack; Collision; V2V communication

1. Introduction

Vehicular adhoc systems (VANETs) are delegated a utilization of portable adhoc system (MANET). The fundamental advantages of VANETs are the potential in giving voyagers solace and they upgrade street wellbeing and vehicle security while shielding driver's protection from assaults executed by enemies. As of late VANETs have risen to turn the consideration of scientists in the field of remote and portable interchanges. Vehicular adhoc system are remote systems where every one of the vehicles from the hubs of the system. It is for the driver solace and street security, the between vehicle correspondence give them. Vehicular specially appointed system is subclass of versatile impromptu systems which gives a recognized way to deal with canny transport framework. It is self-sufficient and self-sorting out remote correspondence system, where every one of the hubs in VANET include themselves as servers or customer for trading and sharing data. The system engineering of VANET can be characterized into three classes' pure cellular, pure ad-hoc and hybrid. In TABLE 1 we have shown a brief layered view of vehicular architecture that on which layer what kind of work we do or what kind technology we us.

Table 1: Layered View of Vehicular Architecture

Vehicular Network	Application Type	Safety Intelligent transportation Comfort applications
	QoS	Non real time Soft real time Hard real time
	Scope	Wide area Local area
	Network Type	Ad-hoc Infrastructure based
	Communication Type	V2V V2I

A. V2V communication

Conceivable Deployment in regards to the V2V reference engineering together with the advances in heterogeneous correspondence advances, vehicular systems possibly have two primary sorts of correspondence situations: vehicle-to-vehicle (V2V) correspondence situation and vehicle-to-infrastructure (V2I) correspondence situation [5]. These sorts of correspondence situations permit various organization alternatives for vehicular systems. Vehicular system sending can be incorporated into remote problem areas along the street. Such problem areas can be worked separately at home or at office, or by remote Internet administration suppliers or a coordinated administrator. Vehicles can even speak with different vehicles straightforwardly without a correspondence base, where vehicles can participate and forward data for each other [5]. Based on their particular attributes, the advancements for vehicular correspondence can be classified in the accompanying two classifications [5].

- Vehicle-to-vehicle (V2V) communication scenario and
- Vehicle-to-infrastructure (V2I) communication.

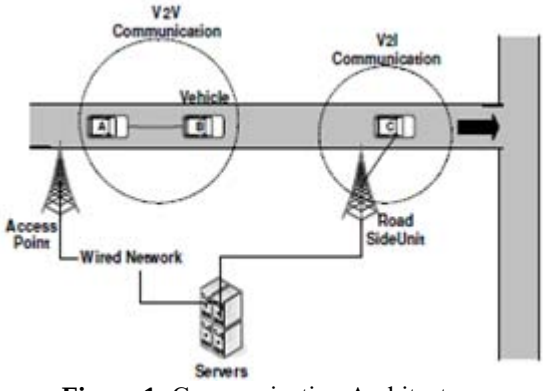


Figure 1: Communication Architecture

As shown in Figure 1. when the vehicles are speaking with the street side unit (RSU) or transmitting the messages with the side framework then this procedure is known as V2I. Then again when vehicles are transmitting information with each other are known as V2V. This V2V correspondence requires some exceptional equipment in the autos like actuator.

B. Major Issues in VANET

There are some issues in VANET. These are as follow:

