Secure Relative Location Determination In Vehicular Network

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 is very useful in vehicular networks although it is vulnerable to various attacks. 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 *SRLD*, which securely determines the relative locations of a set of wirelessly connected vehicles based on the relative locations of each vehicle's surrounding vehicles. *SRLD* uses cryptographic keys to authenticate location messages and uses a vehicle's public key to identify the vehicle while protecting drivers' privacy. To defend against Sybil attacks, *SRLD* employs registration and ticket verification mechanisms. It defends Wormhole and black hole attacks by probabilistically monitoring losses of relative location messages. Analysis and simulation results show that *SRLD* is lightweight and is resilient to Sybil, Wormhole and some other attacks.

Key words: secure vehicular relative location, security, vehicular networks

1 Introduction

Location information is very useful in our daily life. But in many cases, we do not need detailed global location information but only relative location information. The fatality analysis report [1] by National Highway Traffic Safety Administration shows that collision with another motor vehicle is the most common harmful event for fatal and injury crashes. Aided by an accurate view of the relative locations of vehicles nearby, a driver will have better chance discovering vehicles at blind spots and avoiding accidents during lane changes and merges. Furthermore, in vehicular networks, nodes' relative location information can be used to identify the relative location of a message source so that a vehicle driver will be able to tell the relative position of the vehicle that is sending a passing/decelerating message and take corresponding maneuver to prevent the accidents.

In vehicular networks, location information is life-critical but is vulnerable to malicious attacks such as Sybil [16] and Wormhole attacks [9]. 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 [6], 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.

Many non-GPS based positioning and distance estimation techniques have been proposed [12, 22, 5, 2, 3, 18, 7] to determine the relative locations of nodes. However, due to the fact that vehicles are moving at high speed, all of the above mentioned positioning techniques except [12] are not directly applicable for vehicular networks since most of them are designed for in-building environment. Furthermore, all these techniques assume that all nodes are cooperative. Hence these techniques are vulnerable to various attacks.

To authenticate nodes' location claims and determine nodes' relative locations in a hostile environment, [4, 21, 8, 6] have been proposed. They can be classified into two types. One type exploits the properties of radio and sound wave and multilateration techniques [4, 21, 6, 14]. The other uses cryptographic keys to authenticate location information [13]. 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 wave.

Therefore, in this article, we propose a scheme to securely determine the nodes' relative locations in the vehicular network, named *Secure Relative Location Determination* (*SRLD*). *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.

SRLD uses cryptographic keys to authenticate location messages and uses a vehicle's public key for identification and privacy protection. To defend against Sybil attacks, it employs registration and ticket verification mechanism. We also design a scheme to defend against Wormhole attacks by probabilistically monitoring losses of relative location messages.

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

2 Previous Work

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. In [12], V. Kukshya et al. 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 [12] 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 [6] , which generate fake GPS signals that overcome the real GPS signals [23].

There are a number of relative positioning techniques [5, 18, 2] that exploit radio beacons or ultrasonic pulse to infer proximity to a collection of reference points with known coordinates. However, due to the fact that vehicles are moving in a speed about 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, 7], 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 [4, 21, 6, 14]. The other uses cryptographic key to authenticate location information [13]. 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 [4]. D. Liu et al. presented two attack-resistant location estimation techniques [14] provided that the benign beacon signals account for the majority. L. Lazos et al. [13] 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.

3 System Model

3.1 Problem Statement and Assumptions

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

- N: the number of vehicles in the network
- PK_v: public key of vehicle v;
- SK_v: private key of vehicle v;
- LP_v: license plate of vehicle v;
- T_v: authentication ticket vehicle v;
- R: registration interval;

We study the problem of securely determining relative locations in vehicular networks in presence of malicious nodes. Furthermore, we explore 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. Moreover, we focus on determining the relative location among a set of vehicles that are wirelessly connected.

We list next the assumptions in our relative location determination protocol. These assumptions follow the common practices of the contemporary public key infrastructure. In this article, when we use the term *node*, we mean a vehicle in the network.

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. Each vehicle has a tamper-proof electronic license plate, which can only be read by roadside APs. Every R seconds, vehicles register to the roadside APs to indicate that they are active. During registration, APs read the vehicle's electronic license plate and update its registration time.
3. A vehicle's public key [20] is uniquely linked to its license plate. And the roadside APs verify the binding between a vehicle's license plate number and its public key by accessing the interfaces provided by transportation authorities.

Assumption 1 can be implemented by adapting *Secure Socket Layer*(SSL) scheme [17], through which a node can both verify that the AP is not spoofed by malicious attackers and negotiate an asymmetric cryptographic key.

For assumption 3, we follow earlier work [11] that vehicles' public keys and license plates are registered and verifiable at transportation authorities.

