Short-Term Linkable Group Signatures with Categorized Batch Verification

Lukas Malina[1], Jordi Castellà-Roca[2], Arnau Vives-Guasch[2], and Jan Hajny[1]

[1] Department of Telecommunications, Brno University of Technology,
Purkynova 118, Brno, Czech Republic
{malina,hajny}@feec.vutbr.cz
http://crypto.utko.feec.vutbr.cz
[2] Department of Computer Engineering and Mathematics,
Universitat Rovira i Virgili,
Av. Paisos Catalans 26, Tarragona, Catalonia, Spain
{jordi.castella,arnau.vives}@urv.cat

Abstract. In ad hoc wireless networks like Vehicular ad hoc Network (VANETs) or Wireless Sensor Networks (WSN), data confidentiality is usually a minor requirement contrary to data authenticity and integrity. Messages broadcasted from a node to other nodes should be authentic but also keep user's privacy in plenty scenarios working with personal data. Group signatures (GS) are used to provide privacy and authenticity to the users. Moreover, GS with batch verification can be efficient. Nevertheless, the current solutions have practical drawbacks like using an expensive tamper-proof hardware, the computation bottlenecks of the verification and revocation phases, complicated certificate distribution/revocation or omitting important properties like short-term linkability which is demanded in several applications, e.g. change lanes of vehicles in VANETs. To our best knowledge, our solution employs the short group signature with short-term linkability and categorized batch verification for the first time. Our solution provides more efficient signing and verification than compared schemes. Moreover, the solution allows secure and practical registration and revocation of users. The usage of proposed scheme protects the honest users who can now join and securely communicate without losing their privacy.

Keywords: Security, Group Signature, Batch Verification, Privacy, Efficiency, Ad hoc Wireless Network, Short-term Linkability.

1 Introduction

There are a lot of practical and theoretical scenarios where data confidentiality is not too important like data authenticity, integrity and user privacy during communication. For example, privacy is demanded by users in Wireless Body Sensor Networks (WBSN) where nodes are bound to human in order to measure medical data and user position [1]. In WBSN, the users concern about their potential monitoring by a malicious observer. Further, the received messages

J. Garcia-Alfaro et al. (Eds.): FPS 2012, LNCS 7743, pp. 244–260, 2013.

carrying useful data from several tens of nodes must be verified as soon as possible. The same problem with privacy arises in VANETs. For better intuition, we apply our proposed security solution to VANETs. Nevertheless, the solution can be applied to systems where the users' privacy, data authenticity and integrity are required during dense communication.

The wireless communication among vehicles brings many applications which can help drivers, prevent accidents or reduce traffic. A vehicular ad hoc network measures useful data like speed, location, road condition or alerts and distributes them using an On Board Unit (OBU) in a vehicle in order to increase security on roads and reduce traffic jams. OBU can be an embedded device/a user smartphone or a navigation with VANET application. Self-organized VANET offers two types of communication: wireless communication between a vehicle and a vehicle (V2V), and communication between vehicles and the VANET infrastructure (V2I) represented by Road-Side Units (RSU) which are connected to a fixed infrastructure (eg. Internet). Security in VANETs plays a key role in protecting against bogus and malicious messages, misusing at roads, eavesdropping etc. Common solutions guarantee the message integrity, authentication and non-repudiation. Furthermore, privacy is required due to the possibility of drivers tracking by malicious observers. Moreover, VANETs can serve in a dense urban traffic where hundreds of vehicles communicate in V2V or V2I, so that the security overhead and computation time must be minimal. In this case, the following scenario is considered: *Scenario 1*: A driver, Alice (A), with the car no. 2, which is depicted in Fig.1, can register special events (accidents, traffic jams, roads under construction etc.). Depending on the type of event, A immediately broadcasts a warning message through the wireless V2V communication to all participated cars in VANET. In this scenario, an accident is depicted in Fig.1. Supposing another driver, Bob (B), with the car no. n-1, who is in range and coming closer to A, receives this message. B also receives more messages from another cars in the area. Moreover, other messages can contain contradictory warnings or can be bogus. In short time, B must consider the validity of these

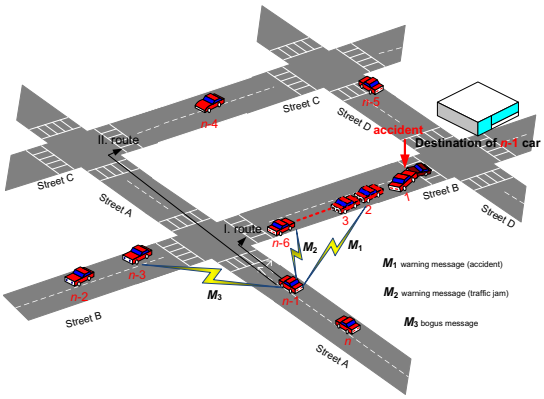

Fig. 1. The VANETs in urban traffic - Scenario 1

messages and quickly decides changing the route (from planed I. to II.). If B makes the right decision, he can avoid the situation referenced by the first warning message. It is obvious that the decision must come in real time and as soon as possible. In another case, a lot of cars periodically broadcast informations about them (speed, direction, location, break alerts etc.) and road conditions (changing of road lanes, distance between cars etc.) each other. The type of information depends on the application used by the car, but message processing must be efficient because the sending period of beacon messages is less than 300 ms [2].

The security proposals are challenged to connect privacy, security, efficiency and capable management in huge vehicular networks. The open problem of *Scenario 1* is how a lot of anonymous messages can be verified in real time. The related work tries to solve this problem using the batch verification of group signatures. But this approach takes more time than expected if the number of malicious messages appeared in batch is $\geq 15\%$ from all messages as is claimed in [3]. In order to improve this issue, we propose a novel solution with categorized batch verification with short-term linkability which can serve to recognize the malicious messages and excludes them from batch. Moreover, the short-term linkability significantly improves the signing phase, so that our scheme provides more efficient signing and verification than related works using GS.

