International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.3, Issue.2, March-April. 2013 pp-1157-1160 ISSN: 2249-6645

A Route map for Detecting Sybil Attacks in Urban Vehicular Networks

V. Geetha Devi, [1] P.Shakeel Ahmed, [2] P.Babu, [3]
V. Hemanth Kumar Raju[4]
[1]*M. Tech (CSE), QCET, NELLORE*
[23]*Associate Professor, CSE, QCET, NELLORE*
[4]*Assistant Professor, CSE, NEC, GUDUR*

Abstract: *Security is important for many sensor network applications. A particularly harmful attack against sensor and ad hoc networks is known as the Sybil attack, where a node illegitimately claims multiple identities. In urban vehicular networks, the location privacy of anonymous vehicles is highly concerned and anonymous verification of vehicles is indispensable. Consequently, an attacker who succeeds in forging multiple hostile identifies can easily launch a Sybil attack, gaining excessively large influence. In Vehicular Ad Hoc Networks (VANETs), the vehicular scenario requires smart signaling, smart road maintenance and other services. A brand new security issue is that the semi-trusted Road Side Units (RSUs) may be compromised. The objective of our work is to propose a Threshold ElGamal system based key management scheme for safeguarding VANET from the compromised RSUs and their collusion with the malicious vehicles. By analyzing the packet loss tolerance for security performance demonstration, followed by a discussion on the threshold our method can promote security with low overhead in Emergency Braking Notification and does not increase overhead in and Decentralized Floating Car Data during security promotion.*

Index Terms: *Sybil attack, location privacy, urban vehicular networks, location-hidden trajectory, Signal Strength Distribution, Security*

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 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 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 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.

The 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.

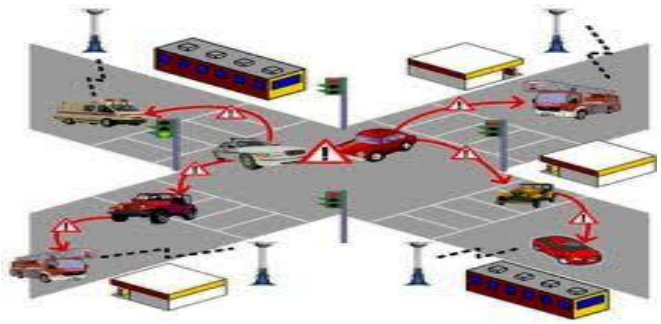

Fig. 1: Vehicular networks

II. Related Work

While it was first described and formalized by Douceur, 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 Douceur's approach, 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 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. 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, Bouassida 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 practice, the complicated outdoor environments can dramatically affect the wireless signal propagation so that RSSI measurements are highly time variant even measured at the same location. Xiao 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 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 enter. 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.

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. 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. 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.

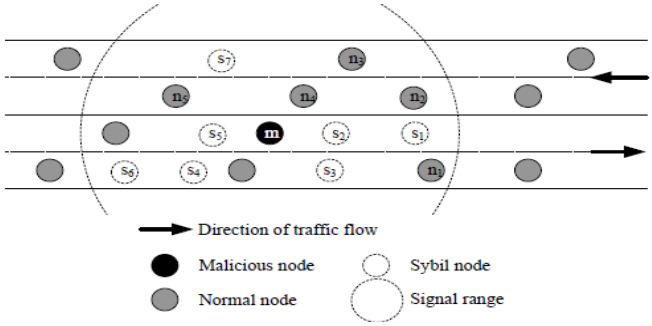

Fig 2: An example VANET under Sybil attacks

III. Models and Design Goals

3.1. System Model and Assumptions

In vehicular networks, a moving vehicle can communicate with other neighboring vehicles or RSUs via inter vehicle communications and roadside-to-vehicle communications. The architecture of the system model, which consists of three interactive components:

- RSU can be deployed at intersections or any area of interest. A typical RSU also functions as a wireless AP which provides wireless access to users within its coverage. RSUs are interconnected (e.g., by a dedicated network or through the Internet via cheap ADSL connections) forming a RSU backbone network.
- On board units (OBUs) are installed on vehicles. A typical OBU can equip with a cheap GPS receiver and a short-range wireless communication module. A vehicle equipped with an OBU can communicate with an RSU or with other vehicles in vicinity via wireless connections.
- Trust authority is responsible for the system initialization and RSU management. The TA is also connected to the RSU backbone network. Note that the TA does not serve vehicles for any certification purpose in Footprint. A vehicle can claim as many arbitrary identities as it needs.

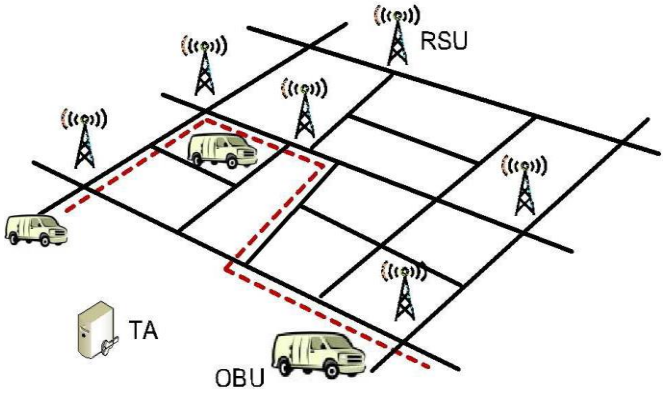

Fig 3: An Illustration of the System Model, Where the Dash Line Indicates the Travel Route of a Vehicle. as the Vehicle Traverses the Area, It Will Encounter Multiple RSUs, Typically Deployed at Intersections.

