Preserving Security and Privacy in Large-Scale VANETs

Bo Qin[1,3], Qianhong Wu[1,2], Josep Domingo-Ferrer[1], and Lei Zhang[4]

[1] Universitat Rovira i Virgili, Department of Computer Engineering and Mathematics UNESCO Chair in Data Privacy, Tarragona, Catalonia
{bo.qin,qianhong.wu,josep.domingo}@urv.cat
[2] Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Computer, Wuhan University, China
[3] School of Science, Xi'an University of Technology, China
[4] Software Engineering Institute, East China Normal University, China
leizhang@sei.ecnu.edu.cn

Abstract. Upcoming vehicular *ad hoc* networks (VANETs) allowing vehicles to talk to each other are expected to enhance safety and efficiency in transportation systems. This type of networks is especially attractive in highly populated urban areas overwhelmed with traffic congestions and accidents. Besides vulnerabilities versus attacks against traffic safety and driver privacy, a large-scale VANET in a metropolitan area raises scalability and management challenges. This paper employs identity-based group signatures (IBGS) to divide a large-scale VANET into easy-to-manage groups and establish liability in vehicular communications while preserving privacy. Each party's human-recognizable identity is used as its public key and no additional certificate is required. This efficiently avoids the complicated certificate management of existing protocols. We further investigate selfish verification approach to accelerate message processing in VANETs. With this approach, a vehicle selects only the messages affecting its driving decisions and validates the selected messages as if they were a single one.

Keywords: Vehicular *ad hoc* networks, Mobile wireless communication, Identity management, Security, Privacy.

1 Introduction

As information and communication technologies (ICT) become increasingly pervasive, vehicles are expected to be equipped in the near future [3] with intelligent devices and radio interfaces, known as On-Board Units (OBUs). OBUs are allowed to talk to other OBUs and the road-side infrastructure formed by Road-Side Units (RSUs). The OBUs and RSUs, equipped with on-board sensory, processing, and wireless communication modules, form a self-organized vehicular network, commonly referred to as VANET, a commercial instantiation of mobile *ad hoc* networks with vehicles as the mobile nodes.

S. Qing et al. (Eds.): ICICS 2011, LNCS 7043, pp. 121–135, 2011.

VANET systems aim at providing a platform for various applications that can improve traffic safety and efficiency, driver assistance, transportation regulation, infotainment, etc. There is substantial research and industrial effort to develop this market. Vehicular communications are supported by the Car2Car Communication Consortium [7] in Europe and the Dedicated Short Range Communications (DSRC) standard [1] in the USA. In Europe, several projects such as SEVECOM [28] and NOW [19] are under way. It is estimated that the market for vehicular communications will reach several billions of euros by 2012.

While the tremendous benefits expected from vehicular communications and the huge number of vehicles are strong points of VANETs, there are still challenges to deploy practical VANETs. A very important one is to guarantee the security of vehicle-generated reports. In what regards security, selfish vehicles may attempt to clear up the way ahead or mess up the way behind with false traffic reports; criminals being chased may disseminate bogus notifications to other vehicles in order to block police cars. Such attacks may result in serious harm, even loss of lives. Another challenge is to protect the privacy of vehicles. VANETs open a big window to observers. It is very easy to collect information about the speed, status, trajectories and whereabouts of the vehicles in a VANET. By mining this information, malicious observers can make inferences about a driver's personality (*e.g.* someone driving slowly is likely to be a calm person), living habits and social relationships (visited places tell a lot about people's lives). This private information may be traded in underground markets, exposing the observed vehicles and drivers to harass (*e.g.* junk advertisements), threats (*e.g.* blackmail if the driver often visits an embarrassing place, like a red-light district) and dangers (*e.g.* hijacks). Finally, VANETs are especially attractive in highly populated urban areas overwhelmed with traffic congestions and accidents. Besides vulnerabilities versus attacks against traffic safety and driver privacy, a large-scale VANET in a metropolitan area raises scalability and management challenges. Therefore, security, privacy and scalable management motivate the work described in this paper.

1.1 Related Work

For VANETs to be viable, the first requirement is to guard them against erroneous information. For example, an attacker may simply put a piece of ice on the vehicle temperature sensor and then a wrong temperature will be reported, even if the hardware sensor is tamper-proof. To counter fraudulent data, detection mechanisms are needed. A general scheme aiming at detection and correction of malicious data was given by Golle *et al.* in 2004 [14]. The authors assume that the simplest explanation of some inconsistency in the received information is most probably the correct one. A specific proposal was made by Leinmüller *et al.* in 2006 [17] and focuses on verifying the position data sent by vehicles. All position information received from a vehicle is stored for some time period; this is used to perform the checks, the results of which are weighted in order to form a metric on the neighbor's trust. Raya *et al.* [23] and Daza *et al.* [9] introduced a threshold

mechanism to prevent the generation of fraudulent messages: a message is given credit only if it was endorsed by a threshold of vehicles in the vicinity.

In addition to guaranteeing correctness of vehicular reports, VANETs should also provide authentication to establish liability for the prevention, investigation, detection and prosecution of serious criminal offences. To meet this requirement, vehicular communications must be signed to provide authentication, integrity and non-repudiation so that they can be collected as judicial evidence. Several proposals (*e.g.*, [21, 24, 25, 32, 33]) suggest the use of a public key infrastructure (PKI) and digital signatures to secure VANETs. To evict misbehaving vehicles, Raya *et al.* further proposed protocols focusing on revoking certifications of malicious vehicles [26]. A big challenge arising from the PKI-based schemes in VANETs is the heavy burden of certificate generation, storage, delivery, verification, and revocation.

