TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving

Xiaodong Lin, *Student Member, IEEE,* Xiaoting Sun, Xiaoyu Wang, Chenxi Zhang, *Student Member, IEEE,* Pin-Han Ho, *Member, IEEE,* and Xuemin (Sherman) Shen, *Senior Member, IEEE*

***Abstract*—In this paper, we propose a Timed Efficient and Secure Vehicular Communication (TSVC) scheme with privacy preservation, which aims at minimizing the packet overhead in terms of signature overhead and signature verification latency without compromising the security and privacy requirements. Compared with currently existing public key based packet authentication schemes for security and privacy, the communication and computation overhead of TSVC can be significantly reduced due to the short *message authentication code* (MAC) tag attached in each packet for the packet authentication, by which only a fast hash operation is required to verify each packet. Simulation results demonstrate that TSVC maintains acceptable packet latency with much less packet overhead, while significantly reducing the packet loss ratio compared with that of the existing *public key infrastructure* (PKI) based schemes, especially when the road traffic is heavy.**

***Index Terms*—Vehicular communications, security, TESLA, hash chain.**

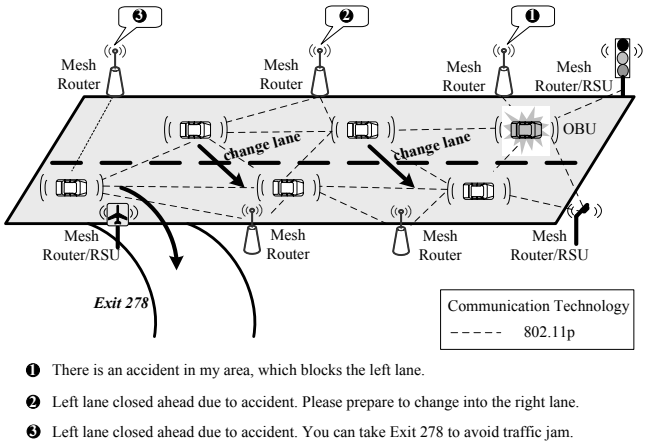


Fig. 1. Road Emergency Response Operation under VANET

I. Introduction

With the advance and pervasiveness in wireless communication technologies, it is envisioned that vehicles will be able to communicate with each other as well as with the roadside infrastructure located in some critical sections of the road. With the wireless communication devices equipped in vehicles (also known as *On-Board Units* (OBUs)) and the *Roadside Units* (RSUs), a self-organized network can be formed, which is called a *Vehicular Ad Hoc Network* (VANET). Due to various envisioned vehicle safety application scenarios and emerging service demands, VANETs have attracted extensive attentions from all aspects of governments, car manufacture industry, and research community.

According to *Dedicated Short Range Communications* (DSRC) [1], each vehicle on the road is broadcasting routine traffic related messages with the information of position, current time, direction, speed, acceleration/deceleration, and traffic events, etc. Emergency messages are sent when any abnormal situation is encountered, such as emergent braking and traffic jam ahead. Routine traffic related messages are one-hop broadcast without message relay, while emergency messages are transmitted through a multi-hop path, where the receiver of the messages continues broadcasting the messages to the following vehicles. Currently, the IEEE 802.11p task group is working on the DSRC standard which enhances the 802.11 protocols to support the wireless communications between vehicles and the roadside infrastructure [2]. By frequently broadcasting and receiving routine traffic related messages, drivers can get better awareness of their driving environment. Early actions can be taken to respond to an abnormal situation to avoid any possible damage or to follow a better route by circumventing a traffic bottleneck. For example, as shown in Fig. 1, whenever there is an accident in highway, several lanes can be blocked, and drivers can experience a long delay. However, the delay can be mitigated if the drivers are informed in advance so that they can follow an enroute or change lane to avoid traffic jam. Also, the scene of the accident could be cleaned in a timely fashion by emergency crews if authorities are reported and police and emergency crews respond to the accidents immediately.

The creation of VANETs is obviously a great plus to the traffic management and road driving safety. However, any malicious behavior of users, such as a modification and replay attack with respect to the disseminated messages, could be fatal to the other users, and should be identified and rejected from the networks. In addition, the user related privacy in-

Manuscript received July 15, 2007; revised October 21, 2007; accepted November 27, 2007. The associate editor coordinating the review of this paper and approving it for publication was W. Liao.

X. Lin, X. Wang, C. Zhang, P.-H. Ho, and X. Shen are with the Centre for Wireless Communications, Department of Electrical and Computer Engineering, University of Waterloo, 200 University Avenue West, Waterloo, Ontario, Canada N2L 3G1 (e-mail: {xdlin, x18wang, pinhan, xshen}@bbcr.uwaterloo.ca; c14zhang@engmail.uwaterloo.ca).

X. Sun is with the David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: x7sun@cs.uwaterloo.ca).

This work was supported by research grants from Natural Sciences and Engineering Research Council of Canada (NSERC).

Digital Object Identifier 10.1109/T-WC.2008.070773

formation, such as the driver's name, license plate, speed, position, and traveling route, has to be protected and inaccessible by the public. Furthermore, in the case of a dispute such as a crime/car accident scene investigation, the authorities should be able to reveal the identity of the message senders. Such a privacy preservation requirement is also referred to as *conditional privacy*. Therefore, security and privacy are the most fundamental issues in determining the applicability of all the VANET based protocols and devices. The studies on security and privacy in VANETs have been extensively reported in past few years, which can mainly be divided into the following two categories. The first one is by the way of the traditional public key based digital signatures [3], [4], while the other one is group signature based security scheme [5]. In both categories, each message needs to be signed by using an asymmetric algorithm at the sender before it is sent, and the receiver needs to verify the received message. According to DSRC [1], a vehicle sends a message with a time interval from 100ms to 300ms. Obviously, digitally signing messages at a speed of less than 10 messages per second is not an issue for any conventional digital signature scheme, but the signature verification speed is an important performance measure that determines the applicability of VANET application scenario, particularly when the number of messages to be verified is large. The following is a simple example demonstrating the signature verification speed. In the case that $100 \sim 500$ cars are within the communication range, the receiver needs to verify around $1000 \sim 5000$ messages per second, which may lead to a high computation burden to the receivers. Therefore, the corresponding *public key infrastructure* (PKI)-verification algorithm is required to be very efficient; otherwise, a large amount of messages could be lost and sent in vain. Unfortunately, the traditional public key based digital signature techniques are prohibitively inefficient in many cases due to their computational complexity. Furthermore, each packet has to be attached with the corresponding sender's public key certificate, which usually takes a significant portion of the packet size and causes non-trivial additional bandwidth consumption. Therefore, the design of a security scheme in VANETs should also take the following issues into consideration, including signature overhead of each packet, packet sending rate, and requirements on packet loss rate and packet latency [4]. These issues are critical and must be well addressed before the developed scheme can be applicable to practical vehicular communications. Furthermore, a developed security scheme should not compromise the security and privacy level. In this paper, we introduce a new security scheme, called **T**imed Efficient and **S**ecure **V**ehicular **C**ommunication (TSVC) scheme, which is based on TESLA (*Timed Efficient Stream Loss-tolerant Authentication*) [7]. Enlightened by TESLA authentication protocol, the proposed scheme only needs to perform symmetric MAC operation at the receiver, which is sufficient to authenticate the source of the message, instead of performing any asymmetric verification. In addition, since only a short MAC tag is attached at each message, the extra message length and the bandwidth overhead due to the security mechanism can be significantly reduced. Moreover, the proposed scheme is much different from any of the other reported PKI based schemes in the resultant packet loss ratio, which is found almost independent of the traffic density. We will demonstrate by extensive simulation that the proposed TSVC scheme significantly reduces packet loss ratio than the existing PKI based security schemes especially when the traffic is becoming denser while maintaining acceptable packet latency. The proposed scheme is feasible due to the unique features of VANETs, such as a fixed message release interval, and temporally stable geographical groups which will be discussed later.

