Group Signatures for Secure and Privacy Preserving Vehicular Ad Hoc Networks

Lukas Malina
Department of
Telecommunications
Brno University of Technology
Brno, Czech Republic
malina@feec.vutbr.cz

Jan Hajný
Department of
Telecommunications
Brno University of Technology
Brno, Czech Republic
hajny@feec.vutbr.cz

Vaclav Zeman
Department of
Telecommunications
Brno University of Technology
Brno, Czech Republic
zeman@feec.vutbr.cz

ABSTRACT

The security of Vehicular Ad Hoc Networks (VANETs) plays a key role in protecting against bogus and malicious messages, misusing at roads, eavesdropping etc. Nowadays, common cryptographic solutions guarantee message integrity, authentication, non-repudiation and privacy which is required as a serious requirement in VANETs due to the possibility of tracking of drivers by malicious observers. The related and prior works ensure security and privacy. Nevertheless, the efficiency of these schemes is usually low or there is the possibility of denial of services attacks. The main goal of our paper is to provide initial design of a scheme which ensures privacy, security and efficiency. The proposed scheme can also protect against several Denial of Services Attacks. We compare our proposed solution with related solutions and outline the evaluation of our scheme.

Categories and Subject Descriptors

C.2 [**Computer-Communication Networks**]: General - Security and Protection

General Terms

Security

Keywords

Cryptography, Group Signatures, Anonymity, Vehicular Ad Hoc Networks

1. INTRODUCTION

The current security proposals are challenged to connect privacy, security, efficiency and capable management in huge vehicular networks. VANETs can serve in dense urban traffic where hundreds of vehicles communicate in the Inter-vehicle communication (V2V) or the Vehicle to Infrastructure communication (V2I) so the security overhead and computation time must be minimal. Group signatures (GS), pioneered by Chaum and van Heyst [2], provide user anonymity by signing a message on behalf of a group. GS look like a proper solution to preserve efficiency, privacy and security in V2V due to one collective public key, contrary to conventional digital signatures. Newer GS, like the BBS04 scheme [1], use short fixed signature size.

Nevertheless, the algorithms of GS are computationally more demanding than traditional digital signatures. The open problem is how a lot of anonymous messages can be verified in real time. The related and prior 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 in the batch is $\geq 15\%$ from all messages as is claimed in [4], especially if some denial of service attacks appear. Therefore, we propose a novel solution with group signatures employing categorized batch verification and short-term linkability which can recognize the malicious messages and excludes them from the batch. Moreover, the short-term linkability significantly improves the signing phase so our solution provides more efficient signing and verification than related schemes which use GS.

1.1 Related Work

Our work is focused on cryptography-based anonymity employing group signatures. Group signatures (GS) provide security, user anonymity and the traceability of misbehaving users. The scheme called GSIS [5] uses the combination of a group signature based on the BBS04 scheme [1] 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 $|\mathrm{RL}| < T_\tau$, the scheme uses revocation verification algorithm, otherwise, the scheme updates public/private group keys of all non-revoked members. To make verification more efficient, the work [10] proposes GS with batch verification in V2I which takes three pairing operations. This scheme called IBV has several drawbacks such as using tamper proof devices, tracing or impersonation attacks, see [3] for a complete description. The works [11] and [8] can efficiently verify a large number of messages in V2V. These schemes use short GS with fast batch verification (only two pairing operations are used instead of 5 n, where n is the number of messages). Nevertheless, the performance of batch verification degrades in dense V2V

Q2SWinet'12, October 24–25, 2012, Paphos, Cyprus.

communication with bogus messages. The On Board Units (OBUs) must process the messages quickly since they have between 100 ms and 300 ms to process a message. The work [6] employs identity based group signature with the batch verification and provides a scalable management of large VANETs. This scheme proposes efficient management and revocation of members but suffers from more expensive signing and verification phases than common GS.