To guarantee vehicle privacy, some proposals suggest anonymous authentication in VANETs. Among them there are two research lines, *i.e.* pseudonym mechanisms and group signatures. The pseudonym of a node is a short-lived public key authenticated by a certificate authority (CA) in the vehicular PKI ([11, 13, 20]). The pseudonymity approach mainly focuses on how often a node should change a pseudonym and with whom it should communicate. Sampigethaya *et al.* [27] proposed to use a silent period in order to hamper linkability between pseudonyms, or alternatively to create groups of vehicles and restrict vehicles in one group from listening to messages of other groups. To avoid delivery and storage of a large number of pseudonyms, Calandriello *et al.* [5] proposed self-generating pseudonyms with the help of group signatures locally produced by the vehicles. Noting that group signatures can be directly used to anonymously authenticate vehicular communications without additionally generating a pseudonym, Guo *et al.* [15] proposed a group signature-based security framework which relies on tamper-resistant devices (requiring password access) for preventing adversarial attacks on vehicular networks. However, neither concrete instantiations nor simulation results are provided. Lin *et al.* [18] introduced a security and privacy-preserving protocol for VANETs by integrating the techniques of group signatures. With the help of group signatures, vehicle-to-vehicle (V2V) communications are authenticated while maintaining conditional privacy. Wu *et al.* [30] distinguished linkability and anonymity of group signatures to improve the trustworthiness of vehicle-generated messages.

Some recent proposals provide both authentication to establish liability and vehicle privacy in VANETs. When these schemes are implemented in large-scale VANETs in densely populated urban areas, unaddressed challenges remain. Pseudonym-based schemes face the challenge of generating, distributing, verifying and storing a huge number of certificates. Group signature-based schemes in the traditional PKI setting face problems such as how to manage numerous vehicles and especially compromised vehicles. A common concern of both classes of schemes is how to process the large volume of messages received every time unit. These observations call for novel mechanisms to address these challenges in an efficient way.

1.2 Contribution and Plan of This Paper

We propose a set of mechanisms to address the security, privacy, and management requirements in a large-scale VANET. These conflicting concerns are conciliated by exploiting identity-based group signatures (IBGS) and dividing a large-scale VANET into a number of easy-to-manage smaller groups. In the system, each party, including the group managers (*i.e.* the transportation offices) and the signers (*i.e.* the vehicles), has a unique, human-recognizable identity as its public key, and a corresponding secret key generated by some trusted authority. For instance, the public keys of the administration offices, road-side units [16] and vehicles can be, respectively, the administration name, the RSU geographical address and the traditional vehicle license plate. Certificates are no longer needed because the public key of each party is a human-recognizable identity. This feature greatly reduces the security-related management challenges.

After registering to transportation offices, any vehicle can anonymously authenticate any message. These vehicle-generated messages can be verified by the identities (*e.g.* the name) of the transportation offices and the public key of the escrow authority. If a message is later found to be false, the identity of the message generator can be traced by traffic police offices. Considering the redundancy in vehicular communications, we present a selfish verification mechanism to speed up message processing in VANETs. With this technique, although each vehicle may receive a large number of messages, the vehicle only selects for verification those messages affecting its traffic decisions. The selected messages can can be verified in a batch as if they were a single one. These mechanisms are crucial to deploy VANETs in densely populated urban areas.

The rest of this paper is organized as follows. Section 2 describes our design goals and the challenges to those goals. The proposal is specified in Section 3. Section 4 presents an extension to speed up vehicular message verification. The last section is a conclusion.

2 Design Goals and Challenges

2.1 Design Goals

In order to obtain an implementable system to enhance the trustworthiness of V2V communications in a large-scale VANET, we keep in mind the following main design goals:

- **Liability.** The fundamental security functions in vehicular communications consist of ensuring liability for the originator of a data packet. Liability implies that the message author is held responsible for the message generated. To establish liability without disputes, authentication, integrity and non-repudiation must be provided in vehicular protocols. Authentication allows verifying that the message was generated by the originator as claimed, rather than by an impersonator. Integrity guarantees that the message has not been tampered with after it was sent. Non-repudiation implies that the message generator cannot deny message authorship.

- **Anonymity.** There is anonymity if, by monitoring the communication in a VANET, message originators cannot be identified, except perhaps by designated parties. Since message authentication requires knowledge of a public identity such as a public key or a license plate, if no anonymity was provided, an attacker could easily trace any vehicle by monitoring the VANET communication. This would be surely undesirable for the drivers; hence, anonymity should be protect for vehicles.
- **Scalable Management.** For a VANET deployed in a highly populated metropolitan area, managing up to (tens of) millions of vehicles is a substantial concern. Specifically, in such a large VANET, every day some registered vehicles might be stolen or their secret keys might be occasionally leaked. This entails extra burden to manage the system while preserving the liability and the privacy of vehicles. Hence, it is essential to take the scalable management requirement into consideration when the system is designed.

2.2 Challenges to the Goals

It is challenging to simultaneously achieve the above design goals. The first challenge derives from the fact that liability and anonymity are conflicting in nature. The liability requirement implies that cheating vehicles distributing bogus messages should be caught. On the other hand, the anonymity requirement implies that attackers cannot trace the original vehicles who generated reports. Hence, there must be some tradeoff between liability and anonymity in a VANET. A well-designed scheme should protect privacy for honest vehicles while allowing to find the identities of dishonest vehicles.

