Modeling Sybil Attacker Behavior in VANETs

Parastoo Kafil
Department of Computer Engineering,
University of Science and Technology,
Tehran, Iran.
Parastookafil@yahoo.com

Mahmoud Fathy
Department of Computer Engineering,
University of Science and Technology,
Tehran, Iran.
mahfathy@iust.ac.ir

Mina Zolfy Lighvan
Department of computer Engineering
Faculty
University of Tabriz
mzolfy@tabrizu.ac.ir

Abstract— **Vehicular Ad-Hoc Networks (VANET) is mainly designed to provide human safety, traffic management, and infotainment services. The decision how to react on information received from other vehicles always has to be made locally. This made attackers to abuse the information and it will endanger the security of the system and human lives. In VANETs Sybil attack is an identity forging attack that a malicious node impersonates several other nodes in order to disrupt the proper functioning of VANET applications.**

In this paper we discuss and motivate the needs for real traffic simulation with standard network simulation and explain the attack models for an individual Sybil attacker .We consider that the attack model can be changed in each traffic scenario and sophisticated movement path such as urban traffic model having a potentially high influence compared to uniform highway traffic model. Also we simulate and compare attacker models in two positions: near the source and near the destination of data packet sending. The risk analysis shows that the most serious threat arises from a Sybil attacker that distributed forged warning messages near the source of packet sending because of the number of hops between nodes.

Keywords-component; VANETs; sybil; defense; prevent;traffic model

I. INTRODUCTION

Vehicular Ad-Hoc Networks (VANET) is an important component of Intelligent Transportation Systems and used for communication and cooperative driving between cars on the road. VANETs have particular features like: distributed processing and organized networking, a great number of nodes, the distribution and the speed of these nodes, a constrained but highly variable network topology, communication conditions and mobility patterns, signal transmissions blocked by buildings, frequent partition due to the high mobility, and finally there are no significant power constraints [1]. Vehicle can exchange emergency events, traffic events, weather conditions, road data among other vehicles and road side units, as well as delivering advertisements and announcements.

Vehicles are capable of forming ad-hoc networks with no prior knowledge of each other, whose security level is very low and can be attacked easily. Security, however, has always been an issue in vehicular ad-hoc networks which must be seriously considered and a security infrastructure has to be designed and implemented.

In this paper, we focus on Sybil attack where a malicious attacker assumes multiple identities while a normal participant is allowed only one identity by making a large number of fake identities or by stealing from real nodes in the network. Several solutions have been proposed to secure VANETs against Sybil attack [10],[3],[19],[18],[7]. What is missing so far is an in-depth discussion and analysis of attacker and the modeling of attacker behavior in each real traffic model. We analyze various positions of Sybil attack to help to improve the proposed security solutions.

The early stage of development of VANETs does not allow for a significant attack analysis. Modeling all possible Sybil attacker behaviors and Sybil attacks, would be impossible. We reduce the options by specifying a real traffic model of a VANET first. Based on this model, we conduct a risk analysis of each traffic model, possible attack models, vulnerabilities and situations leading to a quantification of the respective risks.

Sybil attacker can create an illusion and it has the potential to inject false information into the networks via a number of fabricated non-existing identities; it can even launch further DoS attacks by impairing the normal operations of data dissemination protocols. For example, in the application of deceleration warning systems, if a vehicle reduces its speed significantly, it will broadcast a warning to the following vehicles. Recipients will relay the message to vehicles further behind. However, this forwarding process can be intervened by a large number of malicious Sybil vehicles. In this way, the malicious adversary can create a massive pileup on the highway, potentially causing great loss of life [2].

We take a detailed look on the position-based attacks and best situations for Sybil attackers that pose high risk to the system based on real mobility information on VANETs. The outcome of this evaluation is that position information is a crucial and endangered subpart of the system. Therefore, we focus on modeling attacks on position information and elaborate on potential attack implementations used by Sybil attackers. Finally, we discuss effort and impact of these concrete attacks serving as a knowledge basis for security system designers. Furthermore, we propose a solution based on

path similarity and evaluate system performance with VANET requirements.