The paper is organized as follow: The next section presents the related work which is focused on the security and privacy protection in VANETs and our contribution is outlined. Then, section 3 presents a basic scheme description, requirements and main cryptographic techniques used in our proposal. Further, section 4 introduces our solution and the phases of our scheme are described. The important phases like signing and verification are evaluated and compared with related solutions in section 5. Section 5 also contains the security consideration. Finally, conclusion and future work are presented in section 6.

2 Related Work and Our Contribution

In this section, we outline the related work and our contribution.

2.1 Related Work

Generally, the protection of privacy in VANETs can be ensured by three approaches, i.e., pseudonyms, group signatures and hybrid schemes. Anonymization through pseudonyms has been proposed in [4] and [5]. The work [6] uses anonymous certificates which are stored in vehicles (usually in a tamper-proof device). This approach uses a set of short-lived pseudonyms and privacy among vehicles is provided by changing these certified public keys. Nevertheless, in large urban VANETs, this approach is burdened by preloading and storing a large number of anonymous certificates with pseudonyms.

Group signatures (GS) in VANETs provide user anonymity by signing a message on behalf of a group. GS guarantee the unlinkability of honest users

and the traceability of misbehaving users. The scheme [7] called GSIS uses the combination of a group signature based on [8] with a hybrid membership revocation mechanism in the V2V communication, and Identity Based Group Signature (IBGS) in the V2I communication. The hybrid membership revocation with the list of revoked members (RL) works with a threshold value T_τ. In case $|\text{RL}| < T_\tau$, the scheme uses revocation verification algorithm, otherwise, the scheme updates the public/private group keys of all non-revoked members. For efficient verification, the authors of [9] propose a GS with batch verification in V2I which takes three pairing operations. This scheme called IBV has several drawbacks such as using tamper proof devices, it is vulnerable to tracking or impersonation attacks, see [10] for a complete description. The works [11] and [12] can efficiently verify a large number of messages in V2V. These schemes use short group signatures with fast batch verification (only two pairing operations are used instead of 5 n, where n is number of messages). Nevertheless, the performance of batch verification degrades in dense V2V communication with bogus messages. The On Board Units (OBUs) must process the messages quickly, they have between 100 ms and 300 ms to process a message [2]. Thus, the computation of expensive pairing and exponentiation on limited On Board Units (OBUs) is a hard requirement to meet because of the short response time. This fact limits the VANETS in practice. The work [13] employs identity based group signature with the batch verification, provides a scalable management of large VANETs and an efficient revocation of members, but suffers from more expensive signing and verification phases than GS.

In [14], vehicles locally generate on the fly short-lived certificates (pseudonyms) with the help of GS. A Certification Authority (CA) maintains the mapping between identities and pseudonyms. One of the drawbacks is the security overhead of messages that consists of the message signature by private short-lived key, public short-lived key and the group signature of public short-lived key. In [15], the solution called TACK uses short-lived keys (ECDSA) to secure V2V messages. Long-term pre-distributed keys (group signatures) are used for anonymous authentication in regions and to gain the new certified temporary key from the Regional Authorities (RAs). TACK supports desirable short-term linkability but in dense V2I communication leads to delay in join phase and OBU must broadcast ECDSA public key with the certificate in V2V. In [10], the two proposals called SPECS include the pseudonyms maintained by Trusted Authorities (TAs), the group signature with 2-pairing batch verification and the positive and negative bloom filter for the effectiveness of the verification phase. Nevertheless, SPECS strongly rely on TAs and Road-Side Units RSUs. Also, the communication delay plays a critical role between TAs and vehicles. In [16] the authors present a Threshold Anonymous Announcement (TAA) service based on the adaptation and amalgamation of direct anonymous attestation and one-time anonymous authentication. The computational cost of the signing algorithm takes only 6 scalar multiplications and 1 pairing operation, and the computational cost of the verification algorithm takes 5 scalar multiplications and 5 pairing operations. Nevertheless, the TAA scheme does not support batch verification.

2.2 Our Contribution

Similarly like in [9], [11], [12] and [17], our proposed solution is based on group signature. We focus on the efficiency of signing/verification, security and privacy protection with respect to computationally limited RSUs. As related works, we assume OBUs with enough computational power for basic modular arithmetic, pairing and cryptographic operations.

- In the V2V communication, our solution provides the efficient signing with short-term linkability. Our proposal uses the modified scheme of Wei et al. (WLZ scheme) [17]. Nevertheless, our solution adds the short-term linkability obtaining a more efficient signing phase than in the WLZ scheme. Moreover, the WLZ scheme is focused on the V2V communication and does not describe the registration and join phases in detail. Finally, the short-term linkability is demanded for several applications [15] and can protect against Sybil and Denial of Services attacks.
- In the V2V communication, our solution provides the efficient categorized batch verification with short-term linkability. Generally in group signatures, the batch verification of n messages is more efficient than individual verification but the complexity of batch computation with bogus messages increases from O(1) to O(ln n). In [3], the authors claim that if $\geq 15\%$ of the signatures are invalid, then batch verification is not more efficient than individual verification. Our proposal modifies the WLZ scheme [17] where the batch verification costs only 2 pairings and $11n$ exponentiations. But the WLZ scheme and related solutions use uncategorized batch verification which can cause less efficient verification if bogus messages appear during attacks like the Sybil attack, the Denial of Services (DoS) attack etc. However, our solution applies categorized batch verification which sorts potential honest messages to the first batch, and potential untrusted messages to the second or third batch with lower priorities so the verification phase can be more efficient and protect against Sybil and DoS attacks.
- In V2I communication, our scheme uses probabilistic cryptography for keeping long-term unlinkability and the privacy protection of drivers. The join or registration phase takes only two messages (request/response) and the scheme does not need tamper-proof devices.
- We avoid the inefficient linear growth of revocation list with the secret keys of members. Our proposal uses the revocation process with the expiration of time stamp in certified pseudonym which revokes members by self. Vehicles have no work with a Revocation List (RL). The proposal uses only a Group Temporary Revocation List (GTRL) broadcasted between group managers to deny malicious members accessing the group of VANET members.

