Privacy-preserving Secure Relative Localization in Vehicular Networks

Lei Tang, Xiaoyan Hong, and Phillip G. Bradford

Department of Computer Science, The University of Alabama,
Box 870290, Tuscaloosa, AL 35487-0290
{ltang,hxy,pgb}@cs.ua.edu

Abstract. Relative location information helps build vehicle topology maps. Such maps provide location information of nearby vehicles to drivers. In building a vehicle topology, one must consider various attacks on vehicular networks. Also the localization system should protect the drivers' identity privacy and make it difficult for the adversary to track vehicles. Many techniques have been proposed for relative positioning and location verification. Due to the high speed and the strict security requirements, the existing relative positioning and location verification techniques are not directly applicable to vehicular networks. Hence we present a scheme called *P-SRLD* [1], which securely determines the relative locations of a set of wirelessly connected vehicles based on the relative locations of each vehicle's surrounding vehicles. *P-SRLD* uses cryptographic keys to authenticate location messages and uses a vehicle's cryptographic pseudonym to identify the vehicle to protect drivers' privacy. To defend against Sybil attacks, *P-SRLD* employs registration and relative location message verification mechanisms. It defends wormhole and black hole attacks by probabilistically monitoring losses of relative location messages. Analysis and simulation results show that *P-SRLD* is lightweight and is resilient to Sybil, wormhole and some other attacks.

Key words: vehicle relative localization, privacy, security, vehicular networks

1 Introduction

Vehicle collision is the most common cause of injuries and fatalities in crashes as reported in the fatality analysis report [1] by National Highway Traffic Safety Administration. With the development of the vehicular networks, one goal is to improve the safety of driving. Research and development has explored the use of global location information in navigation, in services, and message delivery through building network topologies. In all these cases, location information is very useful. In this paper, we propose an alternative approach that does not need

[1] Part of this paper was presented on 2nd International Conference on Mobile Ad-hoc and Sensor Networks, volume 4325, page 543-554, Hong Kong, China, December 2006.

detailed global location information but only relative vehicle location information. To justify the importance of such an approach, we first emphasize that aided by an accurate view of the relative locations of vehicles nearby, a driver will be able to discover nearby vehicles, including those at blind spots and avoiding accidents during lane changes and merges. Furthermore, in vehicular ad-hoc networks or VANETs in short, nodes' relative location information can be used to identify the relative location of a message source. So a driver can tell the relative position of the vehicle that is sending a passing/decelerating message and take corresponding maneuver to prevent accidents. Also without revealing a vehicle's location, the node obtains additional protection for location privacy.

Motivated by relative location methods, we consider the vulnerability to malicious attacks in the vehicular networks. As recognized that location information is life-critical, using the location and relative location must be able to defend malicious attacks such as Sybil [19] and wormhole attacks [12]. To make sure that the location information is not forged or altered by malicious nodes, we need to determine the nodes' location and verify the authenticity of their location claims in presence of malicious nodes.

The vehicles' relative locations can be computed from their accurate global locations, which can be obtained by using GPS-based techniques. But since a GPS satellite simulator is able to generate fake GPS signals that flood the real GPS signals [7], GPS-based solutions are not secure in vehicular networks without authenticating GPS signals. In addition, using vehicles' precise locations to compute their relative locations may raise privacy concern of the drivers who are unwilling to expose their precise locations.

Location privacy is very important and some schemes [24, 10, 11] have been presented to protect the vehicle location privacy and communication privacy. An adversary could illegally track a specific vehicle if the localization system exposes a vehicle's identity. Using a non-changing pseudonym as vehicle identity does not solve the problem since the non-changing pseudonym still provides a way to track a vehicle. Ideally, a driver should be able to know the relative locations of nearby vehicles, but all vehicles should not let other vehicles to know their identity (e.g. license plate number, vehicle owner, and etc.) with the only exception that a driver can see the license plate of another vehicle. Hence, we design our system in a way that a vehicle is represented by its cryptographic pseudonym that changes every time, thereby making the adversary difficult to obtain vehicle identities and correlate a vehicle's relative location to its identity.

Many non-GPS based positioning and distance estimation techniques have been proposed [15, 26, 6, 2, 3, 20, 8] to determine the relative locations of nodes. However, since vehicles are moving at high speeds, all of the above mentioned positioning techniques except [15] are not directly applicable for vehicular networks. Indeed, most of this work is designed for deployment in buildings. Furthermore, these techniques assume that all nodes are cooperative. Hence these techniques are vulnerable to various attacks.

Methods for authenticating nodes' location claims in a hostile environment have been proposed in [5, 25, 9, 7]. They can be classified into two types. One

type exploits the properties of radio and sound wave and multilateration techniques [5, 25, 7, 17]. The other uses cryptographic keys to authenticate location information [16]. The techniques using multilateration may be impractical for vehicular networks because most of time the number of nodes in the proximity is too few to perform multilateration. And the techniques using ultrasonic sound may be inaccurate since the vehicles are moving in a speed about 1/10 of the speed of sound waves.

