Privacy-Preserving Vehicular Communication Authentication with Hierarchical Aggregation and Fast Response

Lei Zhang, *Member, IEEE,* Chuanyan Hu, Qianhong Wu, *Member, IEEE,* Josep Domingo-Ferrer, *Fellow, IEEE,* and Bo Qin

Abstract—Existing secure and privacy-preserving schemes for vehicular communications in vehicular *ad hoc* networks face some challenges, e.g., reducing the dependence on ideal tamper-proof devices, building efficient member revocation mechanisms and avoiding computation and communication bottlenecks. To cope with those challenges, we propose a highly efficient secure and privacy-preserving scheme based on identity-based aggregate signatures. Our scheme enables hierarchical aggregation and batch verification. The individual identity-based signatures generated by different vehicles can be aggregated and verified in a batch. The aggregated signatures can be re-aggregated by a message collector (e.g., traffic management authority). With our hierarchical aggregation technique, we significantly reduce the transmission/storage overhead of the vehicles and other parties. Furthermore, existing batch verification based schemes in vehicular *ad hoc* networks require vehicles to wait for enough messages to perform a batch verification. In contrast, we assume that vehicles will generate messages (and the corresponding signatures) in certain time spans, so that vehicles only need to wait for a very short period before they can start the batch verification procedure. Simulation shows that a vehicle can verify the received messages with very low latency and fast response.

Keywords: Identity-based signature, security, privacy, vehicular *ad hoc* networks

1 Introduction

As the society is paying more and more attention to transportation safety and efficiency, it is crucial to provide vehicles with current information about traffic conditions. In recent years, a special instantiation of mobile *ad hoc* networks (MANETs) known as vehicular *ad hoc* networks (VANETs) has been brought out, whose primary goal is to enhance the safety and efficiency of road traffic. In VANETs, vehicles are able to communicate with each other, which dramatically increases their awareness of their driving environment [33].

A typical VANET consists of three main kinds of entities, i.e., trusted authority (TA), roadside units (RSUs) and vehicles with embedded on-board units (OBUs). The TA is responsible for the maintenance of the entire system. RSUs are deployed along the roadside. They act as forwarding stations or perform some authentication work to alleviate the burden of the TA. OBUs help vehicles to collect and process the information related to their driving circumstances, and to communicate with other entities. There are three types of communication in VANETs: vehicle-to-vehicle (V2V), vehicle-to-roadside (V2R) and roadside-to-vehicle (R2V). VANET communication empowers vehicles in an unprecedented way. For instance, V2V and R2V allow a certain vehicle to gain a better understanding of its driving environment and thereby avoid accidents, jams or other troubles. In turn, V2R enables the vehicle to become itself a source of traffic information. Also, R2V and V2R can provide the vehicles with value-added services (e.g., internet access, navigation and real-time multimedia streaming applications [23]).

The potential growth and the business opportunities of VANETs have attracted a lot of attention from both academia and industry [23], [25], [26], [33]. However, benefits usually come with challenges. One of the most important challenges is security [34], [41]. In VANETs, the messages transmitted are often life-critical. It is essential to ensure that the messages received by a vehicle are authenticated and non-repudiatable. Another main challenge is about privacy [14], [16], [24], [37]. Vehicles are usually personal devices that are kept for a long time. If an attacker can link together the data sent/received by a vehicle, he can infer a lot about the personal behavior of the vehicle's usual driver [31]. Therefore, vehicle privacy must be protected. Nonetheless, security sometimes conflicts with privacy. The former requires knowing the origin of messages, while the latter requires that no entity (other than the message generator) can trace a message to its generator. Consequently, it is a challenge to find an optimal trade-off between security and privacy. In fact, conditional privacy is usually considered

• *Lei Zhang and Chuanyan Hu are with Shanghai Key Laboratory of Trustworthy Computing, Software Engineering Institute, East China Normal University, China, and State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, China; Qianhong Wu is with School of Electronics and Information Engineering, Beihang University, China and State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 100093, China and Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan, China; Josep Domingo-Ferrer is with the Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, Catalonia; Bo Qin is with Key Laboratory of Data Engineering and Knowledge Engineering, Ministry of Education, School of Information, Renmin University of China, Beijing, China (e-mail: leizhang@sei.ecnu.edu.cn, chuanyanhu@ecnu.cn, qhwu@xidian.edu.cn, josep.domingo@urv.cat, bo.qin@ruc.edu.cn).*

in VANETs. In other words, vehicle privacy is guaranteed under normal circumstances but, if a false message (one containing deceptive information) is found, the TA can retrieve the message generator's identity.

Besides security and privacy, aggregation of cryptographic witnesses is another challenge. In a VANET, a traffic management authority (TMA) monitors the vehicles and uses RSUs to collect messages from the vehicles. Based on those messages, the TMA can optimize the driving conditions of vehicles, e.g., by reducing the traffic congestion via adaptative switching of traffic lights depending on vehicle density, by estimating traffic jams and warning on them, etc. However, millions of vehicles may exist in a VANET, which implies that huge volumes of data may be sent to the TMA, thereby causing data transmission congestion and storage burden. Sophisticated techniques for regular message compression have been proposed in [22], [50]. Yet these techniques do not work on cryptographic witnesses, because compression may destroy them (e.g., compressing a certificate destroys it). Hence, aggregating cryptographic witnesses is more challenging, so we will focus on it rather than on compression of regular messages.

1.1 Related Work

Extensive studies have been published [12], [13], [20], [23], [36], [45], [46] to realize conditional privacy-preserving communications in VANETs. Roughly, they can be classified into two categories: protocols based on pseudonyms and protocols based on group signatures.

In the first category, the foundational work was done by Raya et al. [33]. They proposed a concrete protocol based on traditional signatures and anonymous certificates, in which pseudonyms are used to hide the real identities of users in traditional certificates. Before verifying the validity of a signature, a verifier needs to check the validity of the corresponding certificate. Further, to achieve vehicle privacy, each pseudonym and its corresponding certificate must be short-lived. Otherwise, a vehicle could be tracked by a global attacker based on vehicular messages and the certificate. Therefore, vehicles have to store large amounts of anonymous certificates. Besides, vehicles can be corrupted by attackers. This implies a heavy certificate revocation management. To mitigate the certificate verification and revocation management costs, a popular approach is to use identity-based cryptography, in which the public key of an entity is just its identity (or pseudonym). However, most existing identity-based schemes are predicated on bilinear maps, which are costly to compute [42]. In [42], an identity-based protocol which requires constant bilinear map operations is proposed. In this scheme, each vehicle can generate pseudonyms and corresponding private keys off-line. Nevertheless, the scheme requires that the system master key be loaded in an (ideally) tamper-proof device which is secure against any attacks. This is a very strong assumption (see [32], [36], [46]). If the system master key is recovered by an attacker, the whole system will be at risk. Similar protocols can be found in [13], [20].

Protocols based on group signatures [9] are presented in [23], [25], [37], [44], [49]. In such protocols, a vehicle can sign messages on behalf of the whole group. No entity (other than the group manager) can distinguish the real signer among the group members. Therefore, protocols in this class can easily achieve conditional privacy. However, they face substantial communication and verification costs as well as the member revocation problem. The communication and verification costs of a group signature are much higher than the ones of a traditional signature. Further, if vehicles can be revoked, there is usually a high cost to check whether group members have been revoked or not; it may even be necessary to set up again the whole group. For a large-scale VANET, those costs seem too high in practice. We note that group signatures with verifier-location revocation [7] can be used to alleviate the member revocation problem. However, they have a limitation similar to the one of the schemes using certificate revocation lists: as the number of revoked vehicles in the system grows, they becomes very inefficient.

Batch verification [11], [28] is widely employed in privacy-preserving schemes for secure vehicular communications to accelerate signature verification. It is useful if multiple signatures need to be verified at once. However, existing batch verification based schemes in VANETs assume that vehicles generate messages (and the corresponding signatures) at random time points [13], [20], [18], [36]. A vehicle may receive only a few messages in a short time span. Therefore, to take full advantage of the batch verification technique, a vehicle usually has to wait to get enough messages, which results in additional delay.

Compared to efforts on security and privacy in VANETs, the literature on aggregating vehicle-generated cryptographic witnesses is rare. By applying short signatures in the PKI setting, Zhu *et al.* [48] proposed a protocol for aggregation of *emergency messages* in VANETs. Though the signatures can be aggregated into a single one, the certificates from different users cannot. This is problematic, as a certificate is much longer than a signature. Aggregation technologies are also used in [38] to enable each vehicle to verify the received signatures and corresponding certificates simultaneously. However, this scheme is designed for the PKI setting, so certificate management remains a problem. Aggregation techniques for identity-based cryptographic witnesses eliminate the need for certificates and hence reduce the transmission/storage overhead. However, the existing schemes in this class are based on strong assumptions that an attacker cannot recover the system master secret stored in the tamper-proof device [32], [36], [46] or they only consider the aggregation of cryptographic witnesses generated on the same message [19]. Further, the above schemes only handle cryptographic witness aggregation in a single entity. In the real world, the social organization usually has a hierarchical architecture. How to aggregate the cryptography witnesses by taking hierarchy into account is more challenging.