3.2 System Architecture

The vehicular network consists of road-side APs and wireless communication enabled vehicles. The APs are connected through wired Internet and 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 an architecture.

Relative locations of nodes are stored in a table called *Relative Location Table* (RLT). The structure of RLT is as follows.

{Relative Location, Public Key, Seq}

In the table, the *Public Key* field records the public key of a vehicle whose link to a license plate has been proved by the APs. The *Relative Location* field specifies the relative location of that vehicle. The *Seq* field records the sequence number of the relative location beacon message received from the corresponding vehicle.

In our scheme, we use the vehicle's public key to identify the 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 public key as identifier has the advantage of not revealing the vehicle privacy information to other vehicles since the link between a vehicle's public key and its license plate number is only verifiable through the interface provided by transportation authority, which is not accessible for normal people.

There are two types of messages in the network. One is the relative location beacon messages. The other is the generic messages such as deceleration message and other general communication messages. In this article, when we use the term *message*, we mean generic message.

Given the RLT, we can determine the relative location of message source. To prevent malicious nodes from fabricating messages, every message is signed by the message source using its private key. When a vehicle receives a message, it will first locates the relative location of the message source according to the public key of the message source. Then the message receiver verifies the validity of the message source's signature using the public key of the message source stored in the RLT.

In next section, we introduce how to construct RLT through $SRLD$.

4 Design of the *SRLD* Protocol

Fig. 2 illustrates a vehicular network comprising multiple lanes. The rationale of $SRLD$ scheme is to construct a graph showing the relative locations of nodes within radio range by using the relative location information of each node's surrounding nodes. Specifically, each node will use video sensor to read the license plates of nodes 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 node uses directional RFID reader to read the electronic license plates of the nodes between front left and rear left(i.e.

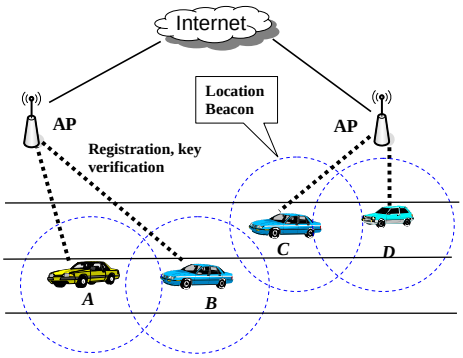


Fig. 1. System Architecture

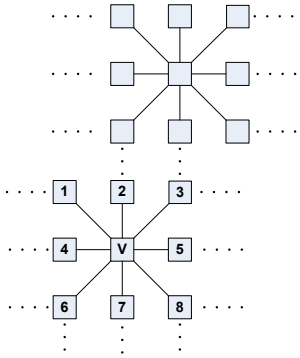


Fig. 2. Relative Locations Graph

node 4 in Fig. 2) and the nodes between front right and rear right. If every node 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 network.

When most of time all nodes are on a single lane, then each node only needs to propagate its predecessor and successor information instead of relative locations of all surrounding nodes. Due to the limit of space and the reason that the rationale of determining vehicle relative locations in multi-lane scenario is essentially the same as in single-lane scenario, we describe our scheme in a single-lane scenario.

4.1 SRLD Protocol

SRLD protocol is showed in Fig. 3. *SRLD* may work in two modes: *AP mode* and *distributed mode*, which are called *SRLD-AP* and *SRLD-D*, respectively. Their difference is as follows. In *SRLD-AP*, APs compute the *RLT* and propagate it to vehicles. In *SRLD-D*, vehicles distributedly construct *RLT* by exchanging the relative locations of each vehicle's surrounding vehicles.

In the first phase of *SRLD-AP* and *SRLD-D*, a vehicle v in the vehicular network obtains the license plate number LP_p of its immediate predecessor p using the video cameras mounted on the front of v. Then v requests an authentication tickets T_p from p and send T_p to a AP to authenticate it. The format of T_p is as follows: $T_p = \{PK_p,\ TS,\ E_{SK_p}(LP_p||TS)\}$.

When verifying the validity of T_p, AP first check the binding between LP_p and PK_p by accessing the interface provided by transportation authorities. Furthermore, AP verifies that the timestamp TS in T_p does not exceed 10 seconds to prevent stale tickets. Similarly, v requests a ticket T_s from its immediate successor and checks the validity of T_s. If working in *SRLD-AP* mode, AP will also record the predecessor and successor information of the node v when checking the tickets T_p and T_s.