Therefore, in this article, we propose a scheme to securely determine the nodes' relative locations in the vehicular network, named *Privacy-preserving Secure Relative Location Determination* (*P-SRLD*). *P-SRLD* is distinguished from existing relative positioning schemes in that it does not require GPS or other location information but only the relative locations of each vehicle's surrounding vehicles. Essentially, with the technique introduced in the article, every node is able to construct an image of the relative locations of a set of nearby nodes that are wirelessly connected.

P-SRLD uses cryptographic keys to authenticate location messages and uses cryptographic pseudonyms as vehicle identifiers to protect the drivers' privacy and make it difficult for the adversary to track a vehicle. To defend against Sybil attacks, it employs a registration and relative location message verification mechanism. To defend wormhole and blackhole attacks, we design a mechanism that probabilistically monitors the losses of relative location messages. We also analyzes how *P-SRLD* defends the replay and denial-of-service attacks.

The rest of the article is organized as follows. Section 2 introduces the existing relative positioning, location verification and location privacy protection techniques. Section 3 describes the system model and the problem statement. Section 4 presents the design of *P-SRLD* scheme and section 5 analyzes the resilience of *P-SRLD* against Sybil, wormhole, black hole, replay, denial-of-service attacks and the privacy protections provided by *P-SRLD*. The performance of *P-SRLD* is simulated in section 6. Finally, we conclude in section 7.

2 Previous Work

Security and privacy are two important issues in vehicular networks. In [24, 10, 11], various schemes protecting vehicle location privacy and communication privacy are discussed. Securely determining nodes' relative locations include determining relative locations and verifying the authenticity of relative locations in presence of malicious nodes. The first problem is referred as relative positioning problem and the second problem is referred as relative position verification problem.

2.1 Relative Positioning Techniques

The nodes' accurate positions obtained using GPS devices can be used to compute their relative locations of nodes. V. Kukshya et al. [15] presented a technique to estimate the relative locations of neighboring vehicles based on the exchange

of their individual GPS coordinates. And it uses a trilateration technique to estimate relative locations during GPS outages. The relative positioning solution in [15] requires vehicles to cooperate and does not consider security issues so it is vulnerable to various types of attacks. Moreover, GPS devices can be spoofed by GPS satellite simulators [7] , which generate fake GPS signals that overcome the real GPS signals [27].

There are a number of relative positioning techniques [6, 20, 2] that exploit radio beacons or ultrasonic pulses to infer proximity to a collection of reference points with known coordinates. However, due to the fact that vehicles may move at a speed of 1/10 of the sound wave speed (about 331 m/s), the above mentioned positioning techniques may be inaccurate in vehicular network scenario.

Furthermore, there are some IEEE 802.11 wireless network based positioning techniques [3, 8], which learn the location of wireless devices by studying the radio signal property observed at base stations.

2.2 Position Verification Techniques

Positioning techniques introduced in 2.1 are vulnerable to malicious attacks. For instance, attackers may give false positions. Many techniques have been proposed to verify positions and to prevent malicious attacks. They can be classified into two types. One type exploits the properties of radio and sound wave and multilateration technique [5, 25, 7, 17]. The other uses cryptographic keys to authenticate location information [16]. We summarize some of them below.

S.Brands and D. Chaum presented a protocol to determine an upper-bound on the distance between the verifier and the prover [5]. D. Liu et al. presented two attack-resistant location estimation techniques [17] provided that the benign beacon signals account for the majority. L. Lazos et al. [16] proposed a secure localization scheme (SeRLoc) for wireless sensor networks based on directional antennas.

However, the above-mentioned location verification techniques are not directly applicable to the vehicle networks. First, the multilateration techniques are not suitable for vehicular network because often the number of nodes in the proximity is too few to perform multilateration. And directional antennas are not efficient when used on the linear topology of vehicular networks.

2.3 Privacy Protection Techniques

K. Sampigethaya *et al.* [24] proposed a scheme that exploits silent period and mobility group to protect vehicle location privacy. Through extending silent periods, a vehicle is "hidden" among its neighboring vehicles.

J. Freudiger *et al.* [10] proposed using vehicular mix-zones to protect vehicles location privacy. Their approach exploits road intersections and vehicle mobility diversity to defend location tracking adversarial attacks.

In [11], J. Guo *et al.* presented a group signature based privacy-preserving VANET communication scheme. Based on the feature of the group signature

scheme that the signatures are verifiable using the group public key but are not traceable to the signers, their scheme protects the privacy of the message signer. Compared with [11], a vehicle in *P-SRLD* does not carry a large number of cryptographic keys. Instead, a vehicle receives a public key from the transportation authority upon entering VANET and uses it to secure and anonymize the communication between the vehicle and the transportation authority.