1.2 Contributions and Paper Organization

Existing VANET solutions that provide security and privacy face some challenges, e.g., reducing the dependence on ideally tamper-proof devices, building efficient member revocation mechanisms and avoiding computation and communication bottlenecks. This paper proposes a highly efficient identity-based aggregation and conditional privacy-

preserving scheme for vehicular communications, which addresses the above challenges.

In our scheme, vehicles communicate with each other using short-term pseudonyms and without certificates, which alleviates the overheads of certificate verification, revocation management and storage. Short-term pseudonyms (and corresponding private keys) are issued by a TA called key generator center (KGC) and can be updated online through a protocol predicated on identity-based signcryption which offers efficient member authentication. With the short-term pseudonyms and corresponding private keys, a vehicle can anonymously generate identity-based aggregate signatures with one-time common strings (which are used when signing a message). To make sure the scheme works well, the vehicles have to obtain common strings synchronously. Otherwise, the merits of the chosen identity-based aggregate signature scheme cannot be fully exploited. This is achieved by our protocol for common string synchronization. All the messages signed under the same common string by different vehicles can be aggregated and verified simultaneously.

Our scheme enables hierarchical aggregation. In VANETs, a TMA has to collect the messages sent by vehicles for traffic analysis. Here, we consider a hierarchical architecture which includes a TMA center, sub-TMAs, RSUs and vehicles. Vehicles work as leaf nodes and broadcast signed safety-related messages. The messages signed under the same common string can be aggregated and verified by the nearby RSUs. The aggregated messages are later forwarded to the sub-TMAs for traffic analysis. A sub-TMA can re-aggregate and verify the messages received from RSUs in its domain. The sub-TMAs may also forward urgent or important messages to the TMA center for a decision. The TMA center will perform the final aggregation and verification. In each aggregation step above, the aggregated signature is as short as a single signature from a vehicle. With our hierarchical aggregation technique, we significantly improve the performance of the system by reducing the computing/storage overheads of the vehicles and related parties.

Batch verification techniques (and aggregate signatures [8][1]) employed so far in conditional privacy-preserving schemes for secure vehicular communications all assume that vehicles generate messages at fully random time points. As a consequence, to take advantage of batch verification, a vehicle has to wait for a sufficient number of messages. However, the time cost of waiting for messages often overrides the savings of subsequent batch verification. Unlike the existing batch verification based schemes, we assume that vehicles generate messages close to certain time points. In our scheme, we divide each message sending period into two time segments with the same time span. A vehicle will generate a message only in the first several milliseconds of a time segment. By this mechanism, vehicles only need to wait for a very short period, and then they can start the batch verification procedure. Simulations show that our scheme has a low verification delay and a low loss rate. Therefore, our scheme achieves signature (hierarchical) aggregation, batch verification, and low latency.

1. For the difference between batch verification and aggregate signature, please refer to [15]. However, since an aggregate signature scheme allows a verifier to verify multiple signatures at the same time, we still call an aggregate signature scheme is a scheme which supports batch verification.

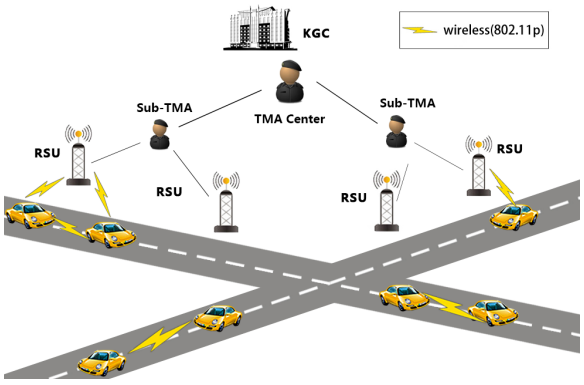


Fig. 1: System architecture

We note that our scheme is mainly designed for periodically generated messages (i.e., messages containing driving information of a vehicle such as speed, location and direction). A vehicle, occasionally, may also broadcast non-periodically generated (emergency) messages, (e.g., hard brake message). For such messages, a vehicle can use the current common string to generate the corresponding identity-based aggregate signature scheme and send out the signed message. A receiver can verify the message independently and immediately.

The remainder of this paper is organized as follows. In Section 2, we illustrate the system architecture, the security and privacy requirements and some related technical preliminaries. Our concrete scheme is proposed in Section 3. Section 4 proves the security of our scheme, and its efficiency is evaluated in Section 5. Section 6 compares our approach with the scenario of fully random message generation. Section 7 is a conclusion.

2 Background

2.1 System Architecture

Our system consists of four main entities, i.e., KGC, TMAs, RSUs and vehicles. The system architecture is illustrated in Figure 1.

- The KGC is a trusted authority. It bootstraps the whole system. All the vehicles and RSUs have to register to the KGC before joining a VANET.
- RSUs are deployed along the roadside to assist the communications among vehicles and the KGC.
- Vehicles move on roads. They communicate with each other, RSUs or the KGC via RSUs.
- A sub-TMA collects the messages from the vehicles through RSUs. With these messages, the sub-TMA optimizes the driving conditions of vehicles. Urgent or important messages are forwarded by the sub-TMAs to the TMA center for a decision.

The V2V, V2R and R2V communications use wireless networks based on IEEE 802.11p [1], [40]. The rest of communications are through wired links which enjoy high bandwidth, low delay and low bit error rate.

2.2 Design Goals

Many kinds of attacks threaten the system (e.g., message replay, message modification, movement tracking). To avoid these attacks, several security and privacy features are needed:

- **Message authentication**. A message receiver should be able to check that the received message is unaltered and the message generator is a legitimate entity in the system.
- **Non-repudiation**. The message sender cannot deny having sent the message.
- **Message confidentiality**. All sensitive communications should remain inaccessible to anyone other than the senders and the corresponding receivers.
- **Privacy**. Under normal circumstances, a message receiver should be unable to guess the real identity of the message generator or distinguish whether two messages come from the same generator. This implies that an attacker cannot trace a vehicle based on the received messages.
- **Traceability**. The generators of false messages should be traceable. To this end, an authority should be able to disclose the real identity of a message sender when there is a dispute. In our scheme, the KGC will fulfill this role.

Besides the above traditional security and privacy requirements, this paper addresses the requirements of fast response and cryptographic witness (signature) aggregation:

- **Fast response**. Once the messages sent by nearby vehicles have been received, an entity must start the verification procedure as soon as possible.
- **Low transmission/storage overhead**. It must be possible for an entity to aggregate the received messages, especially the cryptographic witnesses. Furthermore, it must be possible to a higher-level aggregator (e.g., TMA) to re-aggregate the aggregated messages.

2.3 Identity-based Public Key Cryptosystem, Aggregate Signatures and Signcryption

Identity-based public key cryptosystems (ID-PKC) are introduced to eliminate the certificate management problem in traditional PKI-based public key cryptosystems [7], [35]. In an ID-PKC, the public key of an entity is just its identity (and usually some auxiliary information, e.g., validation period). The private key of the entity is generated by a trusted authority referred to as key generator center (KGC) based on the identity of the entity. In VANETs, we can use a driver's license number as the real identity of a vehicle and the location of an RSU (e.g., street name||city name) as the identity of the RSU. In this paper, we will employ identity-based aggregate signatures and identity-based signcryption to guarantee the security of the system.

An aggregate signature scheme is a signature scheme that supports aggregation: given n signatures on n messages under such a scheme, these signatures can be aggregated into a single signature whose size is constant and whose validity implies the validity of the n signatures. To verify that the n signatures are respectively valid for the n original messages, the verifier just needs to verify the aggregate signature. In this paper, we use an extended identity-based aggregate signature scheme [17] for secure vehicular communications. The scheme in [17] is the most efficient of its kind but, in order to fully exploit its efficiency, all the signers in an aggregated set must obtain the same one-time-use common string when signing a message. However, due to the high mobility of vehicles, it seems hard for them to get such one-time strings. We therefore propose a protocol for common string synchronization. Every verifier is then able to aggregate a set of signatures under the same common string and verify the signatures simultaneously. We note that the aggregate signature scheme in [17] is implemented with symmetric pairings. However, asymmetric pairings have better security properties and can lead to considerably shorter signatures/ciphertexts than symmetric pairings. To enjoy the advantages of asymmetric pairings, we convert this scheme into one based on asymmetric pairings.

A signcryption scheme [10], [47] combines the functions of digital signature and encryption, i.e., confidentiality, message authentication and non-repudiation. Further, some signcryption schemes also satisfy '*ciphertext anonymity*' whereby a ciphertext hides the identities of both the sender and the recipient from third parties. This property can be used to achieve the *privacy* requirement in VANETs. Though a signcryption scheme combines digital signature and encryption, its computational cost and communication overhead are much smaller than those of sign-then-encrypt schemes [47]. In our proposal, we will employ an extended identity-based signcryption scheme in [10] to help vehicles update their pseudonyms and corresponding private keys. This signcryption scheme has been proven to satisfy confidentiality, message authentication, non-repudiation and ciphertext anonymity. We note that the signcryption scheme in [10] is also implemented with symmetric pairings. We convert it into one based on asymmetric pairings.