The remainder of the paper is as follows. In Section II we classify Sybil attack. In Section III, we define our attack model in three traffic models designed for VANET. After defining our basic system assumptions, we examine the security issues of the system by an in-detail risk analysis in Section IV and explain Sybil attacker models; Followed by the attack analysis in Section V. We simulate our model and there, we discuss and motivate for a consideration of the most imminent risk of a Sybil attacker and in VI. We have our simulation results which are modelled and evaluated. The results of the risk analysis as well as the attacker model are then summarized in Section VII. as conclusion.

II. SYBIL ATTACK CLASSIFICATION AND RELATED WORKS

The Sybil attack was first defined and described by Douceur in [3]. It consists in sending multiple messages from one node with multiple identities while a normal node is allowed only one identity. Applications of the Sybil attack to VANETs have been discussed in [4], [5] and show the importance of Sybil nodes detection in VANET. Based on [3] an important result is that without a logically centralized authority, Sybil attacks are always possible (i.e. may remain undetected) except under extreme and unrealistic assumption of resource parity and coordination among entities [6].

Ad hoc routing protocols are used to find a path through the cooperative network. Each node needs a unique address to participate in the routing. Often addresses are assigned as an IP addresses or MAC address. Because all communications are conducted over the broadcast channel, nothing but these identities is available to determine what nodes are present in the network. In unsecured routing protocols, such as DSR or AODV, these address-based identifiers can be easily falsified by malicious nodes, which present an opportunity for a Sybil attack. However, allowing unauthenticated address presents [7].

Sybil attacks can be classified into three categories based on type of communication, identity and their participation in the network .These categories are briefly discussed below [8]:

a) *Communication Category:* When an honest node sends a radio message to Sybil node, one of the malicious nodes listens to the message. In the same way, messages sent from Sybil nodes are actually sent from one of the malicious devices. Communication to/from Sybil nodes can be direct or indirect.
In direct mode, all Sybil nodes created by malicious node communicate with legitimate nodes. In indirect communication, legitimate nodes reach the Sybil nodes through a malicious node.

b) *Identity Category:* In a Sybil attack, an attacker creates a new Sybil identity. This identity can be a random 32 bit integer (fabricated identity) or attacker can spoof the legitimate identity of one of its neighbours (stolen identity).

c) *Participation Category:* Multiple Sybil identities created by malicious nodes can simultaneously participate in an attack or the attacker can present these Sybil identities one by one. A particular identity may leave or join the network many times, i.e., one identity is used at a time. The number of identities used by the attacker is equal to or less than the number of physical identities. An attack through multiple Sybil nodes can adversely affect proper functioning of network.

In addition, some papers categorized Sybil attack in spoofing attacks and some in identity stealing attacks [8], [9]. We categorize Sybil attack as an impersonating attack as below:

- **Sybil attack with identity stealing:** where a malicious node pretends to be an honest node by stealing the identities of other nodes and hence, all the messages directed to that victimized node are received by the attacker.
- **Sybil attacks with identity generating**: where a malicious vehicle generates fabricated non-existing vehicle identities belong to real network by knowing network identity generating algorithms.

Sometimes identity stealing is easier than generating new identities and some networks using self-generated algorithms [10] to make new identities to prevent against identity stolen attacks and make it harder to be stolen by an attacker. However, in both models the vehicle that spoofs identities of other vehicles or the vehicle that making new identities as real nodes in the network, is called Sybil attacker and the vehicles whose identities get spoofed or generated by Sybil attacker are called Sybil vehicles which are the images of real vehicles.

A typical Sybil attack is shown in Fig. 1.

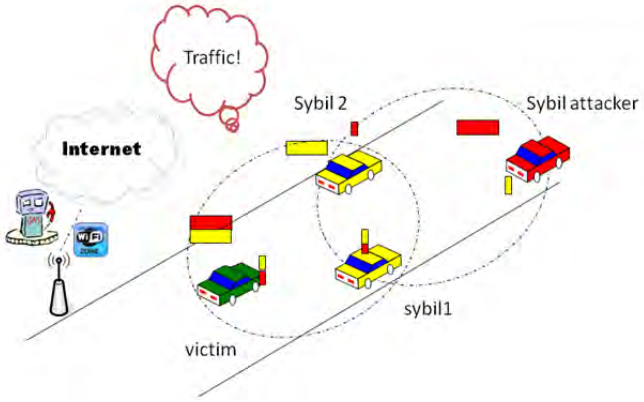

Figure 1. Sybil attacker is sending fake traffic messages with illusions (sybil1 and Sybil2) and the victim thinks messages are come from more than one vehicle.