The remainder of the paper is organized as follows. Section II discusses the related work. Section III presents the proposed TSVC scheme. In Section IV, the security of the proposed scheme is analyzed. Performance evaluation is presented in Section V through extensive simulation. Finally, Section VI concludes the paper.

II. Related Work

A number of previous studies have tackled the issues of security and privacy in VANETs [3]–[6]. Raya *et al* in [3] introduced a security protocol in VANETs by way of installing a large number of private keys and the corresponding anonymous certificates (probably 43,800 certificates) for each vehicle. A vehicle randomly selects one of the anonymous certificates and uses its corresponding private key to sign each launched message. The other vehicles use the public key of the sender enclosed in the anonymous certificate to authenticate the source of the messages. Instead of taking any real identity information of the drivers, these anonymous certificates are generated by taking the pseudo IDs of the vehicles. Each certificate has a short life time to meet the driver's privacy requirement. Also, the whole list of anonymous certificates corresponds to a unique real identity of the drivers are kept by the authorities in order for the police to verify the real-world identities of the vehicle owners in the occurrence of any possible traffic dispute.

The *Vehicle Safety Communications* (VSC) project group [4] proposed to using a list of short-lived anonymous certificates to keep the privacy of the drivers. The certificates are blindly signed by the *Certificate Authority* (CA) in order to deal with the insider attacks, e.g., CA abuses its authority and mishandles driver information. A linkage marker is devised for the escrow authorities to connect the blindly signed anonymous certificates with the corresponding vehicle together. In [5], a security protocol based on group signature and Identity-based signature scheme was proposed to meet the unique requirements of vehicular communication networks. The proposed protocol not only guarantees security and privacy, but also provides easy traceability property when the identity of the sender of a message has to be revealed by the authority. In [6], a secure traffic aggregation scheme was developed to minimize the communication overhead and initiate a tradeoff between the security and efficiency. First, the map or the geographic region is dissected into predetermined small cells (e.g., every 400 meters along the road), each of which determines a dynamic vehicle group. A unique group leader is automatically elected as the one who is the closest to the geographic center of the cell. The dissemination of messages is delegated to each group leader who performs message aggregation for all the vehicles in the group and forwards the messages to the

neighboring groups. Although this scheme may yield low communication overhead, the vehicle closest to the center of a cell may change frequently, leading to a frequent update of the group leader of a cell (e.g., once in a few seconds). The update of the group leader consumes all the efforts such as negotiation and reselection of the leader, and aggregation of new signatures. Therefore, the scheme can be further improved in terms of the efficiency and practical applicability. This paper aims to reduce the overhead incurred in the security scheme without compromising the security and privacy preserving. Compared with [6], we follow a more natural and dynamic approach to group the vehicles on the road. In addition, a designated group leader is not required, which largely reduces the resultant computation overhead in negotiating for a new group leader, identifying group members, or realizing the roles as relay nodes, etc.

III. Timed Efficient and Secure Vehicular Communications Scheme

A. Preliminaries

1) One-Way Hash Chain: One-way hash chain was first proposed in [8] for the secure password authentication, which quickly became an important cryptographic primitive in many other applications, such as micropayment systems [9], secure data forwarding in wireless ad hoc networks [10], and stream data authentication [11]. A one-way hash chain is a repeated application of a hash function $H(x)$ to randomly selected seed S, which has the following properties:

- $H(x)$ can take a message of arbitrary-length input and produce a message digest of a fixed-length output;
- Given x, it is easy to compute $y = H(x)$. However, it is hard to compute $x = H^{-1}(y)$, when given y.
- Given x, it is computationally infeasible to find $x^{'} \neq x$ such that $H(x^{'}) = H(x)$;
- It is computationally infeasible to find any two pair x and $x^{'}$ such that $x^{'} \neq x$ and $H(x^{'}) = H(x)$.

The operation result of the hash function for $n-1$ times is denoted as $h_1, h_2, \cdots, h_n$, respectively, where $h_1 = H(h_2)$, $h_{i-1} = H(h_i)$, $h_n = S$, $1 < i \leq n$. h_1 is called the *tip* or the *commitment* of the chain. Then, the holder of the hash chain can release the chain elements in the opposite order of the order that the chain is generated. In this way, any hash chain element can be kept secret until it's released, and upon receiving a chain element, its authenticity can be easily validated with a simple hash operation.

One-way hash chain can always be used to reduce the authentication load of a series of messages. However, the main problem of the hash chain mechanism is the lack of ability in handling message loss. Further, the traditional one-way hash chain has a fixed length, but the number of messages varies with application. In addition, the messages to be authenticated should be known in advance which incurs a big constraint for most real time applications.

2) TESLA Authentication Protocol: TESLA is an efficient and message-loss tolerant protocol for broadcast authentication with low communication and computation overhead [7]. It is widely used in areas of sensor networks [12]. It uses one-way hash chain where the chain elements are the secret keys to compute *message authentication code* (MAC). With TESLA, a sender sends data packets at a predefined schedule, which has been known in advance to the receivers as well as the commitment to a hash chain as a key commitment. Each hash chain element as a MAC key corresponds to a certain time interval. For each packet, the sender attaches a MAC tag to it. This MAC tag is derived using the next corresponding MAC key in the hash chain based on negotiated key disclosure delay schedule between the sender and the receiver. Obviously, upon receiving the packet, the receiver can't verify the authenticity of the packet yet. After key disclosure delay, the sender discloses MAC key, and then the receiver is able to authenticate the message after verifying the released MAC key is indeed the corresponding element of the chain. One requirement for TESLA scheme is the loose synchronization among the nodes. The disadvantage is the delayed message authentication.

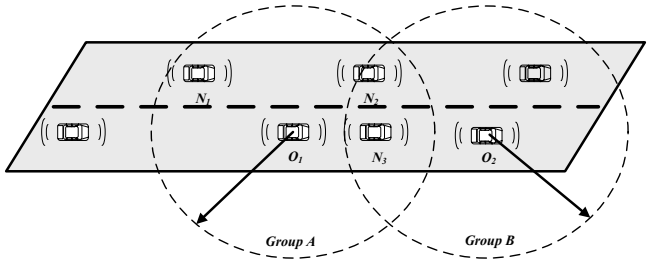


Fig. 2. Dynamic virtual vehicle group formation

B. System Formulation

Let each vehicle act as a leader and form a dynamic group with the current neighboring vehicles that are within its transmission range. In Fig. 2, vehicles O_1, N_1, N_2, and N_3 form a vehicle group with vehicle O_1 as the leader. Obviously, a vehicle may belong to many dynamic groups, e.g., vehicle N_3 belongs to group B with vehicle O_2 as the leader as well. We assume that the maximum delay of a message traveling within a typical transmission range over a wireless channel can be estimated. In [4], the estimated communication latency is identified to be about 10ms. Also, all the vehicles are loosely synchronized, which can easily be achieved by some time synchronization protocols [7], [13], [14]. Currently, there exist two methods for the sender and the receivers to be time synchronized, i.e., direct time synchronization and indirect time synchronization [15]. Considering the high-mobility of vehicles in VANET and loose time synchronization requirement, we prefer all the vehicles synchronize securely via an external time reference, i.e., indirect time synchronization. For example, each vehicle is equipped with a highly accurate atomic clock and then the clock can be synchronized to a central time server during its annual or bi-annual vehicle check, such as license renewal, emission test. We divide the message authentication into two categories based on the message type: routine message and emergency message, where the former one obviously dominates the total traffic amount while the latter one is much less frequent. In this work, we concentrate on solving the former one.

The general idea of the proposed scheme for the routine

traffic related messages is described as follows. As a sender, a hash chain is generated in advance before using them as encryption keys to generate MAC codes. A signature is produced for the first message with the conventional public key signature technique. For the following messages, on the other hand, the MAC tag of each message is computed with the corresponding encryption key in the hash chain, which is disclosed after a short delay. Messages can be authenticated when the encryption keys are released. Based on the expected transmission delay of each message along with the serial number of the key used in a hash chain, the receiver can check whether the next hash key used to generate the MAC tag of the received message has been released or not. If not, the message should be discarded to prevent message forgery attack.