2.4 Pairings

Most of the existing identity-based schemes use pairings (a.k.a. bilinear maps). Let $\mathbb{G}_1$, $\mathbb{G}_2$ be two additive cyclic groups and $\mathbb{G}_T$ be a multiplicative cyclic group, all with the same prime order q, and P_1, P_2 be random elements in $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. A pairing is a map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ satisfying 1) (Bilinearity) $\hat{e}(aP_1, bP_2) = \hat{e}(P_1, P_2)^{ab}$ for any $a, b \in \mathbb{Z}/q\mathbb{Z}$; 2) (Non-degeneracy) $\hat{e}(P_1, P_2) \neq 1_{\mathbb{G}_T}$; 3) (Computability) There exists an efficient algorithm to compute $\hat{e}(P_1, P_2)$. If $\mathbb{G}_1 = \mathbb{G}_2$ the pairing is symmetric; otherwise it is asymmetric.

3 Our Scheme

In this section, we describe our proposal for secure vehicular communications. To simplify the presentation, we collect in Table 1 the notations employed in the rest of this paper.

3.1 High Level Description

At a high level, our proposed scheme can be described in terms of four protocols: system setup, protocol for STP and STK distribution, protocol for common string synchronization, and protocol for vehicular communications.

TABLE 1: Notations

Notation	Description
KGC	The key generation center
V_i	A vehicle
R_j	An RSU
$H_{\{1\sim6\}}$	Hash functions
$E_k(\cdot)/D_k(\cdot)$	A symmetric encryption/decryption scheme, where $E_k(\cdot)$ is the encryption algorithm, $D_k(\cdot)$ is the decryption algorithm, and k is the key used for encryption and decryption
$ID_{\{V_i,R_j,kgc\}}$	The identity of V_i, R_j or the KGC
$B_{j,kgc}$	The private key of R_j or the KGC
LP	Long time period
LTP	Long-term pseudonym
LTK	Long-term private key corresponding to an LTP
vp	Validity period
STP	Short-term pseudonym
STK	Short-term private key corresponding to an STP
CS	Common string
$\|\|$	The message concatenation operation
$\oplus$	The exclusive-OR (XOR) operation
τ_i	A timestamp

In the first protocol, the KGC sets up the whole system. It generates the system global parameters and the master key. For each registering vehicle, the KGC generates a long-term pseudonym LTP and the corresponding private key LTK. Each RSU also needs to register to the KGC. However, since the privacy of an RSU does not need to be protected, the KGC just issues a private key for an RSU based on the real identity of the RSU. The second protocol mainly deals with the distribution of the short-term pseudonym STP and the short-term private key STK to a vehicle. According to [33], an STP and the corresponding STK used for secure communications should be short-lived, so that frequent updates of the STP-STK pairs are needed in practice. We propose an online distribution protocol for vehicles to renew their STPs and corresponding STKs. The third protocol ensures that vehicles can obtain synchronized common strings when signing. The last protocol implements secure and privacy-preserving vehicular communications. In this protocol, a vehicle uses its STPs and STKs to sign messages under common strings by means of a modified identity-based aggregate signature scheme. A vehicle or an RSU is able to aggregate a set of signatures under the same common string into a single aggregate signature which can be verified at low cost. The signatures received by RSUs can be re-aggregated by sub-TMAs and the TMA center. Finally, if a false message is found, the KGC can find the real identity of the message generator.

3.2 System Setup

The KGC maintains a member list ML and bootstraps the whole system as follows:

1) On input a security parameter ℓ, generate two cyclic additive groups $\mathbb{G}_1$ and $\mathbb{G}_2$ and one cyclic multiplicative group $\mathbb{G}_T$ all with the same large prime order q. Let the generator of $\mathbb{G}_1$ be P_1 and the generator of $\mathbb{G}_2$ be P_2. It is required that there exists a bilinear map $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ and a computable isomorphism ψ from $\mathbb{G}_2$ to $\mathbb{G}_1$ with $\psi(P_2) = P_1$ [6].
2) Choose a symmetric encryption/decryption scheme $E_k(\cdot)/D_k(\cdot)$.
3) Select six hash functions $H_1 : \{0,1\}^* \to \mathbb{G}_1, H_2 : \{0,1\}^* \to \mathbb{G}_2, H_3 : \{0,1\}^* \to \mathbb{Z}/q\mathbb{Z}, H_4 : \{0,1\}^* \to \{0,1\}^{l_1}, H_5 : \{0,1\}^* \to \{0,1\}^{l_2}, H_6 : \{0,1\}^* \to \{0,1\}^{l_3}$.
4) Choose (ζ, λ) as the system master key, where $\zeta \in \mathbb{Z}/q\mathbb{Z}$ and λ is chosen from the key space of $E_k(\cdot)/D_k(\cdot)$.
5) Set $U_1 = \zeta P_1, U_2 = \zeta P_2, P_{kgc} = H_2(ID_{kgc}), B_{kgc} = \zeta P_{kgc}$, where ID_{kgc} is the identity of the KGC.
6) Set $pub = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \hat{e}, P_1, P_2, U_1, U_2, \psi, H_1 \sim H_6,\ E_k(\cdot)/D_k(\cdot), l_1, l_2, l_3, ID_{kgc}, P_{kgc})$ as the system public parameters.

A vehicle V_i has to pre-load the system public parameters pub and register to the system. When V_i registers to the system, the KGC chooses a symmetric key k_i from the key space of the symmetric encryption scheme, and generates an LTP (e.g., valid for one month) and the corresponding private key as follows:

1) Choose a long time period LP_i (e.g., $[01.2015, 02.2015]$). Compute $pid_i = H_4(ID_{V_i}||LP_i)$, and set $LTP_i = pid_i||LP_i$, where ID_{V_i} is the real identity of V_i.
2) Compute $P_{V_i} = H_1(LTP_i)$ and set $LTK_i = \zeta P_{V_i}$ as V_i's long-term private key.
3) Distribute (k_i, LTP_i, LTK_i) to V_i and add the record (ID_{V_i}, k_i, LTP_i) to ML.

When V_i receives (k_i, LTP_i, LTK_i) from the KGC, it computes $P_{V_i} = H_1(LTP_i)$. Then V_i stores $(k_i, LTP_i, LTK_i, P_{V_i})$ locally.

Each RSU also needs to pre-load pub and register to the KGC. For an RSU R_j, the KGC computes $B_j = \zeta P_{R_j}$ as R_j's private key, where $P_{R_j} = H_2(ID_{R_j})$ and ID_{R_j} is the real identity of R_j.

3.3 Protocol for STP and STK Distribution

To protect the privacy of a vehicle, the STP and the corresponding STK of the vehicle should be changed frequently. Thus, numerous STP-STK pairs will be needed. However, if a huge number of STP-STK pairs are stored in a vehicle (e.g., STP-STK pairs for one year), it can be a huge burden to revoke such pairs in case the vehicle is corrupted. Here, we propose a protocol predicated on identity-based signcryption [10] to ensure that vehicles are able to securely reload STP-STK pairs via nearby RSUs. In our protocol, the vehicles only request STP-STK pairs for a short period (e.g., one day) [26]. Note that the LTP and the corresponding LTK of a vehicle may also expire. This protocol allows the vehicle to update its LTP-LTK pair as well.

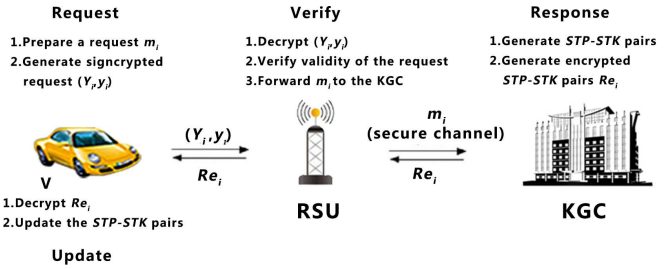


Fig. 2: Basic ideas in the protocol for STP and STK distribution

In this protocol, we assume that: i) a secure channel is pre-established between an RSU and the KGC; ii) the RSU is semi-trusted, i.e., curious but honest. In our protocol, for practicality, the secure channel can be generated using an authenticated key agreement protocol. The protocol consists of four phases: Request, Verify, Reply and Update. In the first phase, a vehicle prepares a request, the request is then signcrypted based on the identity-based signcryption scheme in [10] and sent to the nearby RSU. In the second phase, the RSU verifies the validity of the signcrypted request on behalf of the KGC. If it is valid, the request is forwarded to the KGC. In the third phase, the KGC issues STP-STK pairs for the vehicle. If the LTP and the corresponding LTK of the vehicle are about to expire, a new LTP-LTK pair is also generated. Finally, in the last phase, the vehicle updates its STP-STK pairs (and the LTP-LPK pair if required). Figure 2 illustrates these basic ideas.