- **High Mobility:** Because of high versatility every one of the hubs are not associated appropriately with each other in light of the fact that they need to find out about others conduct first as indicated by learn based plan. It additionally diminishes productivity of the framework.
- **Real-time Guarantee:** VANET applications are utilized for peril cautioning, crash shirking, and mischance cautioning data, so applications include strict due dates for appropriate message conveyance.
- **Privacy and Authentication:** It is required to take after the vehicles for the ID of vehicles from the message they send for validation of all message transmission, which most shoppers won't care for others to think about their own recognizable proof. Along these lines a framework needs to be acquainted which empowers message with obscure to the regular hubs additionally acknowledgment by focal commanding voices in cases like mishaps.
- **Location Awareness**: For the correct area mindfulness GPS framework is required to handle the VANET application. In the event that there is no Proper framework for area ID, postponement is there naturally.
- **Delay in VANET**: In a VANET delay issue ought to be least for the new way recognizable proof. In this framework vehicle and RSU recognize odds of crash between different vehicles are not ready to impart amongst themselves. The framework will gather information about vehicles that are coming in inverse heading and are drawing closer towards the destination. For this, there are numerous wellbeing applications are available in VANET to diminish the street mishap and death toll of the tenants of vehicles. Crash drives the jam issue. To conquer this issue postponement ought to be least.

In this paper, we have discussed about the Sybil attack in OLSR protocol, detect and avoid the Sybil attack introducing a new technique i.e. monitor mode technique. After that we compare the scenarios in which we only detect the Sybil attack with the scenario in which we also avoid the Sybil attack after detecting it and compare the graph of both simulations and observe throughput, packet loss and fuel emission of the car.

The paper is further proceeded as follows. In section II literature survey is reviewed. In section III we have described about the OLSR protocol. In section IV Sybil attack in VANETs has been described. In section V Proposed Methodology is being defined. In section VI Algorithm is being defined. In section VII we have shown the Experimental Results and in section VIII Conclusion is presented followed by the references in section IX.

2. Literature Survey

Some techniques used to detect Sybil attack that is being reviewed are:

a) Position of the Vehicle

It is proposed that vehicular improvised network is a taxonomy category of MANETs that legitimate wireless communication among all the various vehicles. In the VANET routing protocol proficiency must be accommodated to vehicular specific capabilities and needs. In the preceding research routing performance is highly rely on the availability and stability of the wireless links. Statistical analysis based on the dispersion of the strength of signal is used for finding and focalize Sybil vertex in improvised network. Scenario is based on dispersed and localized approach, where every automobile on the road can search the possible Sybil automobile present nearly by checking their exact position. They basically introduce the position confirmation scenario based on the strength of signal [3]. Vehicles as vertex in protocol discover Sybil attacks topically in a collaborative way by studying the rationality of vehicles position with their neighbor nodes. The attack finding, employ the feature of communication and GPS position that are enclosed in the sporadically broadcasted messages affiliated to protection [13].

b) Footprint

Footprint is a Sybil attack detection mechanism which uses the trajectories of vehicles for identification while 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 [14].

c) Road Side Boxes

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 set of fixed nodes called road-side boxes (RSBs) [15].

d) Session Key Certificate

A Detection Technique was proposed 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 [16].

e) Territorial Statistic Sensing

It is presented that sensing of rejoinder (replicated) attacks in WSN (Wireless Sensor Network) had been an existed problem. A territorial statistic sensing scenario against the attack that is Sybil was proposed, which is an efficacious solution for the problem of three key: 1) they refer the Sybil attack by a RSSI (Revised Signal Strength Indication) based diffused sensing mechanism. 2) Their protocols resisted the network from the turgid number of vertices failure caused by Sybil attack. 3) The territorial statistic sensing scenario had been proved, that can maintain the broad sensing probability

with reduce overhead in system by applying experiments [17].

f) OLSR Performance

Performance of OLSR protocol for location and VoIP applications in Manhattan grid scenario has been observed. They have used SUMO and NS3 platforms for simulation. They considered 802.11p standard Two Ray Ground Propagation Loss Model and sent multiple CBR flows over UDP between five pairs of source-destination nodes. As evaluation metrics PDR, throughput and delay are counted. Experimental results show that OLSR protocol can be used for real time scenario and traffic lights for VoIP applications [18].

g) Presence Evidence System

Sybil attack is considered as a serious security threat in WSN and VANET environment. They use RANSAC (Random Sample Consensus) based algorithm to make conjunctive method more strong against outlier data constructed by Sybil vertices. The system is names formally as PES (Presence Evidence System). With PES they were capable to increase the sensing veracity using statistical analysis across an observation period. Ultimately, based on realistic US traffic style and maps, they carry a feigning to check the quality of being doable and efficiency [19].