3 Preliminaries

In this section, we outline the scheme, the requirements and the main cryptographic techniques used in our proposal.

3.1 Scheme Description

Our scheme, depicted in Fig.2, consists of a Trusted Authority (TA), a Group Manager (GM) and a Member (V).

- **TA** issues certified member pseudonyms and generates all public cryptographic parameters in our solution. TA is fully trusted entity in our model and can reveal the real ID of a member in the revocation phase. TA is connected with all group managers and manages the registration of all members.
- **GM** is an entity which manages several Road Side Units (RSUs) and generates group secret keys to members in the join phase. In our proposal, we assume that GM is honest and is securely connected with the own RSUs (e.g. via Transport Layer Security). GM also can trace and open the malicious messages in its own area but GM cannot reveal the member ID.
- **V** is a driver with the certified pseudonym which is embedded in vehicle's OBU. After the registration of the driver in TA and joining in GM's area through the V2I communication, V can send or broadcast messages through the V2V communication. Further, V can report a bogus message through the V2I communication to GM.

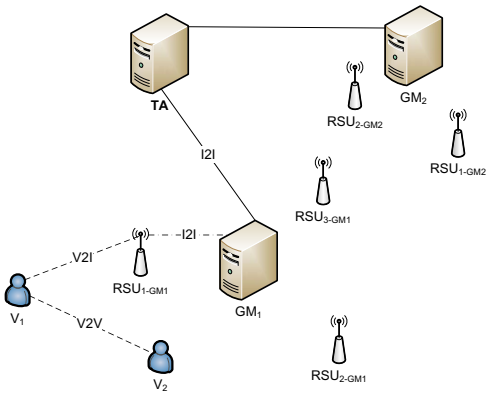

Fig. 2. The parties in our model of secure and anonymous VANET

3.2 Requirements

Our scheme is designed to satisfy these security and practical requirements:

- **Privacy (Revocable Anonymity).** Our scheme protects driver's privacy in the long-term. An honest driver with OBU can use the pseudonym signed by TA to obtain group parameters and keys from GM. Then, its OBU can sign every message on behalf of the group members and keep driver's anonymity. Every malicious driver can be revealed by the collaboration of GM and TA. If some member breaks the rules, his/her messages can be opened by GM and his pseudonym is sent to TA which can extract the member's ID. Next time, when an adversary requests a new pseudonym with a fresh time stamp (e.g. via IETF RFC 3161), TA checks if his/her ID is in the list of globally revoked members.

- **Message Integrity, Authenticity and Non-Repudiation.** In V2V communication, the group signature ensures that message is signed by a vehicle which holds the right and fresh group key pair (authenticity). The system must verify the received messages, i.e., the messages that have not been modified once they have been sent (integrity). Members stay private but can not deny that they created the signed messages (non-repudiation).
- **Short-Term Linkability.** In several VANET's applications like the safe changing of road lanes and the short-term mapping of vehicle movements, the short-term linkability is a desirable property [15]. In a short period, i.e., every 100÷300 ms, the broadcasted V2V beacon messages are used to trace vehicle's position and direction. The current proposals which use group signatures cannot link related messages from one vehicle sent in a short interval. Our scheme balances the privacy of drivers and the linkability of messages which is available only for a short interval. On the other hand, long-term unlinkability is ensured using the probabilistic encryption and changing the pseudonyms in the group signature.
- **Traceability.** When a member misuses the VANETs for his/her own benefit, he/she breaks the rules or causes an accident, the GM obtains his/her pseudonym from his/her signed messages and, sends it to the TA, who revokes the anonymity, and obtains his/her ID.

3.3 Cryptography Background

Our solution employs the ECDSA signature scheme with the public/private keys of TA, GM, V. Additionally, we use a probabilistic ElGamal encryption/decryption during the join of members. The modified short group signature WLZ scheme [17] based on the BBS04 scheme [8] is used in the V2V communication. This scheme uses bilinear maps and is based on q-SDH problem and Decision Linear problem which have been studied in [8].

We follow the notation of [8] for the concept of bilinear maps: G_1, G_2 and G_T are multiplicative cyclic groups of a prime order p. Then, g_1 is a generator of G_1, g_2 is a generator of G_2 and ψ is an isomorphism from G_2 to G_1 that $\psi(g_2) = g_1$. So e is a computable bilinear map $e : G_1 \times G_2 \rightarrow G_T$ with following properties:

- Bilinearity: for all $u \in G_1, v \in G_2$ and $a, b \in Z_p, e(u^a, v^b) = e(u, v)^{ab}$.
- Non-degeneracy: $e(g_1, g_2) \neq 1_{G_T}$.

The q-Strong Diffie-Hellman problem is a hard computational problem where $(q+2)$-tuple $(g_1, g_2, g_2^{\gamma}, g_2^{\gamma^2}, ..., g_2^{\gamma^q})$ is the input and a pair $(g_1^{\frac{1}{x+\gamma}}, x)$ is the output.

The Decision Linear Diffie-Hellman problem. Given $u, v, h, u^a, v^b, h^c \in G_1$ as input and output *yes* if $a + b = c$ and *no* otherwise, detailed in [8].

4 Our Solution

We focus on the practical registration and join of VANET members and the efficient signing/verification of V2V messages. Our solution consists of seven phases: Setup, Registration, Join, Signing, Categorized Verification, Trace, Revocation.