3.2. ATTACKS

In order to launch a Sybil attack, a malicious vehicle must try to present multiple distinct identities. This can be achieved by either generating legal identities or by impersonating other normal vehicles. With the following capabilities, an attacker may succeed to launch a Sybil attack in vehicular networks:

Heterogeneous configuration: malicious vehicles can have more communication and computation resources than honest vehicles. For example, a malicious vehicle can mount multiple wireless cards, physically representing different communication entities. Furthermore, having more powerful resources can also fail those resource testing schemes for detecting Sybil attacks.

Message manipulation: due to the nature of open wireless channels, the attacker can eavesdrop on nearby communications of other parties. Thus, it is possible that the attacker gets and interpolates critical information needed to impersonate others.

3.3. DESIGN GOALS

The design of a Sybil attack detection scheme in urban vehicular networks should achieve three goals:

1. Location privacy preservation— a particular vehicle would not like to expose its location information to other vehicles and RSUs as well since such information can be confidential. The detection scheme should prevent the location information of vehicles from being leaked.
2. Online detection— when a Sybil attack is launched, the detection scheme should react before the attack has terminated. Otherwise, the attacker could already achieve its purpose.
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.

IV. Generating Location-Hidden Trajectory

4.1 Location Hidden Authorized Message Generation

In order to be location hidden, authorized messages issued for vehicles from an RSU should possess two properties. 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.

4.2. 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. With submitted messages, the conversation holder verifies each trajectory and refuses those vehicles that fail the message verification. After that, the conversation holder conducts online Sybil attack detection before further proceeding with the conversation.

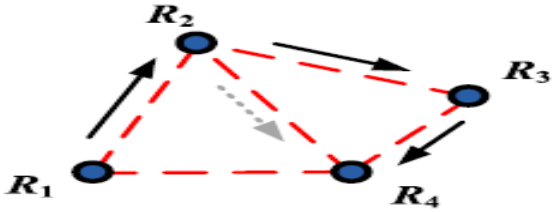

Fig. 4: RSU Neighboring Relationship and the Freedom of Trajectory Generation can Facilitate Sybil Trajectory Generation. In the Above Figure, Neighboring RSUs (Denoted by Dots) are connected with Dash Line. The Solid Arrows Indicate the Actual Sequence of RSUs a Malicious Meet and the Dash Arrow Presents a Possible Forged Trajectory.

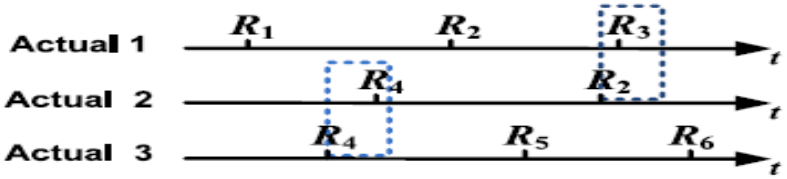

Fig 5: Checking for distinct trajectories by using a check window (denoted as the box of dotted line) and counting the total number of different RSUs contained in a pair of trajectories.

V. Proposed Work

Considering the scenario where a small fraction of RSUs are compromised and developing cost-efficient techniques to fast detect the corruption of an RSU. Here we delve into designing better linkable signer ambiguous signature schemes such that the computation overhead for signature verification and the communication overhead can be reduced. A brand new security issue is that the semi trusted Road Side Units (RSUs) may be compromised by providing a Threshold ElGamal system based key management scheme for safeguarding VANET from the compromised RSUs and their collusion with the malicious vehicles.

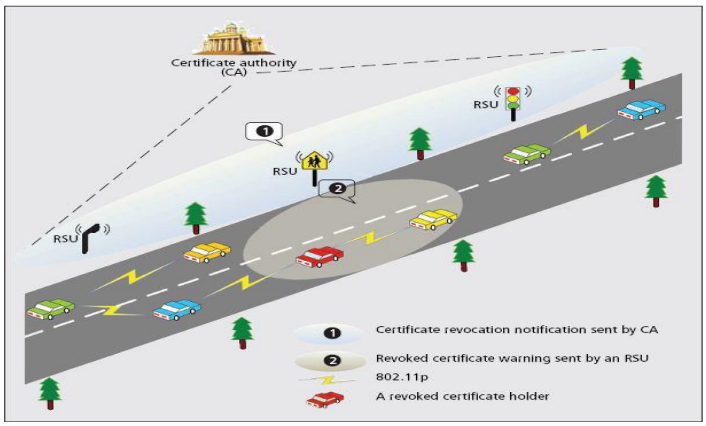

Fig 6: Security Architecture

VI. Conclusion

Secure routing in VANET have been emerging as a cornerstone of Intelligent Transportation Systems (ITSs), contributing to safer and more efficient roads by providing timely information to drivers and concerned authorities. Consecutive authorized messages obtained by an anonymous vehicle from RSUs form a trajectory to identify the corresponding vehicle. Location privacy of vehicles is preserved by realizing a location-hidden signature scheme. Utilizing social relationship among trajectories, Footprint can find and eliminate Sybil trajectories. The Footprint design can be incrementally implemented in a large city.

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] 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.
[5] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," Proc. Int'l Symp. Information Processing in Sensor Networks (IPSN '04), pp. 259-268, Apr. 2004.