Suppose that a vehicle V_i requests fresh STP-STK pairs via its nearby RSU R_j, whose identity is ID_{R_j}. The protocol runs as follows:

[Request] V_i issues a request as follows:

1) Set the request $m_i = (n_i, LTP_i, \tau_i)$, where n_i denotes the number of fresh STP-STK pairs that V_i requests.
2) Signcrypt the request as follows:
   a) Choose $r_i \in \mathbb{Z}/q\mathbb{Z}$, and compute $Y_i = r_i P_{V_i}, h_i = H_3(Y_i||m_i)$, and $Z_i = (r_i + h_i)LTK_i$;
   b) Compute $w_i = \hat{e}(r_i LTK_i, P_{R_j}), y_i = H_5(w_i) \oplus (Z_i||m_i)$, where $P_{R_j} = H_2(ID_{R_j})$.
3) Send (Y_i, y_i) to R_j.

[Verify] In this phase, R_j verifies whether V_i's request is valid. Specifically R_j does:

1) For a single signcrypted request (Y_i, y_i), first decrypt the request by computing
$$w_i' = \hat{e}(Y_i, B_j), y_i \oplus H_5(w_i') = (Z_i||m_i),$$
then check the validity of the timestamp τ_i in m_i, and compute $P_{V_i} = H_1(LTP_i)$ and $h_i = H_3(Y_i||m_i)$, where LTP_i is extracted from m_i and B_j is the private key of R_j.
2) Verify whether the signature is valid by checking
$$\hat{e}(Z_i, P_2) \stackrel{?}{=} \hat{e}(Y_i + h_i P_{V_i}, U_2).$$
If the equation holds, forward m_i to the KGC through a secure channel; otherwise, abort. The correctness of the above signature verification follows from direct algebraic manipulation.

[Reply] For each request $m_i = (n_i, LTP_i, \tau_i)$, the KGC recovers the record (ID_{V_i}, k_i, LTP_i) from ML, and extracts LP_i from LTP_i. KGC generates n_i STPs and corresponding STKs, and returns an encrypted reply to V_i via R_j. If LP_i is about to expire, a new LTP and the corresponding private key are also returned to V_i. Specifically, the KGC goes through the following steps:

1) Select a validity period vp_i (e.g., the current day).
2) For $1 \le j \le n_i$, set $sid_{i,j} = E_\lambda((LTP_i||j) \oplus H_6(vp_i))$ and $STP_{i,j} = sid_{i,j}||vp_i$.
3) For each $STP_{i,j}$, compute the corresponding STK
$$STK_{i,j} = (T_{i,j,0}, T_{i,j,1}) = (\zeta P_{i,j,0}, \zeta P_{i,j,1}),$$
where $P_{i,j,0} = H_1(STP_{i,j}, 0), P_{i,j,1} = H_1(STP_{i,j}, 1)$.
4) If LP_i is about to expire, generate a new LTP, say LTP_i', and the corresponding LTK, say LTK_i', and compute
$$Re_i = E_{k_i}(LTP_i', LTK_i', vp_i||(sid_{i,1}, STK_{i,1})||... ||(sid_{i,n_i}, STK_{i,n_i}));$$
otherwise, compute the ciphertext
$$Re_i = E_{k_i}(vp_i||(sid_{i,1}, STK_{i,1})||... ||(sid_{i,n_i}, STK_{i,n_i})).$$
5) Send Re_i to V_i as the reply.

[Update] When V_i receives the reply Re_i, it decrypts Re_i by computing $D_{k_i}(Re_i)$ to extract
$$(vp_i||(sid_{i,1}, STK_{i,1})||...||(sid_{i,n_i}, STK_{i,n_i}))$$
or
$$(LTP_i', LTK_i', vp_i||(sid_{i,1}, STK_{i,1})||...||(sid_{i,n_i}, STK_{i,n_i}));$$
for $1 \le j \le n_i$, V_i sets $STP_{i,j} = sid_{i,j}||vp_i$; V_i stores
$$(STP_{i,1}, STK_{i,1}), ..., (STP_{i,n_i}, STK_{i,n_i})$$
in the vehicle; V_i sets $LTP_i = LTP_i', LTK_i = LTK_i'$ if LP_i is about to expire.

3.4 Protocol for Common String Synchronization

The protocol for vehicular communications in the next section assumes that vehicles can obtain synchronized common strings when signing. A common string is a (unique) string which is used when signing a message. In our scheme, all the messages signed under the same common string can be aggregated and verified simultaneously. However, messages under different common strings cannot be aggregated and batch verified. In other words, the messages received by a vehicle in a short period can be verified in a batch iff all the messages are signed under the same common string. Further, to guarantee the security and efficiency of our system, it is required that a common string be of one-time use. In this section, we propose a protocol for common string synchronization based on vehicle clocks.

Existing secure and privacy-preserving communication protocols in VANETs assume that vehicles generate and sign safety messages periodically (e.g., every 100 ms) but at fully random time points. Since vehicles send messages periodically rather than continuously, we can restrict the time spans in which they generate and sign safety messages. In this case, we could use the information related to the time spans as the common strings.

Assume the vehicles have access to (loosely) synchronized clocks which have the format

$$MS.S.M.H.D.M.Y.$$

We divide a message sending period δ into t time segments. Each segment is δ/t ms long, i.e., the k-th segment covers the interval

$$[k\delta/t, (k+1)\delta/t) \text{ ms}, 0 \leq k \leq t-1.$$

In this paper, we assume the message sending period is 100 ms. A common string is defined to be

$$k.n.S.M.H.D.M.Y,$$

where $0 \leq k \leq t-1, 1 \leq n \leq 10$ (n is the number of the message sending period within the current second). The time point for a vehicle to generate and send a safety message is restricted to the first several milliseconds of a time segment. We define this period to be τ_s. However, this creates a new problem. If the time segment is too long (e.g. $= 100$ ms) and the vehicle density is high, a vehicle may receive a huge number of messages in a short period, since all the vehicles must generate and send safety messages in τ_s of the same time segment. This will result in a large verification latency. Further, if τ_s is short, this will result in a high channel congestion rate. On the other hand, if the time segment is too short (e.g. ≤ 10 ms), only a few messages will be received by a vehicle, and the benefit of the batch verification cannot be well leveraged, which will result in message loss. In Section 5, we will show how to choose t and τ_s.

We note that our idea is similar to time division multiple access (TDMA) [4], [21], [29], which is a kind of controlled access protocol used for channel acquisition in the MAC layer. TDMA periodically divides the signal into different time slots, so that several transmitters are able to deliver their personal contents during their individual time slots to the receiver(s). Our main goals are to generate synchronized common strings and accelerate the response to vehicle-generated messages, which are goals different from those of TDMA.

3.5 Protocol for Vehicular Communications

Vehicles need to communicate with each other to share their information on driving conditions. This section proposes a secure and privacy-preserving protocol for vehicular communications.

The message format is illustrated in Table 2. The "Payload" field includes safety-related information, such as acceleration, direction and position. "Timestamp" is used to defeat the message replay attack. Further, as defined in the protocol for common string synchronization, the common strings are generated based on the timestamps. The "TTL" field is the **T**ime **T**o **L**ive, which records a timer denoting how long this message will remain in the system. "ID" is a pseudonym of a vehicle. The "Signature" field is a signature on the first four fields. It requires that the signature be valid under the pseudonym of the vehicle.

TABLE 2: Message format

Payload	Timestamp	TTL	ID	Signature
100 bytes	4 bytes	1 bytes	35 bytes	64 bytes

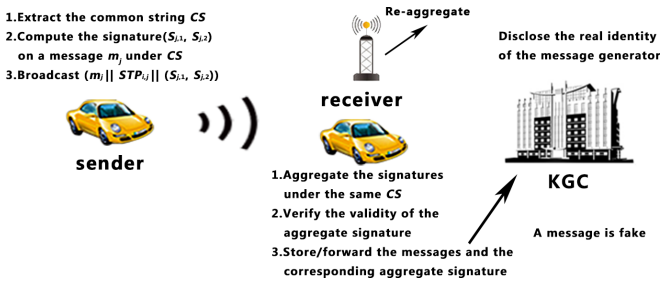


Fig. 3: Basic ideas in the protocol for vehicular communications

The protocol has five phases: Sign, Verify, Store, Re-aggregate and Trace. In the first phase, a vehicle generates a signature on Payload||Timestamp||TTL under a synchronized common string. In the second phase, all the signatures computed under the same common string are aggregated and verified in a batch. In the third phase, if the signatures are valid, the messages and corresponding aggregate signature are stored. Re-aggregation of signatures may occur in the fourth phase. In the last phase, if a false message is found, an efficient algorithm can determine the real identity of the message generator. Figure 3 illustrates these basic ideas. The detailed protocol is as follows:

[Sign] Suppose the safety message is

$$m_j = \text{Payload}||\text{Timestamp}||\text{TTL},$$

and the current STP-STK pair of a vehicle V_i is

$$(STP_{i,j}, STK_{i,j} = (T_{i,j,0}, T_{i,j,1})).$$

V_i first extracts the current common string CS based on the Timestamp, then performs the following steps:

1) Compute $P_{CS} = \psi(H_2(CS))$ and $c_j = H_3(m_j, STP_{i,j}, CS)$.
2) Choose a random $r_j \in \mathbb{Z}/q\mathbb{Z}$ and generate the signature $(S_{j,1}, S_{j,2})$ on m_j, where
$$S_{j,1} = r_j P_{CS} + T_{i,j,0} + c_j T_{i,j,1}, \quad S_{j,2} = r_j P_1.$$
3) Broadcast $M_j = (m_j||STP_{i,j}||(S_{j,1}, S_{j,2}))$.