4.1 Setup

In the first part, TA chooses parameters $(G_1, G_2, g_1, g_2, \psi, e)$ and generates an ECDSA key pair sig_{TA}/ver_{TA}, an ElGamal private key sk_{TA} and a public key pk_{TA}, then releases the public keys and parameters. GMs generate group signature keys, ElGamal private sk_{GM_i} and public pk_{GM_i} keys for the secure V2I communication and publish public keys. Every GM_i randomly selects $r_1, r_2 \in Z_p^*, h \in G_1^*$ and sets u, v such that $u^{r_1} = v^{r_2} = h$. Then, GM_i selects random $\gamma \in Z_p^*$ and computes $w = g_2^{\gamma}$. The group public key is $gpk = (g_1, g_2, u, v, w, h)$ and the manager group secret key is $gmsk = (r_1, r_2)$.

4.2 Registration

In the registration phase, the i-th driver (member) V_i using a vehicle with OBU requests a valid certified pseudonym π_{V_i} from TA. For the first time, TA must physically verify driver's real ID, his/her driving license and OBU's ID number. Then V_i creates an ECDSA key pair sig_{V_i}/ver_{V_i}, gives the public key to TA which stores (ID_{V_i}, ver_{V_i}) in the database, and the signed certificate $cer_{V_i} = sig_{TA}(ID_{V_i}, ver_{V_i})$ is given to V_i. After the first successful registration phase, driver can request his/her next pseudonym online. Assuming that V_i has pk_{TA}, ver_{TA}, the two-message of the registration phase consists of these steps:

1. V_i self-generates ElGamal key pair (sk_{V_i}/pk_{V_i}) and sends the encrypted request $enc_{pk_{TA}}(pk_{V_i}||ID_{V_i}||ver_{V_i}||cer_{V_i}||sig_{V_i}(pk_{V_i}||ver_{V_i}||\ ID_{V_i}))$ to TA.
2. TA decrypts the request and checks if the ID_{V_i} is not revoked in Global Revocation List (GRL), the certificate cer_{V_i} and the member's signature which ensures member's authenticity and commits the pk_{V_i} in the certificate with new ElGamal key pair. Then, TA generates a challenge $c \xleftarrow{R} Z_q$, a time stamp T_l and sends the encrypted response

$enc_{pk_{V_i}}(enc_{pk_{TA}}(ID||ver_{V_i}||c)\ ||T_l||sig_{TA}(T_l||enc_{pk_{TA}}(ID||ver_{V_i}||c)||pk_{V_i}))$ back to V_i. Finally, V_i checks the signature by TA and composes the pseudonym $\pi_{V_i} = pk_{V_i}||enc_{pk_{TA}}(ID||ver_{V_i}||c)||T_l||\quad sig_{TA}(T_l||enc_{pk_{TA}}(ID||ver_{V_i}||c)||pk_{V_i})$ and stores it.

4.3 Join

A vehicle entering the i-th GM_i area (several RSUs) for the first time, requests the group public key and his/her group member secret key. We assume that RSUs managed by GM_i are securely connected through the VANET infrastructure. Let $H()$ be a hash function, and the two-message join phase consists of these steps:

1. V_i sends $\pi_{V_i} = pk_{V_i}||enc_{pk_{TA}}(ID||ver_{V_i}||c)||T_l||sig_{TA}(T_l||enc_{pk_{TA}}(ID||ver_{V_i}||c)||pk_{V_i})$,which is encrypted using pk_{GM_i}, to GM_i.
2. GM_i decrypts π_{V_i} using sk_{GM_i}, verifies π_{V_i} that is signed by TA and controls if $enc_{pk_{TA}}(ID||ver_{V_i}||c)$ is not in Group Temporary Revocation List

(GTRL) and the validity of the time stamp T_l. If π_{V_i} is ok, GM creates $gsk_{V_i} = (x_i, A_i)$, where $x_i = H(enc_{pk_{TA}}(ID||ver_{V_i}||c)||T_l||\gamma), A_i = g_1^{\frac{1}{x_i+\gamma}}$, and stores $(enc_{pk_{TA}}(ID||ver_{V_i}||c), A_i, T_l))$ to the join table and sends gsk_{V_i} encrypted using pk_{V_i} to V_i.

We note that ElGamal encryption/decryption is probabilistic. Due to this fact, an observer can not link two or more encrypted messages if V_i requests gsk_{V_i} for the second time.

4.4 Signing

The signing phase applies the modified short group signature WLZ scheme [17] which is based on the BBS04 scheme [8]. We include a counter k in the OBUs, a member secret key $gsk_{V_i} = (A_i, x_i)$ and a group public key $gpk = (g_1, g_2, h, u, v, w)$. OBU signs a message $M \in (0,1)^*$ and outputs the signature of knowledge $\sigma = (T_1, T_2, T_3, R_2, R_3, R_5, c, s_\alpha, s_\beta, s_x, s_\delta, s_\mu)$.

If $k = 0$, V_i generates $\alpha, \beta, r_\alpha, r_\beta, r_x, r_\delta, r_\mu \in Z_p^*$, and computes

$$\begin{aligned} T_1 = u^\alpha, T_2 = v^\beta, T_3 = A_i h^{\alpha+\beta}, \\ \delta = \alpha x, \mu = \beta x. \end{aligned} \tag{1}$$

$$p_1 = e(T_3, g_2), p_2 = e(h, w), p_3 = e(h, g_2). \tag{2}$$

stores $T_1, T_2, T_3, \delta, \mu, p_1, p_2, p_3$, and computes

$$\begin{aligned} R_1 = u^{r_\alpha}, R_2 = v^{r_\beta}, R_3 = p_1^{r_x} \cdot p_2^{-r_\alpha - r_\beta} \cdot p_3^{-r_\delta - r_\mu}, \\ R_4 = T_1^{r_x} u^{-r_\delta}, R_5 = T_2^{r_x} v^{-r_\mu}, \end{aligned} \tag{3}$$

$$c = H(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5), \tag{4}$$

$$\begin{aligned} s_\alpha = r_\alpha + c\alpha, s_\beta = r_\beta + c\beta, s_x = r_x + cx, \\ s_\delta = r_\delta + c\delta, s_\mu = r_\mu + c\mu. \end{aligned} \tag{5}$$

Finally, V_i sends the message M with the signature $\sigma = (T_1, T_2, T_3, R_2, R_3, R_5, c, s_\alpha, s_\beta, s_x, s_\delta, s_\mu)$ and increases the counter $k{+}{+}$.