The second phase of *SRLD-AP* is already showed in the Fig. 3 so we focus on introducing the second phase of *SRLD-D*, during which every vehicle instead of AP disseminates its immediate predecessor and successor information to other nodes using relative location beacon message B. Suppose B is generated by vehicle v, whose predecessor is p and successor is s. The format of B is as follows.

$$B = \{PK_p,\ PK_v,\ PK_s,\ T_p,\ T_s,\ seq,\ sig'\}$$

$$sig' = E_{SK_v}(\ H(\ \{PK_p,\ PK_v,\ PK_s,\ T_p,\ T_s,\ seq\}))$$

When other nodes receive B from v, they will verify the validity of B. First of all, receivers will check that the signature sig' is valid. Then they communicate with APs to verify the validity of the T_p and T_s and verify that the registrations of p, v and s are within R. If any of the above verifications fails, the receivers will ignore B.

We assume there are N vehicles in a linear topology network and T_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 change 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 a location change to reach all vehicles is as follows:

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

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 APs when working in *SRLD-AP* mode and is executed by individual vehicles when working in *SRLD-D* mode. 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 in the list L is its relative location in the *RLT*.

5 Security Analysis

In this section, we analyze the resilience of *SRLD* to Sybil attacks, Wormhole attacks, denial-of-service attacks and black hole attacks. The goal of the *SRLD* protocol is to verify that the relative location information is not forged or altered by malicious nodes.

SRLD **protocol**

Verification Phase:

1. Node v observes the license plate number of its immediate predecessor p and successor s: LP_p and LP_s. Then node v sends LP_p to p and requests for an authentication ticket T_p from p. Similarly node v requests an authentication ticket T_s from s.
2. Node v sends $\{LP_p, T_p\}$ and $\{LP_s, T_s\}$ to AP to authenticate p and s.

Dissemination Phase of SRLD-D:

1. After verifying p and s, v broadcasts a relative location beacon B to neighbors.
2. When a node receives B, it updates its RLT using B and broadcasts B after verifying the validity of B.

Dissemination Phase of SRLD-AP:

1. APs compute the RLT from the predecessor and successor information collected during the verification phase and disseminate $\{RLT, sig_{AP}\}$ to all nodes. And nodes verify the validity of RLT by checking the signature sig_{AP} using public key of APs.

Fig. 3. *SRLD* Protocol

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 $T_{monitor}$ as 30 seconds.
3. When an AP receives a beacon B, it checks whether B is the same as B_{select}. If B is the same as B_{select}, then AP records the identity of the forwarder of B.
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, AP informs all nodes that x is a possible malicious node.

Fig. 4. *PMLD* Protocol

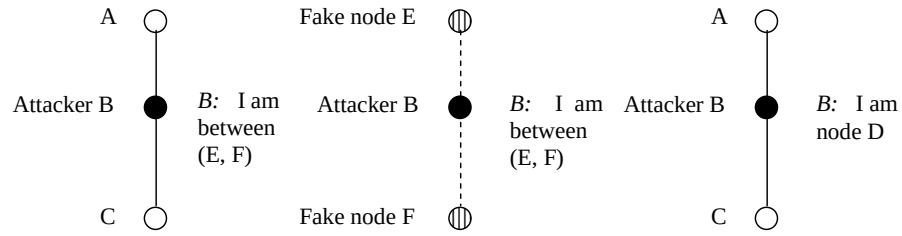
5.1 Sybil Attack

A Sybil attack occurs when a malicious node illegitimately takes on multiple identities as Sybil nodes [16]. First, malicious nodes may spoof roadside APs. Second, adversaries may lie about its predecessor and successor (Figure 5(a)). Third, adversaries may inject relative location information of non-existent nodes (Figure 5(b)). Last, attackers may impersonate legitimate nodes (Figure 5(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 *SRLD*, it is difficult for an attacker to lie about its predecessor and successor since forging the tickets of predecessor or successor is challenging. And the attacks by reusing the stale tickets will be defended by checking whether the timestamps of the tickets have been expired.

For the 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 by consulting roadside APs. Moreover, a node's registration will expire after R, which makes it difficult for adversaries to re-use stale tickets overheard previously.



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

Fig. 5. Attacks against relative location determination schemes

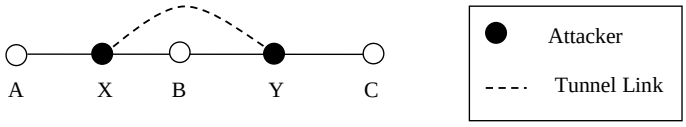


Fig. 6. An example of Wormhole attack.

For the fourth type of attacks, since the receiver verifies the authenticity of the public key of the beacon source and the signature of the message, it is difficult for malicious nodes to impersonate legitimate nodes and alter the beacon messages sent by legitimate nodes unless they know the private key of the source.