The first victim vehicle is observing the accident warning message from a participant vehicle, may doesn't care, because the message is from a participant vehicle (e.g., When a network security strategy is based on vehicles votes to report an emergency event), but when a number of vehicles report an emergency event, the first victim will send a warning message

to all other vehicles. Receivers may forward this message to warn the others. This may put the life of passengers in danger. These face identities are Sybil attacker's illusions. If number of Sybil attackers increases significantly in a network, they can take over the control of the whole network. Number of Sybil vehicles created by a Sybil attacker depends on the communication, storage and computation resources of the attacker and could be from 1 up to the number of vehicles in the network.

A description about Sybil attacker capabilities in vehicular ad-hoc networks has been in [8]. They detailed network problems after a Sybil attack with 1, 5 and 10 attackers. There is no explanation about the number of identities each attacker can take and there is no information about Sybil attacker independency where they are working together or not. However, previous work did not specifically discuss attacker capabilities with respect to position forging. For the development of real attack an understanding of potential countermeasures is needed. Thus, in this paper we summarize our security approaches detecting Sybil attacker or at least implement attack model with real traffic information VANETs.

III. TRAFFIC MODELS

One key component of VANET simulations is the movement pattern of vehicles, also called the mobility model [11]. Mobility models determine the location of nodes in the topology at any given instant, which strongly affects network connectivity and throughput. The current mobility models used in popular wireless simulators such as NS-2 tend to ignore real-world constraints such as street layouts and traffic signs. Consequently, the simulation results are unlikely to reflect the protocol performance in the real world. Some researchers have become interested in 'realistic' mobility patterns for VANETs. In [11], [12] an urban model based on the Stop Sign Model (SSM), the Probabilistic Traffic Sign Model (PTSM), and the Traffic Light Model (TLM) was introduced.

We use our traffic model based on their models and we combine those models with our assumption to have a better result in our attack modeling and to have real results with real data in VANET. These models are evaluated over various parameters such as topology (real maps and controlled grids), vehicular speed, and the wait time at intersections. These models are based on Real Street maps extracted from the US censor bureau TIGER database [13].

For better results in modeling Sybil attack, we introduce three traffic models as below:

a) ***Highway model:*** Roads are modeled as one-directional roads with three lanes in each road. Vehicles start a rather uniform motion in a highway and we assume their motion to a fix target. There are pay tools in some stations and vehicles have to stop in each pay tool. We use the Stop Sign Model (SSM) in [11]. When vehicles reach to pay tools, each vehicle waits for 3 seconds on pay tools and there is no auxiliary road and path is the same for all vehicles.

b) ***Unifirm model:*** This model is an urban model which uses Traffic Light Model (TLM) in [11], also vehicles have a rather uniform motion and streets are modeled as one-directional streets and assume three lanes in each street. There are traffic lights in some streets and each vehicle has to stop for 30 seconds on the stop lights. The initial vehicle positions and their destinations are chosen uniform but their start time is set randomly. Vehicles start to move across the streets and when they see stop lights, they gather and wait to light turns to green. This model is for rather quite streets with single direction, where there are traffic lights to stop. Some of vehicles in this scenario can change their direction to an auxiliary road; therefore path is not the same for all vehicles.

c) ***Urban model:*** This is a real urban traffic model when there are crowded streets with a number of vehicles turn random locations. Under TLM, traffic lights at each intersection are coordinated. We assume bidirectional streets with three speed lines and the intersection at the end of each street and with traffic lights. The lights turn green in such a manner that only traffic along a single pair of opposing sides cross the intersection simultaneously. The initial vehicle positions and their destinations are chosen randomly. Vehicles that need to turn left or right follow the free turn rule once they reach the head of the queue. While the traffic across one pair of opposing roads has the green signal, the remaining have red signal. After fixed period, green signals are rotated to another pair of roads with opposing traffic. Vehicles have completely random motions and there is no prediction about vehicle's direction.