Network volatility is another factor that increases the difficulty of securing VANETs. Connectivity among vehicles can often be highly transient due to their high speeds (*e.g.* think of two vehicles crossing each other in opposite directions in a highway). This implies that protocols requiring multiple rounds or strong cooperation such as voting mechanisms may be impractical. Due to their high mobility, vehicles may never again connect with each other after one occasional connection. This puts the public key infrastructure implemented for securing VANETs under strain: if public-key certificates are used, vehicles are confronted to a lot of certificates probably issued by several different CAs; due to the mobility, there is little hope that caching the verified certificates of vehicles and CAs will result in any significant speed-up of the next verifications.

The size of VANETs deployed in metropolitan areas with millions of vehicles is another challenge. Transportation systems are governed by a constellation of authorities with different interests, which complicates things. A technically, and perhaps politically, convincing solution is a prerequisite for any security architecture. Another challenge is the sheer scale of the network: the system has to manage (tens of) millions of nodes of which some may join or leave the VANET occasionally and some may be compromised. This rules out protocols requiring massive distribution of data to all mobile nodes. Furthermore, in case of high vehicular density in metropolitan areas, each node may be flooded with a large number of incoming messages requiring verification.

3 The Proposal

In this section, we propose an authentication protocol to enforce liability, privacy and scalable management in vehicle-generated messages. Underlying is an efficient IBGS scheme [29] to avoid the heavy burden of certificate generation, delivery and verification in a large-scale VANET. The protocol exploits the features of existing transportation systems to simplify the system administration overhead.

3.1 Underlying Technologies and High-level Description

A number of proposals have employed group signatures [8] to secure VANETs with conditional privacy. For a large VANET, it may be impractical to organize millions of vehicles into a single group. This implies that the group public parameters have to change whenever any vehicle is compromised, which may occur frequently in a large VANET. It is resource-consuming to distribute these frequent changes to all the nodes. Identity-based group signatures are an extension of standard group signatures. As depicted in Figure 1, in an IBGS scheme [29] there are four types of parties, *i.e.* the trusted escrow authority (TEA), the group registration manager (GRM), an identity-opening authority (IOA) and the group members. Each of them has a unique identity, *i.e.* its name. TEA has a public-private key pair and the public key can be accessed by any entity. By taking as input the identity of any entity in the system, TEA generates a private key for that entity. Any group member having obtained a private key from TEA can register to GRM to become a group member and then can anonymously sign any message on behalf of the group. The signature can be verified using TEA's public key and the identities of GRM and IOA. If necessary, IOA can open the identity of the signer of any doubtable signature.

We observe that IBGS can be exploited to simplify the system management while preserving liability and privacy in a large VANET. In most cities, the transportation administration authorities include the public security department, vehicle management bureaus and traffic police offices, who can serve as the TEA, GRMs and IOAs, respectively. The public security department's public key can be stored in each vehicle. The identities of GRMs and IOAs are their respective public keys. Each vehicle's unique identity is also its public key. GRMs and IOAs first need to contact TEA to generate their private keys and set up the corresponding administration units. This human-recognizable identity-based feature eliminates the certificate management requirement of other proposals.

The system management can be further reduced by dividing the huge number of vehicles into groups in light of their regulatory status, *e.g.* one can distinguish groups like police cars, ambulances, fire trucks, taxis, buses, commercial vehicles, personal vehicles, etc. Police cars, ambulances and fire trucks may have privilege on using road, and taxis, buses and commercial vehicles are also run and managed by some organizations (or companies). The personal cars may still be too numerous in densely populated areas and can be further properly divided into smaller groups, *e.g.*, according to the regions where they have registered. One

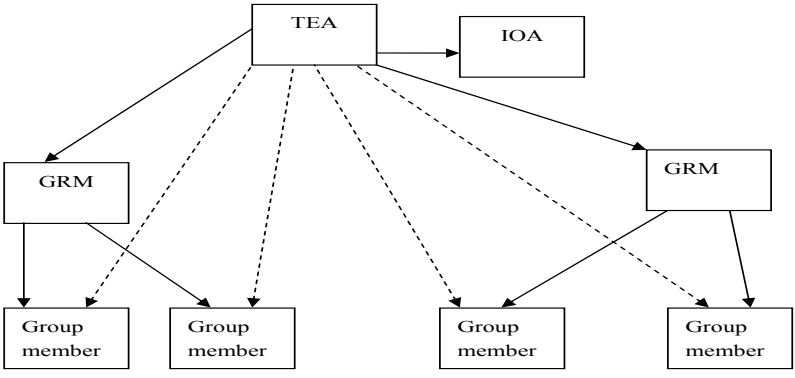

Fig. 1. Model of identity-based group signature

may note that splitting vehicles into smaller subgroups reduces the privacy of vehicles. However, this privacy loss could be minimized if the vehicles are properly divided into subgroups so that the division does not leak more identity information than the one leaked by the vehicles' physical features. For instance, one can easily distinguish police cars from other vehicles from their visible features and organizing the police cars into one sub-group does not leak much information on individual police vehicles. The gains of easy management outweigh a little loss of privacy and the ensuing trade-off between management and privacy seems reasonable in practice.

Employing IBGS can also simultaneously provide liability and privacy in VANET. After registration, a vehicle can authenticate messages without disclosing its identity. When receiving an authenticated message, the receiver can verify it with the stored system public key of TEA and the identity of the group the vehicle belongs to. Note here that the signing vehicle's identity is not required for validation of the signed message due to anonymity. If the verification procedure indicates that the message is authentic (but not necessarily correct), then the receiving vehicle can use it as a proof. This proof can be submitted to the traffic police office for investigation if the message is later found to be incorrect and causes any harm. If necessary, the police can open the identity of the message generator and perhaps punish him/her.