3. OLSR (Optimized Link State Routing) PROTOCOL

OLSR protocol is a table driven protocol which come under proactive routing protocol. It stores the routing table permanently and update it periodically, so the route is available when needed [9]. In OLSR when the topology changes it creates the situation of overflowing of the topology data to every active vertex into the network. Some of the vertices are selected as MPRs (Multi Point Relays) in OLSR. The basic idea behind the OLSR is to decrease the overhead of the data exchange which is done by MPR as shown in Figure 2. To decrease the number of hosts which multicast the data into the network we use MPR. Nodes other than MPR don't multicast the data through route packages in the network. In the network all the neighbors receive the message when source node broadcast it. Then the MPR which do not have the entry of that message in the routing table again broadcast the message. By this decrease in flooding overhead is done [6]. OLSR is valuable for a traffic pattern when a one large subgroup of nodes communicates with other large subgroup of nodes. OLSR routing protocol is needed to get more efficiency, reliability and less throughput and cost. There are three categories of OLSR control messages:

- HELLO messages
- Topology Control (TC) messages
- Multiple Interface (MID) messages.

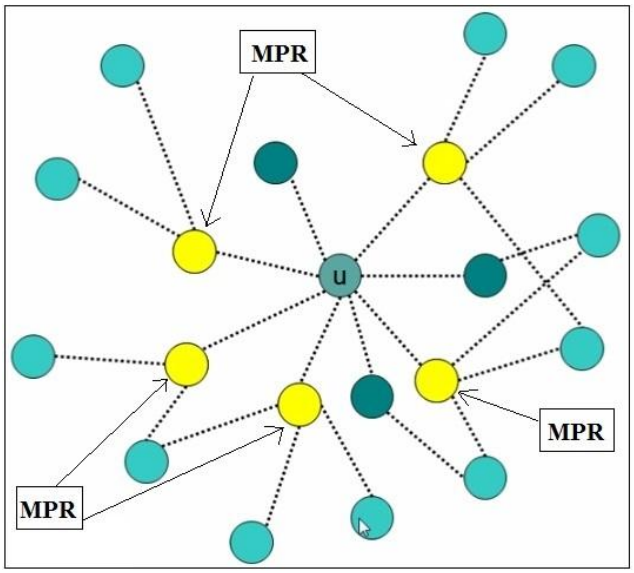


Figure 2: OLSR Protocol Scenario

a) Multi Point Relay (MPR)

MPR is responsible for transmission of messages during flooding and generating link state information. This technique in OLSR protocol will minimize the message overhead and also minimize the number of control messages propagate into the network [1]. With the help of MPRs the problem of congestion is solved in the OLSR because only MPR nodes broadcast the control packet [15]. The Multipoint Relays vertex can be chosen as a neighbor of origin vertex. Every node into the network has a record of nodes selected as MPR. The selection of MPR is acquired by sending HELLO messages among the neighbor vertices. When any of the origin vertex is going to transmit a message to a specific destination vertex, all the routes to other nodes are built prior from any origin vertex. All the nodes into the network maintain a table of routing. That's why the routing overhead for OLSR is less in comparison to other reactive routing protocols and OLSR offers the shortest route from source to destination into the network. As the current route is used so no need of discovering the fresh routes, which minimizes the delay in route discovery.

b) Neighbor Discovery

OLSR requires some method to identify the neighbors and the communication lines state with them. The neighbor discovery session is using HELLO messages, nodes into the network send HELLO messages to their neighbor nodes. These messages are transmitted at a prearranged period to establish the status of link in OLSR.

