A Privacy-aware Reputation-based Announcement Scheme for VANETs

Liqun Chen*, Qin Li†, Keith M. Martin‡, and Siaw-Lynn Ng‡
*Hewlett Packard Labs, Bristol, BS34 8QZ, UK
Email: liqun.chen@hp.com
†School of Computer Engineering, Nanyang Technological University, Singapore, 639798
Email: qin.li@ntu.edu.sg
‡Information Security Group, Royal Holloway, University of London, Egham, TW20 0EX, UK
Email: {keith.martin, s.ng}@rhul.ac.uk

***Abstract*—An announcement scheme is a system that facilitates vehicles to broadcast road-related information in vehicular ad hoc networks (VANETs) in order to improve road safety and efficiency. In this paper, we propose a privacy-aware reputation-based announcement scheme that provides message reliability evaluation, auditability, and robustness.**

I. Introduction

We call a system that facilitates vehicles to exchange messages about vehicle, road, and traffic conditions in a vehicular ad hoc network (VANET) an *announcement scheme*. If messages exchanged are *reliable* (reflecting reality) then the driving environment may become safer and more efficient. Unreliable messages, possibly due to hardware malfunction or driver malicious intention, may result in various consequences from journey delay to accident. Hence, an announcement should have the following functionalities: 1) *message reliability evaluation* – vehicles should be able to evaluate the reliability of messages received, and 2) *auditability* – vehicles that broadcast unreliable messages should be identified and revoked. In addition, an announcement scheme should satisfy the following security requirements: 3) *robustness* – its performance should not be affected by attacks from adversaries, and 4) *privacy awareness* – the privacy of vehicles should be protected, since messages may contain data private to vehicle users. Vehicle privacy has two facets:

- *Anonymity*. The identity of a vehicle should not be revealed from messages broadcast by the vehicle.
- *Unlinkability*. Multiple messages broadcast by the same vehicle should not be linked to each other.

Li et al. [13] proposed a reputation-based announcement scheme that aims to provide message reliability evaluation, auditability, and robustness. This scheme relies on a centralised reputation system with an off-line trusted authority. In this scheme the reliability of a message is evaluated according to the *reputation* of the vehicle that generates this message. The message is considered reliable if the vehicle has a sufficiently high reputation. The reputation reflects the extent to which the vehicle has announced reliable messages in the past. It is computed and updated based on *feedback* reported by other vehicles. The reputation scores of all vehicles are managed by a trusted central authority. A vehicle periodically retrieves its *reputation certificate*, which contains its reputation score, from the central authority. When a vehicle broadcasts a message it attaches its reputation certificate to the message, which allows a receiving vehicle to infer the reliability of the message. The central authority revokes a vehicle whose reputation score decreases beyond a threshold by no longer providing a new reputation certificate.

This approach features the important performance advantage of *immediate evaluation*: upon receiving a message a receiving vehicle is able to immediately evaluate its reliability. This enables the receiving vehicle to respond quickly. In a scheme that does not support immediate evaluation, such as [6,7,12,15,18], a receiving vehicle has to wait until sufficient information is received from other vehicles before the message reliability can be evaluated accurately. However, the scheme in [13] overlooks privacy: messages and feedback are linkable and not anonymous. This drawback may affect vehicles' willingness to participate.

The contribution of this paper is two-fold: 1) we generalise the scheme in [13] and propose an abstraction that we will refer to as the *basic scheme*, and 2) we provide vehicle privacy for the basic scheme.

The rest of this paper is organised as follows. We discuss related work in Section II. In Section III we describe the basic scheme. We then elaborate and analyse our privacy-aware scheme in Section IV. In Section V, we discuss other properties of our privacy-aware schemes and some related issues. We conclude in Section VI.

II. Related Work

There have been a number of announcement schemes proposed to evaluate the reliability of messages in VANETs. These can be categorised into two main groups: the *threshold method* and the *reputation-based method*.

A majority of announcement schemes, e.g. [6,7,12,15,18], use the threshold method: a message is believed reliable if it has been announced by multiple distinct vehicles whose number exceeds a threshold within a time interval. This method

This paper is partially supported by the Natural Science Foundation of China, Project 61063003.

is only suitable for messages that can be broadcast by multiple vehicles. It is not suitable for messages that may be broadcast by only one vehicle, such as *beacons*, which contain the current position, speed, and direction of the broadcasting vehicle [10]. In addition, this method also gives rise to the problem of *distinguishability of message origin* [9] - how to tell if two messages are made by two distinct vehicles if vehicles are anonymous and their activities are unlinkable. Solutions include using a message-linked group signature [18] and one-time anonymous authentication [17].