3.2 System Set-up

Our scheme is realized in bilinear groups ([4]). We use the notations of [31]. Let `PGen` be an algorithm which, on input a security parameter 1^ℓ, outputs a pairing $\Upsilon = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3, g, h, e)$, where finite cyclic groups $\mathbb{G}_1 = \langle g \rangle$ and $\mathbb{G}_2 = \langle h \rangle$ have the same prime order p, and $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_3$ is an efficient non-degenerate bilinear map such that $\hat{e}(g, h) \neq 1$ and for any $a, b \in \mathbb{Z}$, $\hat{e}(g^a, h^b) = \hat{e}(g, h)^{ab}$.

The TEA, *e.g.* the public security department, runs `PGen` and obtains a pairing $\Upsilon = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3, g, h, \hat{e})$ as above. Let g_1, g_2, g_3, g_4, g_5 be randomly selected generators of $\mathbb{G}_1$. Define cryptographic hash functions $H_V : \{0,1\} \rightarrow \mathbb{G}_1$, $H_O : \{0,1\} \rightarrow \mathbb{G}_1$, $H_R : \{0,1\} \rightarrow \mathbb{Z}_p^*$, $H : \{0,1\} \rightarrow \mathbb{Z}_p^*$. The TEA's private key is a randomly chosen value $x \in \mathbb{Z}_p^*$ and its public key is $K = h^x \in \mathbb{G}_2$. Then the public system parameters are $param = (\Upsilon, g_1, \cdots, g_5, H_R, H_V, H_O, H, K)$ which can be accessed by each party in the VANET.

3.3 Key Generation

With this procedure, the TEA generates private keys for the group registration managers (GRMs), the identity-opening authorities (IOAs) and the individual vehicles by taking as inputs their public identities.

- On input the identity ID_R of a GRM, TEA randomly generates $r \in \mathbb{Z}_p^*$ and computes $A = h^r, x_1 = r + H_R(A||ID_R)x \mod p$. Finally GRM gets (x_1, A), where A is an auxiliary string that can be known by the vehicles in the group, and x_1 is the private key of the GRM.
- On input the identity ID_O of an IOA, TEA generates the IOA's private key by computing $x_0 = H_O(ID_O)^x$.
- On input a vehicle's identity ID_V, TEA uses x to compute the vehicles's private key $X = H_V(ID_V)^x$.

3.4 Registration

With this procedure, a vehicle with identity ID_V can register to one of the groups ID_R in the VANET. Note that the vehicle does not need to contact the identity-opening authority and the registration procedure is simple.

- The vehicle firstly proves to the GRM that it knows the secret key $X = H_V(ID_V)^x$ corresponding to its identity ID_V without leaking any information on X. This can be done with the protocol due to Qin *et al.* [22] to guarantee that the vehicle has identity ID_V as claimed.
- GRM randomly selects $e \in \mathbb{Z}_p^*$, and computes $B = (g_5/H_V(ID_V))^{1/(e+x_1)}$. The GRM sends the secret group certificate (B, e, A) to the vehicle via a confidential channel.
- The vehicle accepts the certificate if and only if

$$\hat{e}(g_5, h) = \hat{e}(B, h)^e \hat{e}(B, S) \hat{e}(H_V(ID_V), h),$$

  where $S = AK^{H_R(A||ID_R)} = h^{x_1}$.
- GRM computes $W = \hat{e}(H_V(ID_V), h)$, and records (ID_V, B, e, W) in its local database.

3.5 Authentication of Vehicle-Generated Messages

A registered vehicle ID_V in group ID_R with secret key X and certificate (B, e, A) can anonymously sign message m while allowing the identity-opening authority IOA to open the signature. The detailed instantiation is as follows.

- The vehicle randomly selects $s_1 \in Z_p^*$, and computes
  $s_2 = es_1 \mod p$, $\sigma_0 = g^{s_1}$, $\sigma_1 = Xg_1^{s_1}$,
  $\sigma_2 = H_V(ID_V)g_2^{s_1}$, $\sigma_3 = Bg_3^{s_1}$, $\sigma_5 = \sigma_3^e g_4^{s_1}$.
- The vehicle randomly selects $d \in Z_p^*$ and computes
  $C_1 = \hat{e}(H_V(ID_V), h)\hat{e}(H_O(ID_O), K)^d, C_2 = h^d$.
- The vehicle randomly selects $r_1, r_2, r_3, r_4 \in \mathbb{Z}_p^*, R_1, R_2, R_3 \in \mathbb{G}_1$, and computes
  $\rho_0 = g^{r_1}$, $\rho_1 = R_1 g_1^{r_1}$, $\rho_2 = R_2 g_2^{r_1}$, $\rho_3 = R_3 g_3^{r_1}$,
  $\rho_4 = [\hat{e}(g_1, h)^{-1}\hat{e}(g_2, K)]^{r_1}$, $\rho_5 = \sigma_3^{r_3} g_4^{r_1}$, $\rho_6 = \hat{e}(g_3, h)^{r_2}[\hat{e}(g_3, S)\hat{e}(g_2 g_4, h)]^{r_1}$,
  $\rho_7 = h^{r_4}$, $\rho_8 = \hat{e}(H_O(ID_O), K)^{r_4}\hat{e}(g_2, h)^{-r_1}$.
- The vehicle computes the hash challenge
  $c = H((\sigma_0, \cdots, \sigma_3, \sigma_5)||(\rho_0, \cdots, \rho_8)||A||C_1||C_2||m)$.
- The vehicle computes the responses to the hash challenge
  $z_0 = r_1 - cs_1 \mod p$, $Z_1 = R_1 X^{-c}$, $Z_2 = R_2 H_V(ID_V)^{-c}$, $Z_3 = R_3 B^{-c}$,
  $z_4 = r_3 - ce \mod p$, $z_5 = r_2 - cs_2 \mod p$, $z_6 = r_4 - cd \mod p$.
- The resulting signature σ on message m is:
  $\sigma = (\sigma_0, \cdots, \sigma_3, \sigma_5)||(z_0, Z_1, Z_2, Z_3, z_4, z_5, z_6)||c||A||C_1||C_2$.