c) Neighbor Detection

Neighbor discovery occupies the 1– hop neighbor source and uses only the main address of nodes. As we have discussed early, the neighbor records are closely linked to the link records. Every time a link entry is generated, for a corresponding neighbor record neighbor table is enquired. Note that this neighbor record must be recorded on the node's main address. If there is no record, then we create a new record of neighbor. This mean that a vertex can have numerous record defining various links to the similar neighbor, for each neighbor only one record exists. The value of the neighbor records is also updated whenever any changes had been done to the link set. A neighbor is assumed

to be a symmetric neighbor if at least one set of link is present in the link set linking one of the interfaces to the local interface where symmetric timer is not out of time. When an entry of record is deleted, then it also erases the corresponding neighbor record.

d) Detection of MPR Selector

The mechanism of flooding the MPR rely on the need that nodes have listed to the neighbor who chooses them as a MPR. The nominated MPR neighbors are marked by nodes with HELLO messages by setting the MPR_NEIGHBOUR as a neighbor type. While getting a HELLO messages, a vertex checks the declared neighbors in the messages for entry, which matches with one of the local node address. For instance, if a record has a similar address and the record of that neighbor type is set to MPR_NEIGHBOUR then record is updated or generated in the MPR selected set with the help of HELLO senders main address.

4. Sybil Attack in vanet

It comprises of sending various messages from one hub with different characters. Sybil assault is constantly conceivable aside from the compelling conditions and suppositions of the likelihood of asset equality and coordination among substances. At the point when any hub makes different duplicates of itself then it makes disarray in the system. Guarantee all the illicit and fake ID's and Authority. It can make crash in the system. This kind of circumstance is known as Sybil assault in the system. This framework can assault both inside and remotely in which outer assaults can be confined by confirmation however not inner assaults. As there is balanced mapping amongst character and element in the system.

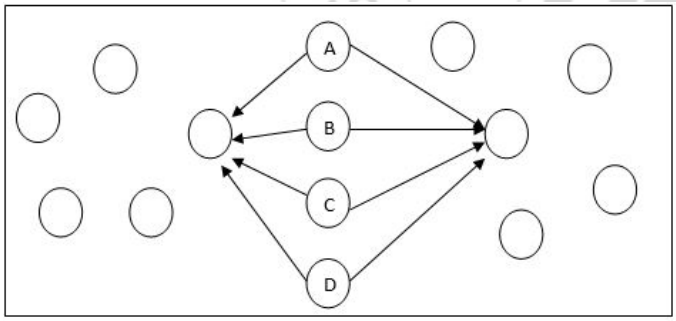
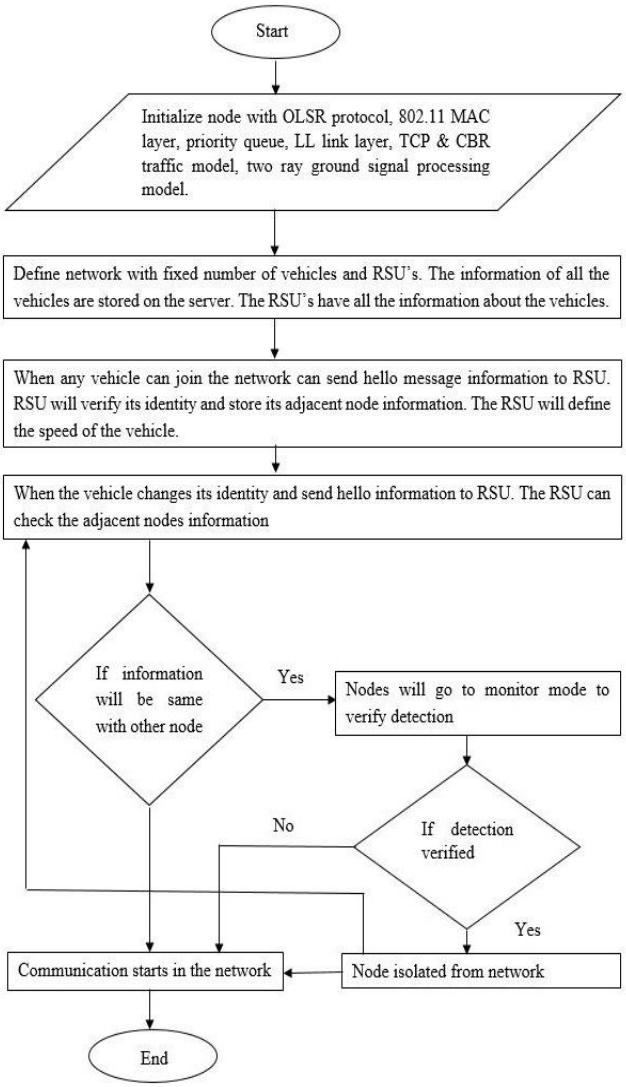