1.2 Our Contribution

We focus on the efficiency of signing/verification, security and privacy protection with respect to computationally limited OBUs and RSUs. In the V2V communication, our solution provides the categorized batch verification and efficient signing with short-term linkability. Our proposal uses the modified group signatures of Wei et al. (WLZ scheme) [9]. Additionally, our solution adds the short-term linkability which assures a more efficient signing phase than in the WLZ scheme and allows the efficient categorized batch verification. Generally in group signatures, 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 $O(\ln\ n)$. The authors of paper [4] claim that if $\geq 15\%$ of the signatures are invalid, then batch verification is not more efficient than individual verification. Our proposal uses the modified scheme of the WLZ scheme 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 or Denial of Service (DoS) attacks. Applying the categorized batch verification 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 the V2I communication, our scheme uses probabilistic cryptography for providing long-term unlinkability and privacy protection of drivers. The join and registration phase take only two messages (request/response) and the scheme does not need tamper-proof devices. We avoid the inefficient linear grow of the revocation list with secret keys of members. Our proposal uses the revocation process based on the expiration of time stamp in certified pseudonym. Vehicles have no computational overhead from dealing with a Revocation List RL.

2. SCHEME DESCRIPTION

This section is divided into four parts: the proposed system model, requirements, the cryptographic background and the description of our scheme.

2.1 The Proposed System Model

Our scheme, depicted in Fig.1, 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.

- **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 securely connected with RSUs. GM can trace and open malicious messages in its area but cannot reveal the member ID.

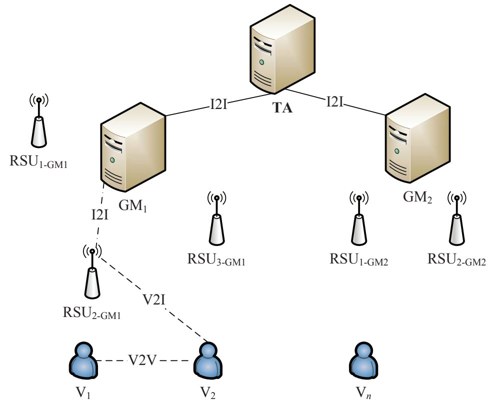

Figure 1: The Parties in Our Model.

- **V** is a driver with the certified pseudonym which is embedded in vehicle's OBU. After the registration of driver in TA and joining in GM's area through V2I communication, V can sign, send or broadcast messages through the V2V communication. Further, V can report a bogus message to GM.

2.2 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, his/her 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 rules, his/her messages can be opened by GM and his pseudonym is sent to TA which can extract member's ID.

- **Non-repudiation, message integrity and authenticity**. In V2V communication, the group signature ensures that messages are signed by V which holds the right and fresh group key pair (authenticity). The system provides the verification of the received messages, i.e., the messages cannot modified once they have been sent (integrity). V stays private but can not deny that he/she 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, short-term linkability is a desirable property [7]. In a short period, i.e., every $100\div300$ 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 sent in a short interval.

2.3 Used Cryptography

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 group signatures of WLZ scheme [9] based on the BBS04 scheme [1] is used in V2V communication. This scheme uses bilinear maps and is based on q-SDH problem and Decision Linear problem which have been studied in [1]. The detailed description of used cryptography is out of the scope of this short paper.

2.4 The Description of Our Solution

Our solution consists of these phases: Setup, Registration, Join, Signing, Verification, Trace, Revocation. The phases are outlined below and the complete description will be published in the full paper.

- **Setup**. $\mathbf{Set}(0,1)^l \rightarrow parameters$

  The parties establish cryptographic $parameters$ like the ElGamal private/public keys and ECDSA key pairs of TA and GMs, where l-bit security is chosen. TA chooses and generates the public parameters of group signatures and GMs set their group manager secret keys and group public keys.

- **Registration**. $\mathbf{Reg}(ID_{Vi}) \rightarrow \pi_{Vi}$

  Assuming that the i-th driver V_i has valid pk_{TA}, ver_{TA}, the two-message registration phase consists of the encrypted request from V_i and response with a 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 public key to TA which stores (ID_{V_i}, ver_{V_i}) to database and the signed certificate $cer_{V_i} = sig_{TA}(ID_{V_i}, ver_{V_i})$ gives to V_i. After the first successful registration phase, the driver can request his/her next pseudonym online. In that case, TA decrypts the request and checks if ID_{V_i} is not revoked in the Global Revocation List (GRL), checks the certificate cer_{V_i} and checks member's signature which ensures member's authenticity and commits pk_{V_i} in the certificate with new ElGamal pair keys. The certified pseudonym π_{V_i} also contains a time stamp T_l that can reduce the length of a Group Temporary Revocation List (GTRL) with revoked pseudonyms.