3.6 Message Verification

Upon receiving a signature σ on message m, the receiving vehicle computes

$$\begin{aligned}
&\sigma_4 = \hat{e}(\sigma_1, h)^{-1}\hat{e}(\sigma_2, K), \sigma_6 = \hat{e}(g_5, h)^{-1}\hat{e}(\sigma_2\sigma_5, h)\hat{e}(\sigma_3, S),\\
&\sigma_8 = C_1 \cdot \hat{e}(\sigma_2, h)^{-1}, \rho_0 = g^{z_0}\sigma_0^c, \rho_1 = Z_1 g_1^{z_0}\sigma_1^c, \rho_2 = Z_2 g_2^{z_0}\sigma_2^c,\\
&\rho_3 = Z_3 g_3^{z_0}\sigma_3^c, \rho_4 = [\hat{e}(g_1, h)^{-1}\hat{e}(g_2, K)]^{z_0}\sigma_4^c,\\
&\rho_5 = \sigma_3^{z_4} g_4^{z_0}\sigma_5^c, \rho_6 = \hat{e}(g_3, h)^{z_5}[\hat{e}(g_3, S)\hat{e}(g_2 g_4, h)]^{z_0}\sigma_6^c,\\
&\rho_7 = h^{z_6} C_2^c, \rho_8 = \hat{e}(H_O(ID_O), K)^{z_6}\hat{e}(g_2, h)^{-z_0}\sigma_8^c, S = AK^{H(A||ID_R)}
\end{aligned} \tag{1}$$

and checks that

$$c = H((\sigma_0, \cdots, \sigma_3, \sigma_5)||(\rho_0, \cdots, \rho_8)||A||C_1||C_2||m) \tag{2}$$

If Equation (2) holds, the message is accepted. Else, the message is rejected.

3.7 Revoking Doubtable Messages

If the verifying vehicle receives a message with a valid signature but the message is doubtable, *e.g.* a bogus message, the verifier can submit the message along with its signature to IOA. IOA can use its secret key x_0 to open the encryption in the signature σ. IOA computes $W = \hat{e}(H_V(ID_V), h) = C_1/\hat{e}(x_0, C_2)$ and looks

up W in the registration table reg. If no entry W is found, IOA reports failure for the tracing procedure, else it outputs the vehicle identity ID_V.

Regarding revocation of malicious signers in group signature-based authentication in VANETs, another subtle issue is the case when some signer's secret key was compromised (*e.g.* stolen) for various reasons. It is a known open problem how to efficiently distinguish the compromised signers in group signatures. Some proposals suggest a public revocation list (by releasing the secret signing information of the compromised signer) and, whenever a verifier verifies a vehicular-generated message [18], the verifying vehicle first checks whether the signer is in the revocation list. If the signer is in the list, then the message will be discarded. Note that the revocation list grows linearly after the system is deployed. Hence, the performance of the system degrades as time passes. Another disadvantage is that one can also determine the authorship of the messages previously signed by the compromised vehicle. Hence, the vehicle's privacy cannot be guaranteed for messages signed before it was compromised.

We observe that the identity-based feature of IBGS-based privacy-preserving VANETs can be exploited to mitigate these disadvantages. When requesting the private key from TEA, each GRM's identity can be appended a tag specifying the lifetime (*e.g.* days or weeks) of the GRM's public key, *i.e.* {`GRM's identity`, `lifetime`}. Before the lifetime expires, each vehicle managed by this GRM contacts the GRM and updates its secret group signing key (see Section 3.4). For the verifying vehicles, they can just verify the received message as in Section 3.6 by additionally comparing their local time with the lifetime of the GRM's public key. This mechanism is very efficient because it only affects a subgroup of vehicles, *i.e.* the signing vehicles managed by the GRM, while the verifying vehicle (which can be any vehicle in the VANET) will not be affected. After employing this approach, an attacker can only sign messages on behalf of the compromised vehicles during a short time interval. If the signed message is false and is forwarded to IOA by the receiving vehicles, the misbehaving compromised vehicle can be located immediately and stopped by police cars.

3.8 Message Size

A vehicular report includes six fields: (`Message Type`; `Payload`; `Timestamp`; `TTL`; `Group ID`; `Signature`). Message ID defines the message type which is about 2 bytes, and the payload field may include information on the vehicle's position, direction, speed, traffic events, event time and so on. According to the DSRC standard [1], the payload of a message is 100 bytes. The timestamp is about 4 bytes and specifies the signature generation time, which is used to prevent replay attacks. It also ensures that an honest vehicle can report the same traffic situation at different times without being accused of multiple signatures on the same message. The TTL field is about 1 byte to specify Time To Live and determines how long the message is allowed to remain in the VANET. Group ID is about 2 bytes used to identify which group the vehicle belongs to. The signature field is the vehicle's signature on the first five fields. We denote the first five fields by m and the whole six fields by M. The length of vehicle-generated

Table 1. Format of vehicle-generated messages (suggested field lengths in bytes)

Mes. Type	Payload	Timestamp	TTL	Group ID	Sig.
2	100	4	1	2	460

messages can be expressed as $L_M = L_{\texttt{MessageType}} + L_{\texttt{Payload}} + L_{\texttt{Timestamp}} + L_{TTL} + L_{\texttt{GroupID}} + L_{\texttt{Signature}}$. To provide a typical security level of 2^{80}, we can set p a 170-bit long prime and then the element in $\mathbb{G}_1$ is 171 bits long [12], and $L_{sig} = 460$ bytes. Thus, $L_M = 2 + 100 + 4 + 1 + 2 + 460 = 569$ bytes. Table 1 summarizes the length of the report fields.