Emergency messages that are sent with a much lower frequency are processed at higher priority. Normal signature and verification schemes are adopted, where the best security assurance and a constant delay can be achieved.

C. TSVC Scheme

1) Vehicle Group Formation: One of the unique features of VANETs is that the vehicles driving on the highway maintain a temporally stable relative distance with the neighboring vehicles. Since the communication range is typically $250m \sim 1000m$ [1], this neighborhood relationship may last from several seconds to several minutes according to the driving speed of individual vehicles. By taking advantage of this property, we can group the vehicles according to their physical locations. For a specific vehicle O_1, all the other vehicles that are within its one-hop communication range are defined as in the same group as O_1. The group relationship is dynamic and is updated when any other vehicle comes into the communication range or any group member leaves the group. The majority of the group members remain stable for a comparatively long time.

2) TSVC Scheme: Let all the vehicles be installed with a list of anonymous public/private key pairs $< PK_i, SK_i >$ in the vehicle registration phase or annual check-up, where the corresponding anonymous certificates are $Cert_i$ with pseudo identities $PVID_i$ as its certificate identities [3]. For the purpose of traceability, vehicle registration authority keeps records of those anonymous certificates and their corresponding real identities. Each pair of keys has a short life time, e.g., a few minutes. Each vehicle has to generate a hash chain $h_1, h_2, ..., h_n$ initiated from a random seed S, where $h_n = S$, and $h_i = H^{j-i}(h_j)$ with $i < j$. Each element in the hash chain is in charge of generating a number of MAC codes for a number of messages as the cryptographic keys and will be released after a short delay δ which is called *key disclosure delay*. Without loss of generality, we assume the number of messages each encryption key works on is 1; thus, each hash element will generate one MAC code for one message. Also we set the time interval in TESLA authentication protocol as the packet release interval which means one data packet and its corresponding key release packet are generated during one time interval.

The length of the hash chain can be predetermined according to the life time of each anonymous certificate and the message sending interval. Once the anonymous public key pairs are updated, a new chain is initiated and comes into role. Note that all the hash chains can be initialized in advance before going into function to reduce system operation delay. Let the routine safety messages sent by a vehicle be denoted as $M_1, M_2, ..., M_k$, and M_i is encapsulated in packet P_i, $1 \leq i \leq k$. Further, let packets be launched with a fixed interval of $300ms$. The packet authentication process is shown in Fig. 3:

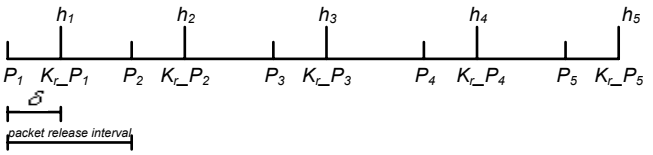


Fig. 3. Relationship between a hash chain and the corresponding packets

There are two categories of packets. The first category is called data packet, denoted as P_i, which is specialized in sending data information while the second category is the *Key Release Packet* (KRP), denoted as kr_P_i, which is dedicated for releasing the encryption keys h_i. Such a design is to reduce the packet end-to-end delay because the interval between two traffic safety packets are usually longer than the maximum tolerable human reaction latency. KRP is disclosed a fixed time δ after the previous data packet is released.

The proposed security scheme is illustrated in Fig. 4. For an arbitrary sender O, it generates the MAC tags of the messages using h_j as the encryption keys, where $1 \leq h_j \leq n$. Therefore, the data packet to be sent has the following format:

$$P_j = \langle PVID, M_j, MAC_{h_j}(M_j||T_j), T_j, index \rangle,\ j \geq 1 \quad (1)$$

where M_j is the safety message, $PVID$ is the pseudo ID of vehicle O, which is kept in accordance with the ID that is being used in the current public key certificate $Cert_O$; T_j is the time when the sender sends the data packet, which is used to defeat replay attack.

Then, the sender O prepares the first key release packet by signing the *commitment* of the hash chain h_1 according to the traditional public key based signature techniques, and the first key release packet has the following format:

$$kr\_P_1 = \langle PVID, Sig_{SK_O}(h_1, index, T_1^{'}), h_1, index, T_1^{'}, Cert_O \rangle, \quad (2)$$

where h_1 is the key, which is used to generate the MAC tag for the first message M_1, $Cert_O$ is the currently used anonymous public key certificate, SK_O is the corresponding private key to $Cert_O$, $T_1^{'}$ is the time when the sender sends the first key release packet, and *index* represents the index of the current hash value in the hash chain that O is releasing in the packet, i.e., 1 for the first key release packet. It is worth pointing out that the KRP is released δ seconds later than the previous data packet. The following key release packet has the following format:

Source O		Receivers $R_1, \cdots, R_n$
First Message:		
Generate hash chain $h_1, h_2, \cdots, h_n$		
Generate the first message M_1		
Compute $MAC_{h_1}(M_1 \| T_1)$		
$P_1 = \langle PVID, M_1, MAC_{h_1}(M_1 \| T_1), T_1, index \rangle$		
	$\xrightarrow{P_1}$	
		Buffer P_1
Wait for δ seconds		
$\sigma = Sign_{SK_O}(h_1, index = 1, T_1^{'})$		
$kr\_P_1 = \langle PVID, \sigma, h_1, index, T_1^{'}, Cert_O \rangle$		
	$\xrightarrow{kr\_P_1}$	
		$V_{PK_O}(h_1, index, T_1^{'}, \sigma) \stackrel{?}{=} 1$ If yes, accept kr_P_1 If no, drop it
		$MAC_{h_1}(M_1 \| T_1) \stackrel{?}{=} MAC_{k_1}(M_1 \| T_1)$ If yes, accept P_1 If no, drop it
...		
Following Messages:		
Generate Message M_j,$j > 1$		
Compute $MAC_{h_j}(M_j \| T_j)$		
$P_j = \langle PVID, M_j, MAC_{h_j}(M_j \| T_j), T_j, index \rangle$		
	$\xrightarrow{P_j}$	
		Buffer P_j
Wait for δ seconds		
$kr\_P_j = \langle PVID, h_j, index = j, T_j^{'} \rangle, j > 1$		
	$\xrightarrow{kr\_P_j}$	
		Verify $h_i \stackrel{?}{=} H^{j-i}(h_j)$ (i is the last successfully received key) If no, drop it If yes, continue. Verify $MAC_{h_j}(M_j \| T_j) \stackrel{?}{=} MAC_{k_j}(M_j \| T_j)$ If so, accept and consume M_j Otherwise drop it

* k_1 and k_j are the hash elements in kr_P_1 and kr_P_j respectively.

Fig. 4. The proposed security scheme

$$kr\_P_j = \langle PVID, h_j, index = j, T_j^{'} \rangle, \ j > 1, \tag{3}$$

where h_j is used to generate the MAC tag for message M_j. Upon receiving the first data packet, the receivers simply put the received packet in the buffer and wait until the first key release packet arrives[1]. After receiving the first key release packet that is signed by the source of the message, the receivers perform the following verification after validating the sender's anonymous certificate $Cert_O$:

$$\begin{cases} V_{PK_O}(h_1, index, T_1^{'}, Sig_{SK_O}(h_1, index, T_1^{'})) \stackrel{?}{=} 1, \\ \text{where } index = 1; \\ MAC_{h_1}(M_1 \| T_1) \stackrel{?}{=} MAC_k(M_1 \| T_1), \end{cases} \tag{4}$$

where k is the h_1 contained in the first key release packet.

Therefore, it is crucial for vehicle O's neighboring vehicles to receive the first key release packet in order to authenticate the data packets from O. Basically, there are two ways to accomplish it by either using any mobile reliable broadcast protocol [20] or treating the missed vehicles as newly joining group members, which will be discussed in Section III-D3.

[1]Whenever receiving any packet, the receivers first checks if the timestamp found in packet is reasonable, and if so, continue. Otherwise, the receivers drop the packet since the receivers could be subject to replay attack.