Figure 3: Sybil Attack

In Figure 3 A, B, C, D nodes are Sybil nodes which create fake or similar identity in the network and collapse the network**.**

5. Proposed Methodology

The vehicular improvised system is the self-designing system in which the vehicles can join or leave the system when they need, and no focal controller is available in VANET. Because of decentralized sort of system a great part of the security issues brought up in the system. The malignant hub can join the system and it might trigger Sybil assault in the system. In this work, calculation will be proposed which confine Sybil assault in the system. A calculation will be proposed which detach Sybil assault in the system. Flow Chart shows the proper flow of steps to be done in order to fulfill the requirements and achieve the target.



Flow Chart: Methodology Flow Chart

6. Algorithm

Input: Road side units, smart cars, malicious car

Output: Detection of Malicious car

1. Set registration process
2. Car send its credentials to road side units
3. **If** (stored credentials == send credentials)
4. Assign identification number;
5. **Else**
6. Repeat step of registration
7. **End if**
8. **If** (Identification== assigned)
9. Communication starts between cars
10. Road side units start gathering information about neighbors
11. **If** (Neighbor information on each road side units == same)
12. No malicious node exits in the network;
13. **Else**
14. Road side units flood ICMP messages in the network
15. Monitoring process= true
16. **End if**

17. **End if**
18. **If** (malicious car== detected)
19. Isolate malicious car with identification number
20. **Else**
21. Repeat process of monitoring
22. **End if**

7. Experimental Results

The whole scenario has been experimented in NS2. There are reproductions of TCP and UDP, some of MAC layer conventions, different steering and multicast conventions over both wired and remote system and so forth. What's more, the after effects of examination of both the systems utilizing different parameters are given in TABLE 2.

Table 2: Simulation Parameters

Network Simulator	NS-2 Version 2.35
Window Size	800 X 800
Number of Mobile Nodes	36
Signal Processing Model	Two Ray Ground
Transmission Range	18m
MAC Layer	802.11
Link Bandwidth	2.4 GHz
Routing Protocol	OLSR
Traffic Model	TCP, CBR
Maximum Node Speed	200 m/s

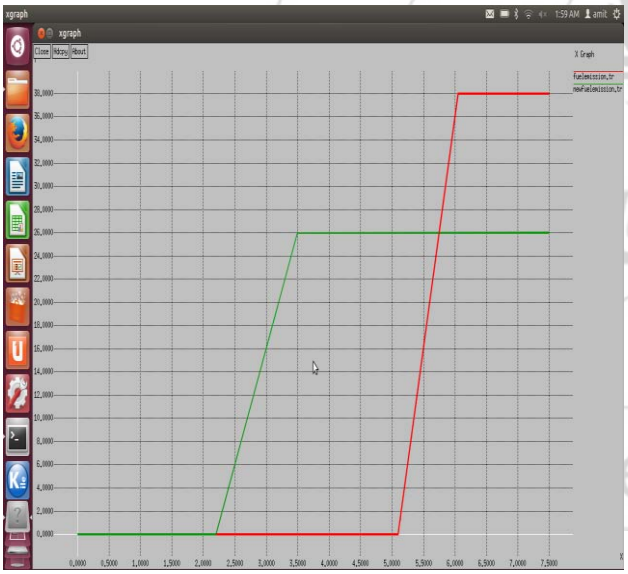


Figure 4: Fuel Emmision

As shown in Figure 4, 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 38. In the proposed scenario as Sybil attack is detected and isolated due to which fuel emission is reduced to 26.