3.9 Security Analysis

We first analyze liability in our vehicular authentication protocol. The underlying IBGS scheme is proven non-frameable in the sense that no player except the trusted TEA can produce a signature that can be accepted by the verification procedure and for which the tracing procedure outputs the identity of a signer who did not generate the signature, even if the attacking players are allowed to collude [29]. This strong security property guarantees that, if a vehicle does not register to the VANET, it cannot generate messages accepted by other vehicles, and no vehicles, IOAs or GRMs can impersonate an innocent registered vehicle to authenticate vehicular communications. In other words, if a message is accepted as valid, it must have been generated by a single registered vehicle and not have been tampered with since it was sent. A message which passes the verification procedure can be used as a convincing argument in accident investigation if necessary. With this feature, the liability desirable in VANETs is properly guaranteed.

The underlying IBGS scheme is shown to be anonymous [29], even if there are only two signers in the group. This implies that no one except the designated IOA can distinguish messages from the various vehicles in a VANET. Thus an attacker cannot trace the vehicles by monitoring the communications in the VANET and the identity privacy of vehicles is well protected.

It is shown that the underlying IBGS is traceable and no group member or set of colluding members can generate a group signature accepted by the verification procedure which is not linkable to the actual signer [29]. In other words, if a vehicular message is accepted, the third-party IOA can always identify the actual message generator. This fact guarantees that cheating vehicles can always be caught by revoking their anonymity whenever fraudulent vehicular communications are detected.

4 Selfish Batch Verification

In a VANET, each vehicle periodically sends messages over a single hop every 300ms within a distance of 10s travel time [1], which means a distance range

between 10m and 300m. This implies that a vehicle will receive a large number of messages to be verified in a given time interval. To see this point, assume that the vehicle is in a 40m wide road with a density of 80 vehicles/km^2; hence, there will be 192 vehicles within a 300m range (backward and forward). In one period of 300ms, the vehicle will receive 192 messages/signatures (excluding multi-hop messages forwarded by neighboring vehicles) to be verified. It requires several milliseconds to verify each group signature and more than 300ms to verify all the received messages if they are verified one by one. This verification delay is much larger than the allowed maximum end-to-end message processing delay, *i.e.* 100ms. Hence, we need additional mechanisms to speed up message verification in large-scale VANETs.

We observe that the great redundancy of vehicular communications can be exploited to alleviate the burden of message verification. Only a small fraction of relevant messages actually need verification. If the number of messages selected for verification is still large, additional ways to reduce the verification overhead need to be devised. In what follows, we employ the batch verification technique ([2, 6, 10, 30]) to enable time-saving message processing in VANETs. This technique exploits the fact that a multi-base exponentiation (pairing) takes a similar time as a single-base exponentiation (pairing).

Lemma 1 (Batch verification lemma). *To verify exponential equations*

$$g_i^{x_i} f_i^{y_i} = 1, \quad \text{for } i = 1, \cdots, n \tag{3}$$

where $x_i, y_i \in \mathbb{Z}_p^*$ are known, and g_i, f_i are two elements of a finite cyclic group $\mathbb{G}$ of prime order p, one can randomly pick a vector $\Delta = (\delta_1, \cdots, \delta_n)$ for $\delta_i \in \{0,1\}^l$ and verify that

$$\prod_{i=1}^{n} g_i^{\delta_i x_i} f_i^{\delta_i y_i} = 1. \tag{4}$$

If Equations (3) are accepted whenever Equation (4) holds, a batch $\{(g_i, f_i) | i = 1, \cdots, n\}$ will be always accepted if it is valid, while an invalid batch will be accepted with probability at most 2^{-l}.

The above claim is ready to be extended to batch verification of bilinear equations since these are indeed exponentiation equations in $\mathbb{G}_3$. In this case, we only need to additionally note that $1 = \hat{e}(g_1, h)^a \hat{e}(g_2, h)^b$ can be equivalently rewritten as $1 = \hat{e}(g_1^a g_2^b, h)$ to save computations due to bilinearity and the fact that exponentiations in $\mathbb{G}_1$ are more efficient than those in $\mathbb{G}_3$.

To employ the above batch verification technique, the basic group signature needs to be extended. That is, the extended signature is now $\sigma' = \sigma || (\sigma_4, \sigma_6, \sigma_8) || (\rho_0, \cdots, \rho_8) || S$. Clearly, this modification does not affect any security property of the group signature because $(\sigma_4, \sigma_6, \sigma_8) || (\rho_0, \cdots, \rho_8) || S$ can be reconstructed from σ (see Section 3.6). The receiving vehicle needs to check Equations (1) and (2).

