Detection of Sybil Attack in City Environment Vehicular Ad Hoc Network

TARUN BANDIL

PG Scholar, Dept of CSE, Galgotias University, India, Email: tarun.bandil4@gmail.com.

Abstract: Malicious vehicle can easily obtain messages between two other communicating entities by eavesdropping on the wireless channel. If malicious vehicle can succeed in using authorized message issued for other vehicle it can masquerade as multiple identities launching a Sybil attack. The goal of detecting Sybil attacks is to ensure that each physical node is bound with only one legal identity. In the Location Hidden Authorized Message Generation Scheme, the Road Side Unit (RSU) is compromised by forged vehicle and also it is not trustworthy. Footprint cannot detect such trajectories. Assume the scenario where a small fraction of RSUs are compromised. The cost-efficient techniques are used to fast detect the corruption of the RSU and the better Linkable Signer-Ambiguous Signature Schemes used to reduce the computation overhead for signature verification and the communication overhead. The threshold ElGamal system based key management Scheme for safeguarding Vehicular Ad-hoc Networks (VANETs) from the compromised RSUs and their collusion with the malicious vehicle.

Keywords: Vehicular Ad Hoc Networks(VANETS), Sybil Attack, Road Side Unit, Location Hidden Trajectory.

I. INTRODUCTION

Now a day wireless communication is one of most vibrant areas in the communication. In wireless computer networks, the ad - hoc network is a method for wireless devices to instantly communicate with each other. Operating in ad-hoc mode allows all wireless devices within range of each other to discover and communicate in peer-to-peer manner without using central access points. The advantage of ad-hoc network are no infrastructure, every computer or device (node) is a router as well as end host nodes are in general autonomous, mobility were dynamic topology, limited energy and computing resources. Vehicular Ad-hoc Networks(VANETs) are expected to implement a variety of wireless technologies such as Dedicated Short Range Communications (DSRC) which is a type of Wi-Fi. Future applications could call for cruise control, making automatic adjustments to keep safe distances between vehicles or alerting the driver of emergency vehicles in the country. Regarding the coverage range of broadcasting a message in VANET, we ask to make sure that the vehicle which is transmitting a message is not a selfish or malicious vehicle.

II. VANETS CHARACTERISTICS

Although VANETs are considered to be a special implementation of Mobile Ad-hoc Networks (MANETs), they have a number of distinctive characteristics that need to be considered when designing them. Those characteristics might be summarized as:

A. Nature of communication

VANETs are based on short-ranged wireless ad-hoc communication, i.e., node-to-node communication, where nodes establish connections with each other to exchange information. This topology is called Ad-Hoc network. However, VANETs can be centralized where a single authority such as a Road Side Unit (RSU) has higher level of control. Communication can take the form of V2V or V2I. Nodes can either act as a host requesting data or a router distributing data. This nature of communication raises many security issues that represent challenges in VANETs.

B. Dynamic nature and Mobility

In VANETs, nodes are constantly changing their locations with different speeds and directions (except RSUs), which make the network very dynamic in nature. A group can rapidly change its structure if a node (vehicle) leaves the group or another joins it. Therefore, establishing security protocols for a group of nodes or even guarantee successful communication is a challenge.

C. Frequent information exchange

In VANETs, nodes are always on the move; hence, information about location, speed, direction, etc., changes frequently. Thus, it is expected that the nodes are continuously exchanging information.

D. Real-time processing

Due to the extremely dynamic nature of nodes in VANETs, information should be processed in real-time to benefit from it. Safety applications such as collision prevention need real-time alerts.

E. Wireless nature

VANETs are completely based on a wireless environment. Nodes are not connected by any sort of physical media. This
raises some security problems in managing VANETs communications.

F. High volatility

In VANETs, nodes are only in range of communication for short periods of time. VANETs can provide communication over 5 to 10 Km, this requires data to be rapidly processed and exchanged.

G. Position detection:

Vehicle position is one of the most valuable pieces of information in VANETs. Vehicle safety applications necessitate that each network device periodically broadcast position reports. A malicious insider generating false beacons whose digital signature is verifiable can cause serious casualty, given the need to locate the transmitter of false reports.

III. OVERVIEW

Sybil attacks detection in city environment vehicular ad hoc networks; however, it’s very difficult. First, Vehicles are authorless. On that point no links of trust, linking claimed recognitions to pure vehicles. Second, Location privacy of vehicles is of big worry. Information about vehicle location can be very latent (e.g. it can be inferred that the vehicle is parked at a mall). It is inhibiting 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, transmissions among the vehicles are too short due to high mobility. A moving vehicle can have only few seconds to transmit data to another vehicle. It is very hard to establish certain trustworthiness among communicating vehicles in such a little time. It makes easy for a malicious vehicle to produce an adversary identity. Short conversation among vehicles call for online detection of Sybil attacks. The detection plan fails if a Sybil attack is observed after the attack has stopped. To alienate the risk of Sybil attacks, It is straight forward to explicitly hold a distinct authorized identity to each vehicle so that each participating vehicle can represent itself only in one case during all communications. Using explicit identities of vehicles causes the potential to completely avoid Sybil attacks, but violates the anonymity concern in city environment vehicular ad hoc networks. As an alternative strategy, resource testing can be directed to differentiate between malicious vehicles and normal vehicles. Where the assessment is established whether a number of identities possess fewer resources than would be required if they were discrete.

IV. PROPOSED SYSTEM

Location-hidden authorized message generation plan. First, The RSU location information is hidden from the resulted authorized message because RSU signatures on message are signer obscure. Second, two authorized messages signed by same RSU in the given time period that are recognizable so it can be used for identification.

A. Certificate authorities

Certificate Authorities (CA) are called CA. They are liable for administrate department in VANET. They contain all the secrets and have liabilities to solve contention. The authority holds the management and recovering. The authority owns the highest protection level. We assume it cannot be compromised.

B. Distributed road side units (DRSUs)

Distributed Road Side Units (DRSUs) are a set of RSUs. RSUs are the key of the authority and disseminate at the road sides. They are utilized to distribute key and storage data from vehicles. In VANET there is a bottleneck problem of RSU. If RSU is compromised, the data cannot be transformed successfully within the coverage area, particularly as the message is significant and has higher security requirements. For the medium protection level, the DRSUs group is semi-trusted. An RSU can be a comparatively simple and powerful device.

C. On board units:

The ordinary vehicles on the road those are efficient to intercommunicate with another vehicle on the road through wireless communication. OUBs are installed on the vehicle. It has the lowest protection level. Because RSU may be compromised, our proposal is to get the power of anti-RSU compromised by a malicious object if any.

D. Key management scheme:

Inception ElGamal system-based key management plan, we cannot find the original plaintext with the help of RSUs whose number is smaller than the threshold value. Inception cryptography achieves the protection necessity as in strict confidence and against Sybil attackers. It also offers availability and data integrity in an adversary environment and can also appoint verification to the correct data sharing. Without disclosing the private key all these can be achieved. Updating the key frequently and successive communication with CA is not necessary. In VANET, It’s very useful for saving energy.

V. SIMULATION AND RESULTS

We will assume the scenario where a little portion of RSUs are compromised. We will develop a technique to quick discover the corruption of an RSU. In this paper simulation is performed on network simulator tool and calculates the packet delivery ratio and average end-to-end delay which is shown in the fig.

Fig1. Packet Delivery Ratio.
VI. CONCLUSIONS
In this paper, we proposed a Threshold Elgamal based key management strategy for security against compromised in city environment of vehicular ad hoc network. The secret key is split into various parts and given out to each RSU in one DSRUs group.

VII. REFERENCES