[Verify] An entity may receive many messages in a very short period, since safety messages are broadcast periodically. Suppose n messages $(M_1 = (m_1||STP_1||(S_{1,1}, S_{1,2})), ..., M_n = (m_n||STP_n||(S_{n,1}, S_{n,2})))$ with the same common string CS are received by an entity. The entity verifies the messages as follows:

1) Compute $S_1 = \sum_{i=1}^{n} S_{i,1}, S_2 = \sum_{i=1}^{n} S_{i,2}, \hat{P}_{CS} = H_2(CS)$.

2) For $1 \leq i \leq n$, compute $P_{i,0} = H_1(STP_i, 0), P_{i,1} = H_1(STP_i, 1)$ and $c_i = H_3(m_i, STP_i, CS)$.
3) Check whether the following equation holds [17]:

$$\hat{e}(S_1, P_2) = \hat{e}(S_2, \hat{P}_{CS})\hat{e}(\sum_{i=1}^{n} P_{i,0} + \sum_{i=1}^{n} c_i P_{i,1}, U_2).$$

If it holds, accept these messages.

[Store/forward] If the above n messages are valid, an entity does not need to store/forward all of them $(M_1 = (m_1||STP_1||(S_{1,1}, S_{1,2})), ..., M_n = (m_n||STP_n||(S_{n,1}, S_{n,2})))$. Instead, it just needs to store/forward

$$((m_1||STP_1), ..., (m_n||STP_n)||(S_1, S_2)).$$

We note that the last field (S_1, S_2) has constant size.

[Re-aggregate] When a sub-TMA or TMA center receives $\hat{t}$ aggregated messages $((m_1^1||STP_1^1), ..., (m_{n_1}^1||STP_{n_1}^1)||(S_1^1, S_2^1)), ..., ((m_1^{\hat{t}}||STP_1^{\hat{t}}), ..., (m_{n_{\hat{t}}}^{\hat{t}}||STP_{n_{\hat{t}}}^{\hat{t}})||(S_1^{\hat{t}}, S_2^{\hat{t}}))$ with the same common string CS, it does:

1) Compute $S_1 = \sum_{\hat{i}=1}^{\hat{t}} S_1^{\hat{i}}, S_2 = \sum_{\hat{i}=1}^{\hat{t}} S_2^{\hat{i}}, \hat{P}_{CS} = H_2(CS)$.
2) For $1 \leq \hat{i} \leq \hat{t}, 1 \leq j \leq n_{\hat{i}}$, compute

$$P_{j,0}^{\hat{i}} = H_1(STP_j^{\hat{i}}, 0), P_{j,1}^{\hat{i}} = H_1(STP_j^{\hat{i}}, 1)$$

and

$$c_j^{\hat{i}} = H_3(m_j^{\hat{i}}, STP_j^{\hat{i}}, CS).$$

3) Check whether the equation $\hat{e}(S_1, P_2) = \hat{e}(S_2, \hat{P}_{CS})$ $\hat{e}(\sum_{\hat{i}=1}^{\hat{t}} \sum_{j=1}^{n_{\hat{i}}} P_{j,0}^{\hat{i}} + \sum_{\hat{i}=1}^{\hat{t}} \sum_{j=1}^{n_{\hat{i}}} c_j^{\hat{i}} P_{j,1}^{\hat{i}}, U_2)$ holds. If it holds, accept these messages.

If the above messages are valid, the TMA stores $((m_1^1||STP_1^1), ..., (m_{n_1}^1||STP_{n_1}^1)), ..., ((m_1^{\hat{t}}||STP_1^{\hat{t}}), ..., (m_{n_{\hat{t}}}^{\hat{t}}||STP_{n_{\hat{t}}}^{\hat{t}}))||(S_1, S_2)$ in its local database.

[Trace] A vehicle may send false messages for its own profit or to disrupt traffic. Therefore, it should be possible to trace the real identity of the vehicle which generated the false message. Suppose the false message is the i-th message in

$$((m_1||STP_1), ..., (m_n||STP_n)||(S_1, S_2)).$$

Assume also the aggregate signature is valid (falsehood is in the content of the i-th message, but the signature of that message was valid). The KGC runs the following tracing process:

1) Extract $sid_{i,j}$ from STP_i, since $STP_i = sid_{i,j}||vp_i$.
2) Compute $D_\lambda(sid_{i,j}) = ((LTP_i||j) \oplus H_6(vp_i))$.
3) Compute $LTP_i||j = ((LTP_i||j) \oplus H_6(vp_i)) \oplus H_6(vp_i)$.
4) Search ML to find a tuple $(ID'_{V_i}, k'_i, LTP'_i)$ that satisfies $LTP_i = LTP'_i$.
5) Output the real identity ID'_{V_i}.

4 Security Analysis

In this section, we show that the proposed scheme meets all the security and privacy requirements described in Section 2.2. We just need to deal with the protocol for STP and STK distribution and the protocol for vehicular communications.

The relation between the protocol for STP and STK distribution and the protocol for vehicular communications is that the private keys used in the second protocol are transferred using the former one. We note that the secret keys (private keys and ephemeral secrets) used in two protocols are independent. Hence, we can prove the security of our system in two steps. The first step is to prove that the protocol for STP and STK distribution is secure and the second step is to prove that the protocol for vehicular communications is secure.

Theorem 1. The protocol for STP and STK distribution satisfies message confidentiality, message authentication, non-repudiation, vehicle privacy and traceability.

Proof Sketch. This protocol is based on the identity-based signcryption scheme in [10], which captures the functions of both digital signature and encryption. In fact, the identity-based signcryption scheme in [10] is proven to satisfy confidentiality, message authentication, non-repudiation and ciphertext anonymity under the bilinear Diffie-Hellman and the computational Diffie-Hellman assumptions. It is easy to see that the protocol for STP and STK distribution satisfies message confidentiality, message authentication, non-repudiation and vehicle privacy. Further, the KGC is able to find the real identities based on LTPs; hence, the protocol also satisfies traceability. For the detailed security analysis, please refer to the supporting materials for this paper in [43].

We note that in this protocol RSUs are used to help the KGC in verifying the requests from vehicles. The LTP of a vehicle is leaked to its nearby RSU, so the RSU could trace a vehicle using the vehicle's LTP. However, by our setting, a vehicle only runs this key distribution protocol once a day; therefore, an RSU can trace a vehicle only rarely. Further, if we set the validity period of LTP short enough (e.g., one day), the LTP of a vehicle can be viewed as a one-time pseudonym. In this case, even if all the RSUs colluded, they could not trace a vehicle.

Theorem 2. The protocol for vehicular communications satisfies individual authentication, non-repudiation, vehicle privacy and traceability.

Proof Sketch. The underlying signature scheme is essentially the identity-based aggregate signature scheme in [17], which is proven to be secure under the computational Diffie-Hellman assumption. It is easy to see that message authentication and non-repudiation are satisfied. As to vehicle privacy, STPs are used to hide the real identity of a vehicle; each STP is only used for a short time period to avoid vehicle tracking. Further, the KGC (and only the KGC) is able to determine the real identity of a vehicle from a certain STP. Thus, traceability is satisfied. For the detailed security analysis, please refer to the supporting materials for this paper in [43].

5 Simulation

This section evaluates the performance of our scheme through several simulations by using NS-2 [2], VanetMobisim [3] and the cryptographic library MIRACL [27]. The notations in our simulations are listed in Table 3. The simulations were run on a Linux machine using an Intel Core i7-4790K at a frequency of 4 GHz. We implemented a BN

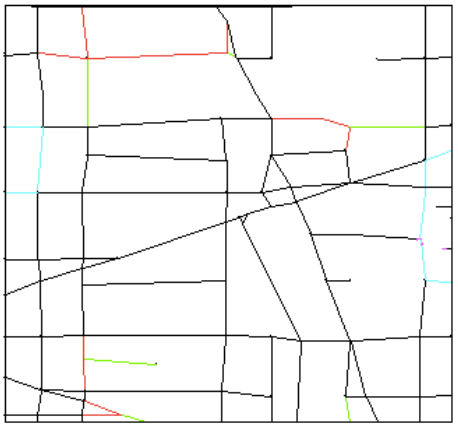


Fig. 4: Simulation scenario 1 km $\times$ 1 km

TABLE 3: Notations in the simulations

Notation	Description
$\mathbb{D}$	Simulation area.
$L_{\mathbb{D}}$	Number of vehicles in the area $\mathbb{D}$.
$M_{l_{\rightarrow}}$	Number of messages sent by a vehicle l.
K_l	Number of vehicles within a one-hop communication range from l.
$T_{sgn}^{l_m}$	Time cost of signing a message m by l.
$T_{trans}^{l_m k}$	Transmission time of m from vehicle l to vehicle k.
MAD	Maximum allowable delay for end-to-end transmission, i.e., 100 ms [44].
τ	A batch period, defined as the time span from the start until the end of message collection before a batch verification.
$M_{l_{\tau\leftarrow}}$	Number of messages received by a vehicle l in τ. The messages received come from the vehicles within a one-hop communication range from l.
$T_{ver}^{M_{l_\tau}\leftarrow}$	Time cost of verifying the messages received by l in τ.
n_{l_m}	Total vehicles (within a one-hop communication range from l) that received message m from l.
n_τ	Maximum number of messages received in τ that can be processed.
n_l	Total number of messages that l received in τ

curve of embedded degree $k = 12$ and 256-bit q. In all the simulations, the road scenario is an area of 1 km $\times$ 1 km represented in Figure 4. Vehicles are randomly distributed in this area with speeds ranging between 50 and 60 km/h. The maximum communication range of each vehicle is set to 300 m. The channel bandwidth bound is 6 Mbps. The size of each message is 204 bytes. For each simulation, we set the simulation time to 100 s.

