Research Paper Engineering

Detection Scheme In Vehicular Networking Area

*Ameena Firdous ** Mohammed Zeeshan Ali

*,** HITS, HYDERABAD, INDIA

ABSTRACT

The Sybil attack is one of the most aggressive and evasive attacks in vehicular networks that can affect on many aspects of network functioning. Thus, its efficient detection is of highest importance. 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 are using footprint of the vehicles which helps for identification based on the location privacy. From technology point of view it aims at V2V andV2I communication to enable novel cooperative applications. RSUs play an important role here.

INTRODUCTION

In a Sybil attack, an individual entity masquerades as multiple simultaneous identities. Researchers have extensively studied Sybil attacks in the other areas of computer net-works such as peer-to-peer (P2P) systems. By manipulating these identities, the adversary can render the result of the applications running on the system questionable, if not incorrect To launch a Sybil attack, the adversary needs only the OSN accounts.

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. 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 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.

RSU Management System

In a V2I environment, the RSU is responsible for the communication between vehicles, roadside infrastructure and the connected traffic management infrastructure. Additionally it is Also responsible for extending the communication range of vehicles and to keep relevant messages available in their coverage area - independently from the network density.

To reduce the complexity and to enhance stability, it is divided into different interacting modules and subsystems, which fulfill well defined and differentiated tasks:

The ***Configuration Management Subsystem*** is responsible for maintaining the set-up of applications and the system itself.

The ***Fault Management Subsystem*** is in charge of qualified handling of exceptional circumstances and failure.

The ***Function Framework*** provides defined and controllable interfaces for functions.

RSU Management Centre architecture

To achieve the above mentioned goals it is necessary to maintain a RSU Management Centre, which fulfils the requirements of high availability and scalability. Figure shows the hardware architecture, which reflects these requirements.

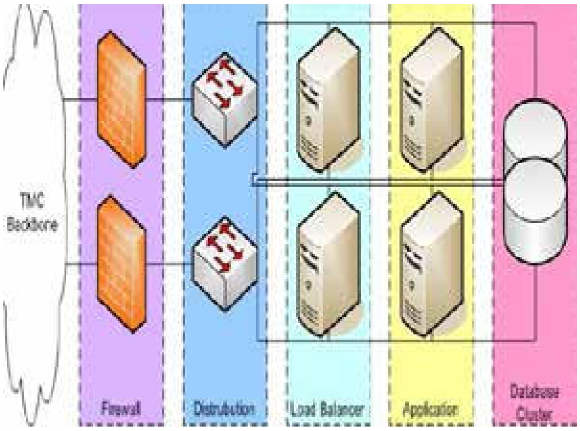

Fig 1. Hardware architecture of RSU management

All traffic directed to the management centre is scanned by the firewalls and afterward forwarded by the switching hardware. Then the traffic will be statistically distributed by the load balancers to the management servers. Those servers all contain the identical set of applications. So the computing power can easily be increased by adding new servers to the management centre. In combination with a database cluster this solves the challenge of scalability. The database cluster contains all information for configuration and management.

Generating Location Hidden Trajectory

Location-Hidden Authorized Message Generation In order to be location hidden, authorized messages issued for vehicles from an RSU should possess two properties, i.e., signer ambiguous and temporarily linkable. The signer ambiguous property means the RSU should not use a dedicated identity to sign messages. The temporarily linkable property requires two authorized messages are recognizable if and only if they are generated by the same RSU within the same given period of time. Otherwise, a long-term link ability of authorized messages used for identification eventually has the same effect as using a dedicated identity for vehicles. This paper, we demonstrate one possible implementation of a location-hidden authorized message generation scheme using linkable ring signature. Linkable ring signature is signer-ambiguous and signatures are linkable as well. Particularly, we choose the linkable ring signature scheme for two reasons: first, it has been proved to be secure; second, it has constant signature size. To meet the requirement of temporarily linkable property, we extend the scheme to support the event-orient link ability property which guarantees that any two signatures are linkable if and only if they are signed based on the same event by the same RSU In our signature scheme, we define an event as a period of time within which two signatures issued from the same RSU are linkable. Thus, an RSU signature consists of three parts: proof of knowledge (pok), event id, and link tag. The pok is a proof that the signature on the message M is legitimate. The event id is a fixed-size bit string derived by a secure cryptographic hash function on an event (i.e., a period of time). The link tag is generated based on the event id and the private key of an RSU. When an event expires, all RSUs in the system simultaneously compute a new event id and link tag for the next event (next period of time). With time variant link tags, the RSU signatures can meet the temporarily linkable requirement. An intuitive way to generate authorized messages for vehicles is that an RSU periodically broadcasts authorized time stamps to the vehicles in its vicinity. This method is simple but not secure. Since a time stamp is not specially generated for a particular vehicle, any other vehicle getting such a time stamp by eavesdropping on the wireless channels can claim its presence at this RSU even though it has never been there at that time. Therefore, time stamps should be generated for individual vehicles. In Footprint, when a vehicle vi approaches an RSU Rk, it demands a time stamp from Rk, using a jth temporarily generated key pair $(K_{v_{i,j}}^{pub},K_{v_{i,j}}^{pri})(K_{v_{i,j}}^{pub},K_{v_{i,j}}^{pri})$ (vi can generate a set of temporary key pairs in advance).

