Sybil Attack Detection in Urban Vehicular Networks

S. Suganya M.E
Assisant Professor Cse Department
R.V.S School Of Engineering And Technology
Dindigul.

Abstract

In urban vehicular networks, where privacy, especially the location privacy of anonymous vehicles is highly concerned, anonymous verification of vehicles is indispensable. Consequently, an attacker who succeeds in forging multiple hostile identifies can easily launch a Sybil attack, gaining a disproportionately large influence. In this paper, we propose a novel Sybil attack detection mechanism, Footprint, using the trajectories of vehicles for identification while still 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. We 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. With the temporal limitation on the linkability of two authorized messages, authorized messages used for long-term identification are prohibited. With this scheme, vehicles can generate a location-hidden trajectory for location-privacy-preserved identification by collecting a consecutive series of authorized messages. Utilizing social relationship among trajectories according to the similarity definition of two trajectories, Footprint can recognize and therefore dismiss "communities" of Sybil trajectories. Rigorous security analysis and extensive trace-driven simulations demonstrate the efficacy of Footprint.

Key words : Sybil attack, location privacy, signer-ambiguous signature, urban vehicular networks, location-hidden trajectory.

I INTRODUCTION

OVER the past two decades, 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 intervehicle 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 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 participating vehicles. 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.

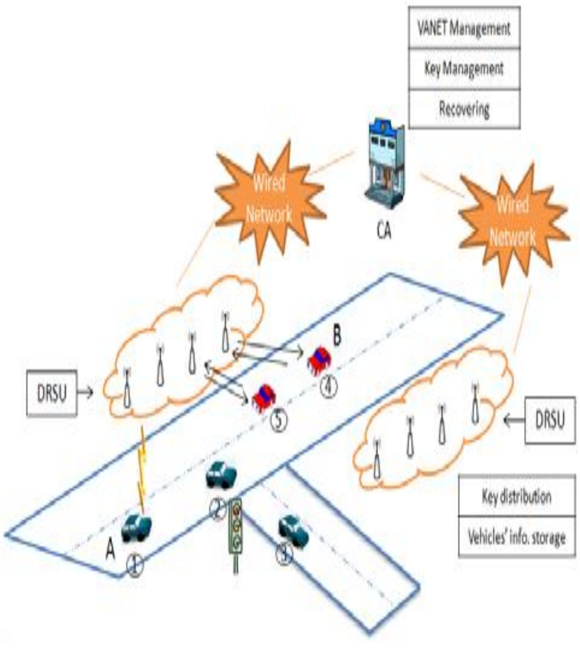
II OVERVIEW

Detecting Sybil attacks in urban vehicular networks, however, is very challenging. First, vehicles are anonymous. There are no chains of trust linking claimed identities to real vehicles. Second, location privacy of vehicles is of great concern. Location information of vehicles can be very confidential. For example, it can be inferred that the driver of a vehicle may be sick from knowing the vehicle is parking at a hospital. It is inhibitive to enforce a one-to-one correspondence between claimed identities to real vehicles by verifying the physical presence of a vehicle at a particular place and time. 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 straight forward 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 the best of our knowledge, to tackling the online Sybil attack detection problem in urban vehicular networks. We propose a novel Sybil attack detection scheme Footprint, using the trajectories of vehicles for identification while still preserving the anonymity and location privacy of vehicles. Specifically, in Footprint, when a vehicle encounters an RSU, upon request, the RSU issues an authorized message for this vehicle as the proof of its presence at this RSU and time. Intuitively, authorized messages can be utilized to identify vehicles since vehicles located at different areas can get different authorized messages. However, directly using authorized messages will leak location privacy of vehicles because knowing an authorized message of a vehicle signed by a particular RSU is equivalent to knowing the fact that the vehicle has showed up near that RSU at that time. In Footprint, we design a location-hidden authorized message generation scheme for two purposes. First, RSU signatures on messages are signer ambiguous which means an RSU is anonymous when signing a message. In this way, the RSU location information is concealed from the final authorized Message. Second, authorized messages are temporarily linkable which means two authorized messages issued from the same RSU are recognizable if and only if they are issued within the same period of time. Thus, authorized messages can be used for identification of vehicles even without knowing the specific RSUs who signed these messages. With the temporal limitation on the link ability of two authorized messages, authorized messages used for long-term identification are prohibited. Therefore, using authorized messages for identification of vehicles will not harm anonymity of vehicles. To be uniquely identified, a vehicle collects a consecutive series of authorized messages as it keeps travelling. Such a sequence of authorized messages constitutes a trajectory of this vehicle. In Footprint, a vehicle is free to start a new trajectory by using a new temporary public key. Furthermore, a malicious vehicle can abuse this freedom to elaborately generate multiple trajectories, trying to launch a Sybil attack. Based on the observation that Sybil trajectories generated by a malicious vehicle are very alike, Footprint establishes the relationship between a pair of trajectories according to our definition of similarity. With this relationship, Sybil trajectories generated by the same malicious vehicle form a “community.” By finding and eliminating “communities” of Sybil trajectories, Footprint can detect and defend against Sybil attacks. The advantages of Footprint are fourfold. First, Footprint does not need the identities of vehicles, which ensures the anonymity of vehicles. Second, no geographical information is leaked in Footprint, which guarantees the location privacy of vehicles. Third, Footprint only needs each vehicle to be equipped with a cheap commercial GPS receiver and DSRC wireless communication module. Last, Sybil attack detection can be online independently conducted by a conversation holder (e.g., an individual vehicle or an RSU) which initializes a conversation among vehicles. Besides the advantages, the main limitation of Footprint is that Footprint requires an infrastructure of RSUs and a trust authority (TA) existing in the system in order to generate trajectories and establish trust among entities, respectively. We verify that Footprint can achieve all design objectives through security, privacy, and performance analysis and extensive trace-driven simulations which involve 2,100 taxies in Shanghai city. Footprint can largely restrict Sybil attacks and enormously reduces the impact of Sybil attacks in urban settings (above 98 percent detection rate).