5.1 Message Delay

The average message delay D_{msg} reflects the average time latency for a message to be received by another vehicle after it is generated. Using the notations in Table 3, D_{msg} is defined as:

$$D_{msg} = \frac{1}{L_{\mathbb{D}}} \sum_{l \in \mathbb{D}} \left(\frac{1}{M_{l_{\rightarrow}}} \sum_{m=1}^{M_{l_{\rightarrow}}} (T_{sgn}^{l_m} + \frac{1}{K_l} \sum_{k=1}^{K_l} T_{trans}^{l_m k}) \right).$$

In our scheme, we assume vehicles will generate messages in τ_s of a time segment. Therefore, after $\tau_s + D_{msg}$ in a time segment, few messages will be received by a vehicle. The average message delay must be taken into account to set the time interval for a vehicle to perform a batch verification.

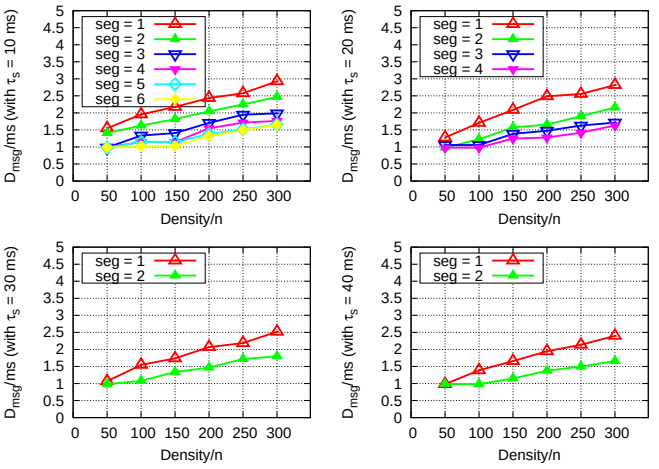


Fig. 5: Message delay as a function of vehicle density (measured as number of vehicles in the 1 km^2 scenario) and segment length (measured as number of segments per 100 ms, e.g. seg$=4$ means a segment length of 25 ms)

Figure 5 shows how the message delay D_{msg} in our protocol varies with vehicle density, different time segment lengths and τ_s. From this figure, it is easy to see that: i) D_{msg} increases with vehicle density for all time segment lengths and τ_s; ii) for a fixed vehicle density, D_{msg} increases with the length of the time segment. For all densities and segment lengths tried, D_{msg} stays below 3 ms. It seems reasonable to set the time Δ_{msg} for a vehicle to start a batch verification as 3 ms after τ_s of a time segment. However, in the real world, vehicles will not generate messages strictly synchronously. Therefore, Δ_{msg} should be greater than 3 ms. In fact, existing protocols for time synchronization may control the synchronization error within 1 ms [5]. However, due to the individual differences of vehicles, we allow vehicle clocks greater flexibility. In this paper, we take $\Delta_{msg} = 5$ ms.

5.2 Verification Delay

We define the verification delay as

$$D_{ver} = \Delta_\tau + \frac{1}{L_{\mathbb{D}}} \sum_{l \in \mathbb{D}} T_{ver}^{M_{l_\tau}\leftarrow},$$

where Δ_τ is the average waiting time of a message before a batch verification and is related to τ_s and Δ_{msg}. It reflects the average time latency for a message to be verified by another vehicle after it is generated. Obviously, D_{ver} should be smaller than MAD.

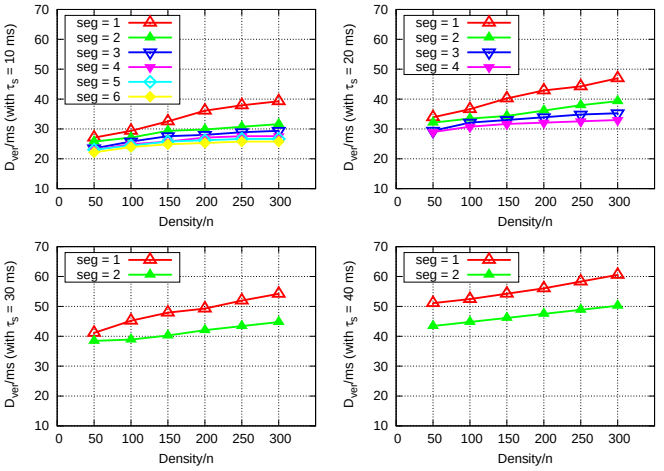


Fig. 6: Verification delay as a function of vehicle density (number of vehicles in the scenario) and segment length (number of segments per 100 ms)

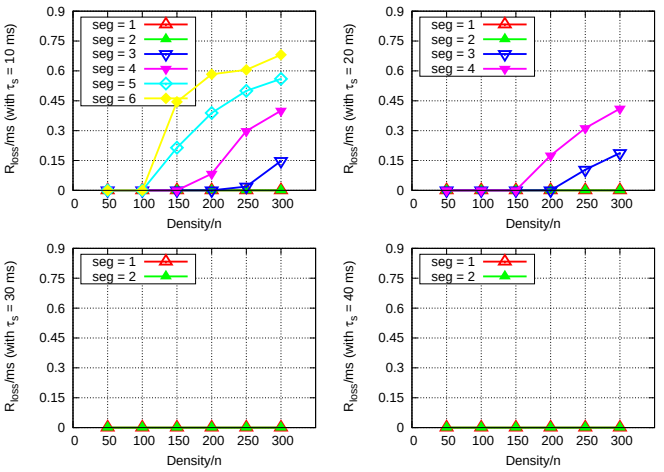


Fig. 7: Verification loss rate as a function of vehicle density (number of vehicles in the scenario) and segment length (number of segments per 100 ms)

From Figure 6, it is easy to see that D_{ver} is much smaller than MAD in all the cases. Further, D_{ver} increases as the length of a time segment grows.

5.3 Verification Loss Rate

The verification loss rate R_{loss} is defined as

$$R_{loss} = 1 - \frac{1}{L_{\mathbb{D}}} \sum_{l \in \mathbb{D}} \frac{n_\tau}{n_l}.$$

Verification loss occurs when the messages received by a vehicle in a batch period cannot be processed before the next batch verification. From Figure 7, it is easy too see that when the length of a time segment is greater than 50 ms, the verification loss rate tends to 0. Therefore, we suggest to take a 50 ms long time segment.

5.4 Messages Received by a Vehicle

In our scheme, we assume vehicles will generate and sign messages in τ_s of a time segment. If τ_s is too short while

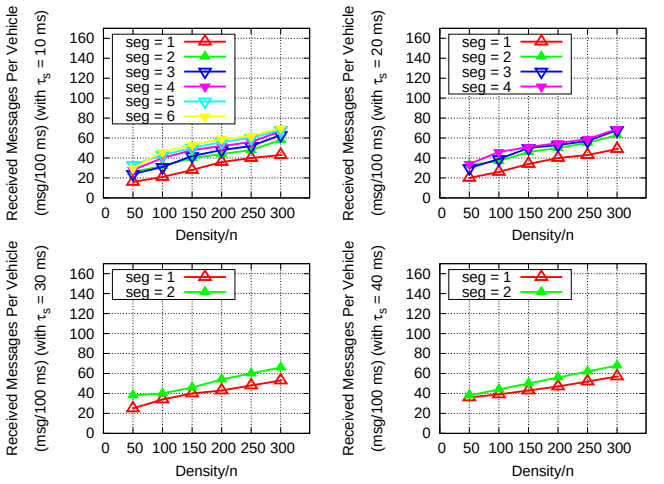


Fig. 8: Received messages per vehicle in 100 ms as a function of vehicle density (number of vehicles in the scenario) and segment length (number of segments per 100 ms)

the time segment is long, then lots of messages should be transmitted in τ_s, which will result in channel congestion. Figure 8 shows the relation among messages received by a vehicle in 100 ms, τ_s and the segment length. Obviously, the messages received by a vehicle grow with vehicle density. Further, the messages received by a vehicle decrease when τ_s gets shorter and the segment gets longer. When the segment length is 100 ms, $\tau_s = 10$ ms and the vehicle density is $300/\text{km}^2$, the number of messages received by a vehicle is much smaller than in other cases. This implies a high channel congestion rate. When $\tau_s \geq 20$ ms and the length of a time segment is 50 ms, the number of messages received by a vehicle for the same vehicle density stays almost the same. Therefore, we suggest to take τ_s equal to 20 ms.