If α and β are unchanged every n messages, the short-term linkability is kept because the pseudonyms of group signature T_1, T_2, T_3 are also unchanged. Thus, for n messages, when $1 \leq k \leq n$, V_i does not need to compute equations 1, 2, contrary the WLZ scheme, but only generates random $r_\alpha, r_\beta, r_x, r_\delta, r_\mu \in Z_p^*$ and computes equations 3, 4 and 5. This reduces all 3 bilinear operations to 0, 10 exponentiations to 9 and 14 multiplications to 9. The concrete VANET application can decide when to fix the counter $k = 0$ and V_i generates new α and β and recomputes the equations 1 and 2.

4.5 Categorized Verification

Our solution uses a categorized verification which sorts the incoming signed messages to three levels of credibility. Due to the short-term linkability, V_i can keep the Temporary List (TL) of known vehicles. Firstly, the received message M_j is checked by V_i if it contains a valid time stamp, real and consistent data. After that, the message with the group signature containing T_3 is checked if T_3 is in TL. If yes, the recorded T_3 with previous validity (W=1) is included and sorted in the first batch. The validity W can be a boolean value which indicates valid (W=1) or invalid (and unknown, W=0) signatures. If no, the signed message with unknown T_3 is sorted to the second batch which is verified after the first batch verification. The rest of signed messages with T_3 linked with W=0 is verified in the third batch at the end of verification if OBU has enough time for this. This approach improves the efficiency of the batch verification process and helps when an attacker, who is out of the group, generates unsigned or corrupted messages.

Batch Verification. Batch verification is investigated in [3], and it verifies n messages in one batch. V_i uses $gpk = (g_1, g_2, h, u, v, w)$ to verify messages $\sigma_j = (T_{j1}, T_{j2}, T_{j3}, R_{j2}, R_{j3}, R_{j5}, c_j, s_{j\alpha}, s_{j\beta}, s_{jx}, s_{j\delta}, s_{j\mu})$ for $j = 1, ..., n$ does:

restores $\overline{R}_{j1} = u^{s_{j\alpha}} T_{j1}^{-c}, \overline{R}_{j4} = u^{-s_{j\delta}} T_{j1}^{s_x}$, computes a new control hash c'_j from received parameters:

$$c'_j = H(M_j, T_{j1}, T_{j2}, T_{j3}, \overline{R}_{j1}, R_{j2}, R_{j3}, \overline{R}_{j4}, R_{j5}).$$

and checks if $c'_j = c_j$. If yes then V_i continues with verification, otherwise, the message with the signature is inconsistent and is refused.

V_i randomly selects $\theta_1, \theta_2, ..., \theta_n \in Z_p$ with l_b bit,

checks batch if

$$\prod_{j=1}^{j=n} R_{j3}^{\theta_j} = e(\prod_{j=1}^{j=n} (T_{j3}^{s_{jx}} h^{-s_{j\delta} - s_{j\mu}} g_1^{-c_j})^{\theta_j}, g_2) \; e(\prod_{j=1}^{j=n} (T_{j3}^{c_j} h^{-s_{j\alpha} - s_{j\beta}})^{\theta_j}, w) \tag{6}$$

and if

$$1_{G_1} = (R_{j5} R_{j2})^{-\theta_j} T_{j2}^{\theta_j s_{jx} - \theta_j c_j} v^{(s_{j\beta} - s_{j\mu})\theta_j}. \tag{7}$$

The signed message is valid if equations 6 and 7 hold. All T_3s from new valid signed messages are added to TL with W=1. In case that the batch verification fails, the divide-and-conquer approach is used to identify the invalid signatures that were added to TL with W=0. The honest messages keep the mark W=1.

Individual Verification. In the end of the divide-and-conquer approach, the final two messages are individually verified.

V_i restores $\overline{R}_1 = u^{s_\alpha} T_1^{-c}, \overline{R}_4 = u^{-s_\delta} T_1^{s_x}$, computes new control hash c' from received parameters:

$$c' = H(M, T_1, T_2, T_3, \overline{R}_1, R_2, R_3, \overline{R}_4, R_5).$$

and checks if $c' = c$. If yes then V_i continues with the verification, otherwise, the message is inconsistent and it is refused.

Then, V_i checks if

$$R_3 = e(T_3, g_2)^{s_x} e(h, w)^{(-s_\alpha - s_\beta)} e(h, g_2)^{(-s_\delta - s_\mu)} (e(T_3, w) e(g_1, g_2)^{-1})^c \tag{8}$$

and

$$1_{G_1} = (R_5 R_2)^{-1} T_2^{s_x - cx} v^{(s_\beta - s_\mu)}. \tag{9}$$

The signed message is valid if equations 8 and 9 hold.

We can see from equations 6 and 8 that individual verification have a cost of 5 pairing operations per one message but batch verification costs only 2 pairing operations per n messages. This is the main reason why we avoid individual verification and propose to use the categorized batch verification.

4.6 Trace

Every bogus signed message can be opened by GM_i using the group manager secret key $gmsk = (r_1, r_2)$. GM_i extracts the part of the member secret group key $gsk_{V_i} \rightarrow A_i = T_3/(T_1^{r_1} \cdot T_2^{r_2})$ and searches the record $(enc_{pk_{TA}}(ID||ver_{V_i}||c), A_i, T_l)$ in the database. The part of the member pseudonym can be sent to TA for revocation.