The receivers will then store the information such as the $PVID$ and T_1 in order to synchronize the later packets that are sent by the same source. In case the verification fails, the packet is dropped. Otherwise, every receiver keeps an entry $(packet\#, source, c_1, Lifetime)$ in its local cache table corresponding to the sender O, in which it stores the packet index, i.e., 1, to the field $packet\#$, $PVID$ to the field source, the authenticated hash chain element h_1 to c_1. $Lifetime$ serves as a timer controlling how long the entry is active. If the timer hits 0, the entry is expired, and removed from the receiver's cache table. Whenever a new packet arrives from a source, the receivers update the timer of the corresponding entry in the table.

When receiving data packet P_j, $j > 1$, the receivers simply put the received packet in the buffer without trying to verify them. As soon as the next key release packet kr_P_j arrives, the receivers will start to verify the previous data packet. At first, the receivers will check the legitimacy of the received hash chain member, which is done by checking if the following equation holds,

$$H^{j-packet\#}(h_j) = c_1 \tag{5}$$

where h_j is included in the key release packet kr_P_j, and c_1 and $packet\#$ are from the entry corresponding to $PVID$, which is found in its local cache table. If the Eq. 5 does

not hold, the packet kr_P_j is dropped; otherwise, the receivers start to validate the data packet P_j by checking if $MAC_{k_j}(M_j||T_j) = MAC_{h_j}(M_j||T_j)$, where M_j, T_j and $MAC_{h_j}(M_j||T_j)$ are the previously buffered values of the data packet, k_j is the hash element in kr_P_j. If the verification succeeds, P_j is accepted and consumed by the application layer, and then, in the entry corresponding to $PVID$, the receivers update the first and third fields with $index$ and h_j along with a new timer for the last field; otherwise, P_j is dropped.

In summary, the proposed scheme can achieve the same guarantee on the message integrity, anonymity, and authenticity as the traditional PKI based schemes, which will be detailed in Section IV. In spite of the anonymity among the public, the scheme can well maintain a conditional traceability property for the authorities such as police, because all the accepted messages can be uniquely tied to an anonymous public key certificate of its sender. Thus, by checking this unique public key certificate, the authority can trace the unique real world identity of the message sender as that in the traditional PKI based schemes.

3) Security Requirement and Key Disclosure Delay δ: The security requirement to prevent the message forgery attack for the TSVC scheme is that the key release waiting time should be longer than the time for a message to travel from the source to all the recipients. If any receiver r can receive the released key before the original data packet arrives at another receiver, e.g., $\overline{r}$, receiver r who holds the key can forge a message by generating a valid MAC tag to this message and sending the tagged message to $\overline{r}$. Note that this forged message can pass $\overline{r}$'s verification. This situation can be avoided by properly choosing the key disclosure delay δ. In the vehicular communications with IEEE 802.11p, since the longest transmission range is about $1000m$ [1], δ should be slightly greater than the time duration for a message to travel for $1000m$ in the wireless channel. In [4], the communication latency is identified as about $10ms$. In our scheme, therefore, δ is set to be $100ms$, which is about 10 times of the communication latency for the concern to achieve absolute safety that also can meet the requirement for the maximum allowable latency. This parameter setting will be verified through simulation as presented in section V.

Before performing a normal message authentication process as discussed above, validity of the messages needs to be checked to see if the security requirement can be met. This means the receivers have to know which interval that packet belongs to and whether the corresponding key has been released already. If it is not true, the packet is dropped without trying to authenticate it. Note that due to the stringent time requirement of the real time applications in VANETs, late or outdated messages should be dropped. Therefore, if a message arrives after the maximum allowable latency such as the maximum human's reaction time, the message should be dropped without putting it into the buffer.

D. Discussion

1) The Capability to Deal with Message Loss: Wireless communication channels are lossy in nature. Inherent from TESLA which is packet loss tolerant, our scheme is also packet loss tolerant. If a data packet is lost, no further action will be taken. On the other hand, if the KRP kr_P_i is lost, the legitimacy of the previous message can still be verified upon receiving kr_P_j with $j > i$. The broken hash chain can be connected by applying the hash function $H(x)$ $j-i$ times and checking if $H^{j-i}(h_j) = h_i$. If so, the newly arrived hash value h_j is acceptable. However, if multiple continuous packets are lost such that the time to wait for the new key release packet is longer than the maximum tolerable message delay, M_j is neglected. In that case, the subsequent messages can still be authenticated when new data packets arrive as we discussed in section V.

2) Bandwidth Efficiency: We analyze the reduction of bandwidth consumption due to the decrease of the average packet size compared with the regular public key based protocols.

For a signed message, additional load caused by security is the length of the certificate of the public key [2] and the digital signature of the message. Among the existing digital signature schemes such as RSA, DSA, ECDSA, and BLS, the most appropriate candidate for the VANET application in terms of the packet overhead and verification time is ECDSA[3]. The minimum additional space caused by ECDSA is 181 bytes for each message, including the digital signature and public key certificate. Thus, the total length of a traditional signed packet is around 281 bytes including the message payload which is around 100 bytes [4].

To evaluate the average cost of delivering a message in our scheme, we assume that the first KRP are signed with the ECDSA scheme and the used hash algorithm is SHA-1; the life time of an anonymous certificate is 10 minutes; routine traffic messages are sent every $300ms$. Thus, the total number of routine traffic messages N_{total} is 2000. The length of data packet is

$$\begin{cases} L_{P_i} &= L_{M_i} + L_{PVID} + L_{MAC} + L_T + L_{index} \\ &= 100 + 4 + 20 + 4 + 4 \\ &= 132 \text{ bytes}, \end{cases} \tag{6}$$

where $timestamp$ and $PVID$ are taken as 4 bytes each, respectively. The length of the first KRP is

$$\begin{cases} L_{kr\_P_1} &= L_{PVID} + L_{sig} + L_{hash} + L_{index} \\ &\quad + L_T + L_{Cert} \\ &= 4 + 56 + 20 + 4 + 4 + 125 \\ &= 157 \text{ bytes}, \end{cases} \tag{7}$$

and the length of the subsequent KRP is

$$\begin{cases} L_{kr\_P_i} &= L_{PVID} + L_{hash} + L_{index} \\ &= 4 + 20 + 4 \\ &= 28 \text{ bytes}, \ i > 1, \end{cases} \tag{8}$$

where $index$ is taken as 4 bytes. Therefore, the average packet length due to the cryptographic algorithm in our scheme is:

[2]We assume that a signing certificate for an OBU is used in our scheme, and the size of an OBU signing certificate is about 125 bytes [27].

[3]We assume that ECDSA-224 is used.

$$\begin{cases} L_{avgP} & = (L_{kr\_P_1} + L_{P_i} \times N_P + L_{kr\_P_i} \\ & \quad \times (N_{kr\_P} - 1))/N_{total} \\ & = (157 + 132 \times 2000 + 28 \times 1999)/2000 \\ & \approx 160 \text{ bytes}, \end{cases} \tag{9}$$

which is much shorter than that of the traditional PKI based digital signature schemes.

3) Tolerating Group Membership Fluctuation: We investigate how to mitigate the impact due to dynamic vehicle group membership fluctuation while maintaining acceptable communication consumption and authentication delay.

The memberships of a group may fluctuate when a vehicle joins or leaves the group. Clearly, the case that the vehicle leaves the transmission range can be easily handled by removing the group leader's entry in its local cache table after a time threshold. The reason that the leaving vehicle keeps the information record of the group leader briefly is to avoid temporary group membership changes. On the other hand, when a vehicle (denoted as A) newly joins the group of vehicle (denoted as O), A needs to catch up with the authentication key information contained in the first key release packet kr_P_1 in order to authenticate any possible received message from O. Intuitively, this issue could be easily solved if A could obtain the first authenticated tip of hash chain kr_P_1 from O, by which A can verify this signed tip of the encryption key h_1 and subsequently authenticate any received message from O. Therefore, it is straightforward and effective in dealing with the membership fluctuation when the fluctuation rate is low; however, it may be subject to heavy signaling and processing overhead when the membership fluctuation is serious. In the following, we introduce an alternative approach where the first authenticated tip of the hash chain kr_P_1 with key release packets is periodically broadcast by each vehicle group, in order to allow a newly joining vehicle to authenticate its received messages at the expense of additional bandwidth assumption in the periodical broadcasting as well as longer authentication delay. It is clear that determining the length of broadcasting period becomes an issue of design, where taking a larger (or smaller) broadcast interval leads to less (or more) bandwidth consumption yet longer (or shorter) authentication delay. Note that the traffic routine/safety messages are designed to provide early warning to the other drivers, and the late arrival of routine/safety messages may significantly diminish their effectiveness. Thus, it is challenging to initiate a graceful tradeoff between the authentication latency and the bandwidth consumption in the effort of periodically broadcasting the tip of hash chain.