IV. SYBIL ATTACKER MODELS

One of the major applications of VANET is to provide safety to drivers by minimizing the number of road accidents through broadcasting safety messages. Safety messages do not require any expensive encryption/decryption operations. In VANET, whenever a node receives a warning or a safety message, it tries to forward it to other nodes by broadcasting it. Generally, no routing protocol is followed for sending safety/warning messages in VANET unless there is a specific requirement for applications such as internet access, or specific type of service requests [8].

When it comes to naming Sybil attackers in our scenario, based on positions they take, four types of Sybil attackers are mentioned:

- *Sybil attacker near source*: when a Sybil attacker is near source of packet sending.
- *Sybil attacker near destination:* when a Sybil attacker is near destination of packet receiving.
- *Sybil attacker out of rout and near source:* when a Sybil attacker is out of routing in the network but near source.
- *Sybil attacker out of rout and near destination:* when a Sybil attacker is out of routing in the network but near destination.

Our simulation results show that a Sybil attacker can have different purposes by attacking in each traffic position or particular location. It means Sybil attacker in some traffic

scenarios, can cause an attack with high risk to the system more than the other positions. Attack models will change in each traffic model and also in each location of a Sybil attacker takes in the network.

V. SYBIL ATTACK SIMULATION IN VANET

In this section, in order to evaluate the behavior of a Sybil attacker and the performance of Vehicular ad hoc network after this attack, we describe various parameters and requirements for simulating Sybil attack. Our work is based on real traffic, explained before. We conducted our experiments using NS-2 version 2.34. An important factor for VANET simulations is a realistic vehicular mobility model that ensures conclusions extracted from simulation results will carry through to real deployments. Therefore we use MOVE to generate realistic mobility models for VANET simulations. MOVE is built on top of an open source micro-traffic simulator SUMO. The output of MOVE is a realistic mobility model and can be immediately used by NS-2 [15]. In our simulation experiments, we used 1 Sybil attackers with four fake identities respectively in the chosen Vehicular Network of 10, 20, 40 nodes. The simulation parameters used, are listed in Table 1.

TABLE I. SIMULATION PARAMETERS

Simulation Parameters	Value
Channel	WirelessChannel
Propagation	TwoRayGround
Netif	Phy/WirelessPhyExt
Mac	Mac/802 11
Queue type	DropTail/PriQueue
Ll	LL
Antenna	Omni Antenna
Queue size	50
Number of total vehicles	40
Vehicle Speed (m/s)	Max 40 m/s
Routing protocol	AODV
Traffic type	CBR
Transmitter/Receiver antenna height	1.5 meters
Simulation area	1400 × 1400m grid, real map
Transmission range	250 m
Street length	1000-2000 m
Accel./Decel. Rate	3 meters/sec2 for TLM

The simulation parameters

The next requirements we added to our simulation are the speed, acceleration and deceleration of vehicles. In many related work there were no acceleration and deceleration change features and the speed of the vehicles was rather uniform. In our feature, vehicles do not change their state to peak speeds instantaneously. They start to accelerate gently from rest up to the maximum possible speed. Similarly, when approaching a stop sign or red light, they decelerate gently to a stop.

The mobility pattern of nodes in a VANET influences the route discovery, maintenance, reconstruction, consistency and caching mechanisms. Static or slow-moving nodes tend to dampen the changes in topology and routing by acting as stable relaying points for packets to/from the neighboring nodes. On the other hand, highly mobile nodes add entropy to the system and cause frequent route churn and packet losses [11].

Our technique attempts to capture how all the identities owned by the same attacking vehicle have to travel together when the vehicle moves. Simulation results show that the highway model which vehicles have a rather uniform motion is better scenario for a Sybil attacker; because behaviors of vehicles are predictable. Also this is happened when vehicles are stopped behind traffic lights in the urban model or the uniform model. We believe that it is better for a Sybil attacker to chaste his victims based on his strategy and finally attacks them.

Sybil attacker is encouraged to use its identity regularly to gain good services in the network. Even if the attacker assumes a large number of identities, each identity has to be used frequently to gain enough reputation to receive good services in the network. If its behavior declines with not using his identities frequently, it results in poor service from the network; therefore, not a successful attack. This will make them easy to detect.