4.7 Revocation

When there are serious circumstances, e.g., an accident, a malicious member is revoked globally by the cooperation of GM_i and TA. GM_i is able to open a message and extract the member pseudonym that is sent to TA. TA broadcasts $rev = (enc_{pk_{TA}}(ID||ver_{V_i}||c), T_l)||sig_{TA}(rev)$ to other active GMs which check the signature and store rev to own GTRLs until the lifetime of this pseudonym expire. TA extracts ID_{V_i} and adds it to GRL so the malicious member can not refresh his/her pseudonym in the next registration phase.

5 Evaluation and Security Consideration

In this section, we outline the evaluation of our solution, the comparison of the signing and verification phases with the related works which are based on group signatures and the security consideration of our solution.

5.1 Performance and Comparison with Related Work

We compare our proposal based on the BBS04 scheme [8] with the related VANETs schemes which use group signatures, the scheme of Wei et al. (WLZ scheme) [17], GSIS [7], Zhang et al. [11] and Ferrara et al. [3]. In our comparison, we omit the WS2010 scheme [12] due to the the problem in message signing which is pointed out in [17]. The verification of the TAA scheme [16] takes 5

scalar multiplications and 5 pairing operations but the TAA scheme does not support batch verification.

Generally, the time of bilinear pairing T_p is considered the most expensive operation (tens times more expensive than exponentiation operation T_e) and exponentiation is more expensive than multiplication T_m. Nevertheless, the actual processing time also depends on the input size to those operations. Due to the fact that related works are also based on the BBS04 scheme [8] we assume the same lengths of parameters (the MNT curves with $G_1 = 176$ bits, $G_T = 528$ bits and $Z_p = 162$ bits). The work [18] shows that the modular arithmetic operations like addition and subtraction can be computed more efficiently than multiplication and exponentiation. Due to this fact, we omit these fast operations in this performance evaluation.

Table 1. The comparison of the verification phases

V2V scheme:	Our scheme & WLZ scheme[17]	GSIS [7]	Zhang et al. [11]	Ferrara et al. [3]
Batch:	yes	no	yes	yes
Length of signature:	$5G_1, G_T, 5Z_p$ (2380 bits)	$3G_1, 6Z_p$ (1500 bits)	$7G_1, G_T, 5Z_p$ (2570 bits)	$3G_1, G_T, 6Z_p$ (2032 bits)
Performance of batch verification				
Pairings	**2**	5n	2	2
Exponentiation	**11n**	12n	14n	13n
Multiplication	11n+1	**8n**	17n	10n+1
Performance of individual verification				
Pairings	5	5	5	5
Exponentiation	**10**	12	12	12
Multiplication	9	8	8	8

The proposal based on the group signature BBS04 scheme [8] and motivated by Wei et al. (WLZ) [17] reaches more efficient batch verification ($2\ T_p + 11n\ T_e$), where n is the number of messages, and individual verification ($5\ T_p + 10\ T_e$) than the compared schemes, see Table 1. But the related solutions like Zhang et al. [11], Ferrara et al. [3], the WS2010 scheme [12] and also the WLZ scheme [17] use uncategorized batch verification that can be negatively affected by malicious and bogus messages ($\geq 15\%$ from all messages). To our best knowledge, our proposal applies categorized batch verification with short-term linkability in VANET for the first time. Our categorized batch verification with the temporary list of known vehicles reaches the high correctness of the important first batch in case when the bogus or damaged signed messages appear in the V2V communication.

As we can see in Table 2, our proposal significantly improves the performance of the signing of x messages with short-term linkability and it costs less operations than in the signing phase of the WLZ scheme. Pairing ($3 \Rightarrow 0$), exponentiations ($10 \Rightarrow 9$) and multiplication ($14 \Rightarrow 9$) operations are reduced.

Table 2. The comparison of the signing phases

V2V scheme:	Our scheme	WLZ scheme [17]	GSIS [7] & Zhang et al. [11] & Ferrara et al. [3]
Short-term linkability:	yes	no	no
Performance of signing for the first message / the next messages			
Pairings	3 / **0**	3 / 3	3 / 3
Exponentiation	12 / **9**	10 / 10	12 / 12
Multiplication	12 / **9**	14 / 14	12 / 12

Our scheme is implemented as a proof of concept in JAVA and uses the Java Pairing Based Cryptography (jPBC) Library [1]. The implementation employs MNT curves type D with the embedding degree $k = 6$, 171 b order curve and pre-generated parameters d840347-175-161.param and is tested on a machine with Intel(R) Xeon(R) CPU X3440 @ 2.53GHz, 4 GB Ram, Windows 7 Professional. The signing phase of our scheme with short linkability takes approx. 60 ms per one signature and the signing phase of the related schemes [3], [7], [11] and [17] based on BBS scheme takes approx. 160 ms per one signature. The verification of a single signature takes approx. 207 ms using our scheme and approx. 224 ms using related schemes. If the batch verification is employed then the verification of one signature takes approx. 50 ms so the batch verification of 10 signatures takes approx 500 ms.

5.2 Security Consideration

In this section, we outline the security consideration of our solution, that is based on the cryptographic primitives which are secure and widely accepted.

Proposition 1. *In the registration phase between V_i and honest TA, the scheme preserves message confidentiality, integrity and authenticity.*

Claim 1. *The request and response messages are confidential.*

Proof. We suppose that breaking the security of the ElGamal encryption is at least as hard as the decision Diffie-Hellman problem, as is proven in [19]. Then, the registration phase keeps confidential communication between V_i and TA due to the encryption every message by $enc_{pk_{TA}}$ and $enc_{pk_{V_i}}$. Only holder of the ElGamal private key sk_{TA} respectively sk_{V_i} can decrypt the message.

