A Novel Sybil Attack Detection Mechanism in Urban Vehicular Networks

J. Geetha Renuka[1], Syed Gulam Gouse[2]

[1]*M. Tech, Nimra College of Engineering & Technology, Vijayawada, A.P., India.*
[2]*Professor, Dept. of CSE, Nimra College of Engineering & Technology, Vijayawada, A.P., India*

ABSTRACT: *In vehicular networks, moving vehicles are enabled to communicate with each other using inter vehicle communications as well as with road side units (RSUs) in vicinity via roadside-to-vehicle communications. In urban vehicular networks where the privacy, especially the location privacy of the vehicles should be guaranteed vehicles need to be verified in an anonymous manner. A wide spectrum of applications in such a network relies on collaboration and information aggregation among the participating vehicles. Without the identities of participants, such applications are vulnerable to the Sybil attack where a malicious vehicle masquerades as multiple identities, overwhelmingly influencing the result. The consequence of Sybil attack happening in urban vehicular networks can be vital. For example, in safety-related applications such as hazard warning, passing assistance and collision avoidance biased results caused by a Sybil attack can lead to severe car accidents. This paper presents a novel method for detecting sybil attacks in urban vehicular networks.*

KEYWORDS: *Malicious vehicle, RSU, Sybil attack, Trajectory.*

I. INTRODUCTION

Recent advances in various Dedicated Short Range Communication (DSRC) techniques provide easy and effective communication between the vehicles with high mobility. A Vehicular Ad Hoc Network (VANET)[1] is a type of Mobile Ad Hoc Network (MANET) where intermediate nodes are moving vehicles connected using DSRC to form a multi-hop network. Drivers are provided critical information from VANET, which helps their safe and comfortable driving, such as intersection collision avoidance, emergency warning of approaching vehicles, news group broadcast, opportunistic access into internet, etc. One specific application we envision is the information exchange over the VANET in the urban area. Urban vehicular networks are quite different from those with inter-city environment in many aspects, such as the the complexity of road network structure, traffic density and the like. Drivers on different vehicles exchange information, such as emergency warnings, witness of accidents, traffic conditions, among the citywide network to assist driving. Each vehicle acts as an information provider that observes the surrounding environment and contributes useful information to the VANET. Meanwhile each urban vehicle is also an information consumer that queries the items of particular interest and retrieves them from the VANET.

The recent gain of interest for wireless communication in Vehicular Ad hoc Network (VANET) implies an always increasing the number of potential applications in this kind of network. These applications have different goals going from driving assistance (road traffic alert or emergency brake) to the comfort of the passenger (distributed games). All these applications need to exchange data using other vehicles. The communication security problem must be taken into account due to the critical goal of safety related to functions such as emergency brake. As data is broadcasted over a shared communication media, it is simple for a malicious vehicle to intercept, inject or modify data in VANET. Moreover, due to the limited communication range of the vehicle, the cooperation between nodes is essential. Exchanging data with other nodes allows to discover its neighborhood and to share data. This necessity of co- operation shows the vulnerability of these networks if no security mechanism is available. How to trust data received from the other node? Is this node even a physical entity? The multiplication of fake nodes in a wireless network in order to launch different kind of attack called as the Sybil attack [2].

The Sybil attack was first described and formalized by in [2]. It consists in sending multiple messages from one node , called the attacker node, with multiple identities. Hence, the attacker simulates several nodes in the overall network. Different types of attacks that can be launched using Sybil nodes in sensor networks are described in [3]. Applications of the Sybil attack to VANETs have been discussed in [4][5]. Goal of these attacks may be simply to give illusion of a traffic jam to force the other vehicles to leave the road to the benefit of the attacker. Nevertheless, the attack may be more dangerous, trying to provoke collision in the vehicle platoon [4]. This shows the importance of Sybil attack detection in urban vehicular networks.

II. EXISTING WORK

There are so many methods used previously to detect sybil attacks. They are explained as follows: To eliminate the threat of the Sybil attacks, it is straightforward to explicitly bind a distinct authorized identity (e.g., PKI-based signatures) [6][7] to each vehicle so that each participating vehicle can represent itself only once during all communications. Using explicit identities of vehicles has the potential to completely avoid Sybil attacks but violates the anonymity concern in the urban vehicular networks. As an alternative scheme, resource testing [8][9] can be conducted to differentiate between malicious and the normal vehicles, where the judgment is made whether a number of identities possess fewer resources (e.g., computational and storage ability) than would be expected if they were distinct. This scheme fails in heterogeneous environments where the malicious vehicles can easily have more resources than normal ones.