3 System Model

3.1 System Architecture

Our system consists of road-side access points (APs), Department of Motor Vehicle (DMV) server, and wireless communication enabled vehicles. The APs are able to connect to DMV server through wired Internet to verify vehicles. Also they collectively provide a wireless radio that covers the entire road. Vehicles carry public keys of Certification Authority (CA) to verify CA signatures of APs. Fig. 1 depicts such architecture.

3.2 Problem Statement and Assumptions

First of all, the notations and terminologies used in this article are defined as follows.

- PK_v: public key of vehicle v;
- SK_v: private key of vehicle v;
- LP_v: license plate of vehicle v;
- N: the number of wirelessly connected vehicles;
- T_v: authentication ticket vehicle v;
- $E_k(.)$: encryption operation using key k;
- $E_k^{-1}(.)$: decryption operation using key k;
- $a||b$: b is concatenated to a;
- R: registration interval;
- I: location beacon interval;
- RLT_i: relative location table of a vehicle i;
- RL_i: relative location of a vehicle i;
- ψ_i: cryptographic pseudonym of a vehicle i;

In our adversarial model, we assume that DMV can be trusted whereas roadside APs and vehicles may be compromised by the adversary. In this article, when we use the term *node*, we mean a vehicle in the network.

We study the problem of determining the vehicles' relative locations with the following design goals: 1) resistant to fake location claims; 2) decentralized relative location determination, meaning that each node computes its own image of the network topology and the images may vary due to the varying arrival times of location beacon messages; 3)protect vehicle identity and location privacy so that the adversary is unable to track a vehicle.

We list next the assumptions in our relative location determination protocol. These assumptions follow the common practices of the contemporary public key infrastructure. Moreover, we focus on determining the relative location among a set of vehicles that are wirelessly connected.

1. Vehicles are able to verify the Certification Authority (CA) certificates of the roadside APs (*Access Points*). And the communications between the nodes and the roadside APs are encrypted using asymmetric cryptography.
2. We use RSA public-key cryptography [23]. And we assume a vehicle's public key is uniquely linked to its license plate, which is verifiable at transportation authorities (e.g. DMV (Department of Motor Vehicle) in USA).

Assumption 1 can be implemented by using the authentication and key exchange mechanism of *Transport Layer Security*(TLS) scheme [4], through which a node can both verify that the AP is not spoofed by malicious attackers and negotiate an asymmetric cryptographic key.

For assumption 2, we follow earlier work [14] that the public keys and license plates of vehicles are registered and verifiable at transportation authorities.

3.3 System Overview

A vehicle v stores the relative locations of the other vehicles in a table called *Relative Location Table* (RLT). An entry i in RLT is of the following format.

$$\{RL_i, \psi_i, TS_i\}$$

ψ_i denotes the pseudonym of a vehicle i whose relative location has been verified. RL_i specifies the relative location of i. The TS_i field records the most recent timestamp of the relative location beacon message received from i. Every I seconds, a vehicle disseminates the relative location information of its surrounding vehicles to other vehicles using relative location beacon message B. And a vehicle also re-calculate its RLT every I seconds. Since the vehicular network safe message sending interval is usually on the order of hundredths of millisecs [24], we set I as 800 ms.

In our scheme, we use time-varying cryptographic pseudonyms to identify a vehicle rather than using its license plate number. Using a vehicle's license plate number as the vehicle identifier will expose the license plate numbers of the vehicles on the road, which may raise privacy concerns. Using pseudonyms has the advantage of not revealing vehicle identity information to other drivers on the road. And it is hard for the adversary to link a vehicle's ever-changing cryptographic pseudonyms to the vehicle due to the lack of decryption key.

In next section, we introduce how to construct RLT through *P-SRLD* protocol.

4 Design of the *P-SRLD* Protocol

Fig. 2 illustrates a vehicular network comprising multiple lanes. The rationale of *P-SRLD* scheme is to construct a topology graph showing the relative locations

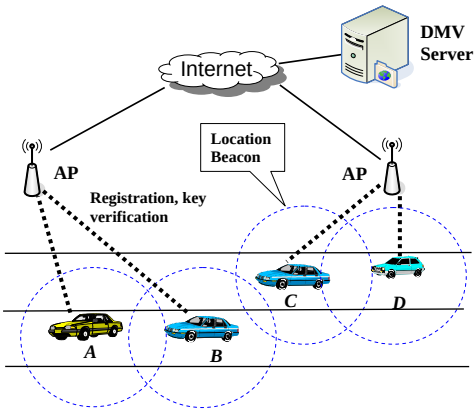


Fig. 1. System Architecture

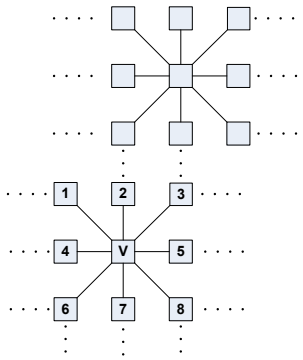


Fig. 2. Relative Locations Graph

of vehicles within a few radio hops by using the relative location information of each vehicle's surrounding vehicles. Usually, a driver does not need to know the relative locations of the vehicles faraway. Also the practice of only calculating relative locations of the vehicles in proximity reduces message overheads and improves *RLT* calculation speed. So the system administrator could configure the TTL(time to live) parameter of the location beacon messages according to vehicular network density. For instance, in busy city traffic conditions, TTL of the location beacon message can be configured as a small number (e.g. 2), which means a driver may know relative locations of the vehicles within a radius of approximately 500 meters assuming radio transmission range to be 250 meters.

