Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.578 – 584

RESEARCH ARTICLE

Sybil Attack Detection with Reduced Bandwidth Overhead in Urban Vehicular Networks

D. Balamahalakshmi
Department of Computer Science and Engineering, V.S.B Engineering College, Karur
Email: balavishnud@gmail.com

Mr. K.N. Vimal Shankar
Assistant Professor
Department of Computer Science and Engineering, V.S.B Engineering College, Karur
Email: mecsevsbec@gmail.com

ABSTRACT

Urban vehicular networks should have more location privacy. For Sybil attack detection previously they proposed a footprint concept to detect the Sybil attack by using the trajectory information generated by multiple RSUs also to preserve the location of vehicle. The RSU will generate the location and timing information to vehicle whenever it passes through RSU. Using this message the verification will be carried and also it will consider failed RSU for verification. Reducing the message size is not covered in this system. To achieve this, the repeated occurrences of adjacent RSUs are eliminated in the proposed system. So that the length of the trajectory information is reduced without loss of information and also the bandwidth overhead is reduced.

Keywords- *Sybil Attack Detection, Less bandwidth, signature verification*

I. INTRODUCTION

A Vehicular Ad-Hoc Network or VANET is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. In VANET, or Intelligent Vehicular Ad-Hoc Networking, defines an intelligent way of using Vehicular Networking. In VANET integrates on multiple ad-hoc networking technologies such as Wi-Fi IEEE 802.11p, WAVE IEEE 1609, WiMAX IEEE 802.16, Bluetooth, IRA, ZigBee for easy, accurate, effective and simple communication between vehicles on dynamic mobility. Effective measures such as media communication between vehicles can be enabled as well as methods to track the automotive vehicles.

A Sybil attack is one in which an attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities, using them to gain a disproportionately large influence. A reputation system's vulnerability to a Sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the reputation system treats all entities identically. A Sybil attack is one in which an attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities, using them to gain a disproportionately large influence. A reputation system's vulnerability to a Sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the reputation system treats all entities identically. In urban vehicular networks where the privacy, especially the location privacy of vehicles should be guaranteed vehicles need to be verified in an anonymous manner. Without 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 vehicular networks can be vital. For example, in safety-related applications such as hazard warning, collision avoidance, and passing assistance, biased results caused by a Sybil attack can lead to severe car accidents. Therefore, it is of great importance to detect Sybil attacks from the very beginning of their happening.

Detecting Sybil attacks in urban vehicular networks, however, is very challenging. First, vehicles are anonymous. Second, location privacy of vehicles is of great concern. Location information of vehicles can be very confidential. Third, conversations between vehicles are very short. Due to high mobility of vehicles, a moving vehicle can have only several seconds to communicate with another occasionally encountered vehicle. It is difficult to establish certain trustworthiness among communicating vehicles in such a short time. This makes it easy for a malicious vehicle to generate a hostile identity but very hard for others to validate.

Furthermore, short conversations among vehicles call for online Sybil attack detection. The detection scheme fails if a Sybil attack is detected after the attack has terminated. To eliminate the threat of Sybil attacks, it is straightforward to explicitly bind a distinct authorized identity (e.g., PKI-based signatures) 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 urban vehicular networks. As an alternative scheme, resource testing can be conducted to differentiate between malicious and 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 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, 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 (e.g., bad GPS signals due to urban canyons, inaccurate localizations due to highly dynamic wireless signal quality). Recently, two group-signature-based schemes 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 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 a biased or no final decision. As a result, there is no existing successful solution, to tackling the online Sybil attack detection problem in urban vehicular networks. The Sybil attack has been a severe and pervasive problem in many forms. In a Sybil attack, an attacker can launch a Sybil attack by forging multiple identifies, gaining a disproportionately large influence. In the literature, there have been many different approaches proposed to detect or mitigate the attack.

Many studies have followed focusing on how to establish trust between participating entities based on trusted public key cryptographies or certificates in distributed systems, for example, P2P systems sensor networks and mobile ad hoc networks. Although deploying trusted certificates is the only approach that has the potential to completely eliminate Sybil attacks, it also violates both anonymity and location privacy of entities. In addition, most of these schemes rely on a centralized authority that must ensure each entity is assigned exactly one identity. Moreover, it is possible for an attacker to violate the assumption, getting more than one identities. This mechanism also has the problem of key revocation which is challenging, particularly in wireless mobile networks. Another category of Sybil attack detection schemes is based on resource testing. The goal of resource testing is to determine if a number of identities possess fewer resources than would be expected if they were independent. The resources being tested can be computing ability, storage ability, and network bandwidth, as well as IP addresses. These schemes assume that entities have homogeneous hardware configurations.