6 Comparison

In this section, we compare the verification delay of our scheme with the scheme based on the traditional batch verification method (with fully random message generation). For better comparability, the scheme we compare with also uses the (extended) identity-based aggregate signature scheme in [17]. However, vehicles generate messages at fully random time points. Further, we assume the messages received by a vehicle in a batch use all the same common string so that the vehicle can verify the messages simultaneously.

Figure 9 shows the relationship among the average verification delay D'_{ver}, the vehicle density and the batch period, where

$$D'_{ver} = \Delta_\tau + \frac{1}{L_{\mathbb{D}}} \sum_{l \in \mathbb{D}} T_{ver}^{M_{l\tau\leftarrow}},$$

and Δ_τ is the average waiting time of a message before a batch verification. By comparing Figures 6 and 9, it is easy to see that D'_{ver} is much larger than D_{ver} for the same batch period. If we set the time segment to 50 ms and $\tau_s = 20$ ms, then the scheme in Section 3 is about 1.45 times more efficient than the scheme based on traditional

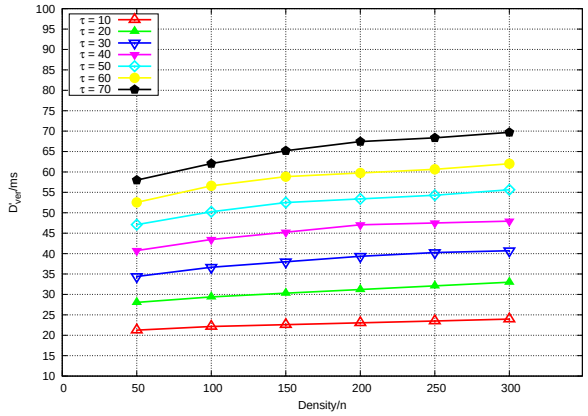


Fig. 9: Verification delay with fully random message generation, as a function of vehicle density and batch period length (ms)

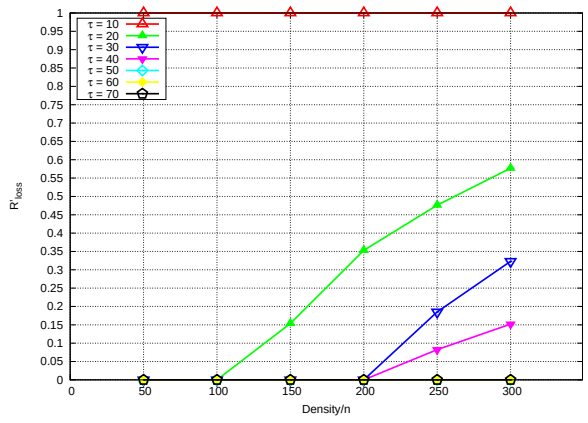


Fig. 10: Verification loss with fully random message generation, as a function of vehicle density and batch period length (ms)

batch verification. We note that taking shorter batch periods would reduce D'_{ver} but it would have the drawback of increasing the verification loss rate, as discussed next.

Figure 10 shows the relationship among the verification loss rate R'_{loss}, the vehicle density and the batch period, where

$$R'_{loss} = 1 - \frac{1}{L_{\mathbb{D}}} \sum_{l \in \mathbb{D}} \frac{n_\tau}{n_l}.$$

It is easy to see that the verification loss rate is high when $\tau \leq 40$ ms and vehicle density is high. In particular, when $\tau = 10$ ms, the verification loss rate goes towards 1. This is due to the fact that too short a batch verification period does not allow completing the batch verification within the period (as some messages may arrive randomly during the entire period). When $\tau \geq 50$, the verification loss rate goes towards 0. By comparing Figures 7 and 10, we find $\tau = 50$ ms is the optimal batch period in both schemes.

Figure 11 shows the relationship between the received messages per vehicle and the vehicle density when the batch period length is 50 ms. It is easy to see that when seg=2 (or the batch period length is 50 ms) and $\tau_s \geq 20$ ms, the number of messages received with our scheme of Section 3 is comparable to the number of messages received

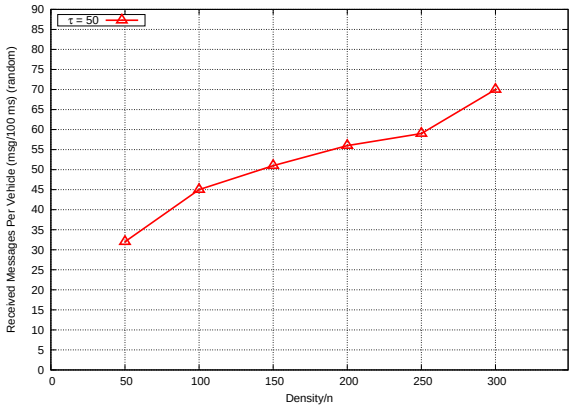


Fig. 11: Received messages per vehicle with fully random message generation

with random message generation. This implies that, when seg=2 and $\tau_s \geq 20$ ms in the scheme of Section 3, only a few messages are lost due to the compression of message generation and transmission time.

7 Conclusion

We have proposed an identity-based scheme for signature hierarchical aggregation and fast response to anonymous vehicle-generated messages. In our scheme, all the vehicles and RSUs are identity-based, which alleviates the overheads of certificate verification and management. The vehicles in our scheme generate an aggregate signature based on synchronized common strings within a short time span. With this mechanism, the transmission/storage overhead of an entity is significantly reduced, and a vehicle only needs to wait for a very short period before it can start the batch verification procedure. Simulations show that our scheme has very low latency and enables a fast response to anonymous vehicle-generated messages.

Acknowledgments and Disclaimer

Thanks go to Bao Liu and Jian Liu for the simulation and proof reading. The following funding sources are gratefully acknowledged: NSF of China (grants 61572198, 61202465, 61321064, 61103222, 61173154, 61003214, 61272501 and 61370190); China National Key Basic Research Program (973 program, project 2012CB315905); Shanghai NSF (grant 12ZR1443500); Shanghai Chen Guang Program (12CG24); Science and Technology Commission of Shanghai Municipality (grant 13JC1403500); Beijing Natural Science Foundation (project 4132056); European Commission (project H2020-644024 "CLARUS"); Spanish Govt. (projects TIN2011-27076-C03-01 and TIN2014-57364-C2-1-R); Govt. of Catalonia (grant 2014 SGR 537 and ICREA Acadèmia Prize to J. Domingo-Ferrer); Templeton World Charity Foundation (project "CO-UTILITY"); Fundamental Research Funds for the Central Universities of China; the Research Funds of Renmin University of China (No. 14XNLF02). J. Domingo-Ferrer leads the UNESCO Chair in Data Privacy, but the views in this paper do not commit UNESCO.

REFERENCES

[1] IEEE 802.11P, Online Available: http://grouper.ieee.org/groups/802/11/Reports/tgp-update.htm

[2] The Network Simulator-ns, Online Available: http://www.isi.edu/nsnam/ns/

[3] VanetMobiSim, Online Available: http://vanet.eurecom.fr/

[4] M. Almalag, S. Olariu and M. Weigle, "TDMA cluster-based MAC for VANETs (TC-MAC)", *Proc. World of Wireless, 2012 IEEE International Symposium on Mobile and Multimedia Networks (WoWMoM)*, pp.1 -6 2012

[5] R. Ben-El-Kezadri and G. Pau, "TimeRemap: Stable and accurate time in vehicular networks", *IEEE Communications Magazine*, vol. 48, no. 12, pp.52 -57 2010

[6] D. Boneh, B. Lynn and H. Shacham, "Short signatures from the Weil pairing" *Advances in Cryptology - ASIACRYPT 2001*, pp.514 -532 2001

[7] D. Boneh and H. Shacham, "Group signature wih verifier-local revocation", *Proc. 11th ACM conference on Computer and communications security (CCS'04)*, pp.168 -177 2004

[8] D. Boneh, C. Gentry, B. Lynn and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps", *Advances in Cryptology - EUROCRYPT 2003*, pp.416 -432 2003

[9] D. Chaum and E. Van Heyst, "Group signatures", *Advances in Cryptology - EUROCRYPT'91*, pp.257 -265 1991

[10] L. Chen and J. Malone-Lee, "Improved identity-based signcryption", *Public Key Cryptography - PKC 2005*, pp.362 -379 2005

[11] J. Cheon and J. Yi, "Fast batch verification of multiple signatures", *Public Key Cryptography - PKC 2007*, pp.442 -457 2007

[12] T. Chim, S. Yiu, L. Hui and V. Li, "VSPN: VANET-Based Secure and Privacy-Preserving Navigation", *IEEE Transactions on Computers*, vol. 63, no. 2, pp.510 -524 2014

[13] T. Chim, S. Yiu, L. Hui and V. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs", *Ad Hoc Networks*, vol. 9, no. 2, pp.189 -203 2011

[14] H. Eun, H. Lee and H. Oh, "Conditional privacy preserving security protocol for NFC applications", *IEEE Transactions on Consumer Electronics*, vol. 59, no. 1, pp.153 -160 2013

[15] A. Ferrara, "Practical short signature batch verification", *Topics in Cryptology - CT-RSA 2009*, pp.251 -260 2009