Message Verification

As the proof that a vehicle v_i was present near certain RSU R_k at certain time, an authorized message issued for v_i can be verified by any entity (e.g., a vehicle or an RSU) in the system.

In the case that an entity needs to verify v_i, v_i will sign on an authorized message M, $S_{R_k}S_{R_k}$(M) generated by RSU R_k using $K_{R_k}^{pri}K_{R_k}^{pri}$ and then send $L_{R_k}L_{R_k}$= M||$S_{R_k}S_{R_k}$(M)||$S_{v_{i,j}}^{pri}S_{v_{i,j}}^{pri}$(M|| $S_{R_k}S_{R_k}$(M) to the entity. The message verification process consists of two steps:

1. Ownership verification: The entity first takes $K_{v_{i,j}}^{pub}K_{v_{i,j}}^{pub}$from M, checking whether $V_{K_{v_{i,j}}^{pub}}(S_{K_{v_{i,j}}^{pri}}$ $V_{K_{v_{i,j}}^{pub}}(S_{K_{v_{i,j}}^{pri}}$(M, $S_{R_k}S_{R_k}$(M)))=M||$S_{R_k}S_{R_k}$(M).

2. Legitimacy verification: If the authorized message passes the ownership verification, the entity further examines whether the signature contained in the authorized message is signed by a legitimate RSU.

Sybil Attack Detection

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

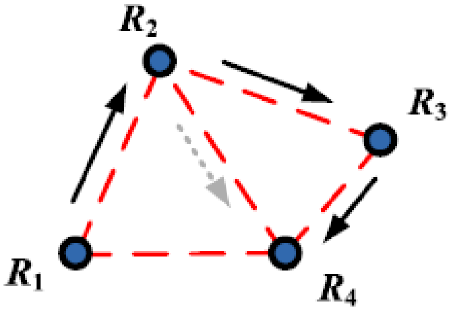

Fig.2 RSU relationship and Sybil trajectory generation.

Problem Definition

Recall that, in Footprint, vehicles have widefreedom to create their trajectories. For example, a vehicle is allowed to request multiple authorized messages from an RSU using different temporary key pairs. Thus, a vehicle can use different authorized messages for different conversations.

We define the Sybil attack detection problem as: Given a set of trajectory- embedded authorized messages within an event, how can the conversation holder recognize real vehicles and Sybil ones The online Sybil attack problem is hard due to three following factors:

First, authorized messages generated vehicles are asynchronous. The asynchrony of messages makes the judgment directly based on this fact impractical. Second, authorized messages are temporarily linkable, which means there is no invariable between an RSU signature and the real RSU who signed this signature.

For example, in Fig.an attacker can legally generate multiple trajectories which appear different from each other even under a very simple RSU topology. Assume the real path of the attacker is {R_1,$R_{2,}$$R_{3,}$$R_4$} (indicated by solid arrows). It can start a new trajectory at any RSU by using a different temporary key pair. Therefore, besidesthe trajectory{R_1,$R_{2,}$$R_{3,}$$R_4$},trajectories like {$R_1$,$R_2$,$R_3$},{$R_{2,}$$R_{3,}$$R_4$},{$R_{1,}$$R_2$},{$R_{2,}$$R_3$},{$R_{3,}$$R_4$},{$R_1$}{$R_2$},{$R_3$}and{$R_4$} are all legitimate.

Fig 3. Checking for distinct trajectories by using a check window

CONCLUSIONS AND FUTIRE WORK

In this, we have developed a detection scheme F for urban vehicular networks. Consecutive authorized messages obtained by an anonymous vehicle from RSUs form a trajectory to identify the corresponding vehicle. With the proposed detection mechanism having much space to extend, we will continue to work on several directions. First, in Footprint, we assume that all RSUs are trustworthy. However, if an RSU is compromised, it can help a malicious vehicle 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 future work, 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. Second, 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.

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, Sept. 2010. | 2. Rech, Bernd: “SIM-TD - Sichere Intelligente Mobilität Testfeld Deutschland” in: Verkehrsmanagement German Federal Ministry of Economics and Technologie, Halle 2008 | 3. R. Lu, X. Lin, H. Zhu, and X. Shen, “An Intelligent Secure and Privacy-Preserving Parking Scheme through Vehicular Communications,” IEEE Trans. Vehicular Technology, July 2010. |