To find out the relative locations of the surrounding vehicles, each vehicle will use its video sensors to read the license plates of vehicles on front left, front, front right, rear left, rear and rear right (i.e. node 1,2,3,6,7,8 in Fig. 2). And each vehicle uses directional RFID reader to read the electronic license plates of the vehicles between front left and rear left(i.e. vehicle 4 in Fig. 2) and the vehicle between front right and rear right. Intuitively, if every node in a connected graph propagates the relative locations of its surrounding nodes to other nodes, then eventually every node will be able to build a graph showing the relative locations of all nodes in the graph. Using this approach, a vehicle in *P-SRLD* constructs a topology graph showing the relative locations of the vehicles nearby. The details of an algorithm constructing *RLT* is given in section 4.2.

When nodes are on a single lane, each node only needs to propagate its predecessor and successor information instead of relative locations of all surrounding nodes. But the way of determining vehicle relative locations in multi-lane scenario is similar to the way in single-lane scenario because in both scenarios vehicle relative locations are constructed using the relative location information of each vehicle's surrounding vehicles. The only difference is that the surrounding vehicles of a vehicle in single-lane scenario are its predecessor and successor whereas a vehicle could have more surrounding vehicles in multi-lane scenario

such as the one shown in Fig. 2. The privacy-preserving and security mechanism of both scenarios are the same. Due to the above reason and the reason of reducing the formula length, we describe our scheme in a single-lane scenario.

4.1 *P-SRLD* Protocol

Through *P-SRLD* protocol, a vehicle distributedly constructs its *RLT* using the relative location beacons received from other vehicles. *P-SRLD* protocol has three main components: *Vehicle Registration*, *Vehicle Pseudonym Authentication*, and *Location Beacon Dissemination*.

First component involves DMV authentication and vehicle registration to DMV. Upon registering into a vehicular network, a vehicle v will obtain a session public key of DMV (i.e PK_{DMV}) and the DMV's signature on PK_{DMV}. To defend an adversary impersonating DMV, v verifies PK_{DMV} using CA certificate of DMV and DMV's signature on PK_{DMV}. Also, every R seconds, v sends $\{E_{PK_{DMV}}(PK_v),\ E_{SK_v}(PK_v)\}$ to DMV, which decrypts $E_{PK_{DMV}}(PK_v)$ to obtain PK_v. If DMV finds that $E^{-1}_{PK_v}(E_{SK_v}(PK_v))$ equals PK_v, DMV marks v as a registered user and updates the registration time of v in its database. The reason of requiring a vehicle v to periodically register to DMV is to make it hard for the adversary to forge non-existent vehicles. The analysis of how the registration mechanism defends malicious attacks are described in section 5.1.

Second component involves requesting and authenticating cryptographic pseudonyms from vehicles. A vehicle requests a cryptographic pseudonym from each of its surrounding vehicles and verifies the validity of these pseudonyms. The cryptographic pseudonym obtained from a vehicle x will be used to identify x during the relative location calculation process.

We now describe how a vehicle v requests and authenticates a cryptographic pseudonym from the vehicle p immediately in front of it. First v obtains p's license plate number LP_p using its front video camera. Then v requests an authentication ticket T_p from p and send T_p to a AP to authenticate T_p. The format of T_p is as follows:

$$T_p = \{\psi_p,\ TS_p,\ E_{PK_{DMV}}(LP_p||r),\ r,\ sig_p\}.$$

r is a random string and TS_p is the current time of p. $\psi_p = E_{PK_p}(LP_p||TS_p||r_p)$ and r_p is a random string known only by p. And

$$sig_p = E_{SK_p}(\psi_p||TS_p||E_{PK_{DMV}}(LP_p||r)||r).$$

T_p is sent to DMV server to verify its validity. DMV obtains LP_p by decrypting $E_{PK_{DMV}}(LP_p||r)$. Based on LP_p, DMV finds PK_p and uses PK_p to check that $E^{-1}_{PK_p}(sig_p) = \psi_p||TS_p||E_{PK_{DMV}}(LP_p||r)||r$ and the timestamp TS_p is less than I seconds old to prevent stale tickets. If T_p is valid, DMV returns $sig_{DMV}(\psi_p||TS_p) = E_{SK_{DMV}}(\psi_p||TS_p)$ to v. Similarly, v requests tickets from other surrounding vehicles and authenticate them.