- **Join**. $\mathbf{Join}(\pi_{Vi}) \rightarrow gsk_{Vi}$

  V_i, entering the i-th GM_i area (several RSUs) for the first time, requests a 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. The two-message join phase consists of the encrypted request with π_{V_i} and the response with a member secret key gsk_{V_i}. GM_i verifies π_{V_i} signed by TA, and checks the validity of the time stamp and if π_{V_i} is not in GTRL. Then, GM_i computes gsk_{V_i} using his/her group manager secret key, sends it and records π_{V_i}, gsk_{V_i} to his/her database.

- **Signing**. $\mathbf{Sig}(M, gsk_{V_i}, gpk) \rightarrow \sigma$

  The signing phase applies the modified short group signature WLZ scheme [9] which is based on the BBS04 scheme [1]. We include a counter k, the member secret key gsk_{V_i}, the group public key gpk and a plain message $M \in (0,1)^*$. OBU signs M and outputs a group signature σ containing 12 elements which consist of the proofs of knowledge (8 elements), group pseudonyms T_s (3 elements) and a hash value as self-challenge (1 element). The pseudonyms are equal for x messages until k is reset to 0.

- **Verification**. $\mathbf{Ver}(M, gpk, \sigma) \rightarrow$ valid/invalid

  Our solution uses the categorized verification which sorts 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. After receiving a message with the group signature containing group pseudonyms T_s, V_i checks if T_s are in TL. If yes, recorded T_s with the previous validity (W=1) are sorted to the first batch. If no, the signatures with unknown T_s are sorted to the second batch which is verified after the first batch verification. The rest of signed messages with T_s 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. For a batch to be valid, all n messages in the batch must be valid. All T_s 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 are added to TL with W=0.

- **Trace**. $\mathbf{Trace}(M, \sigma, gmsk) \rightarrow gsk_{V_i}, \pi_{Vi}$

  Every bogus signed message can be opened by GM_i using the group manager secret key $gmsk$. GM_i extracts the part of the member secret group key gsk_{V_i} and finds the record in database. The part of the member pseudonym can be sent to TA for revocation

- **Revocation**. $\mathbf{Rev}(\pi_{Vi}) \rightarrow ID_{V_i}$

  If a malicious member causes e.g. an accident or breaks the rules by cheating in VANETs, he/she is revoked globally by the cooperation of GM_i and TA. GM_i is able to open a message and extract a pseudonym that is sent to TA. Then, TA broadcasts a notification rev with the revoked pseudonym to other active GMs which check the signature of TA and store rev to own GTRLs until the lifetime of this pseudonym T_l expires. 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.

3. THE EVALUATION OF OUR SOLUTION

In this section, the comparison of our solution with the related work and the evaluation of categorized batch verification are outlined.

3.1 The Comparison with Related Work

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. In performance evaluation, we omit the fast operations like addition, subtraction or hash. Our proposal significantly improves the performance

Table 1: The Comparison of Our Solution with the Related Solutions

V2V scheme:	Our scheme	WLZ [9]	GSIS [5] & Zhang et al. [11] & Ferrara et al. [4]
Short-term linkability:	**yes**	no	no
Performance of signing for the messages excluding the first sent message			
Pairings	**0**	3	3
Exponentiation	**9**	10	12
Multiplication	**9**	14	12

of the signing of x messages with short-term linkability and costs the lowest number of operations in comparison to the related schemes, see Table 1. Pairing operations are reduced $3 \Rightarrow 0$, exponentiations $10 \Rightarrow 9$ and multiplication $14 \Rightarrow 9$. Our proposal based on the group signature scheme of Wei et al. (WLZ) [9] reaches the efficient batch verification in ($2\ T_p + 11n\ T_e$) operations and individual verification in ($5\ T_p + 10\ T_e$) operations.