VI. PERFORMANCE EVALUATION

Our simulation results extracted from NS2 which has been widely accepted as a reliable simulation tool for computer communication networks both in academia and industry. We do not propose a method for defense against Sybil attacker and assumed that the area of interest was covered by a set of beacons which a participating node could determine its location over real mobility for VANET. We assumed the presence of a Sybil attacker which possesses 4 identities. Each Sybil opened a randomly-chosen number of connections to the target, with the average of 2 connections per Sybil. We varied the number of honest nodes between 39, which opened a CBR at 20Kbps to the target.

VII. SIMULATION RESULTS

We use AODV [15] mobile ad hoc routing protocol. Each honest vehicle observed AODV requests and the CBR. Sybil attacker randomly uses the identities and positions of other vehicles in the network and may cause harm to the network by fabricating fake messages, or sending his messages instead of real messages. In our work, when a Sybil attacker wants to send a packet, instead of using real identity and position, it selects a random vehicle identity and position and applies it to the packet. Although, the Sybil attacker drops all received packets and do not forward any packets. Simplified, respective Sybil packet comprises the five fields as shown in Figure 1. It shows that Sybil attacker as a packet sender, sends his identity (stolen or fake) and there are number of hops between sender and receiver. As a forwarder, Sybil attacker drops sender's packet and sends his packet to the next hop by fake positions and fake or stolen identities.

Sybil ID as source ID	Sybil position	Hop count	Destination ID	Sybil Seq #

Figure 2. Sybil attacker as source (Sybil attacker do not forward any packets, he drops them and sends his packets instead.)

Sybil attacker has to show his identity frequently, so he has to show different positions to pretend they are real, if the network uses location finder algorithms, it is hard to use his position each time he sends packet, so it makes him easy to find.

Vehicles move together and they share routing packets and all warning and safety messages. Our performance feature is evaluated in the number of packets lost per second.

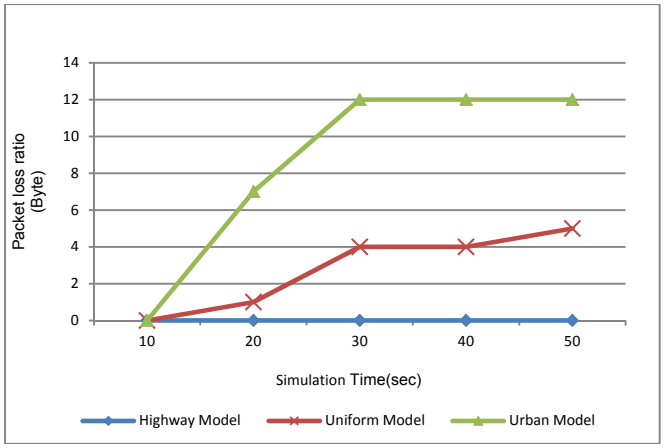

Figure 3. Three traffic models when there is no Sybil attack in the network.

In Fig. 3 we have our VANET with three traffic models but no Sybil attacker. The packet loss shown in this figure is because of each traffic model problems. Based on our simulation, urban model has the most packet loss among the other models.

Fig. 4 shows highway model and the packet loss ration vs. time. Based on our simulation results, Sybil attack in this model is with high packet loss ratio. In comparison with figure 3, Sybil attack in uniform model and with figure 4, Sybil attack in urban model, packet loss in highway model is the most packet loss among all traffic models. We believe that it is because of vehicle's rather uniform mobility and a Sybil attacker can predict vehicles movement path and can attack in his best scenario; it is also shown in figure 3 when in uniform model vehicles have to stop on traffic lights which is another predictable scenario for Sybil attacker. In time 40 seconds, in uniform model, vehicles after a rather uniform motion stops on traffic light and it causes more packet loss. In highway model from time 20 seconds, attack starts. But in urban model, there are lots of intersections and unpredictable motions for vehicles; so that a Sybil attack is not successful like the other models. Traffic lights stop time set randomly, and there is no good predictable motion for vehicles except in the streets with a heavy traffic behind stop sign. We are not considering this scenario in this work; we put it for futures work.