III DESIGN CONSIDERATION

Location-hidden authorized message generation scheme. 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 are recognizable so that they can be used for identification.



Certificate Authorities

Certificate Authorities (CA) are called CA and are responsible as administrate department in VANET. They hold all the secrets and have responsibilities to solve disputes. They are used to do VANET management, key management and recovering. The authority has the highest security level. We assume it cannot be compromised.

Distributed Road Side Units (DRSUs)

RSUs are agents of the authority and deployed at the road sides. Distributed Road Side Units (DRSUs) are a set of RSUs. They are used to distribute key and store information from vehicles. However, there is a bottleneck problem of RSU in original VANET. If the RSU is compromised, the message in its coverage cannot be transformed successfully, especially as the message is important and has higher safety requirements. The DRSUs group is semi-trusted with the medium security level. An RSU can be a powerful device or a comparatively simple one. The set of RSUs in a DRSUs group is comparatively simple ones.

On Board Units

On Board Units (OBUs)are ordinary vehicles on the road that have ability to communicate with each other through radio. After registered information on CA as required, an ordinary vehicle can join VANET and be assigned some initial values. OBUs have the lowest security level. Because semi-trusted RSU may be compromised, our proposal is to develop the ability of anti-RSU compromised by malicious object if any. Several RSUs cooperate together as a DRSUs group, instead of one RSU.

Key management scheme

Threshold ElGamal system-based key management scheme, we cannot get the original plaintext with the help of RSUs whose number is less than the threshold value. Even if some of the semi-trusted road side units are physically captured, attackers need to capture threshold of nodes for monitoring. Threshold cryptography achieves the security needs as confidentially and integrity against malicious attackers. It also provides data integrity and availability in a hostile environment and can also employ verification of the correct data sharing. All these can be achieved without revealing the private key. Thus, DRSUs do not need to update key frequently and communicate with CA continually. This is helpful for saving energy in VANET.

IV IMPLEMENTATION AND RESULT

We will consider the scenario where a small fraction of RSUs are compromised. We will develop cost-efficient techniques to fast detect the corruption of an RSU. We will delve into designing better linkable signer-ambiguous signature schemes such that the computation overhead for signature verification and the communication overhead can be reduced.

This paper implements reprogramming protocol by using the Network-simulator tool. Network simulator tool is used to develop protocol implementation and provides performance evaluation of this protocol. Network simulator shows the packet flow that is visualization result of the protocol.

V CONCLUSION

In this paper, we propose a Threshold ElGamal-based key management scheme for protection against RSU compromise in VANET. The private key is divided into several pieces and distributed to each RSU in one DRSUs group. Our proposal system guarantees the successful recovery probability especially helpful for EBN scenario and does not influence the efficiency application in DFCD scenario. This is capable to be away from exposing the privacy of sender to receivers.

REFERENCES

[1] 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.

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

[3] J.R. Douceur, “The Sybil Attack,” Proc. First Int’l Workshop Peer-to-Peer Systems (IPTPS ’02), pp. 251-260, Mar. 2002.

[4] J. Eriksson, H. Balakrishnan, and S. Madden, “Cabernet: Vehicular Content Delivery Using WiFi,” Proc. MOBICOM ’08, pp. 199-210, Sept. 2008.

[5] M. Castro, P. Druschel, A. Ganesh, A. Rowstron, 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.