Third component is about the location beacon dissemination and verification. Every I seconds, a vehicle disseminates its immediate predecessor and successor

information to other nodes using the relative location beacon message B. Suppose B is generated by a vehicle v, whose predecessor is p and successor is s. The format of B is as follows:

$$B = \{\psi_p,\ TS_p,\ \psi_v,\ TS_v,\ \psi_s,\ TS_s,\ sig_{DMV}(\psi_p||TS_p),\ sig_{DMV}(\psi_v||TS_v),\\ sig_{DMV}(\psi_s||TS_s), E_{PK_{DMV}}(LP_v||r),\ r,\ sig'\},$$

$$sig' = E_{SK_v}(\psi_p||TS_p||\psi_v||TS_v||\psi_s||TS_s||sig_{DMV}(\psi_p||TS_p)||\\ sig_{DMV}(\psi_v||TS_v)||sig_{DMV}(\psi_s||TS_s)).$$

When other nodes receive B from v, they will verify the validity of B. First of all, a receiver will request DMV to check that the signature sig' is valid. DMV will obtain LP_v by decrypting $E_{PK_{DMV}}(LP_v||r)$ and find PK_v corresponding to LP_v. Then DMV using PK_v to verify sig'. In addition, using PK_{DMV}, the receiver checks that $sig_{DMV}(\psi_p||TS_p)$, $sig_{DMV}(\psi_v||TS_v)$, and $sig_{DMV}(\psi_s||TS_s)$ are indeed the DMV's signatures on ψ_p, ψ_v, ψ_s, TS_p, TS_v, and TS_s. Lastly, the receiver verifies that TS_p, TS_v, and TS_s are less than I seconds old. If any of the above verifications fails, the receivers will ignore B. Otherwise, using the relative location information in location beacon messages received, the receiver re-calculates the relative locations of the vehicles, which are stored in its RLT.

Assuming there are N vehicles in a linear topology network and $Time_h$ is the time needed for propagating B to a one-hop neighbor and processing it, we now compute how long it takes for a location beacon message to reach all vehicles. The largest number of hops traveled by B ranges from $N-1$ to $\lceil \frac{N}{2} \rceil$. So on average the time for B to reach all vehicles is as follows:

$$Time_h \times \frac{1}{N} \times (N-1+N-2+\ldots+\frac{N}{2}+(\frac{N}{2}+1)+\ldots+N-1) = 0.75 \times N \times Time_h.$$

4.2 RLT Construction Algorithm

Now we present an algorithm to construct RLT using the relative location beacons received. RLT construction algorithm is executed by a vehicle every I seconds. The algorithm is as follows and its time complexity is $O(N^2)$.

1. From beacon messages received, search for a node h which has no predecessor. Add h to list L as list head. Make pointer P point to h.
2. Find the node s which is the successor of the node pointed by P. Then add s to list L and make pointer P point to s.
3. Continue step 2 until all nodes in the beacon messages are added to the list L. The relative location of a node i in the list L is its relative location RL_i in the RLT. After determing the relative location of i, $\{RL_i, \psi_i, TS_i\}$ is stored in RLT.

PMLD **protocol**

1. When an AP receives a predecessor/successor authentication request, it probabilistically determines if it monitors the beacon message B_{select} corresponding to this authentication request. If it determines to monitor B_{select}, it conducts the following steps to monitor which nodes faithfully forward the B_{select}.
2. Notify all APs to monitor who is forwarding B_{select} within $T_{monitor}$. Here we set $T_{monitor}$ equal to I.
3. When an AP in monitoring status receives a beacon B, it checks whether B is the same as B_{select}.
4. After $T_{monitor}$, APs know that who have forwarded B_{select} and who have not. APs then increment the *malicious value* of those nodes that did not forward B_{select}. After the *malicious value* of a node x reaches a threshold value, APs view x as a possible malicious node.

Fig. 3. *PMLD* Protocol

5 Security and Privacy Analysis

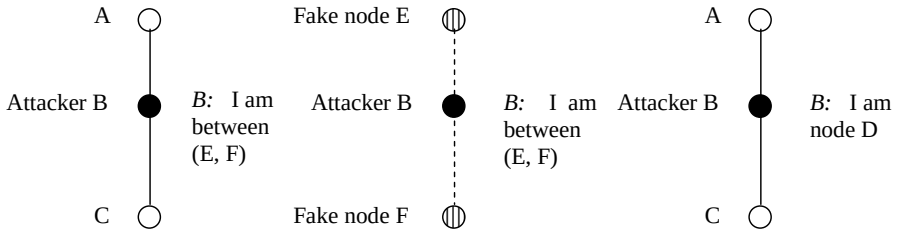
In this section, we analyze the privacy characteristics of *P-SRLD* and its resilience of to Sybil attacks, wormhole attacks, denial-of-service attacks, black hole attacks and location errors (discussed together with Sybil attacks). The goal of the *P-SRLD* protocol is to protect the location privacy of drivers and verify that the relative location information is not forged or altered by malicious nodes.

