I J C T A, 9(11) 2016, pp. 5335-5342

A STUDY ON DETECTING AND AVOIDING SYBIL ATTACK IN OLSR PROTOCOL

Amit Kumar[*] and Varun Singla[**]

Abstract: VANET is a subset of MANET which provides a different approach for telematics. It is the recently developed technology to achieve traffic safety and efficiency where various routing protocol and security measurement plays an important role. As many previous works had shown, 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 paper 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.

Key Words: Optimized Linked State Routing (OLSR); Road Side Unit (RSU); Multi Point Relay (MPR); Internet Service Provider (ISP); Revised Signal Strength Indication (RSSI); Wireless Sensor Networks (WSN).

1. INTRODUCTION

VANETs present a rapidly emerging, challenging class of MANETs. VANET is characterized by a very high node mobility and limited degree of freedom in the mobility pattern. Hence, Ad-hoc protocol adapt continuously to the unreliable conditions, whence growing effort in the development of communication protocols which are specific to vehicular networks [1]. VANETs are conducted with moving vehicles and roadside infrastructure because of high mobility and continuous topological changes happen. VANETS is a self-directed and self composable wireless communication network, where vertices include themselves either as client or server for communication [8]. Author explained packet drop ratio increases due to low success ratio at destination side [21]. VANETs are expected to support a large ordered array of components of nomadic distributed application that range from alert dissemination of traffic and distribution of files [22].

[*] Pursuing M.Tech School of Computer Science and Engineering, Lovely Professional University, Phagwara (Punjab), India, Email: amitkumar.171292@gmail.com

[**] Assistant Professor School of Computer Science and Engineering, Lovely Professional University, Phagwara (Punjab), India, Email: varun.17705@lpu.co.in

Table 1
Layered View Of Vehicular Networks

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

Based on unique characteristics, the vehicular communication has been categorized into two parts:

1. Vehicle to Vehicle communication (V2V)
2. Vehicle to Infrastructure communication (V2I) [8].

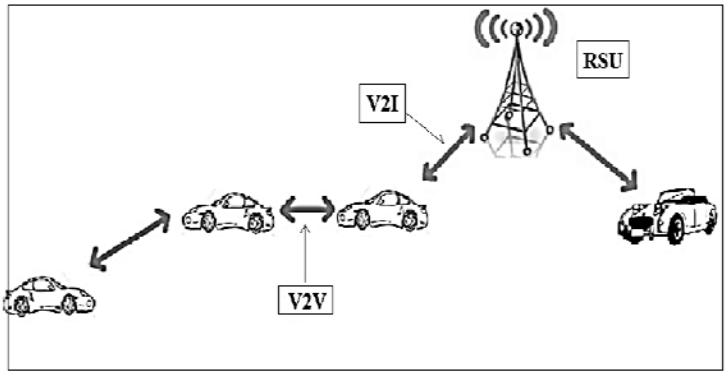


Figure 1 Vehicular Communication

In the above described diagram when the vehicles are communicating with the road side unit (RSU) or transmitting the messages with the side infrastructure then this process is known as V2I. On the other hand when vehicles are transmitting data with each other are known as V2V. This V2V communication requires some special hardware in the cars like actuator.

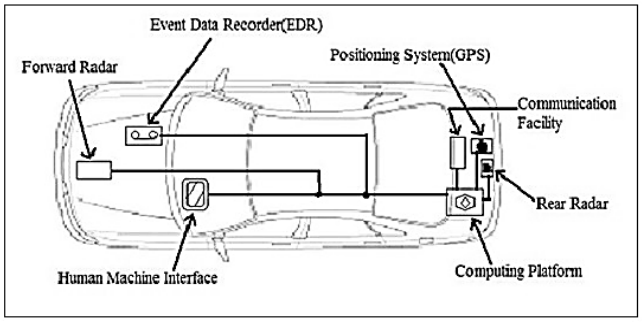


Figure 2 Modern Vehicle Network Of Actuators On Wheels

In this paper, we have discussed about the LAR protocol, its shortcomings and proposed a novel technique to overcome the problem of Broadcasting in LAR protocol. After that we compare the novel technique with the existing LAR protocol graphically and observe the throughput of the network and delay in transmitting a message.

The rest of the paper follows the process like this. In section II we describe LAR protocol. In Section III literature survey is reviewed. In section IV Problem Formulation is being defined. In section V Research methodology is being defined and in section VI Conclusion is presented followed by the references in section VII.