We first consider a single-lane highway scenario as shown in Fig. 5, where vehicle A is entering the transmission range of O. We are interested in how many vehicles are affected by the test slot in the proposed security mechanism. Assume that each vehicle is at the center of an imaginary cell defined by its transmission range R, and the vehicle location on highway are randomly distributed according to a uniform distribution with density η vehicles per unit kilometer. This assumption has been widely adopted in traffic flow modeling [16]–[18]. The probability density function of the distance between vehicle A and reference vehicle O is given by

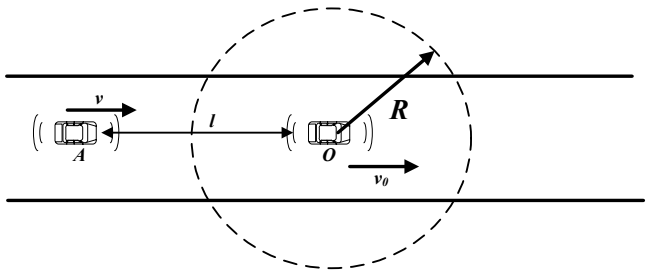


Fig. 5. Single-lane highway scenario

$$f(l) = \frac{1}{T(v - v_o)_{max}}, \ 0 \le l \le T(v - v_0)_{max}, \tag{10}$$

where l denotes the distance between A and O, and v_0 and v are the reference velocity and entering velocity, respectively. This assumption is reasonable due to the following aspects: 1) in any time snapshot each vehicle may have equal probability of being placed on the lane segment; 2) regularly, there are few hotspots on the highway which have higher density than other areas on the road. In the city, we can frequently see that some areas are crowded with cars, such as taxi loading/unloading area, but vehicles seldom gather on the highway under normal situation. Moreover, v is assumed to follow a truncated Gaussian distribution with parameter $(\overline{v}, \sigma)$. On the highway, drivers must observe the speed restrictions; however, there are still a few overspeeding vehicles and low speed vehicles. Khoury et al in [19] used the FHWA(Federal Highway Administration) Highway Statistics 2002, and applied the Monte-Carlo simulation model as well as a closed form analytical estimation model to demonstrate that the vehicle speed on the highways fit into a truncated Gaussian distribution. Thus, the probability that A enters the O's virtual cell in test time T is denoted as $P(l - R < (v - v_0)T|v)$, and can be expressed as:

$$\begin{cases} P_T & = Prob\{\text{one vehicle enters the} \\ & \qquad \text{transmission range within T}\} \\ & = \int\int P(l < (v - v_0)T + R|v) f(v)\, dl dv \\ & = \dfrac{1}{\sigma\sqrt{2\pi} T(v - v_0)_{max}} \displaystyle\int_{v_L}^{v_H} ((v - v_0)T \\ & \quad + R) \cdot exp(-\tfrac{v - \overline{v}^2}{2\sigma^2})\, dx, \ \text{where } v > v_0 \end{cases} \tag{11}$$

or $P_T = 0$, $v \le v_0$. On a single lane, each vehicle has the probability of entering the reference cell, P_T, which can be regarded as a "success" trial; and the probability of not entering, $1 - P_T$, can be regarded as a "failure" trial. If the number of vehicles on the lane, which is approximated by $\eta T(v - v_0)_{max}$, is supposed to be n independent trials, we can use the Binomial distribution to model the distribution of the number of vehicles entering the reference cell. Then, the average number of entering vehicles is given by

$$E[k] = nP_T \tag{12}$$

where n is the number of vehicles on the lane, which can be approximated by $\eta T(v - v_0)_{max}$.

Notice that with the assumption of uniform distribution for the vehicles along each lane, single-lane scenario can be

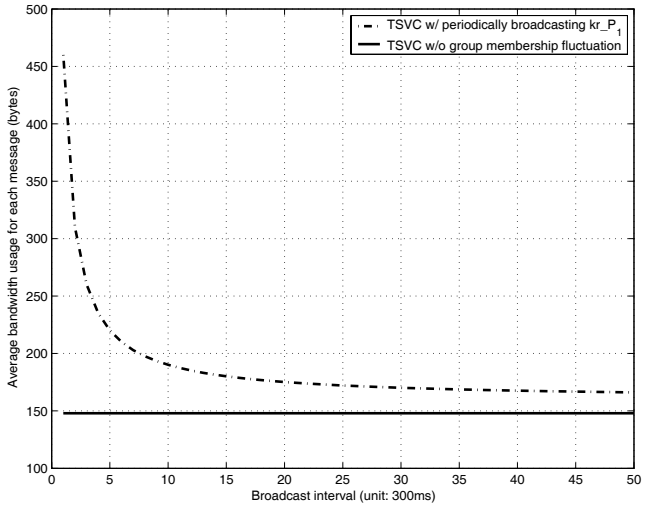


Fig. 6. Average bandwidth usage of different broadcast intervals

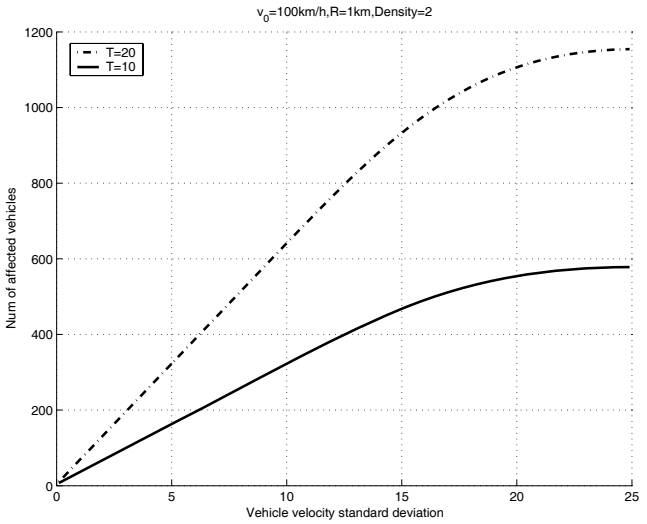


Fig. 7. Affected vehicles due to vehicle velocity standard deviation

easily extended to a multiple-lane scenario by multiplying the number of lanes to attain $E[k]$. Because of the radio reflection among vehicles, the virtual cell may be taken as a rectangle, which validates our assumption.

Fig. 6 shows the average bandwidth consumption of each message corresponding to different broadcast intervals for disseminating the authenticated tip of hash chain. It is observed that the larger the broadcast interval is, the smaller the average bandwidth is consumed by each message. In addition, the bandwidth consumption decreases less significantly after the broadcast interval reaches around 10. More interestingly, the saving of bandwidth becomes steady after the broadcast interval is greater than 20. Thus, with the simulation configurations, it is suggested that the broadcast interval is set to around 6 seconds, which is the knee in the curve obtained in the analysis, such that the vehicles can fully enjoy the most rapid decrease of bandwidth consumption while increasing broadcast interval.

Also, from Fig. 6, we observe that the saving of bandwidth usage is very limited when $T = 20$ is used as the broadcast interval instead of 10. Based on the fact that a vehicle is able to sense the velocity of an approaching vehicle, our suggested policy for achieving adaptive authenticated tip broadcasting is described as follows. When a vehicle observes that there is a large velocity deviation among neighboring vehicles, it takes a small broadcast interval, such as $T = 10$, which can help it to achieve an acceptable authentication delay at the expense of larger bandwidth consumption. Otherwise, it takes a normal broadcast interval such as $T = 20$ in order to obtain the optimal gain between the authentication delay and bandwidth consumption.