In addition to [13] there have been several announcement schemes based on reputation systems, such as [8,14,16]. These schemes adopt a decentralised infrastructure. In [8], the reliability of a message is gauged by verifying opinions appended to the message by other vehicles, which may be a heavy computational burden. In [14], reliability is either role-based (certain types of vehicles such as traffic patrol are more trustworthy), majority-based (similar to the threshold method), or experience-based (trust is established from past interactions). The scheme of [16] uses current observations and past behaviour to determine trustworthiness. Both [16] and the experienced-based scheme may be problematic in a large VANET environment where vehicles generally do not have long-term relationships. Storing all this information may also be a problem. In all these schemes, neither robustness against collusion of adversaries nor privacy are provided. It is also not clear how rogue vehicles are revoked.

Compared with existing threshold and reputation-based schemes, the scheme [13] features: 1) immediate evaluation of reliability of messages (including beacons), 2) revocation of malicious vehicles, 3) robustness against both external and internal adversaries, and 4) a good level of efficiency. However, the scheme in [13] does not provide privacy protection for vehicles.

This paper provides a generalisation of the scheme in [13], based on which we propose a privacy-aware announcement scheme that additionally provides a good level of privacy protection for vehicles.

III. The Basic Scheme

In this section, we describe an abstraction of the scheme in [13] (see Figure 1). This has a centralised architecture with off-line central authorities. We assume that *vehicles* are mobile entities equipped with short-range wireless communication devices. They: 1) generate and broadcast messages, 2) receive messages and evaluate their reliability, and 3) report feedback. There are two logical off-line central authorities: a *reputation server* (RS), and an *administrative server* (AS). The RS computes *reputation* for vehicles based on *feedback* reported by vehicles. The AS: 1) enrols new vehicles and revokes malicious vehicles, 2) provides vehicles with reputation endorsement, and 3) collects feedback from vehicles. We assume that the AS has multiple remote wireless communication interfaces to intermittently communicate with vehicles in a convenient and frequent manner (for example once a day). Note that we do not require constant communication between a vehicle and the AS. We assume that the RS and AS are trusted, and communication between the RS and AS is secure (authenticated, confidential, and integrity protected). We assume that each of the vehicles and the AS has a clock, and the clock of a vehicle is loosely synchronised with that of the AS. We also assume that the communication between the AS and a vehicle, and those between vehicles, are public and thus subject to attacks.

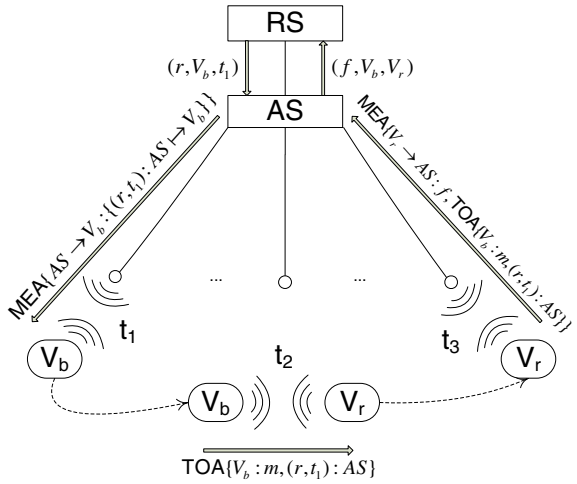

Fig. 1. The basic scheme.