In vehicular networks, this assumption cannot hold since malicious vehicles can easily have more powerful resources than the normal vehicles. Sybil Guard is an interesting scheme studying the social network among entities. In this scheme, human-established real-world trust relationship among users is used for detecting Sybil attacks. Since even the attacker can generate as many as Sybil identities, building relationship between honest users and Sybil identities is much harder. Thus, there exists a small “cut” on the graph of trust relationship between the forged identities and the real ones. However, this scheme cannot be used in vehicular networks, since it is very challenging to establish such trust relationship among vehicles. This is because vehicles are highly mobile. Communications often happen among temporarily met and unfamiliar vehicles. To exploit the fact that one single vehicle cannot present at multiple locations at the same time, they have proposed a detection mechanism utilizing localization technique based on Received Signal Strength Indication (RSSI). In this scheme, by successively measuring the RSSI variations, the relative locations among vehicles in vicinity can be estimated. Identities with the same estimated locations are considered as Sybil vehicles.

In addition to the inaccuracy of RSSI measurements, this scheme also needs all neighboring vehicles to collaborate which may suffer a Sybil attack against the detection scheme itself. In the scheme, the trust authority distributes a number of pseudonyms for each vehicle.

Abused pseudonyms can be detected by RSUs. Since RSUs are heavily involved in the detection process, this scheme requires the full coverage of RSUs in the field. It is infeasible in practice due to the prohibitive cost. Furthermore, in such a scheme, vehicles should managed by a centralized trusted center. Each time RSU
detects suspicious pseudonyms, it should send all the pseudonyms to the trust center for further decision, which makes the trust center be the bottleneck of the detection. Recently, two group-signature-based schemes have been proposed, ensuring that a verifier vehicle can identify those trustworthy messages from messages sent from neighboring vehicles. A message sent from a neighboring vehicle is said to be trustworthy if the content of the message is identical with at least a certain number of messages sent from other neighboring vehicles.

To suppress duplicated messages from the same vehicle, particular group signature schemes are adopted for vehicles to sign on messages so that the anonymity of each vehicle can be achieved. Meanwhile, if a vehicle generates two signatures on the same message, these two signatures can be recognized by the verifier vehicle. One practical issue of these schemes is that they cannot handle similar but different messages. It is often the case that multiple vehicles observing the same driving environment will generate different messages with very similar semantics. In this case, the resolved trustworthy messages might be a minority of all observations which results in a biased or no final decision.

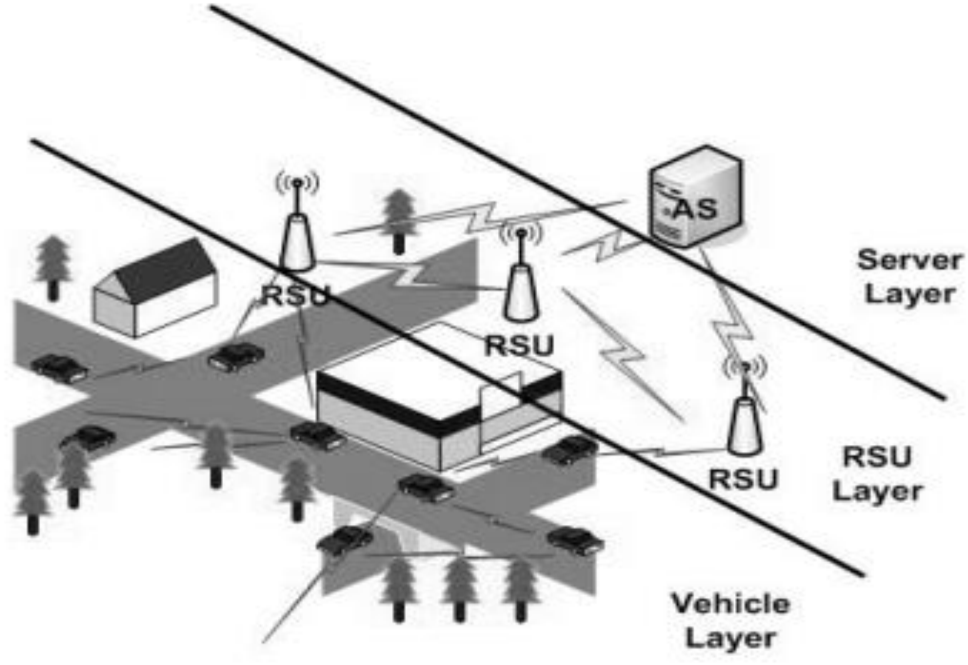
The most relevant work to Footprint is the Sybil attack detection scheme. In this scheme, a number of location information reports about a vehicle are required for identification. RSU periodically broadcasts an authorized time stamp to vehicles in its vicinity as the proof of appearance at this location. Vehicles collect these authorized time stamps which can be used for future identity verification. In, trajectories made up of consecutive time stamps and the corresponding public keys of RSUs are used for identification.