Next, we investigate the impact of adopting the proposed periodic broadcasting mechanism on newly joining vehicles. Let the average velocity $\overline{v}$ on a highway be $100km/h$. Fig. 7 illustrates the average number of affected vehicles (denoted as $E[k]$) versus vehicle velocity standard deviation (denoted as σ) with respect to different broadcast intervals. It is observed that under small σ, the number of affected vehicle is moderate and does not necessarily increase significantly with the increase of σ. However, the number of affected vehicle increases significantly with the increase of σ when σ is large. This indicates that the length of broadcast interval may impose a significant impact on the proposed mechanism in terms of the average number of affected vehicles, especially when σ is large.

IV. Security Analysis

The security of the proposed TSVC scheme is analyzed as follows.

- Data source privacy: The privacy of the data source is well protected because each vehicle is preloaded with a list of anonymous public/private key pairs as well as their corresponding public key certificates at the initialization stage. When a vehicle broadcasts the data packets, it just needs to pick up one pair of keys, where the private key is used to sign the first key release packet. Therefore, the real identity will not be disclosed during the whole TSVC scheme since only the pseudo ID of the data source has been used. Furthermore, since each anonymous public key certificate has a short life time, it is difficult to track an individual driver by way of an anonymous certificate.
- Traceability: The authorities can always reveal the real identities of the message senders by looking up in the database for matching between a real identity and the pseudo ID in order to guard the truth when there is any dispute.
- Data source authentication: With the proposed TSVC scheme, the data source can be efficiently authenticated to fit into the vehicular communication scenarios, which is described as follows: The first key release packet was signed by a private key corresponding to one anonymous public key certificate, where ECDSA is used. Since ECDSA is a secure and efficient digital signature scheme, anyone can explicitly authenticate the first key release packet. Afterwards, the key enclosed in the first key release packet can then be used to authenticate the first data packet. At the same time, since the secure one-way function is employed in the scheme, the subsequently

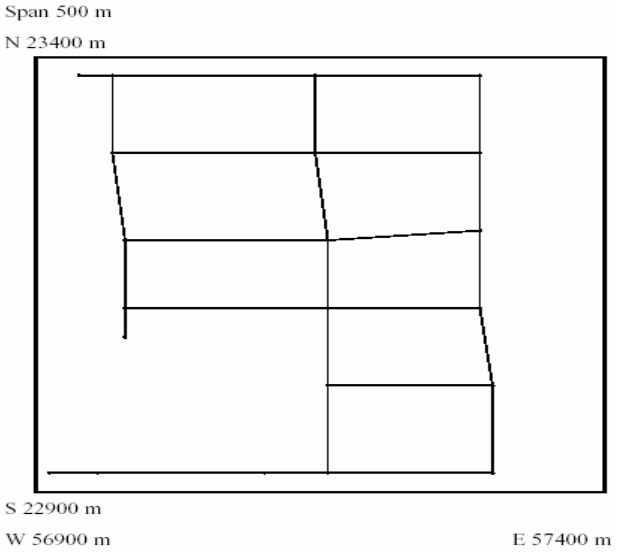


Fig. 8. A city map generated by [22] with span of 500 meters

arriving data packets can also be fast authenticated. If an adversary can forge the first authenticated key release packet, it will contradict with the hardness of the elliptic curve discrete logarithm problem. On the other hand, if an adversary can forge the latter authenticated packets, it will contradict with the one-way assumption of secure hash function. Therefore, the data source authentication can be achieved in our TSVC scheme.

- Resilient to the replay attack: Because a timestamp is embedded into each packet to verify its validity, the replay attack is also prevented.

V. Performance Evaluation

Simulation is conducted to verify the efficiency and applicability of the proposed scheme using ns-2 [26]. We are interested in the system performance concerning with the average *Packet Delay* (PD) and average *Packet Loss Ratio* (PLR) under the proposed security scheme, which is further compared with a number of traditional public key based security schemes. For the PLR, we only consider the packet loss caused by security mechanisms instead of lossy wireless channels.

Roadside communication on both scenarios of highway and city traffic supporting three lanes in each direction is simulated. In the highway scenario, each vehicle is first located with an even inter-vehicle distance and then starts traveling with a uniformly random speed within a range of $v \pm 10km/hr$, where v is the average velocity of each vehicle in the simulation. In the city scenario, in order to fully estimate the real world city road environment and vehicular traffic, we use the mobility model generation tool developed in [22], which is specialized to generate realistic traffic scenario files for vehicles in ns-2. This tool takes advantages of the publicly available *Topologically Integrated Geographic Encoding and Referencing* (TIGER) database from the U.S. Census Bureau, which contains detailed street maps for each city in the USA. The map adopted in the simulation is in Fig. 8 which corresponds to a part of the Afton Oaks area, Houston, TX, USA. Vehicles are first scattered randomly on one intersection of the roads and repeatedly move towards another randomly selected intersection along the path constrained by the map. Vehicles are driving with a random fluctuation range of $5miles/hr$ according to the road speed limit that ranges from $35 \sim 75miles/hr$. All the simulation parameters are listed in Table I.

TABLE I
SIMULATION CONFIGURATION

Highway simulation range	$2500m * 50m$
City simulation range	$500m * 500m$
Communication range	$300m$
Simulation time	$100s$
Channel bandwidth	$6Mbs$
Wireless Protocol	802.11
Pause time	$0s$
Digital signature signing delay	$1.52ms$
Message verification delay	$4.14ms$
MAC generation/verification delay	$1ms$
Length of TSVC data packet	120 $bytes$
Length of signed message	200 $bytes$
Buffer size for TSVC	80 $packets$ *
Buffer size for PKI	2 $packets$

* The buffer size should be large enough to store the number of messages that will be received during the key disclosure delay δ.

We first run a simulation to test the message transmission time through the wireless channel based on the highway situation with IEEE 802.11p. Because most of the transmission delay is incurred by wireless channel contention, which means the longest transmission time happens when the density of the traffic is the highest, we simulate the crowded traffic scenario in which the communication range is set as $300m$, and the inter-vehicular distance is set as $5m$. From the simulation result, the longest transmission delay is $6.467ms$. Therefore key disclosure delay δ for the later experiments is conservatively set as $100ms$ which is much larger than the actual delay and thus ensures the absolute security.

We then run two sets of simulations. The first set of simulations investigates the impact of the vehicle's moving speed in high way scenario, whereas the second set of simulations investigates the impact of vehicle's density in both highway and city scenario.

The metric of PD is composed of all the periods since the moment that the data packet is formed at the sender's side from the application layer to the moment that the receiving vehicle has the opportunity to react to the received data. Therefore, the latency for a successful transmission of a message is given by

$$t_{sign}(M)+t_{trans}+t_{queue}+t_{verify}(Cert)+t_{verify}(M) \quad (13)$$

for the traditional public key based protocols, and

$$t_{trans} + t_{queue} + t_{verify}(MAC) + t_{1-hash} \quad (14)$$

for the TSVC scheme. The delay induced by any cryptographic operation in the proposed scheme is automatically considered as ns-2 simulation delay according to the measurement of those algorithms based on cryptographic library MIRACL [25].