Claim 2. *The request message is authentic and can not be modified by an unauthorized entity.*

Proof. Message integrity and authenticity are ensured by the ECDSA signature scheme. The request message is unforgeable due to the commitment of the member public key pk_{V_i} in the member's certificate and in the signed part of request by V_i using ECDSA signature key sig_{V_i}. Assumining that the ECDSA signature

[1] (Available on `http://gas.dia.unisa.it/projects/jpbc/index.html`).

scheme is secure under the Elliptic Curve Discrete Logarithm Problem (ECDLP) and the used hash function is preimage resistant and collision resistant, then, if the request message was modified, the verification by the stored ECDSA key ver_{V_i} of the signature would be incorrect.

Claim 3. *The creation of a fraudulent pseudonym is computationally unfeasible nowadays.*

Proof. If an unathorized entity wants to create a pseudonym π_{V_i}, he/she needs the ECDSA private key sig_{TA} of TA. Supposing that ECDSA is secure nowadays, only trusted TA with its private ECDSA key sig_{TA} can sign π_{V_i}. Moreover, if a fraudulent π_{V_i} was sent to V_i having TA's public ECDSA key ver_{TA} then the signature of π_{V_i} would be invalid.

Proposition 2. *In the join phase between members (V_i) and honest Group Managers GM_i the proposed scheme preserves message confidentiality, integrity, authenticity and member's privacy.*

Claim 4. *The request and response messages are confidential.*

Proof. Every V_i who wants to join a group maintained by GM_i, must send the ciphertext (pk_{V_i} and π_{V_i}) encrypted using the certified ElGamal public key pk_{GM_i} to GM_i. GM_i decrypts and checks if π_{V_i} is valid and sends gsk_{V_i} encrypted using pk_{V_i}. Only V_i knows the corresponding ElGamal private key and can decrypt the message with gsk_{V_i}. Assuming that GM_i is honest, the members joining keeps the message confidentiality, integrity and authenticity due to the ElGamal properties.

Claim 5. *The pseudonym π_{V_i} is anonymous.*

Proof. Assuming that ElGamal encryption/decryption is probabilistic, an observer is unable to link two or more request/response messages because ciphertexts are different although π_{V_i} is used several times. The pseudonym π_{V_i} created by TA does not contain the plaintext of the user identity (ID) but it contains the encrypted fragment $enc_{pk_{TA}}(ID)$. GM_i and other entities without the private ElGamal key sk_{TA} are not able to open the member's ID. Hence, the privacy protection of members is ensured in the join phase.

Proposition 3. *In the V2V communication between V_i, the proposed scheme ensures message integrity, authenticity, member's privacy and revocation.*

Claim 6. *Group signatures of messages keep integrity, authenticity and non-repudiation.*

Proof. The signing and verification phases employ the group signature with the short-term linkability to ensure the message authenticity and integrity, the driver anonymity in long-term way and non-repudiation. Our scheme modifies the WLZ scheme [17] based on the BBS04 scheme [8] and inherits all its security features including the correctness. Besides honest GM_i, only a valid group member V_i can sign a message on behalf the group. If an attacker without valid $gsk_{V_i} = (A_i, x_i)$ tries to modify the message, he/she must recompute hash c

and some signature parts. Assuming that hash function is secure and the Discrete Logarithm problem holds then the computation of the proof of knowledge $(s_{j\alpha}, s_{j\beta}, s_{jx}, s_{j\delta}, s_{j\mu})$ without x_i is unfeasible nowadays. If the proof of knowledge $(s_{j\alpha}, s_{j\beta}, s_{jx}, s_{j\delta}, s_{j\mu})$ is incorrectly computed then the equations 6, 7 and 8, 6 would be not equal. The complete formal analysis can be in [8].

Claim 7. *The drivers are anonymous, untraceable by the all entities besides honest TA and their anonymities is revocable by the collaboration GM and TA.*

Proof. The group signatures contain the group members' pseudonyms T_1, T_2, T_3 which are a linear encryption of members' secret key A_i and random α and β. The short-term linkability of messages does not violate the drivers' privacy. When the counter k is set to 0 and V_i generates a new α an β then, the new signatures start to be unlinkable with old ones because contain new pseudonyms T_1, T_2, T_3. Supposing the Strong Diffie-Hellman assumption holds, every correct message of a malicious member can be opened only by GM with $gmsk = (r_1, r_2)$, and $gsk_{V_i} = (A_i, x_i)$ can be extracted. Malicious members can be revoked by the collaboration of TA and GM.

Proposition 4. *The proposed signature scheme protects against DoS attacks, Sybil attacks and replay attacks.*

Claim 8. *The categorized verification protects against DoS and Sybil attacks.*

Proof. If a malicious driver Eve (E) starts the Sybil attack which is a special kind of the DoS attack then she broadcasts bogus messages that contain fake pseudonyms and signatures. Meanwhile, the honest drivers (C, D, F,...) send messages that contain valid pseudonyms and signatures announcing an accident (sent by D) or a traffic jam (sent by C). If existing solutions are used, E can flood the uncategorized batch verification process and paralyze drivers who must discard some messages. Our proposal implements categorized batch verification. Driver Bob (B) has a Temporary List (TL) of honest drivers. We suppose that Bob's TL keeps the list of known and honest drivers like D, F,... using the property of short-term linkability which keeps the pseudonym T_3 unchanged for a short time. If B receives all messages, he checks the TL and collects the messages containing known T_3 to the first batch and verifies them. Therefore, the warning message referencing the accident from driver D is verified in time. The messages with unknown pseudonyms like C are collected to the second batch. The potentially untrusted messages from E with validity W=0 are verified in the third batch only if Bob's OBU has free time and computational capacity for this. If Eve tries to replay recent a valid pseudonyms together with false signatures then the recomputed hash c'_j is not equal to received hash c_j due to time stamps in messages. For this reason, Eve is not able to mount a successful DoS attack against the batch verification of signatures.