However, these schemes did not take location privacy into consideration since RSUs use long-term identities to generate signatures. As a result, the location information of a vehicle can be inferred from the RSU signatures it collects. In Footprint, authorized messages issued from RSUs are signer-ambiguous which means the information about the location where the authorized message was issued is concealed, and temporarily linkable which means using a single trajectory for long-term identification of a vehicle is prohibited. Therefore, the privacy of location information and identity of vehicles are preserved in Footprint.

II. INFRASTRUCTURE CONSTRUCTION

A single network consists of multiple RSUs and a Trusted Authority (TA).In general, Footprint integrates elegant techniques namely, infrastructure construction and Sybil attack detection.

A vehicle equipped with an OBU can communicate with an RSU or with other vehicles in vicinity via wireless connections. Authentication Server (AS) is responsible for the system initialization and RSU management. The AS is also connected to the RSU backbone network. This will manage all RSUs. A minimum number of available RSUs can achieve the maximum service coverage in terms of served traffic amount as well as good fairness in terms of geographical distribution. After the deployment of RSUs, a vehicle needs authorized messages from each RSU it passes by as a proof of its presence. Such authorized messages are location secreted which refers to that RSU signatures are signer ambiguous and the authorized messages are temporarily linkable. The consecutive number of authorized messages is taken for verification of vehicle, which is based on the timing information provided by the RSUs. We design a location-hidden authorized message generation vehicle by checking all other identities 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.



III. SYBIL ATTACK DETECTION

The location information for the vehicle should be secret. The authorized message is signer ambiguous. The detection scheme should prevent the location information of vehicles.

When a Sybil attack is launched, the detection scheme should react before the attack has happened. Otherwise, the attacker achieves his target. The essence of Sybil attacks happening is that the decision is made based on group negotiations. To eliminate the possibility that a Sybil attack is launched against the detection itself, the detection should be conducted independently by the verifier without collaboration with others. Using the trajectory of vehicles we can identify the Sybil attack. It is based on timing information of vehicles. For Security we use two type of signature**.** In the partial signature creation, the input provided as two pair namely private key of the road side unit and public key of the vehicle, the message should be provided then the message should be encrypted and partial signature value executed in the application. The partial signature verification is verified depend upon the selection of road side unit and vehicle identity number.

The full signature creation is done by as two pair namely private key of the road side unit and public key of the vehicle and data traversed to road side unit to on board unit for further reference then the output are partial signature value and encrypted message.

IV. CONCLUSION AND FUTURE WORK

In Footprint, we assume that all RSUs are reliable. However, if an RSU is compromised, it makes a malicious vehicles to generate fake legal trajectories (e.g., by inserting link tags of other RSUs into a forged trajectory).In that case, Footprint cannot detect such trajectories. However, the corrupted RSU cannot deny a link tag generated by it nor forge link tags generated by other RSUs, which can be utilized to detect a compromised RSU in the system. In this paper the compromised RSU also considered for the verification. Repeated occurrences of adjacent RSUs are eliminated in this system. So that the length of the trajectory information is reduced without loss of information and also the bandwidth overhead is reduced. With this proposed detection mechanism we will continue the work on several directions. For example we will look into designing better linkable signer-ambiguous signature schemes such that the computation overhead for signature verification and the communication overhead can be reduced.

REFERENCES

[1] Shan Chang, Yong Qi Footprint: Detecting Sybil Attacks in Urban Vehicular Networks Member, IEEE, Hongzi Zhu, Member, IEEE, Jizhong Zhao, Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE JUNE 2012

[2] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, “An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications,” IEEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, Sept. 2010.

[3] R. Lu, X. Lin, H. Zhu, and X. Shen, “An Intelligent Secure and Privacy-Preserving Parking Scheme through Vehicular IEEE Trans. Vehicular Technology, vol. 59, no. 6,pp. 2772-2785, July 2010.

[4] J.R. Douceur, “The Sybil Attack,” Proc. First Int’l Workshop Peer-to- Peer Systems (IPTPS ’02), pp. 251-260, Mar. 2002.
[5] J. Eriksson, H. Balakrishnan, and S. Madden, “Cabernet: Vehicular Content Delivery Using WiFi,” Proc. MOBICOM ’08, pp. 199-210, Sept. 2008.
[6] M. Castro, P. Druschel, A. Ganesh, A. Rostrum, and D.S. Wallach, “Secure Routing for Structured Peer-to-Peer Overlay Networks,” Proc. Symp. Operating Systems Design and Implementation (OSDI ’02), pp. 299-314, Dec. 2002.
[7] B. Dutertre, S. Cheung, and J. Levy, “Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust,” Technical