Considering the fact that a vehicle can present itself at only one location at a time, then localization techniques or other schemes like the Global Positioning System (GPS) aiming to provide location information of vehicles can be exploited to detect hostile identities. However, these schemes often fail in
complicated urban settings- for example bad GPS signals due to urban canyons, inaccurate localizations due to highly dynamic wireless signal quality. Later, two group signature-based schemes [10][11] have been proposed, where a message received from multiple distinct vehicles is considered to be trustworthy. Using group signatures can provide anonymity of vehicles and suppress the Sybil attacks by restraining duplicated signatures signed by the same vehicles. One practical issue of these schemes is that different messages with similar semantics may be ignored from making the decision, which leads to either a biased or no final decision.

Recently, location hidden authorized message generation scheme have been proposed, where the RSU signatures on the messages are signer ambiguous so that the RSU location information is concealed from the resulted authorized message and two authorized messages signed by the same RSU within the same given period of time are recognizable so that they can be used for identification purpose. The issue of this scheme is that the RSU is considered to be trust worthy, which can also be compromised.

III. PROPOSED WORK

A. Attack Model: In order to launch the Sybil attack, a malicious vehicle must try to present multiple distinct identities. This can be achieved by either generating a legal identity or by impersonating other normal vehicles. With the following capabilities, an attacker may succeed to launch a Sybil attack in urban vehicular networks: Heterogeneous configuration— malicious vehicles can have more communication and computation resources than the honest vehicles.

B. Design Goals: The design of a Sybil attack detection scheme in urban vehicular networks should achieve the following three goals:
1. Location privacy preservation: A particular vehicle would not like to expose its location information to other vehicles and the RSUs as well since such information can be confidential. The detection scheme should prevent the location information of the vehicles from being leaked.
2. Online detection: When a Sybil attack is launched, then the detection scheme should react before the attack has terminated. Otherwise, the attacker vehicle could already achieve its purpose.
3. Independent detection: The essence of Sybil attack happening is that the decision is made based on the group negotiations. To eliminate the possibility that the Sybil attack is launched against the detection itself, the detection should be conducted independently by the verifier without collaboration with others.

C. RSU Deployment: In Footprint, vehicles require authorized messages issued from the RSUs to form trajectories, which should be statically installed as the infrastructure. When considering the deployment of the RSUs, two practical questions are essential. A simple solution is to deploy RSUs at all intersections. This can result fine trajectories with a sufficient number of authorized messages which will facilitate the recognition of the vehicle. However, deploying such a huge number of RSUs in one time is prohibitive due to high cost.

D. Location hidden authorized Message Generation: In order to be location hidden, authorized messages issued for the vehicles from an RSU should possess two properties. The temporarily linkable property requires that two authorized messages are recognizable if and only if they are generated by the same RSU within the same given period of time.

E. Sybil attack Detection: During a conversation, upon request from the conversation holder, all the participating vehicles provide their trajectory-embedded authorized messages issued within specified event for identification. With submitted messages, the conversation holder verifies that each trajectory and refuses those vehicles that fail the message verification. After that, the conversation holder conducts an online Sybil attack detection before further proceeding with the conversation.

In Footprint, vehicles have wide freedom to create their own trajectories. For example, a vehicle is allowed to request multiple authorized messages from the RSU using different temporary key pairs. Thus, the vehicle can use different authorized messages for different conversations. This capability, however, can be leveraged by a malicious vehicle that tries to launch the Sybil attack by using multiple different messages in a single conversation. The Sybil attack problem is hard due to three following factors:

1. Authorized messages generated for different vehicles are to be asynchronous.
2. Authorized messages are temporarily linkable, which means that there is no invariable mapping between an RSU signature and the real RSU who signed this signature.
3. A malicious vehicle can abuse the freedom of the trajectory generation and the neighbor relationship among RSUs to generate elaborately designed trajectories.

For example, in Figure 1, an attacker can legally generate multiple trajectories which appear different from each other even under a very simple RSU topology. Assume that the real path of the attacker is {R1, R2, R3, R4} (indicated by solid arrows). It can start a new trajectory at any RSU by using a temporary key pair. Therefore, besides the trajectory {R1, R2, R3, R4}, trajectories such as {R1, R2, R3}, {R2, R3, R4}, {R1, R2}, {R2, R3},{R3, R4}, {R1}, {R2}, {R3} and {R4} are all legitimate. In addition, knowing the neighboring relationship of both R2 andR4, the attacker can generate forged trajectories like {R1, R2, R4}, {R1, R4}, and {R2, R4} (indicated by the dash arrow).