Challenges

It is vital to specify the important challenges in VANET:

- **Signal fading and distortions**: Objects like other vehicles or buildings act as obstacles between two communicating vehicles which is one of the challenge that can affect the efficiency of VANET.
- **Bandwidth limitations**: Absence of a central coordinator that controls the communications between nodes, and which has the responsibility of managing the bandwidth and contention operation.
- **Connectivity**: Owing to the high mobility and rapid changes of topology, which lead to a frequent fragmentation in networks, the time duration required to elongate the life of the link communication should be as long as possible.
- **Small effective diameter**: Owing to the small effective network diameter of a VANET, that leads to a weak connectivity in the communication between nodes.
- **Routing protocol**: Because of the high mobility of nodes and rapid changes of topology, designing an efficient routing protocol that can deliver a packet in a minimum period of time with few dropped packets is considered to be a critical challenge in VANET.

2. OLSR (OPTIMIZED LINK STATE ROUTING) PROTOCOL

OLSR protocol is a table driven protocol which come under proactive routing protocol. It store the routing table permanently and update it periodically, so the route are available when needed [9]. In OLSR when the topology changes it creates the situation of overflowing of the topology data to every active vertices 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. 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 communicate 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:

1. HELLO messages
2. Topology Control (TC) messages
3. Multiple Interface (MID) messages.

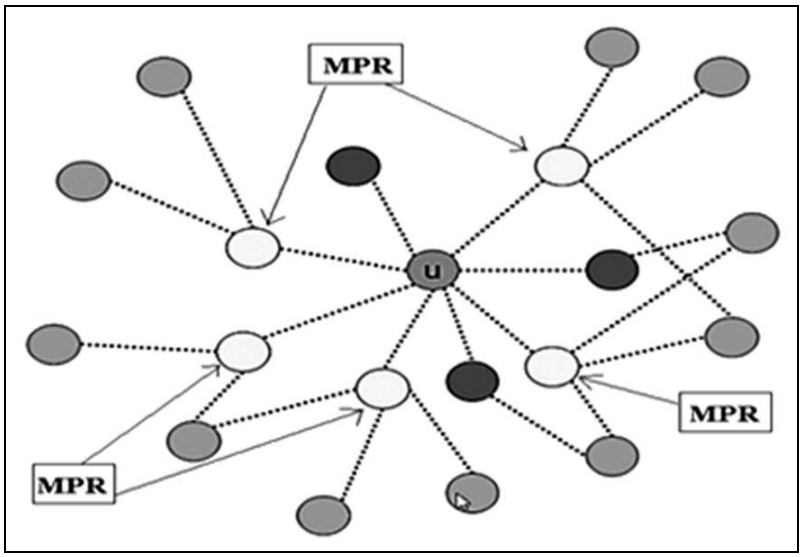


Figure 3 OLSR Protocol Scenario

2.1 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 maintains 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.

2.2 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.

2.3 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, than 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 exist. 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 erase the corresponding neighbor record.

2.4 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.

3. SYBIL ATTACK IN VANET

It comprises of transmitting multiple messages from one vertex with numerous identities. Sybil attack is always feasible except the dangerous conditions and hypothesis of the possibility of source parity and synchronization among entities. A node creates the confusion in the network by creating many copies of itself and take the responsibility of all the authorities that the fake and illegal ID's have. Due to which a confusion is created in the network. This whole scenario of confusion can be termed as network under Sybil attack. By this system attack can happen in both the ways i.e. externally and internally. External attacks can be limited by the process of authentication but we cannot control the internal attacks. As between the entity and the identity of the node there is one to one mapping in the network.

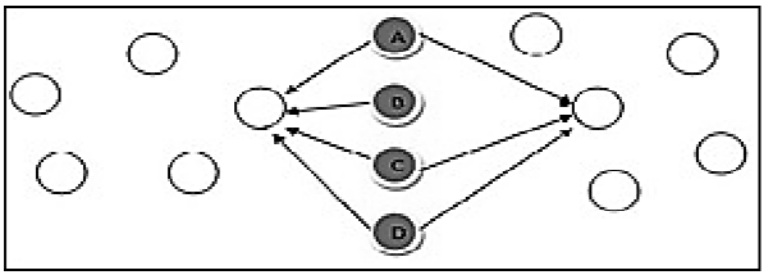


Figure 4: Sybil Attack

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

4. LITERATURE SURVEY

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

4.1 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 [7].

4.2 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 [8].

4.3 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) [10].

4.4 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 [11].

4.5 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 [12].

4.6 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 [13].