A. Protocols and Algorithms Required

This basic scheme requires:

- A secure mutual authentication protocol MEA, which provides both communicating parties with assurance of: 1) each other's identity, and 2) freshness of communication. We denote by $\mathsf{MEA}\{A \to B : m\}$ the message m sent from A to B after the assurances of MEA have been established. Vehicles will use MEA as part of reputation retrieval and feedback reporting. MEA can be instantiated by any suitable authentication protocol.
- A secure *two-origin authentication* protocol TOA. If A broadcasts a message (m_1, m_2), TOA provides a receiver with assurance that: 1) m_1 originates from A, 2) m_2 originates from a third party C, and 3) m_2 is associated with A. We denote by $\mathsf{TOA}\{A : m_1, m_2 : C\}$ the message (m_1, m_2) sent by A with the assurances of TOA provided. Vehicles will use TOA to broadcast messages. TOA can easily be implemented using, for example, a digital signature scheme.
- An aggregation algorithm Aggr. The RS will use it to aggregate feedback and produce reputation for vehicles.
- A feedback analysis algorithm Detect. The RS will use it to identify malicious vehicles from feedback.
- A decreasing function TimeDiscount that takes input a time difference and outputs a value in $[0, 1]$, and $\mathsf{TimeDiscount}(0) = 1$.
- A threshold Ψ in $[0, 1]$, to determine whether a reputation score is sufficiently high.

B. Description of the Basic Scheme

The basic scheme consists of the following protocols:

Scheme initialisation. The scheme is initialised as follows: 1) the AS installs MEA and TOA, generates any keys required; 2) the AS regulates its clock, and deploys its remote wireless communication interfaces; and 3) the RS creates a database, and installs Aggr and Detect.

Vehicle registration. The AS registers a new vehicle V as follows: 1) generates keys to be used by V, 2) installs MEA, TOA, TimeDiscount in V and securely sends V with Ψ and the keys, and 3) requests RS to create a record in its database for V.

Reputation retrieval. When a vehicle V_b drives into the proximity of a wireless communication interface at time, say t_1, it retrieves its reputation credential as follows: 1) V_b and the AS execute MEA to establish a mutually authenticated channel; 2) the AS retrieves from RS the reputation r of V_b at time t_1, denoted by (r, V_b, t_1); 3) the AS generates a reputation credential, denoted by $\{(r, t_1) : AS \mapsto V_b\}$; and 4) the AS sends $\{(r, t_1) : AS \mapsto V_b\}$ to V_b in the mutually authenticated channel, denoted by $\mathsf{MEA}\{AS \rightarrow V_b : \{(r, t_1) : AS \mapsto V_b\}\}$.

Message broadcast. At any time, say t_2, V_b broadcasts message m as follows: 1) V_b takes m and $\{(r, t_1) : AS \mapsto V_b\}$ as input to generate $\mathsf{TOA}\{V_b : m, (r, t_1) : AS\}$, and broadcasts it; 2) a receiving vehicle V_r verifies it and extracts m, r, and t_1 upon successful verification; 3) V_r retrieves the current time t_2 from its clock and and computes the time-discounted reputation $r' = r \cdot \mathsf{TimeDiscount}(t_2 - t_1)$; 4) if $r' \geq \Psi$, then V_r considers V_b as reputable and m as reliable; otherwise, V_r considers V_b as disreputable and m as unreliable.

Feedback reporting. When V_r has experience about the event described by message m, it is able to judge the reliability of m. Then V_r can voluntarily report feedback as follows: 1) V_r assigns a feedback f based on its experience about the reliability of m; 2) when V_r drives into the proximity of a wireless communication interface, V_r and the AS execute MEA to establish a mutually authenticated channel; 3) the V_r sends f and $\mathsf{TOA}\{V_b : m, (r, t_1) : AS\}$ to the AS in the mutually authenticated channel, denoted by $\mathsf{MEA}\{V_r \rightarrow AS : f, \mathsf{TOA}\{V_b : m, (r, t_1) : AS\}\}$; 4) the AS verifies $\mathsf{TOA}\{V_b : m, (r, t_1) : AS\}$; 5) upon successful verification, the AS sends (f, V_b, V_r) to the RS, who stores it in the database; 6) the RS uses Aggr and all feedback stored in the database to update the reputation of V_b.

Vehicle revocation. The RS periodically uses Detect on all feedback stored in the database to identify malicious vehicles, and reports to the AS. The AS revokes them by no longer providing them with reputation credentials.

C. Robustness of the Basic Scheme

The robustness of this scheme can be evaluated with respect to the following attacks: 1) *message fraud*: an adversary deceives a vehicle into believing that a false message m' is reliable, and 2) *reputation manipulation*: an adversary unfairly inflates or deflates the reputation of a vehicle.

We categorise adversaries into two groups: 1) *external adversaries* who attack the system without joining as legitimate vehicles, and 2) *internal adversaries* who are legitimate vehicles that attack the system.

