ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

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, Tamilnadu, India[1]

ABSTRACT: Previously, in urban vehicular networks the location privacy of vehicle is more considerable. An attacker can easily launch a Sybil attack by succeeding multiple hostiles. They proposed a Sybil attack detection mechanism, footprint and trajectory of vehicle for identification also preserving the location privacy of vehicle. The RSU will generate the authorized message when the vehicle passes through the RSU. The authorized message consists of appearance of vehicle at particular location and at particular time. This will be taken into verification whenever required. The verification considers the series of authorized message generated by multiple RSU. In this paper we implement a mechanism (Trusted Authority (TA) Information) to overcome the failure of RSU and also decrease the false positive rate (incorrect identification-real vehicle as fraudulent).Accurate security analysis and extensive trace-driven simulations express the efficacy of Footprint.

KEYWORDS- Onboard Unit (OBU), Roadside Unit (RSU), Sybil Attack Detection, Trusted Authority (TA).

I. INTRODUCTION

In past years, vehicular networks have been emerging as a cornerstone of the next-generation Intelligent Transportation Systems (ITSs), contributing to safer and more efficient roads by providing timely information to drivers and concerned authorities. In vehicular networks, moving vehicles are enabled to communicate with each other via inter vehicle communications as well as with road-side units (RSUs). Because, the mobility of vehicle is very high. Due to high mobility of vehicles, a moving vehicle could not communicate with another vehicle. It is difficult to found 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 to authenticate. The detection scheme fails if a Sybil attack is detected after the attack has happened. To eliminate the threat of Sybil attacks, an authorized identity (e.g., PKI-based signatures)is generated to each vehicle. so that each participating vehicle can represent itself only once during all communications. Using explicit identities of vehicles we can avoid Sybil attacks but violates the anonymity concern in urban vehicular networks. The resource testing can be conducted to differentiate the 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 have more resources than normal vehicle.

In urban vehicular networks the location privacy of vehicles should be assured, vehicles need to be verified in an anonymous manner. Without identities of vehicles, such applications are vulnerable to the Sybil attack where a malicious vehicle masquerades as multiple identities. Sybil attack may cause 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 more important. Location information of vehicles can be very secret. Considering the fact that a vehicle can present itself at only one location at a same time, localization techniques or other schemes like the Global Positioning System (GPS) focusing to provide location information (Time and Place) of vehicles. However, these

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

schemes often fail in complicated urban settings. lately, 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 detecting Sybil attacks by restricting 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 partial or non final decision. As a result, there is no successful solution, to tackling the online Sybil attack detection problem in urban vehicular networks. In a Sybil attack, an attacker can launch a Sybil attack by forging multiple identifies, gaining a disproportionately large influence. There have been many different approaches proposed to detect or mitigate the attack.

Many studies have followed and focusing on how to establish trust between participating entities based on trusted public key cryptographies or certificates in distributed systems, In addition, most of these schemes rely on a centralized authority that must ensure each entity is assigned exactly one identity to a particular vehicle. Moreover, it is possible for an attacker to violate the assumption, getting more 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. To exploit the fact that one single vehicle cannot present at multiple locations at the same time, they have proposed a Sybil attack detection scheme where the location of a particular vehicle can be determined by the RSSI measurements taken at other participating 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.

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 same 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 used 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 schemes proposed in. In these schemes, a number of location information reports about a vehicle are required for identification. In an 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. But the more important thing is that RSU failure. In this paper we implement a mechanism (TA record)to overcome the failure of the RSU, when the vehicle reaches the collapsed RSU it will not generate any authorized message for identification. So the neighbor RSU will take response for this and will send identity

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

request to TA. It will contains all the RSUs identities send response to the requested RSU. From this information it can easily verify he Vehicle by checking all other identities.