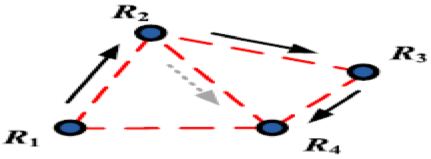

Figure 1: Sybil Trajectory Generation

F. Social Relationship among Trajectories: Despite the asynchrony and temporarily linkable properties of the authorized messages, there are two basic facts that can be exploited to judge whether two trajectories are from two actual vehicles. First, it is very hard, if not impossible, for a single vehicle to traverse between a pair of RSUs shorter than a given time limit. Second, within a limited time period, the total number of RSUs traversed by using a single vehicle is less than a limit. Based on these features an exclusion test is used to examine whether two trajectories are distinct. There are two cases where a pair of trajectories can pass this test. In first case, there are two distinct RSUs appearing within a sliding time window (called check window) when checking two trajectories. We can set the size of the check window equals to traverse time limit. For example, in Figure 2, trajectories T 1 and T 2 are distinct since there exists a pair of different RSUs within the check window, denoted by the box of dash line, i.e., R2 and R3. In the second case, the number of RSUs contained in the merged RSU sequence of the two trajectories is larger than the trajectory length limit.

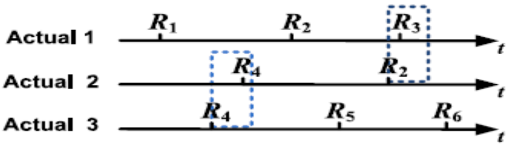

Figure 2: Checking for distinct trajectories a check window

IV. CONCLUSION

Malicious vehicle can easily obtain messages between two other communicating entities by using eavesdropping on the wireless channel. Footprint, all messages delivered through wireless communication. If a malicious vehicle can succeed in using authorized message issued for other vehicle it can masquerade as multiple identities launching a Sybil attack. In existing systems, location Hidden Authorized Message Generation Scheme was implemented In this scheme the Road Side Unit (RSU) is compromised by the forged vehicle and also it is not trustworthy. If an RSU is compromised, it can help a malicious vehicle generate fake legal trajectories, for example by inserting link tags of other RSUs into a forged trajectory. In that case, Footprint mechanism cannot detect such trajectories. However, the corrupted RSU cannot deny a link tag generated by itself nor forge the link tags generated by other RSUs, which can be utilized to detect a compromised RSU in the system. In our proposed work, first, consider the scenario where a small fraction of the RSUs are compromised. We will develop cost-efficient techniques to fast detect the corruption of the RSU. Second, we will delve into designing process better linkable Signer-Ambiguous Signature Schemes such that the computation overhead for signature verification and the communication overhead can be reduced. Third, a threshold ElGamal system based key management scheme for safeguarding urban vehicular networks from the compromised RSUs and their collusion with the malicious vehicle.

REFERENCES

[1]. C. Harsch, A. Festag, and P. Papadimitratos, "Secure Position-Based Routing for VANETs," In Proc. of IEEE VTC, 2007.
[2]. J. Douceur. The Sybil Attack. In First International Workshop on Peer-to-Peer Systems, pages 251–260, March 2002.
[3]. J. Newsome, E. Shi, D. Song, and A. Perrig. The Sybil Attack in Sensor Networks: Analysis & Defenses. In Proceedings of the third international symposium on Information processing in sensor networks, pages 259–268, 2004.
[4]. J. Blum and A. Eskandarian. The Threat of Intelligent Collisions. IT Professional, 6(1):24–29, January-February 2004.
[5]. M. Raya and JP. Hubaux. Securing Vehicular Ad Hoc Networks. Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks, 15(1):39– 68, 2007.
[6]. M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D.S.Wallach, “Secure Routing for Structured Peer-to-Peer Overlay Networks,” Proc.
[7]. Symp. Operating Systems Design and Implementation (OSDI ’02), pp. 299-314, Dec. 2002.
[8]. S.Chang, Y.Qi, H.Zhu, J.Zhao, and X.Shen, “Footprint: Detecting Sybil Attacks in Urban Vehicular Networks”, IEEE Trans. Parallel and Distributed Systems, vol.23, June. 2012.
[9]. C. Piro, C. Shields, and B.N. Levine, “Detecting the Sybil Attack in Mobile Ad Hoc Networks,” Proc. Securecomm and Workshop, pp. 1-11, Aug. 2006.
[10]. N. Borisov, “Computational Puzzles as Sybil Defenses,” Proc. Sixth IEEE Int’l Conf. Peer-to- Peer Computing (P2P ’06), pp. 171-176, Oct. 2006.
[11]. Q. Wu, J. Domingo-Ferrer, and U. Gonzalez Nicola´ s, “Balanced Trustworthiness, Safety and Privacy in Vehicle-to-vehicle Communications,”
[12]. IEEE Trans. Vehicular Technology, vol. 59, no. 2, pp. 559-573, Feb. 2010.
[13]. L. Chen, S.-L. Ng, and G. Wang, “Threshold Anonymous Announcement in VANETs,” IEEE J. Selected Areas in Comm., vol. 29, no. 3, pp. 1-11, Mar. 2011.