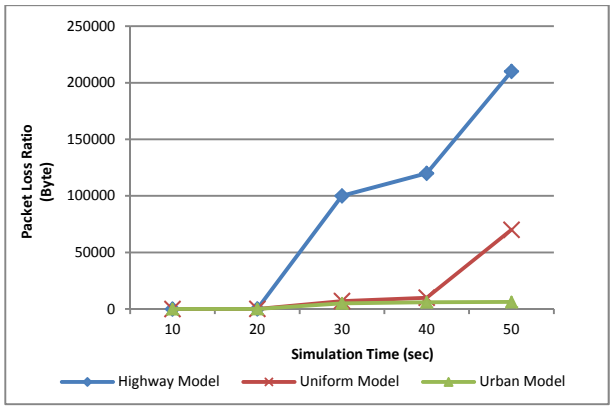

Figure 4. Three traffic models when there is a Sybil attack in the network

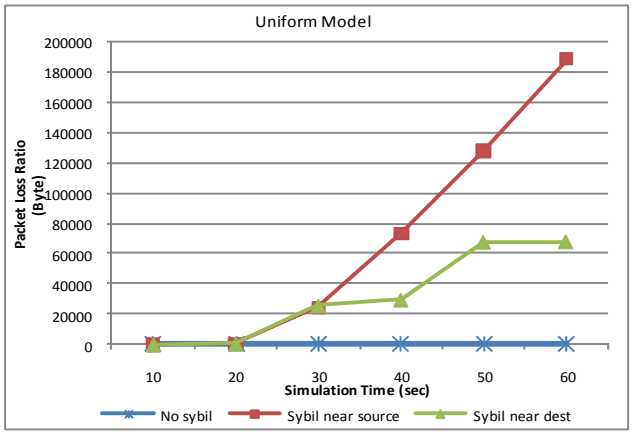

Figure 5. Sybil attack near source and near destination in uniform model.

Based on our experiments, Sybil attackers who attack in various positions may have various purposes. For example when a Sybil attacker tries to be near packet sender, attack can be deeper than attack near destination. Simulation results in three various traffic models show that Sybil attack near source is more dangerous than Sybil attack near destination and defense against it, is harder. This is because the hop counts between source and destination. When there are less hop counts between the Sybil attacker and the victims, attack is more successful.

In fig. 5, Sybil attack near destination, after time 20 seconds packet loss is started. We believe this is because of unpredictable motion of vehicles which is better for an attacker to attacks near destination rather than source because of unpredictable motion of vehicles. In highway model, attack near source is more risky and it is more successful because of the mobility of vehicles. In fig. 5, our VANET is simulated with uniform model and three positions were assumed. When Sybil attack is near source, packet loss ratio is more than Sybil attack near destination. It is also shown in fig. 6 with highway model, but in urban model, in fig. 7, Sybil attack near destination is a little bit dangerous than Sybil attack near source and we think this is because of unpredictable movement of vehicles.