II. SYSTEM MODELS DESIGN

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

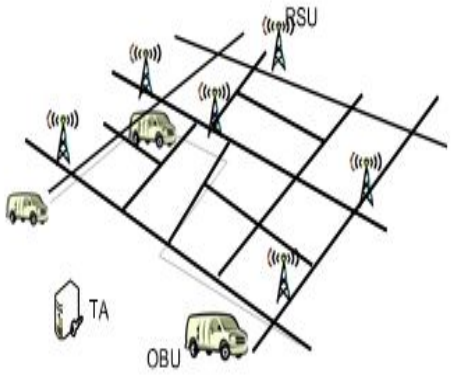


Fig. 1. An illustration of the system model, where the dash line indicates the travel route of a vehicle. As the vehicle traverses the area, it will encounter multiple RSUs, typically deployed at intersections.

2.1 INFRASTRUCTURE CONSTRUCTION

This includes Onboard Unit of vehicle, Trusted Authority and Roadside Unit.

2.1.1Onboard Unit (OBU)

A vehicle equipped with an OBU can communicate with an RSU or with other vehicles in vicinity via wireless connections. we simply refer to a vehicle as a vehicle equipped with an OBU in this paper. A vehicle can be malicious if it is an attacker or compromised by an attacker.

2.1.2 Trust Authority (TA)

Trust authority is responsible for the system initialization and RSU management. The TA is also connected to the RSU backbone network. This will manage all RSUs.

2.1.3 Road Side Unit (RSU)

More purposely, we design a methodology to deploy 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

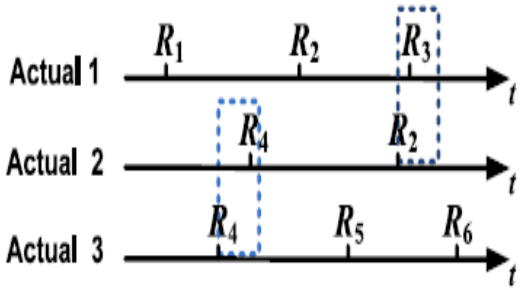
Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

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

During a conversation, upon request from the conversation holder, all participating vehicles provide their trajectory embedded authorized messages issued within specified RSU.



Note that the attacker cannot generates a trajectory like fR1; R3g because R1 is not a neighbor of R3. In the case of this example, R3 only expects signatures signed by R2 and R

IV. DESIGN GOALS

The Sybil attack detection mechanism has developed to achieve the following.

4.1 Location privacy preservation—The location information fo the vehicle should be secret.the authorized message is signer ambigious.The detection scheme should prevent the location information of vehicles.

4.2 Online detection— when a Sybil attack is launched, the detection scheme should react before the attack has happened. Otherwise, the attacker achieve his target

4.3 Independent detection— 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.

4.4 RSU failure consideration---The failure RSU message is also considered while the verification of vehicle.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

V. PERFORMANCE ANALYSIS

We test the performance of Footprint in recognizing fake trajectories (issued by malicious vehicles) and real ones (provided by honest vehicles) through Trace-driven simulations. We consider two key metrics for the performance evaluation.

5.1False positive error: It is the proportion of all actual Trajectories that are incorrectly identified as forged trajectories.

5.2False negative error: It is the proportion of all forged Trajectories that are falsely identified as actual trajectories.

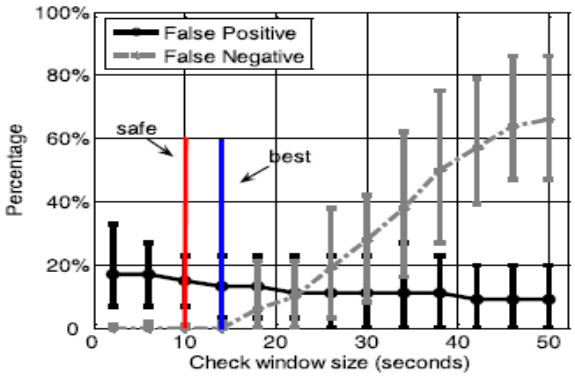


Fig2: Check window size versus false positive error and false negative error

VI. 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 itself 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.

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.

[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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

[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 Report SRI-SDL-04-02, SRI Int'l, Apr.

[8] J. Newsome, E. Shi, D. Song, and A. Perrig, Information Processing in Sensor Networks (IPSN '04), pp. 259-268,Apr. 2004.