5.1 Sybil Attack

A Sybil attack occurs when a malicious node illegitimately takes on multiple identities as Sybil nodes [19]. First, malicious nodes may spoof roadside APs. Second, adversaries may lie about its relative locations (Figure 4(a)). Third, adversaries may inject relative location information of non-existent nodes (Figure 4(b)). Last, attackers may impersonate legitimate nodes (Figure 4(c)).

For the first type attacks, since nodes will first verify the CA certificate of roadside APs and the communication between roadside APs and nodes are encrypted using asymmetric cryptography, it is hard for the attackers to impersonate APs, alter message content, or fabricate messages between APs and vehicles.

For the second type of attacks, in *P-SRLD*, it is difficult for an attacker to lie about its relative locations (e.g. who are its predecessor and successor). First, the adversary will not be able to obtain a location ticket T_p from a vehicle p unless the adversary sees p's license plate. Second, the attacks by reusing the stale tickets overheard will be defended by checking whether the timestamps of the tickets have been expired. Finally, even if the adversary obtains valid location



(a) Inject wrong location info (b) Forge non-existent nodes (c) Impersonate legitimate node

Fig. 4. Attacks against relative location determination schemes

tickets from other vehicles, it is hard to inject incorrect relative location information without being discovered. This is because wrong location messages will conflict with other location announcements sent by legitimate nodes. In [22], M. Raya et al. proposed a system called LEAVE to detect and evict misbehaving vehicles. Attackers can be discovered in the situation when honest vehicles account for majority. With a mechanism similar to LEAVE, a vehicle could detect possible attackers if the location beacon messages from these vehicles conflict with the majority. When discovering possible attackers, a vehicle sends the received beacon message to AP to warn AP that the initiator of the beacon is a possible attacker. If a vehicle is warned by many vehicles as a possible attacker, its location beacon messages will be regarded as malicious by AP and hence rejected by other vehicles. In summary, every vehicle forwards the beacon messages received from possible attackers to APs, which decrypt the identities of the beacon initiators and fail the authentication of the location beacons from the attackers.

For the third type of attacks, malicious nodes are unable to insert non-existent nodes because the receivers will verify the registrations of the nodes included in the relative location beacons. Moreover, every vehicle signs on its location ticket, which is difficult to forge.

Similarly, for the fourth type of attacks, since the receiver verifies the authenticity of the location beacon signature and the signatures on cryptographic pseudonyms and corresponding timestamps, it is difficult for malicious nodes to impersonate legitimate nodes and alter the location beacon messages sent by legitimate nodes.

5.2 Wormhole Attack

Another significant attack is the wormhole attack, where malicious nodes collude to selectively discard relative location messages of legitimate nodes. Figure 5 illustrates a basic wormhole attack. The attackers control node X and Y, which are connected by a tunnel link. Relative location messages received by X are tunneled to Y and retransmitted at Y, and vice versa. By selectively discarding

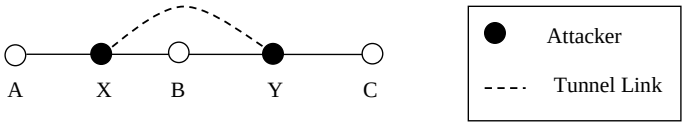


Fig. 5. An example of wormhole attack.

messages, colluding attackers may launch DoS attacks and prevent some nodes from being known to others. For instance, X and Y may only transmit relative location messages initiated by A and C while discarding all relative location messages initiated by B. Thus, other nodes will not know the presence of B.

Some countermeasures have been presented to defend the wormhole attacks [28, 12]. Y. Hu et al. proposed a MAC layer protocol named TIK [28] to restrict the packet's maximum allowed transmission distance, which prevents wormhole attacks by detecting if the packet traveled further than that is allowed. In [12], the authors presented an approach to detect wormhole attack, which depends on nodes maintaining accurate sets of their neighbors.

However, there is no solution designed specifically for defending wormhole attacks in vehicular network. Hence, we propose *Probabilistic Message Loss Detection (PMLD)* protocol, which defend wormhole attacks by probabilistically monitoring the losses of relative location messages.

$PMLD$ protocol is showed in Fig.3. In *PMLD*, we assume legitimate nodes account for majority and if a node A can hear node B then B can hear A. APs probabilistically select a beacon message B_{select} and check if there are attackers discarding the selected beacon message. Since every location beacon will be authenticated by AP, AP records the identity of a forwarder v of beacon B_{select} when v authenticates B_{select} at AP. Hence, AP knows the identities of the forwarders and malicious nodes expose themselves when they discard B_{select}. In *PMLD* protocol, monitoring is performed probabilistically so that malicious nodes will not know which messages are going to be monitored.