Let the vehicle select n message-signature pairs (m_i, σ_i') for batch verification, where $1 \leq i \leq n$ and $\sigma_i' = \sigma_i || (\sigma_{4,i}, \sigma_{6,i}, \sigma_{8,i}) || (\rho_{0,i}, \cdots, \rho_{8,i}) || S_i$. Then the vehicle needs to verify the equations:

$\sigma_{4,i}\hat{e}(\sigma_{1,i},h)\hat{e}(\sigma_{2,i}^{-1},K)=1$, $\sigma_{6,i}^{-1}\hat{e}(g_5^{-1}\sigma_{2,i}\sigma_{5,i},h)\hat{e}(\sigma_{3,i},S_i)=1$,
$\rho_{4,i}^{-1}\hat{e}(g_1^{-z_{0,i}},h)\hat{e}(g_2^{z_{0,i}},K)\sigma_{4,i}^{c}=1$, $\rho_{6,i}^{-1}\hat{e}(g_3^{z_{5,i}}(g_2g_4)^{z_{0,i}},h)\hat{e}(g_3^{z_{0,i}},S_i)\sigma_{6,i}^{c_i}=1$,
$\rho_{8,i}^{-1}\hat{e}(H_O(ID_{O_i})^{z_{6,i}},K)\hat{e}(g_2^{-z_{0,i}},h)\sigma_{8,i}^{c_i}=1$, $\sigma_{8,i}^{-1}C_{1,i}\hat{e}(\sigma_{2,i}^{-1},h)=1$,
$\rho_{0,i}^{-1}g^{z_0}\sigma_{0,i}^{c_i}=1$, $\rho_{1,i}^{-1}Z_{1,i}g_1^{z_{0,i}}\sigma_{1,i}^{c_i}=1$, $\rho_{2,i}^{-1}Z_{2,i}g_2^{z_{0,i}}\sigma_{2,i}^{c_i}=1$,
$\rho_{3,i}^{-1}Z_{3,i}g_3^{z_{0,i}}\sigma_{3,i}^{c_i}=1$, $\rho_{5,i}^{-1}\sigma_{3,i}^{z_{4,i}}g_4^{z_{0,i}}\sigma_{5,i}^{c,i}=1$,
$\rho_{7,i}^{-1}h^{z_{6,i}}C_{2,i}^{c_i}=1$, $S_i^{-1}A_iK^{H(A_i||ID_{R_i})}=1$

and

$c_i=H((\sigma_{0,i},\cdots,\sigma_{3,i},\sigma_{5,i})||(\rho_{0,i},\cdots,\rho_{8,i})||A_i||C_{1,i}||C_{2,i}||m_i)$.

Note that the first six equations, the middle five equations and the last two equations excluding the hash computation c_i are in the same finite cyclic groups $\mathbb{G}_3$, $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. Then Lemma 1 can be applied to each of those three batches of equations. We roughly compare the overheads of individual message verification with those of batch verification. For n messages, without using the batch approach, we need $O(N)$ multi-base pairing computations and multi-base exponentiations, as well as n hashes. However, after the batch verification is applied, the verifying vehicle needs only $O(1)$ multi-base pairing computations and multi-base exponentiations, as well as n hashes. According to state-of-the-art experimental results [10], a typical pairing takes tens of times longer than one exponentiation in $\mathbb{G}_1$, and compared to an exponentiation, the overhead of a hash computation is negligible. Hence, the batch approach offers a significant cost reduction and is very useful to speed up message verifications when the vehicular density is high, as in metropolitan areas.

5 Conclusions

The first VANETs are likely to be deployed in urban areas which particularly suffer from traffic accidents and congestions. In addition to vulnerabilities to attacks against traffic safety and drivers' privacy, a large-scale VANET in a metropolitan area poses a management problem. This paper proposed a set of mechanisms which conciliate system management, security and privacy requirements very well. We exploited IBGS to divide a large-scale VANET into easy-to-manage groups and establish liability in vehicular communications while preserving privacy. We further presented a selfish batch verification approach to accelerate message processing in VANETs. These techniques make our protocol scalable for deployment in big metropolitan areas.

Acknowledgments. This paper are partly supported by the EU 7FP through project "DwB", the Spanish Government through projects CTV-09-634, PTA2009-2738-E, TSI-020302-2010-153, PT-430000- 2010-31, TIN2009-11689, CONSOLIDER INGENIO 2010 "ARES" CSD2007-0004 and TSI2007-65406-C03-01, by the Government of Catalonia under grant SGR2009-1135, and by the NSF of China under grants 60970116, 61173154, 61003214, 91018008, 61021004, 61100173 and 11061130539. The authors also acknowledge support by the Fundamental Research Funds for the Central Universities of China through Project

3103004, Beijing Municipal Natural Science Foundation through Project 4112052, and Shaanxi Provincial Education Department through Scientific Research Program 2010JK727. The fird author is partially supported as an ICREA-Acadèmia researcher by the Catalan Government. The authors are with the UNESCO Chair in Data Privacy, but this paper does not necessarily reflect the position of UNESCO nor does it commit that organization.