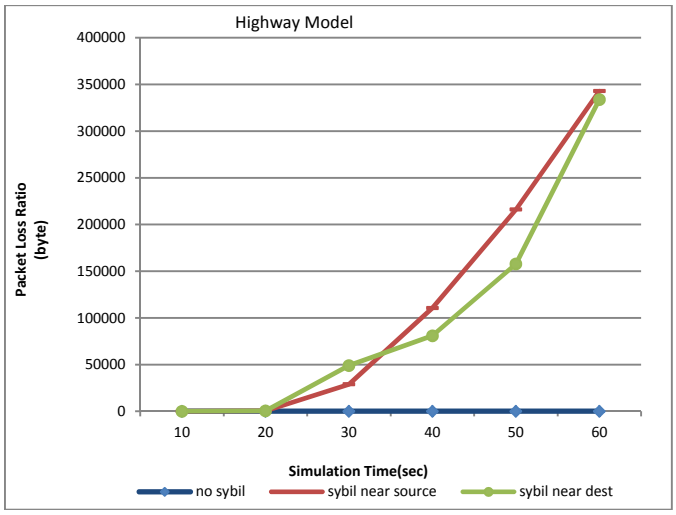

Figure 6. Sybil attack near source and near destination in highway model

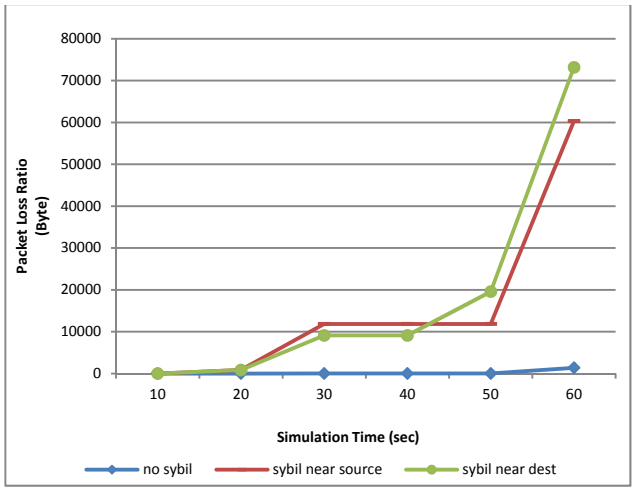

Figure 7. Sybil attack near source and near destination in urban model

We assume another scenario for a Sybil attacker, when a Sybil attacker tries to not show his identities, for example when a Sybil attacker was aware of detecting algorithms in the network or when he wants to not show his identities and make them easy to guess, i.e. when he steals his identities or when he wants to avoid from location based defense algorithms.

In fig. 8 when a Sybil attacker tries to attack out of network routing, it can be possible. He waits for awhile out of source and he evaluates his position, suddenly he can attack and cause packet loss. This attack must be very quick and he must show his identities for a short time to get good services and routing benefits; so this attack can be possible but it is not as strong as when he is sharing routing algorithms. Fig. 8 shows this attack near source of packet sending and near destination of packet receiving. Our simulation results are with 20 vehicles and uniform traffic model in Fig. 8. In this model, attack near source in compare with attack out of rout- near destination and out of rout-near source is with more packet loss and two kinds of attacks out of rout can happen with lower packet loss at the same time.

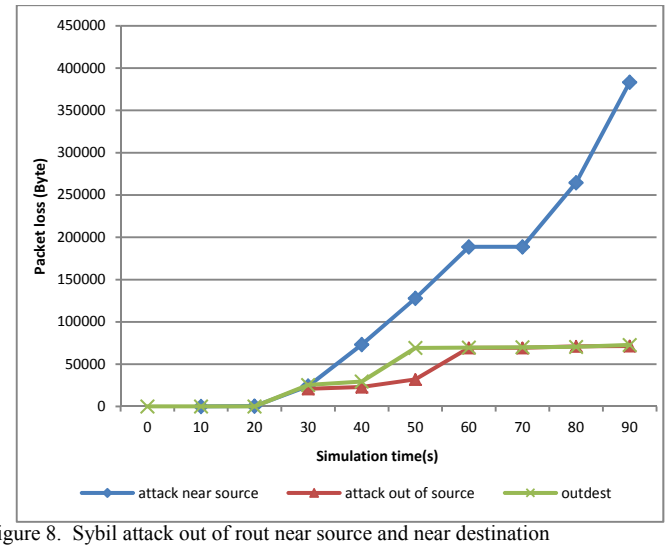

Figure 8. Sybil attack out of rout near source and near destination

VIII. CONCLUSION

In this paper we had a review on Sybil attack, one of the famous attacks on Vehicular ad-hoc Networks. Sybil attacker can forge identities of other vehicles in VANETs and use them in his purposes. Mobility plays a critical role in accurate simulation of VANETs. Without a realistic mobility model, simulation of VANETs and Sybil attacker are not accurate. In this paper, we introduced three traffic models based on real traffic models for VANET. Also we introduced four different kind of a Sybil attacker based on positions he takes to attack in VANET. We found that a Sybil attacker can have lots of scenarios to attack in different positions and those attacks are in different levels of risk. This finding motivates the more detailed investigation of attacks from Sybil attackers. Based on our work, a Sybil attacker near source of rout is more dangerous because of the number of hops between sender and receiver of a packet. In attack near source, there are number of hops between sender and receiver of a packet where there are fewer hops between sender and a Sybil attacker, so that attack can be deeper and with more packet loss. In attack near destination, there are number of hops between sender and receiver and those hops can share routing benefits and other protocols, so that attack can be with less packet loss. We found that some Sybil attackers may want to cheat some routing algorithms on the network and avoid sharing routing packets. They can be out of rout and attack in a good position. This attack is with less packet loss, but it is possible. In our traffic models, Sybil attacker who attacks in highway model, is more successful than Sybil attacker how attacks in urban model. We believe this is because of rather uniform and predictable movement of vehicles. In urban model, Sybil attacker is not aware of movement and it is also hard to know about routing algorithms.