3.2 The Evaluation of Categorized Batch Verification

A malicious driver Eve (E) starts the Sybil attack which is a special kind of the Denial of Service (DoS) attack. She broadcasts bogus messages that contain fake pseudonyms and signatures. Meanwhile, the honest drivers send messages that contain valid pseudonyms and signatures announcing an accident, traffic jam etc. 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 to fix this. Driver Bob (B) has a Temporary List (TL) of honest drivers. Bob's TL keeps the list of known and honest drivers using the short-term linkability which keeps the pseudonyms T_s unchanged for a short time. If B receives all messages, he checks the TL and collects the messages containing known T_s to the first batch and verifies them. Therefore, the warning messages referencing the accident by known drivers are verified in time. The incoming messages with unknown pseudonyms are collected to the second batch. The untrusted messages from E are verified in the third batch only if Bob's OBU has free time and computational capacity for this. Due to this feature, the categorized verification protects against DoS attacks and Sybil attacks.

4. CONCLUSION

The short paper introduced our novel scheme for secure and anonymous Inter-vehicle communication using short-term linkable group signature with categorized batch verification. Unlike related work, our proposed solution uses categorized batch verification that can sort out potentially honest and bogus messages. Using this feature, our verification phase causes less errors in the important first batch which verifies the potentially honest messages. Therefore, our solution protects against the Sybil and Denial of Services attacks. Moreover, the short-term linkability significantly improves the performance of the signing phase which is more efficient than signing in related solutions that also use group signatures. Having these prerequisites for the efficient, secure and privacy preserving scheme in VANET, our future work is aimed at the investigation of categorized batch verification and short-term linkability in dense urban traffic, especially, at the determination of the parameters, e.g., the size of counter k affecting the short-term linkability.

5. ACKNOWLEDGMENTS

Research was sponsored by the Technology Agency of the Czech Republic project TA02011260 and the Ministry of Industry and Trade of the Czech Republic project FR-TI4/647. Jan Hajny was supported by the Fulbright Commission and Brno Municipality - Ph.D. Talent grant.

6. REFERENCES

[1] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *Proc. Adv. Cryptology-Crypto 04, ser. LNCS 3152*, pages 41–55. Springer-Verlag, 2004.

[2] D. Chaum and E. Van Heyst. Group signatures. In *Proceedings of the 10th annual international conference on Theory and application of cryptographic techniques*, EUROCRYPT'91, pages 257–265, Berlin, 1991. Springer-Verlag.

[3] T. W. Chim, S.-M. Yiu, L. C. K. Hui, and V. O. K. Li. Specs: Secure and privacy enhancing communications schemes for vanets. *Ad Hoc Networks*, 9(2):189–203, 2011.

[4] A. L. Ferrara, M. Green, S. Hohenberger, and M. Ø. Pedersen. Practical short signature batch verification. In *Topics in Cryptology - The Cryptographers' Track at the RSA Conference*, volume 5473, pages 309–324. Springer, April 2009.

[5] X. Lin, X. Sun, P. han Ho, and X. Shen. Gsis: A secure and privacy preserving protocol for vehicular communications. In *IEEE Transactions on Vehicular Technology*, volume 56, pages 3442–3456, 2007.

[6] B. Qin, Q. Wu, J. Domingo-Ferrer, and L. Zhang. Preserving security and privacy in large-scale vanets. In *Proceedings of the 13th international conference on Information and communications security*, ICICS'11, pages 121–135, Berlin, 2011. Springer-Verlag.

[7] A. Studer, E. Shi, F. Bai, and A. Perrig. Tacking together efficient authentication, revocation, and privacy in vanets. In *SECON*, pages 1–9. IEEE, 2009.

[8] A. Wasef and X. S. Shen. Efficient group signature scheme supporting batch verification for securing vehicular networks. In *IEEE International Conference on Communications (ICC)*, 2010.

[9] L. Wei, J. Liu, and T. Zhu. On a group signature scheme supporting batch verification for vehicular networks. In *International Conference on Multimedia Information Networking and Security*, pages 436–440, Los Alamitos, CA, USA, 2011. IEEE.

[10] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen. An efficient identity-based batch verification scheme for vehicular sensor networks. In *INFOCOM*, pages 246–250. IEEE, 2008.

[11] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer. A scalable robust authentication protocol for secure vehicular communications. In *IEEE Transactions on Vehicular Technology 59(4)*, pages 1606–1617, 2010.