References

1. 5GHz Band Dedicated Short Range Communications (DSRC), ASTM E2213-03, http://www.iteris.com/itsarch/html/standard/dsrc5ghz.htm
2. Bellare, M., Garay, J.A., Rabin, T.: Fast Batch Verification for Modular Exponentiation and Digital Signatures. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 236–250. Springer, Heidelberg (1998)
3. Blau, J.: Car talk. IEEE Spectrum 45(10), 16 (2008)
4. Boneh, D., Lynn, B., Shacham, H.: Short Signatures from the Weil Pairing. Journal of Cryptology 17(4), 297–319 (2004)
5. Calandriello, G., Papadimitratos, P., Lioy, A., Hubaux, J.-P.: Efficient and Robust Pseudonymous Authentication in VANET. In: ACM International Workshop on Vehicular Ad Hoc Networks-VANET, pp. 19–28. ACM Press (2007)
6. Camenisch, J., Hohenberger, S., Pedersen, M.Ø.: Batch Verification of Short Signatures. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 246–263. Springer, Heidelberg (2007)
7. Car2Car Communication Consortium, http://www.car-2-car.org/
8. Chaum, D., van Heyst, E.: Group Signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (1991)
9. Daza, V., Domingo-Ferrer, J., Sebé, F., Viejo, A.: Trustworthy Privacy-Preserving Car-generated Announcements in Vehicular Ad-Hoc Networks. IEEE Transaction on Vehehicluar Technology 58(4), 1876–1886 (2009)
10. Ferrara, A.L., Green, M., Hohenberger, S., Pedersen, M.Ø.: On the Practicality of Short Signature Batch Verification, http://eprint.iacr.org/2008/015.pdf
11. Fonseca, E., Festag, A., Baldessari, R., Aguiar, R.L.: Support of Anonymity in VANETs - Putting Pseudonymity into Practice. In: IEEE Wireless Communications and Networking Conference-WCNC, pp. 3400–3405. IEEE Press (2007)
12. Galbraith, S.D., Paterson, K.G., Smart, N.P.: Pairings for Cryptographers, http://eprint.iacr.org/2006/165.pdf
13. Gerlach, M., Festag, A., Leinmüller, T., Goldacker, G., Harsch, C.: Security Architecture for Vehicular Communication. In: WIT 2005 (2005), http://www.network-on-wheels.de/downloads/wit07secarch.pdf
14. Golle, P., Greene, D., Staddon, J.: Detecting and Correcting Malicious Data in VANETs. In: ACM International Workshop on Vehicular Ad Hoc Networks-VANET, pp. 29–37. ACM Press (2004)
15. Guo, J., Baugh, J.P., Wang, S.: A Group Signature Based Secure and Privacy-preserving Vehicular Communication Framework. In: Mobile Networking for Vehicular Environments 2007, pp. 103–108 (2007)
16. Lee, J.-H., Lee-Kwang, H.: Distributed and Cooperative Fuzzy Controllers for Traffic Intersections Group. IEEE Transactions on Systems, Man & Cybernetics 29(2), 263–271 (1999)

17. Leinmüller, T., Maihöfer, C., Schoch, E., Kargl, F.: Improved Security in Geographic Ad-Hoc Routing through Autonomous Position Verification. In: ACM International Workshop on Vehicular Ad hoc Networks-VANET, pp. 57–66. ACM Press (2006)
18. Lin, X., Sun, X., Ho, P.-H., Shen, X.: GSIS: A Secure and Privacy Preserving Protocol for Vehicular Communications. IEEE Transaction on Vehehicluar Technology 56(6), 3442–3456 (2007)
19. Network on Wheels, http://www.network-on-wheels.de/
20. Papadimitratos, P., Buttyan, L., Hubaux, J.-P., Kargl, F., Kung, A., Raya, M.: Architecture for Secure and Private Vehicular Communications. In: International Conference on ITS Telecommunications, pp. 1–6 (2007)
21. Parno, B., Perrig, A.: Challenges in Securing Vehicular Networks. In: HOTNETS 2005, http://conferences.sigcomm.org/hotnets/2005/papers/parno.pdf
22. Qin, B., Wu, Q., Susilo, W., Mu, Y.: Publicly Verifiable Privacy-Preserving Group Decryption. In: Yung, M., Liu, P., Lin, D. (eds.) Inscrypt 2008. LNCS, vol. 5487, pp. 72–83. Springer, Heidelberg (2009)
23. Raya, M., Aziz, A., Hubaux, J.-P.: Efficient Secure Aggregation in VANETs. In: ACM International Workshop on Vehicular Ad hoc Networks-VANET, pp. 67–75. ACM Press (2006)
24. Raya, M., Hubaux, J.-P.: The Security of Vehicular Ad-Hoc Networks. In: ACM Workshop on Security of Ad hoc and Sensor Networks-SASN, pp. 11–21. ACM Press (2005)
25. Raya, M., Hubaux, J.-P.: Securing Vehicular Ad Hoc Networks. Journal of Computer Security 15(1), 39–68 (2007)
26. Raya, M., Papadimitratos, P., Aad, I., Jungels, D., Hubaux, J.-P.: Eviction of Misbehaving and Faulty Nodes in Vehicular Networks. IEEE Journal Selected Areas in Communication 25(8), 1557–1568 (2007)
27. Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Matsuura, K., Sezaki, K.: CARAVAN: Providing Location Privacy for VANET. In: ESCAR 2005, http://www.ee.washington.edu/research/nsl/papers/ESCAR-05.pdf
28. Secure Vehicle Communication, http://www.sevecom.org/
29. Wei, V.K., Yuen, T.H., Zhang, F.: Group Signature Where Group Manager, Members and Open Authority Are Identity-based. In: Boyd, C., González Nieto, J.M. (eds.) ACISP 2005. LNCS, vol. 3574, pp. 468–480. Springer, Heidelberg (2005)
30. Wu, Q., Domingo-Ferrer, J., González-Nicolás, U.: Balanced Trustworthiness, Safety and Privacy in Vehicle-to-vehicle Communications. IEEE Transaction on Vehehicluar Technology 59(2), 559–573 (2010)
31. Wu, Q., Mu, Y., Susilo, W., Qin, B., Domingo-Ferrer, J.: Asymmetric Group Key Agreement. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 153–170. Springer, Heidelberg (2009)
32. Zarki, M.E., Mehrotra, S., Tsudik, G., Venkatasubramanian, N.: Security Issues in a Future Vehicular Network. In: European Wireless (2002), http://www.ics.uci.edu/~dsm/papers/sec001.pdf
33. Zhang, L., Wu, Q., Solanas, A., Domingo-Ferrer, J.: A Scalable Robust Authentication Protocol for Secure Vehicular Communications. IEEE Transactions on Vehicular Technology 59(4), 1606–1617 (2010)