In future work, we will investigate mechanisms to detect the presented attacks. Moreover, currently proposed systems to distinguish between trustworthy and untrustworthy behavior will be analyze regarding false negative detections. Recently, we proposed our vehicle behavior evaluation framework on VANET realistic mobility and we found some similar behavior of Sybil attackers with same position. Path similarity can be a

good behavior to find Sybil attacker and his Sybil identities. We will examine our framework for more than one Sybil attacker and more real traffic models.

REFERENCES

[1] Y. Kumar, P. Kumar, and A. Kadian, "A Survey on Routing Mechanism and Techniques in Vehicle to Vehicle Communication (VANET)," International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.1 , pp135–143, Feb 2011.

[2]

[3] B. Xiao1, B. Yu1 and C. Gao, "Detection and Localization of Sybil Nodes in VANETs," workshop in wireless ad hoc networks and sensor networks, vol. 3, DIWANS '06, pp. 1–8, 2006.

[4] J. Douceur, "The Sybil attack," Proceedings of the International Workshop on Peer to Peer Systems, pp. 251–260, March 2002.

[5] J. Blum and A. Eskandarian, "The Threat of Intelligent Collisions," IT Professional, pp.24–29, January-February 2004.

[6] M. Raya and JP. Hubaux, "Securing Vehicular Ad Hoc Networks," Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks, vol. 2, pp. 39–68, 2007.

[7] G. Guette and B. Ducourthial "On the Sybil attack detection in VANET," IEEE International conference on Mobile Adhoc and Sensor Systems, 2007.

[8] C. Piro , C. Shields and B. Neil Levine, "Detecting the Sybil attack in mobile ad hoc networks," Second International Conference on Security and Privacy in Communication Networks , IEEE Press, 2006.

[9]

[10] J. Grover, D. Kumar, M. Sargurunathan, M.S. Gaur and V. Laxmi, "Performance evaluation and detection of sybil attacks in vehicular Ad-Hoc networks" Communications in Computer and Information Science Vol. 89 CCIS, pp. 473-482, 2010.

[11] B. Neil Levine, C. Shields and N. Boris Margolin, "A Survey of Solutions to the Sybil Attack," Tech report 2006-052, University of Massachusetts Amherst, Amherst, October 2006.

[12] H. Lu and J. Li and M. Guizani, "A novel ID-based authentication framework with adaptive privacy preservation for VANETs," IEEE Computing, Communications and Applications Conference , February 2012.

[13] A. Mahajan , N. Potnis , K. Gopalan and A. Wang, "Urban mobility models for VANETs," IN PROC. OF 2ND WORKSHOP ON NEXT GENERATION WIRELESS NETWORKS, 2006.

[14] A. Mahajan , N. Potnis , K. Gopalan and A. Wang, "Modeling vanet deployment in urban settings," 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems, pp. 151-158, 2007.

[15] Tiger - topologically integrated geographic encoding and referencing

[16] system. http://www.census.gov/geo/www/tiger/.

[17] K. Lan and C. Chou, "Realistic Mobility Models for Vehicular Ad hoc Network (VANET) Simulations,"IEEE 8th International Conference on ITS Telecommunication, October 2008.

[18] S. Park, B. Aslam, D. Turgut and C. Zou, "Defense against Sybil attack in vehicular ad hoc network based on roadside unit support," 28th IEEE conference on Military communications, pp. Pages 37-43, NJ, USA , 2009.

[19] T. Zhou, R. Choudhury, "Privacy-Preserving Detection of Sybil Attacks in Vehicular" forth annual conference on mobile and Ubiquitous Systems: Networking & Services, Aug, 2007.