5.2 Wormhole Attack

Another significant attack is a Wormhole attack, where malicious nodes collude to selectively discard relative location messages of legitimate nodes. Figure 6 illustrates a basic Wormhole attack. The attackers control node X and Y, which are connected by a tunnel link. Regular messages and relative location messages received by X are tunneled to Y and retransmitted at Y, and vice versa. By selectively discarding 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 [24, 9]. Y. Hu et al. proposed a MAC layer protocol named TIK [24] 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 [9], 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 De-*

tection (PMLD) protocol, which defend Wormhole attacks by probabilistically monitoring the losses of relative location messages. When working in *SRLD-AP* mode, APs instead of the vehicles propagate relative locations so the attackers are unable to launch Wormhole attacks. But *PMLD* protocol can be used to defend Wormhole attacks when the system works in *SRLD-D* mode.

$PMLD$ protocol is showed in Fig.4. 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 each beacon message will be transmitted by every node in the network, 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 [10], 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 [10], the above watchdog-like method [15] 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 monitoring message transmissions and inform legitimate nodes about 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.

5.4 Replay Attack and Denial-of-Sevice Attack

During Replay attacks, attackers retransmit stale messages recorded previously. In *SRLD-AP*, since *RLT* is transmitted by APs with asymmetric cryptography, it is difficult to launch Replay attacks. In *SRLD-D*, since each location message has a sequence number and a signature, it is hard for attackers to inject stale location messages since they are unable to forge the message signature.

Moreover, malicious nodes may initiate denial-of-service attacks such as constantly retransmitting stale messages or garbage messages, the normal wireless transmission around the malicious nodes 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 nodes physically. Roadside APs record the electronic license plates of

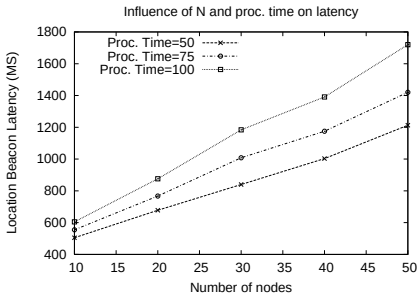


Fig. 7. Latency vs. N and processing time

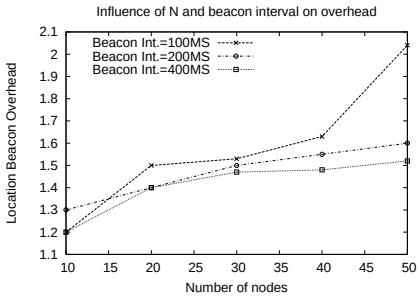


Fig. 8. Overhead vs. N and beacon int.

the attacking nodes and report the positions of attacking nodes to law enforcement department to stop the attacking nodes.

6 Evaluation

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

- *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 [19]. The nodes in the network move according to the mobility pattern of the vehicles on the free way. The nodes use IEEE 802.11b radio to communicate. When measuring *location beacon latency*, we vary N and the processing time of a location beacon on each node. Fig. 7 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. 8 shows that when N becomes larger or when beacon interval shinks, location beacon overhead increases due to the increase of radio collisions.

7 Conclusions and Future Plan

In this paper, we have presented $SRLD$, a novel scheme for securely determining the relative locations of vehicles in vehicular networks. $SRLD$ does not require any GPS or accurate position information but only the relative locations of each vehicle's surrounding vehicles. $SRLD$ uses cryptographic keys to authenticate relative location messages and uses a vehicle's public key 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 will evaluate the scheme under the aforementioned attacks. Moreover, we plan to evaluate $SRLD$ 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. Brands and D. Chaum. Distance-bounding protocols. In *EUROCRYPT '93*, pages 344–359, 1994.

[5] 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.

[6] S. Capkun and J.-P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *IEEE INFOCOM*, 2005.

[7] 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.

[8] D. Singelee, and B. Preneel. Location verification using secure distance bounding protocols. *International workshop on wireless and sensor networks security*, 2005.

[9] L. Hu and D. Evans. Using directional antennas to prevent wormhole attacks. In *Network and Distributed System Security Symposium (NDSS)*, February,2004.

[10] 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.

[11] J.-P. Hubaux, S. Capkun, and J. Luo. The security and privacy of smart vehicles. *IEEE Security and Privacy*, 2(3):49–55, 2004.

[12] 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.

[13] L. Lazos and R. Poovendran. SeRLoc: Robust localization for wireless sensor networks. *ACM Trans. Sen. Netw.*, 1(1):73–100, 2005.

[14] 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.

[15] 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.

[16] J. Newsome, R. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: Analysis and defenses. In *IPSN '04)*, Apr. 2004.

[17] P. Persiano and I. Visconti. A secure and private system for subscription-based remote services. *ACM Trans. Inf. Syst. Secur.*, 6(4):472–500, 2003.

[18] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan. The cricket location-support system. In *MobiCom '00*, pages 32–43, 2000.

[19] Qualnet Network Simulator. `http://www.qualnet.com/`.

[20] 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.

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

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

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

[24] 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.