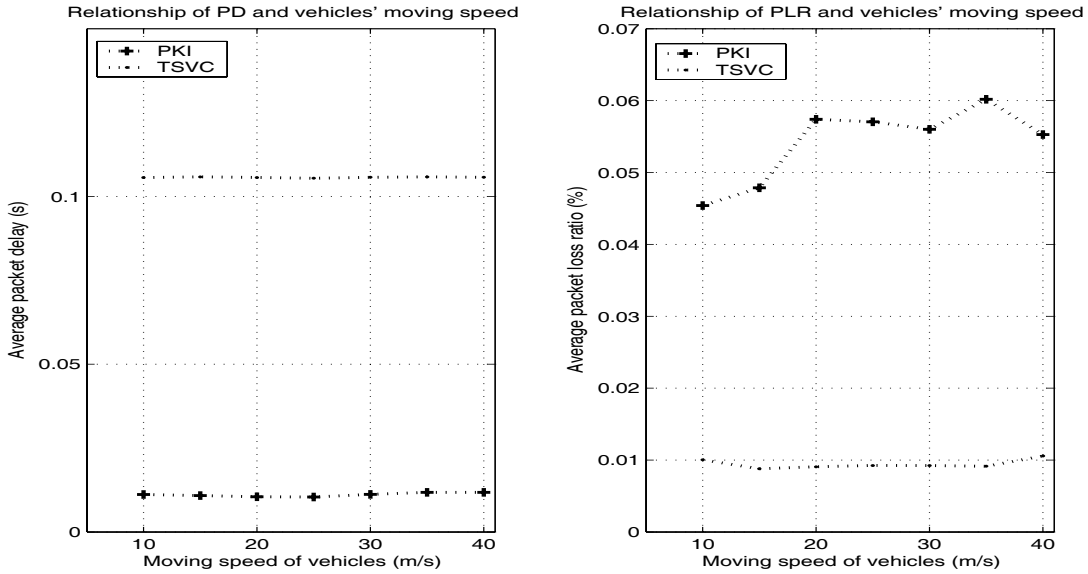


Fig. 9. Impact of vehicles' moving speed

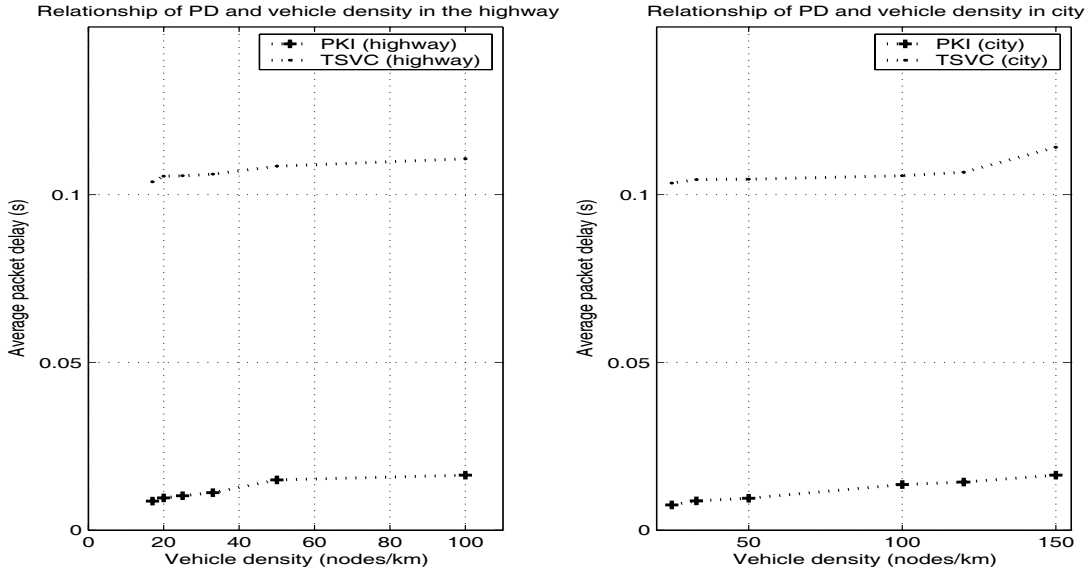


Fig. 10. Relationship of PD and vehicle density

A. Impact of Vehicle Moving Speed

In the first set of simulations, v (i.e., the average speed of the vehicles) is changed from $10m/s \sim 40m/s$ ($36km/hr \sim 144km/hr$). The initial inter-vehicle distance is 30 meters. The simulation results on the PD and PLR are shown in Fig. 9. In both of the schemes, the variation of speed does not affect much on PD and PLR. It can be seen that the proposed TSVC scheme yields larger PD which is negligibly higher than the key disclosure delay δ. The delay for TSVC is slightly higher than $100ms$. According to [4], the maximum allowable message latency is around $100ms$ to meet the human beings' reaction. Thus, both of the two schemes can meet this requirement. For PLR, TSVC yields much lower packet loss ratio compared with that of PKI based schemes under this normal traffic density.

B. Impact of Vehicle Density

In the second set of simulations, the impact of node density for both highway and city traffic is studied. The city traffic has different traffic model with highway scenario and is usually denser than that in the highway. From Fig. 10, it can be seen that TSVC has higher but acceptable packet delay than PKI. Moreover, the packet delay for both of the two schemes does not vary a lot with the increase of the traffic density. From Fig. 11, the traditional public key based protocol suffers a much higher packet loss ratio which has reached to 47% when the vehicle density is greater than 40 which makes it infeasible in practical use; however, our TSVC scheme maintains stable packet loss ratio which is not affected by the increase of the vehicle density.

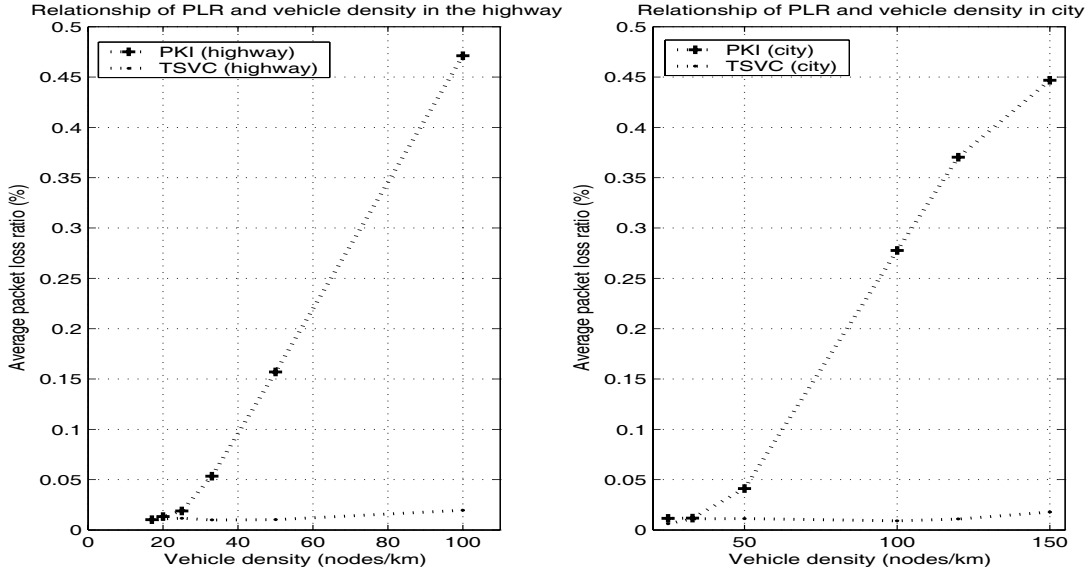


Fig. 11. Relationship of PLR and vehicle density

VI. Conclusions

We have proposed a novel TSVC security scheme for achieving efficient and secure vehicular communication, which not only meets the various security requirements and the driver's conditional privacy requirement, but also achieves high efficiency in terms of packet overhead and computation latency. We have demonstrated its practicality to the real-world applications. Our current research is to investigate the secure key revocation of compromised vehicles in VANETs, which is an important issue for any security scheme.

Acknowledgment

This research is partly supported by NSERC (Natural Sciences and Engineering Research Council of Canada). The authors would like to thank Dr. Minghui Shi for his helpful discussions.

References

[1] "Dedicated Short Range Communications (DSRC)." [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[2] "U.S. Department of Transportation, National Highway Traffic Safety Administration, Vehicle Safety Communications Project, Final Report," Apr. 2006.

[3] M. Raya and J.-P. Hubaux, "A security of vehicular ad hoc networks," in *Proc. SASN*, Alexandria, VA, Nov. 2005.