5.3 Black Hole Attack

An attack similar to wormhole attack is black hole attack [13], in which a malicious node behaves like a black hole and discards all or a fraction of the relative location beacons passing it. Black hole attacks may create network partition so that a vehicle is unable to know the relative location of interested vehicles due to the network partition.

Black hole attackers can be detected by neighboring nodes, which identify and put the attackers on blacklist. However, as Y. Hu et al. pointed out in [13], the above watchdog-like method [18] may enable attackers to add legitimate nodes to blacklists and interfere the normal function of legitimate nodes.

In our system, we employ *PMLD* protocol as the countermeasure of Black hole attacks. The APs identify the black hole attackers by probabilistically mon-

itoring message transmissions and fail the authentication of the location beacons from the attackers. Compared with watchdog-like method, our approach exploits the authority of APs and will not cause legitimate nodes to be blackmailed by attackers. And even if an AP is compromised, the compromised AP is unable to blackmail a legitimate vehicle since it cannot forge the legitimate vehicle's signatures.

5.4 Replay Attack and Denial-of-Sevice Attack

During replay attacks, attackers retransmit stale location messages recorded previously. In *P-SRLD*, each location message beacon message has time stamps and signatures. Hence, it is hard for attackers to inject stale location messages since they are unable to forge the signatures.

Moreover, malicious vehicles may initiate denial-of-service attacks such as constantly retransmitting stale location messages or garbage messages, the normal wireless transmission around the malicious vehicles will be severely affected due to the heavy radio collisions. Denial-of-service attacks are difficult to prevent due to the sharing nature of wireless medium. One way to resume communication in face of the denial-of-service attacks is to switch channels. Another way is to stop attacking vehicles physically. The affected drivers may record the license plates of the attacking vehicles and report their positions to law enforcement department to stop the attacking vehicles.

5.5 Privacy Analysis

Ideally, a vehicle localization system will not allow a nefarious user to violate privacy of vehicular traffic. A vehicle using this system should have the relative location information of the vehicles in proximity, but all vehicles should not let other vehicles to know their identity (e.g. license plate number, vehicle owner, and etc.). Clearly, visually, a person may see the license plate of another vehicle, but the number of license plates in sight of the adversary is limited for any time–giving a solid measure of anonymity.

First we analyze the privacy of our system if a vehicle x is compromised. A vehicle p is identified by $\psi_p = E_{PK_p}(LP_p||TS||r_p)$. The cryptographic pseudonym ψ_p changes based on time and the random r_p which is only known to p. Unless x has visually seen LP_p and requested the ψ_p from p, it will be hard for x to link ψ_p to LP_p due to the difficulty of decrypting ψ_p and the fact that ψ_p changes every time.

Next we analyze how a compromised AP, called AP_x, will affect privacy in our system. It is possible for AP_x to hear and store location tickets and location beacons. However, in all these location messages, a vehicle p's pseudonyms are encrypted and change every time. So it is difficult for AP_x to correlate ψ_p to p.

6 Evaluation

In this section, we evaluate *P-SRLD* regarding to the following two metrics.

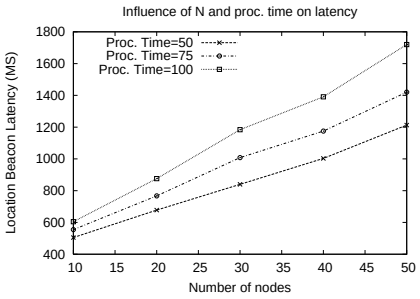


Fig. 6. Latency vs. N and processing time

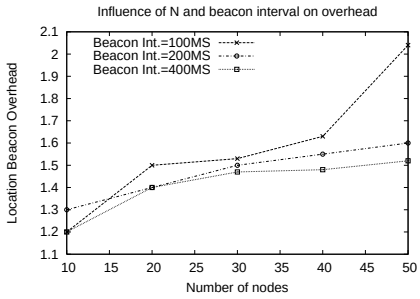


Fig. 7. Overhead vs. N and beacon int.

- *location beacon latency:* This metric measures the maximal time it takes for a location beacon message to reach all nodes.
- *location beacon overhead:* This metric measures on average how many messages are sent on each node to propagate a location beacon to all nodes.

We conduct the simulations using Qualnet Network Simulator [21]. The nodes in the network maintain linear topology with the mobility speed of the vehicles on the free way. The nodes use IEEE 802.11b radio with 2M bps data rate to communicate. When measuring *location beacon latency*, we vary N and the processing time (unit: ms) of a location beacon on each node. Fig. 6 demonstrates that the larger the processing time the larger the location beacon latency and the location beacon latency is linearly proportional to N. Moreover, we measure the influences of N and location beacon interval on *location beacon overhead*. Fig. 7 shows that when N becomes larger or when beacon interval shrinks, location beacon overhead increases due to the increase of radio collisions.