Claim 9. *The proposed signature scheme protects against replay attacks.*

Proof. Every message M contains besides position speed etc. also a time stamp with actual time and date. Before verification, every received message is checked

if the time stamp is actual and valid. If an attacker without valid $gsk_{V_i} = (A_i, x_i)$ wants replies an old message with valid signature of a user, he/she must modify the time stamp to valid and actual one, then, recomputes hash c_j, and recomputes all parts $s_{j\alpha}, s_{j\beta}, s_{jx}, s_{j\delta}, s_{j\mu}$ of the signature. Anyway, recomputing valid $s_{jx}, s_{j\delta}, s_{j\mu}$ without x_i is unfeasible under the Discrete Logarithm problem.

6 Conclusions

In this paper, we have presented our anonymous solution using short-term linkable group signature with categorized batch verification. Our proposed solution deals with anonymous and secure signing/verification of messages in the V2V communication which is more efficient than related works. Further, the solution provides practical and secure registration, join and revocation of members in VANETs. The short-term linkability significantly improves the signing phase and is demanded in several VANET applications. Our categorized batch verification provides less errors in the important first batch of potentially honest messages. Moreover, the categorized batch verification protects against Sybil and DoS attacks. Our future plans are aimed at the investigation of categorized batch verification and short-term linkability in dense traffic. The variable values, e.g., the size of counter k affecting short-term linkability, will be determined for various traffic scenarios.

Acknowledgments. This work was partially supported by the Technology Agency of the Czech Republic project TA02011260; the Ministry of Industry and Trade of the Czech Republic project FR-TI4/647; the Spanish Ministry of Science and Innovation (through projects eAEGIS TSI2007-65406-C03-01, CO-PRIVACY TIN2011-27076-C03-01, ICTW TIN2012-32757, ARES-CONSOLIDER INGENIO 2010 CSD2007-00004 and Audit Transparency Voting Process IPT-430000-2010-31), by the Spanish Ministry of Industry, Commerce and Tourism (through projects eVerification2 TSI-020100-2011-39 and SeCloud TSI-020302-2010-153) and by the Government of Catalonia (under grant 2009 SGR 1135).

References

1. Sun, J., Fang, Y., Zhu, X.: Privacy and emergency response in e-healthcare leveraging wireless body sensor networks. Wireless Com. 17(1), 66–73 (2010)
2. Hussain, R., Kim, S., Oh, H.: Towards Privacy Aware Pseudonymless Strategy for Avoiding Profile Generation in VANET. In: Youm, H.Y., Yung, M. (eds.) WISA 2009. LNCS, vol. 5932, pp. 268–280. Springer, Heidelberg (2009)
3. Ferrara, A.L., Green, M., Hohenberger, S., Pedersen, M.Ø.: Practical Short Signature Batch Verification. In: Fischlin, M. (ed.) CT-RSA 2009. LNCS, vol. 5473, pp. 309–324. Springer, Heidelberg (2009)
4. Gerlach, M., Festag, A., Leinmuller, T., Goldacker, G., Harsch, C.: Security architecture for vehicular communication. In: The 5th International Workshop on Intelligent Transportation (March 2007)

5. Fonseca, E., Festag, A., Baldessari, R., Aguiar, R.: Support of anonymity in VANETs - putting pseudonymity into practice. In: Proceedings of IEEE Wireless Communications and Networking Conference (WCNC), Hong Kong (March 2007)
6. Raya, M., Hubaux, J.P.: Securing vehicular ad hoc networks. J. Comput. Secur. 15, 39–68 (2007)
7. Lin, X., Sun, X., Han Ho, P., Shen, X.: GSIS: A secure and privacy preserving protocol for vehicular communications. IEEE Transactions on Vehicular Technology 56, 3442–3456 (2007)
8. Boneh, D., Boyen, X., Shacham, H.: Short Group Signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004)
9. Zhang, C., Lu, R., Lin, X., Ho, P.H., Shen, X.: An efficient identity-based batch verification scheme for vehicular sensor networks. In: INFOCOM, pp. 246–250. IEEE (2008)
10. Chim, T.W., Yiu, S.M., Hui, L.C.K., Li, V.O.K.: SPECS: Secure and privacy enhancing communications schemes for VANETs. Ad Hoc Networks 9(2), 189–203 (2011)
11. 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)
12. Wasef, A., Shen, X.S.: Efficient group signature scheme supporting batch verification for securing vehicular networks. In: IEEE International Conference on Communications, ICC (2010)
13. Qin, B., Wu, Q., Domingo-Ferrer, J., Zhang, L.: Preserving Security and Privacy in Large-Scale VANETs. In: Qing, S., Susilo, W., Wang, G., Liu, D. (eds.) ICICS 2011. LNCS, vol. 7043, pp. 121–135. Springer, Heidelberg (2011)
14. Calandriello, G., Papadimitratos, P., Hubaux, J.-P., Lioy, A.: Efficient and robust pseudonymous authentication in VANET. In: Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks, VANET 2007, pp. 19–28. ACM, New York (2007)
15. Studer, A., Shi, E., Bai, F., Perrig, A.: Tacking together efficient authentication, revocation, and privacy in VANETs. In: SECON, pp. 1–9. IEEE (2009)
16. Chen, L., Ng, S.L., Wang, G.: Threshold anonymous announcement in VANETs. IEEE Journal on Selected Areas in Communications 29(3), 605–615 (2011)
17. Wei, L., Liu, J., Zhu, T.: On a group signature scheme supporting batch verification for vehicular networks. In: International Conference on Multimedia Information Networking and Security, pp. 436–440. IEEE C. S., Los Alamitos (2011)
18. Malina, L., Hajny, J.: Accelerated modular arithmetic for low-performance devices. In: The 34th International Conference on Telecommunications and Signal Processing (TSP), pp. 131–135 (August 2011)
19. Tsiounis, Y., Yung, M.: On the Security of ElGamal Based Encryption. In: Imai, H., Zheng, Y. (eds.) PKC 1998. LNCS, vol. 1431, pp. 117–134. Springer, Heidelberg (1998)