[4] U.S. Department of Transportation, "National highway traffic safety administration," in *Veh. Safety Commun. Project, Final Report. Appendix H: WAVE/DSRC Security*. Apr. 2006.

[5] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442-3456, 2007.

[6] M. Raya, A. Aziz and J.-P. Hubaux, "Efficient secure aggregation in VANETs," in *Proc. VANET*, California, USA, Sept. 2006.

[7] A. Perrig, R. Canneti, D. Song, and J. D. Tygar, "The TESLA broadcast authentication protocol," *RSA Cryptobytes*, vol. 5, no. 2, pp. 2-13, 2002.

[8] L. Lamport,"Password authentication with insecure communication," *Commun. of the ACM*, vol. 24, no. 11, pp. 770-772, 1981.

[9] R. Rivest and A. Shamir, "PayWord and MicroMint: two simple micropayment schemes," in *Proc. SPW*, LNCS, Springer-Verlag, vol. 1189, pp. 69-87, Berlin, 1996.

[10] Q. Huang, I. Avramopoulos, B. Liu, and H. Kobayashi, "Secure data forwarding in wireless ad hoc networks," in *Proc. ICC*, Seoul, Korea, May 2005.

[11] P. Golle and N. Modadugu, "Authenticating streamed data in the presence of random packet loss," in *Proc. ISOC NDSS*, San Diego, California, USA, Feb. 2001.

[12] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "Spins: security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 11, pp. 521-534, 2002.

[13] M. Reiter, "A security architecture for faulttolerant systems," Ph.D. thesis, Department of Computer Science, Cornell University, Aug. 1993.

[14] M. Reiter, K. Birman, and R. van Renesse, "A security architecture for fault-tolerant systems," *ACM Trans. Computer Syst.*, vol. 12, no. 4, pp. 340-371, Nov. 1994.

[15] V. Roca, A. Francillon, and S. Faurite, "The use of TESLA in the ALC and NORM protocols." [Online]. Available: http://www.ietf.org/internet-drafts/draft-ietf-msec-tesla-for-alc-norm-02.txt

[16] M. Nekovee, "Modeling the spread of worm epidemics in vehicular ad hoc networks," in *Proc. Veh. Technol. Conf.*, Montreal, Canada, Sept. 2006.

[17] F. Dion, H. Rakha, and Y. kang, "Comparison of delay estimates at under-saturated and over-saturated pre-timed signalized intersections," *Transportation Research Part B: Methodological*, vol. 38, no. 2, pp. 99-122, 2004.

[18] J. Zhao, Y. Zhang, and G. Cao, "Data pouring and buffering on the road: a new data dissemination paradigm for vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3266-3277, 2007.

[19] J. E. Khoury and A. Hobeika, "Incorporating uncertainty into the estimation of the passing sight distance requirements," *Computer-Aided Civil and Infrastructure Eng*, vol. 22, no. 5, pp. 347-357, 2007.

[20] T. L. Willke and N. F. Maxemchuk, "Coordinated interaction using reliable broadcast in mobile wireless networks," in *Proc. Networking 2005*, Waterloo, Canada, May 2005.

[21] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "LHAP: a lightweight hop-by-hop authentication protocol for ad-hoc networks," in *Proc. MWN*, May 2003.

[22] A. K. Saha and D. B. Johnson, "Modeling mobility for vehicular ad hoc networks," in *Proc. VANET*, Philadelphia, PA, USA, Oct. 2004.

[23] K. Ren, W. Lou, K. Zeng, and P. J. Moran, "On broadcast authentication in wireless sensor networks," *IEEE Trans Wireless Commun.*, vol. 6, no. 11, pp. 4136-4144, Nov. 2007.

[24] H. Zhu, X. Lin, P.-H. Ho, X. Shen, and M. Shi, "TTP based privacy preserving inter-WISP roaming architecture for wireless metropolitan area networks," in *Proc. IEEE Wireless Commun. Networking Conf. (WCNC'07)*, Hong Kong, China, Mar. 2007.

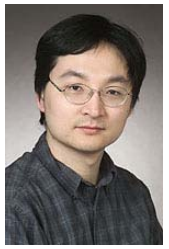
[25] "Multiprecision Integer and Rational Arithmetic C/C++ Library (MIRACL)." [Online]. Available: http://indigo.ie/ mscott/.
[26] The Network Simulator - ns-2. [Online]. Available: http://nsnam.isi.edu/nsnam/index.php/User_Information.
[27] "IEEE Std 1609.2-2006, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages," 2006.

Xiaodong Lin (S'07) is currently working toward his Ph.D. degree in the Department of Electrical and Computer Engineering at the University of Waterloo, Ontario, Canada, where he is a Research Assistant in the Broadband Communications Research (BBCR) Group. His research interests include wireless network security, applied cryptography, and anomaly-based intrusion detection.

Xiaoting Sun received the B.E. degree from Harbin Institute of Technology, Harbin, China, in 2003. She is currently working toward the Master' s degree with the David. R. Cheriton School of Computer Science, University of Waterloo, Waterloo, ON, Canada. Her research interests include wireless network security and privacy and security issues in vehicular communication networks.

Xiaoyu Wang received her B.S. degree in Electrical Engineering from Tongji University, Shanghai, China and the M. A. Sc degree in Electrical and Computer Engineering from Concordia University, Montreal, Quebec, Canada. She has been most recently a doctoral student in the Department of Electrical and Computer Engineering, University of Waterloo, ON, Canada. Her research interests focus on MAC protocol design, performance analysis, opportunistic spectrum sensing and access of cognitive radio systems.

Chenxi Zhang (S'07) received his B.E. and M.E. degree from the School of Computer Science and Technology at the Harbin Institute of Technology, China, in 2003 and 2005, respectively. He is a Ph.D. student in the Department of Electrical and Computer Engineering at the University of Waterloo, Canada. His research interests include wireless network security and vehicular network security.



Pin-Han Ho (M'04) received his B.Sc. and M.Sc. Degree from the Electrical and Computer Engineering department in the National Taiwan University in 1993 and 1995. He started his Ph.D. study in the year 2000 at Queen's University, Kingston, Canada, focusing on optical communications systems, survivable networking, and QoS routing problems. He finished his Ph.D. in 2002, and joined the Electrical and Computer Engineering department at the University of Waterloo, Waterloo, Canada, as an assistant professor at the same year. Professor Pin-Han Ho is the author/coauthor of more than 100 refereed technical papers and book chapters, and the co-author of a book on optical networking and survivability. He is the recipient of Distinguished Research Excellent Award in the ECE department of University of Waterloo, Early Researcher Award (Premier Research Excellence Award) in 2005, the Best Paper Award in SPECTS'02, ICC'05 Optical Networking Symposium, and ICC'07 Security and Wireless Communications symposium, and the Outstanding Paper Award in HPSR'02.

Xuemin (Sherman) Shen (M'97-SM'02) received the B.Sc. (1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a Professor and University Research Chair, and the Associate Chair for Graduate Studies, Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research focuses on mobility and resource management in interconnected wireless/wireline networks, UWB wireless communications systems, wireless security, and ad hoc and sensor networks. He is a co-author of three books, and has published more than 300 papers and book chapters in wireless communications and networks, control and filtering. Dr. Shen serves as the Technical Program Committee Chair for IEEE Globecom'07, General Co-Chair for Chinacom'07 and QShine'06, the Founding Chair for IEEE Communications Society Technical Committee on P2P Communications and Networking. He also serves as a Founding Area Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS; Editor-in-Chief for PEER-TO-PEER NETWORKING AND APPLICATION; Associate Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, KICS/IEEE JOURNAL OF COMMUNICATIONS AND NETWORKS, *Computer Networks*, *ACM/Wireless Networks*, and WIRELESS COMMUNICATIONS AND MOBILE COMPUTING (WILEY), etc. He has also served as Guest Editor for IEEE JSAC, IEEE WIRELESS COMMUNICATIONS, and IEEE COMMUNICATIONS MAGAZINE. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002 from the Faculty of Engineering, University of Waterloo. Dr. Shen is a registered Professional Engineer of Ontario, Canada.