4.7 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

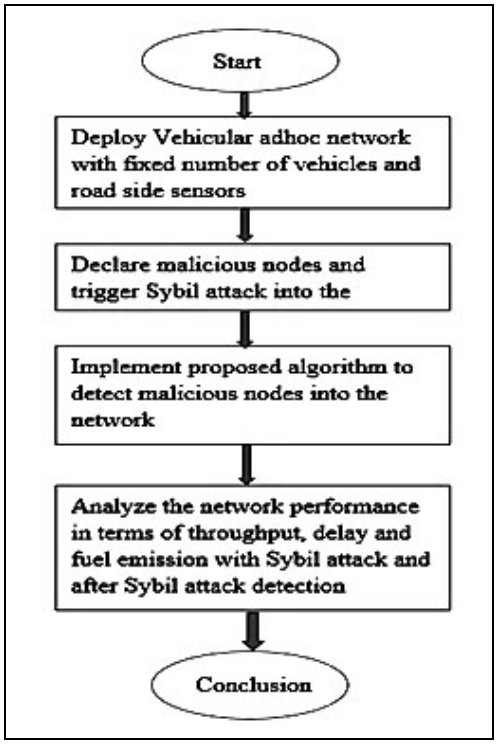
analysis across an observation period. Ultimately, based on realistic US traffic style and maps, they carry a feigning to check the quality of being doable and efficiency [14].

5. PROBLEM FORMULATION

The Vehicular systems employ wireless ad-hoc Networks and GPS to determine and maintain the inter-vehicular separation necessary to ensure the one hop and multi hop communications needed to maintain spacing between vehicles. The VANET is the self-configuring type of network, in which the vehicles can move freely in the network. In such type of network, there are more chances that mischievous vehicles can join the network and trigger some type of attack. All the problems are raised if some of the wrong information can be flooding in the network by malicious vehicles. These mischievous vehicles can reduce the network performance by activating some security attack. Among the possible attacks Sybil attack is the most harmful attack which is possible in the network. This attack will reduce the network performance. In this work, I will detect malicious vehicles in the network which is responsible to trigger such type of attacks.

6. RESEARCH METHODOLOGY

In self-configuring vehicular Ad-hoc network vehicles can connect to the network or can leave the network when they need, and no central controller is present in VANET. Due to decentralized type of network much of the security issues raised into the network. The mischievous node can connect to the network and it can activate Sybil attack into the network. In this work, algorithm will be proposed which isolate Sybil attack in the network.



Flow Chart 1 Basic Scenario

7. CONCLUSION

As explained earlier, the VANET is the self-configuring type of network, in which the vehicles can move freely in the network. In such type of network, there are more chances that mischievous

vehicles can join the network and trigger some type of attack. All the problems are raised if some of the wrong information can be flooding in the network by malicious vehicles. These mischievous vehicles can reduce the network performance by activating some security attack. Among the possible attacks Sybil attack is the most harmful attack which is possible in the network. This attack will reduce the network performance. The Sybil attack reduce OLSR protocol performance in terms of delay and throughput. In this work, improvement will be proposed in OLSR protocol which will detect and isolate malicious nodes which leads to reduce in network delay and increase network throughput.

References

[1] Huhtonen, A. (2004). Comparing AODV and OLSR protocol. Helsinki University of Technology Telecommunication Software and Multimedia Laboratory.

[2] Tonnesen, A. (2004, August). Implementation and extending the Link State Routing Protocol. Oslo. 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.

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

[4] 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.

[5] Ravikumar, Y. (2010, June). Acase study on MANET Routing Protocols Performance over TCP and HTTP. Master Thesis Electrical Engineering.

[6] 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.

[7] 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.

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

[9] Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty, "P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks", IEEE Journal On Selected Areas in Communications, Vol. 29, No. 3, pp. 582 – 594,2011.

[10] 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.

[11] 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.

[12] 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 Complex, Intelligent, and Software Intensive Systems 2013.

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

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

[15] Ganan, C., Munoz, J. L., Esparza, O., Mata-Diaz, J., & Alins, J." PPREM: privacy preserving revocation mechanism for vehicular ad hoc networks", Computer Standards & Interfaces, 36(3), pp-513-523, 2014.

[16] 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.

[17] N.D.M. Nuri and H. Hasbullah, "Strategy for efficient routing in VANET", 2010 International Symposium in Information Technology (ITSim), Kuala Lampur, pp. 903-908, June 2010.

[18] S. Dashtinezhad, T. Nadeem, B. Dorohonceanu, C. Borcea, P. Kang, and L. Iftode, "Traffic view: A driver assistant device for traffic monitoring based on car-to-car Communication", in Proc. 59th IEEE Semiannual Veh. Technol. Conf., Milan, Italy, May 2004, pp. 2946-2950.