[16] J. Freudiger, M. Manshaei, J. Hubaux and D. Parkes, "On non-cooperative location privacy: a game-theoretic analysis", *Proc. 16th ACM conference on Computer and communications security*, pp.324 -337 2009

[17] C. Gentry and Z. Ramzan, "Identity-based aggregate signature", *Public Key Cryptography - PKC 2006*, pp.257 -273 2006

[18] D. He, C. Chen, S. Chan and J. Bu, "Secure and efficient handover authentication based on bilinear pairing functions", *IEEE Transactions on Wireless Communications*, vol. 11, no. 1, pp.48 -53 2012

[19] R. Heijden, S. Dietzel and F. Kargl, "SeDyA: secure dynamic aggregation in VANETs", *Proc. 6th ACM conference on Security and privacy in wireless and mobile networks (WiSec'13)*, pp.131 -142 2013

[20] S. Horng, S. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li and M. Khan, "b-SPECS+: Batch verification for secure pseudonymous authentication in VANET", *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp.1860 -1875 2013

[21] J. Huang and Y. Chiu, "A scheme to reduce merging collisions in TDMA-based VANETs", *Proc. 2013 IEEE International Symposium on Wireless and Pervasive Computing (ISWPC)*, pp.1 -4 2013

[22] J. Jiru, L. Bremer and K. Graffi, "Data aggregation in VANETs - A generalized framework for channel load adaptive schemes", *Proc. 39th Annual IEEE Conference on Local Computer Networks (LCN 2014)*, pp.394 -397 2014

[23] X. Lin, X. Sun, P. Ho and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications", *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp.3442 -3456 2007

[24] R. Lu, X. Li, T. H. Luan, X. Liang and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs", *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp.86 -96 2012

[25] R. Lu, X. Lin, H. Zhu, P. Ho and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications", *Proc. 27th IEEE Conference on Computer Communications (INFOCOM 2008)* 2008

[26] Z. Ma, F. Kargl and M. Weber, "Pseudonym-on-demand: a new pseudonym refill strategy for vehicular communications", *Proc. 68th IEEE Vehicular Technology Conference (VTC Fall 2008)*, pp.1 -5 2008

[27] Multiprecision Integer and Rational Arithmetic Cryptographic Library, Avaliable: http://www.certivox.com/miracl/

[28] D. Naccache, D. M'Raihi, S. Vaudenay and D. Raphaeli, "Can D.S.A be improved? Complexity trade-offs with the Digital Signature Standard", *Advances in Cryptology - EUROCRYPT'94*, pp.77 -85 1995

[29] H. Omar, W. Zhuang and L. Li, "VeMAC: A TDMA-based MAC protocol for reliable broadcast in VANETs", *IEEE Transactions on Mobile Computing*, vol. 12, no. 9, pp.1724 -1736 2013

[30] P. Papadimitratos, L. Buttyan, J-P. Hubaux, F. Kargl, A. Kung and M. Raya, "Architecture for secure and private vehicular communications", *Proc. 7th International Conference on Intelligent Transportation Systems (ITS 2007)*, pp.1 -6 2007

[31] A. Pathan, "Security of Self-Organizing Networks: MANET, WSN, WMN, VANET", CRC Press 2011

[32] S. Ravi, A. Raghunathan and S. Chakradhar, "Tamper resistance mechanisms for secure embedded systems", *Proc. 17th IEEE International Conference on VLSI Design*, pp.605 -611 2004

[33] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks", *Journal of Computer Security*, vol. 15, no. 1, pp.39 -68 2007

[34] G. Samara, W. Al-Salihy and R. Sures, "Security issues and challenges of Vehicular Ad Hoc Networks (VANET)", *Proc. 4th IEEE International Conference on New Trends in Information Science and Service Science (NISS)*, pp.393 -398 2010

[35] A. Shamir, "Identity-based cryptosystems and signature schemes" *Advances in Cryptology - CRYPTO'84*, pp.47 -53 1985

[36] K. A. Shim, "CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks", *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp.1874 -1883 2012

[37] J. Sun, C. Zhang, Y. Zhang and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks", *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 9, pp.1227 -1239 2010

[38] A. Wasef and X. Shen, "ASIC: Aggregate signatures and certificates verification scheme for vehicular networks", *Proc. 2009 IEEE Global Telecommunications Conference (GLOBECOM 2009)*, pp.4489 -4494 2009

[39] Q. Wu, J. Domingo-Ferrer and U. González-Nicolás, "Balanced trustworthiness, safety and privacy in vehicle-to-vehicle communications", *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp.559 -573 2010

[40] X. Yin, X. Ma and K. Trivedi, "An interacting stochastic models approach for the performance evaluation of DSRC vehicular safety communication", *IEEE Transactions on Computers*, vol. 62, no. 5, pp. 873 -885 2013

[41] S. Zeadally, R. Hunt, Y. Chen, A. Irwin and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges", *Telecommunication Systems*, vol. 50, no. 4, pp.217 -241 2012

[42] C. Zhang, R. Lu, X. Lin, P. Ho and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks", *Proc. 27th IEEE Conference on Computer Communications (INFOCOM 2008)*, pp.246 -250 2008

[43] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer and B. Qin, "On the security of privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response", http://arxiv.org/abs/1508.01575

[44] L. Zhang, Q. Wu, A. Solanas and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications", *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp.1606 -1617 2010

[45] L. Zhang, Q. Wu, B. Qin and J. Domingo-Ferrer, "Practical privacy for value-added applications in vehicular ad hoc networks", *Proc. 5th International Conference on Internet and Distributed Computing Systems (IDCS 2012)*, pp.43 -56 2012

[46] L. Zhang, Q. Wu, B. Qin and J. Domingo-Ferrer, "APPA: Aggregate privacy-preserving authentication in vehicular ad hoc networks", *Proc. 14th Information Security Conference (ISC 2011)*, pp.293 -308 2011

[47] Y. Zheng, "Digital signcryption or how to achieve cost (signature + encryption) $\ll$ cost (signature)+ cost (encryption)", *Advances in Cryptology - CRYPTO'97*, pp.165 -179 1997

[48] H. Zhu, X. Lin, R. Lu, P. Ho and X. Shen, "AEMA: An aggregated emergency message authentication scheme for enhancing the security of vehicular ad hoc networks", *Proc. 2008 IEEE International Conference on Communications (ICC'08)*, pp.1436 -1440 2008

[49] X. Zhu, S. Jiang, L. Wang and H. Li, "Efficient privacy-preserving authentication for vehicular ad hoc networks", *IEEE Transactions on Vehicular Technology*, vol. 63, no. 2, pp.907 -919 2014
[50] J. Ziv and A. Lempel, "A universal algorithm for sequential data compression", *IEEE Transactions on Information Theory*, vol. 23, no. 3, pp.337 -343 1977



Lei Zhang received his Ph.D. degree in computer engineering from Universitat Rovira i Virgili, Tarragona, Spain, in 2010. He is an Associate Research Fellow with Software Engineering Institute, East China Normal University, Shanghai, China. Before this, he had been a Postdoctoral Researcher with Universitat Rovira i Virgili. His fields of activity are information security, cryptography, data privacy, and network security. He has been a holder/co-holder of 7 China/Spain funded projects. He has authored over 50 publications. He has served in the program committee of several international conferences in information security and privacy. He is a member of IEEE.



Chuanyan Hu is currently a master student in Software Engineering Institute, East China Normal University, China. Her fields of activity are information security, data privacy, network security, wireless sensor network.



Qianhong Wu received his Ph.D. in Cryptography from Xidian University in 2004. Since then, he has been with Wollongong University (Australia) as an associate research fellow, with Wuhan University (China) as an associate professor, and with Universitat Rovira i Virgili (Spain) as a research director. He is currently a professor in Beihang University in China. His research interests include cryptography, information security and privacy, VANET security and cloud computing security. He has been a holder/co-holder of 8 China/Australia/Spain funded projects. He has authored 7 patents and over 110 publications. He has served in the program committee of several international conferences in information security and privacy. He is a member of IACR and IEEE.



Josep Domingo-Ferrer is a Distinguished Professor of Computer Science and ICREA-Acadèmia Researcher at Universitat Rovira i Virgili, Tarragona, Catalonia, where he holds the UNESCO Chair in Data Privacy. His research interests include data privacy, data security and cryptographic protocols. He received MSc and PhD degrees in Computer Science from the Autonomous University of Barcelona, Catalonia; he also holds an MSc in Mathematics. He is an IEEE Fellow and an Elected Member of Academia Europaea and he has received a Google Research Award. He has authored over 350 publications and 5 patents, and his current H-index is 44.



Bo Qin received her Ph.D. degree in Cryptography from Xidian University in 2008 in China. Since then, she has been with Xi'an University of Technology (China) as a lecturer and with Universitat Rovira i Virgili (Catalonia) as a postdoctoral researcher. She is currently a lecturer in the Renmin University in China. Her research interests include pairing-based cryptography, data security and privacy, and VANET security. She has been a holder/co-holder of 5 China/Spain funded projects. She has authored over 60 publications and served in the program committee of several international conferences in information security.