Figure 5: Packet Loss

As shown in Figure 5, packet loss graph is shown in which packet loss in existing and proposed scenario is shown and it is analyzed 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 5 packets and in proposed scenario it is 4 packets.

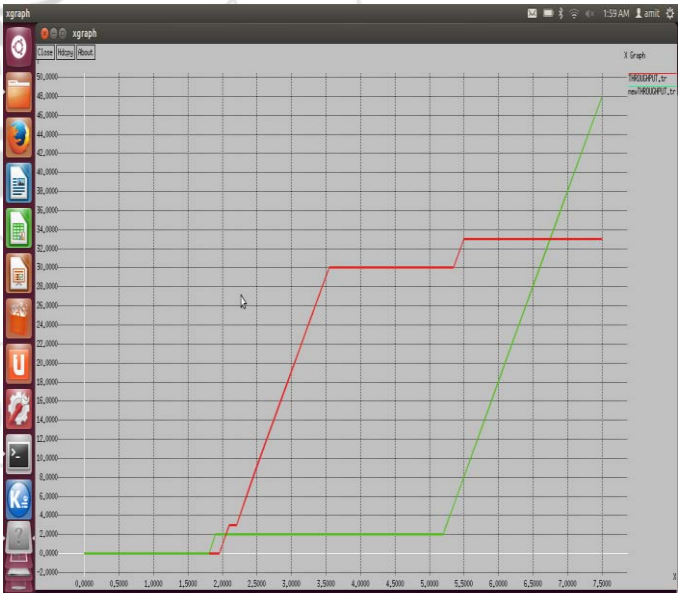


Figure 6: Throughput

As shown in figure 6, throughput graph of proposed and existing schemes is shown with red and green line. Due to isolation of Sybil attack from the network throughput is increased to 48 packets and due to Sybil attack in the network throughput will be 33 packets.

8. Conclusion

In VANET numerous attacks has been trigger by the pernicious hub. In this manner keeping in perspective above difficulties there is a need to enhance the effectiveness of OLSR convention with the goal that it might have the

capacity to control both, the components which make remote correspondence inconsistent furthermore bolster the above application difficulties to an expansive degree. Every one of the issues examined in this paper can be raised on the off chance that a portion of the wrong data can be flooding in the system. The wrong data can be flooding in the system by malignant vehicles. These malevolent vehicles can debase the system execution by setting off some security assault. In this work, a novel procedure has been proposed to identify vindictive vehicles and disengage Sybil assault from the system. This will enhance system execution.

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.

[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.

[13] 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.

[14] Al-Ani, M. R. (february, 2011). Simulation and Performance Analysis Evaluation for Varient MANET Routing Protocols. International journal of advancement and computing Technology, 2011.

[15] 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.

[16] 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.

[17] Evjola Spaho, Makoto Ikeda, Leonard Barolli, Fatos Xhafa, Vladi Kolici and Makoto Takizawa, "Performance Evaluation of OLSR Protocol in a Grid Manhattan VANET Scenario for Different Applications", Seventh International Conference on

[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.

Complex, Intelligent, and Software Intensive Systems 2013.

[18] Bo Yua, Cheng-Zhong Xua, Bin Xiao, "Detecting Sybil attacks in VANETs", J. Parallel Distrib. Comput. 73 (2013) 746–756 2013.

[19] Manpreet kaur, K. (2013, February). Optimize OLSR with cognitive in Wireless mesh Network. International journal of Engineering and Advanced Technology.