7 Conclusions and Future Plan

In this paper, we have presented *P-SRLD*, a privacy-preserving scheme for securely determining the relative locations of vehicles in vehicular networks. *P-SRLD* does not require any GPS or accurate position information but only the relative locations of each vehicle's surrounding vehicles. *P-SRLD* uses cryptographic keys to authenticate relative location messages and uses a vehicle's cryptographic pseudonym to identify the vehicle for protecting the driver's privacy. The scheme is designed to defend against Sybil attacks, wormhole attacks, black hole attacks, and replay attacks. In the future, we plan to evaluate *P-SRLD* in the multi-lane scenario.

References

[1] Fatality analysis reporting system (FARS) web-based encyclopedia. http://www-fars.nhtsa.dot.gov/.

[2] A. Ward, A. Jones, and A. Hopper. A new location technique for the active office. *IEEE Personal Communications Magazine*, 4(5):42–47, October 1997.
[3] P. Bahl and V. N. Padmanabhan. RADAR: An in-building RF-based user location and tracking system. In *IEEE Infocom 2000*, volume 2, pages 775–784, 2000.
[4] S. Blake-Wilson, M. Nystrom, D. Hopwood, J. Mikkelsen, and T. Wright. RFC 3546: Transport Layer Security (TLS) Extensions, 2003.
[5] S. Brands and D. Chaum. Distance-bounding protocols. In *EUROCRYPT '93*, pages 344–359, 1994.
[6] N. Bulusu, J. Heidemann, and D. Estrin. GPS-less low cost outdoor localization for very small devices. *IEEE Personal Communications Magazine*, 7(5):28–34, October 2000.
[7] S. Capkun and J.-P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *IEEE INFOCOM*, 2005.
[8] P. Castro, P. Chiu, T. Kremenek, and R. R. Muntz. A probabilistic room location service for wireless networked environments. In *UbiComp '01*, pages 18–34, 2001.
[9] D. Singelee, and B. Preneel. Location verification using secure distance bounding protocols. *International workshop on wireless and sensor networks security*, 2005.
[10] J. Freudiger, M. Raya, and M. Feleghhazi. Mix zones for location privacy in vehicular networks. In *WiN-ITS 07*, 2007.
[11] J. Guo, J. Baugh, and S. Wang. A group signature based secure and privacy-preserving vehicular communication framework. In *Proceedings of the Mobile Networking for Vehicular Environments (MOVE) workshop in conjunction with IEEE INFOCOM*, 2007.
[12] L. Hu and D. Evans. Using directional antennas to prevent wormhole attacks. In *Network and Distributed System Security Symposium (NDSS)*, February,2004.
[13] Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: a secure on-demand routing protocol for ad hoc networks. In *MobiCom '02*, pages 12–23, 2002.
[14] J.-P. Hubaux, S. Capkun, and J. Luo. The security and privacy of smart vehicles. *IEEE Security and Privacy*, 2(3):49–55, 2004.
[15] Kukshya, V.; Krishnan, H.; Kellum, C. Design of a system solution for relative positioning of vehicles using vehicle-to-vehicle radio communications during gps outages. *Vehicular Technology Conference 2005*, 2:1313–1317, October 2005.
[16] L. Lazos and R. Poovendran. SeRLoc: Robust localization for wireless sensor networks. *ACM Trans. Sen. Netw.*, 1(1):73–100, 2005.
[17] D. Liu, P. Ning, and W. Du. Attack-resistant location estimation in wireless sensor networks. In *IPSN '05*, pages 99–106, Los Angeles, California, USA, 2005.
[18] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *MobiCom '00*, pages 255–265, 2000.
[19] J. Newsome, R. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: Analysis and defenses. In *IPSN '04)*, Apr. 2004.
[20] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan. The cricket location-support system. In *MobiCom '00*, pages 32–43, 2000.
[21] Qualnet Network Simulator. `http://www.qualnet.com/`.
[22] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux. Eviction of misbehaving and faulty nodes in vehicular networks. *IEEE Journal on Selected Areas in Communications*, 25(8):1557–1568, 2007.
[23] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 26(1):96–99, 1983.
[24] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran. Amoeba: Robust location privacy scheme for vanet. *IEEE Journal on Selected Areas in Communications*, 25(8), 2007.

[25] N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In *WiSe '03*, pages 1–10, New York, NY, USA, 2003.

[26] Y. Shang, W. Ruml, Y. Zhang, and M. P. J. Fromherz. Localization from mere connectivity. In *MobiHoc '03*, pages 201–212, 2003.

[27] J. S. Warner and R. G. Johnston. Think GPS cargo tracking = high security? Think again. Technical report, Los Alamos National Laboratory,2003.

[28] Y. Hu, A. Perrig, and D. Johnson. A defense against wormhole attacks in wireless ad hoc networks. In *Proc. of INFOCOM 2003*, San Francisco, CA, USA, 2003.