In order to perpetrate a message fraud attack, an adversary could: a) impersonate a registered vehicle to retrieve a reputation credential and then broadcast false messages, or b) forge a legitimate broadcast message. In order to conduct reputation manipulation, an adversary could: c) impersonate a registered vehicle to report feedback. An adversary cannot perform a)-c) if MEA and TOA are secure and the AS and vehicles manage their secret keys appropriately.

In addition, an internal adversary can conduct message fraud by broadcasting a false message itself. This however will result in a decrease in its reputation, and excessive message frauds will eventually get itself revoked from the system. An internal adversary can also conduct reputation manipulation by providing false feedback itself, either in isolation or in collusion with other internal adversaries. There are several approaches to prevent this: 1) *proof of spatial proximity*: a receiving vehicle has to prove to the AS its distance from the sending vehicle when receiving the message, allowing only neighbouring vehicles (those indeed receive the message from the sending vehicle) to report feedback; 2) *permanent identity*: vehicle identity is permanent, to prevent identity change; 3) *secret key binding*: the secret keys of a vehicle are known to only the vehicle itself, to prevent colluding internal adversaries from acting on behalf of each other; and 4) *data mining*: the AS can analyse received feedbacks to detect malicious feedback. We do not specify any concrete techniques in this basic scheme in order to make it inclusive of any possible techniques (in [13] some instantiations are provided).

D. Privacy Unawareness of the Basic Scheme

However in this basic scheme neither MEA nor TOA provides anonymity or unlinkability. We now propose a privacy-aware announcement scheme that realises privacy aware MEA and TOA.

IV. Privacy-aware Announcement Scheme

In this section we describe our privacy-aware announcement scheme (See Figure 2). We require:

- A secure *group signature scheme* [1,4,5], denoted by $\mathsf{GS} = (\mathsf{GKeyGen}, \mathsf{GJoin}, \mathsf{GSign}, \mathsf{GVerify}, \mathsf{Open})$ where GKeyGen, GJoin, GSign, GVerify and Open denote group public key generation, group member secret key generation, group member signing, group verification, and signer revealing algorithms, respectively. A group signature scheme has the following properties: 1) each group member can sign messages; 2) a receiver can verify whether the signature was signed by a group member, but cannot discover which group member signed it; 3) any two messages signed by a group member cannot be linked; and 4) a signature can be "opened" by a group manager to reveal the signer of the message.
  We will use GS to realise a privacy-aware TOA, denoted by TOA^+ (we will show how TOA^+ is achieved later).
- A secure *probabilistic encryption scheme* [3,11], denoted by PE. This has the property that encryption of

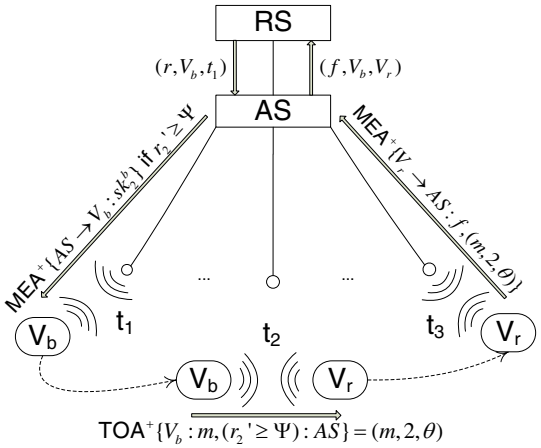

Fig. 2. Our privacy-aware scheme.

the same plaintext using the same encryption key twice yields two different ciphertexts which are statistically indistinguishable. We will use PE to realise a privacy-aware MEA, denoted by MEA^+, by combination of PE and MEA: $\mathsf{MEA}^+\{V \to AS : m\} = \mathsf{PE}\{\mathsf{MEA}\{V \to AS : m\}\}$.

A. Description of the Privacy-aware Scheme

In this section, we specify the changes that our privacy-aware scheme makes to the basic scheme:

Scheme Initialisation. In addition to Steps 2 and 3 of the basic scheme, our privacy-aware scheme requires that: 1) The AS installs GS, MEA^+, TimeDiscount, and Ψ, and generates keys required. 2) The time is divided into intervals $(\mathbb{T}_0, \mathbb{T}_1, \mathbb{T}_2, \cdots)$. For example, each time interval can be one day. For each interval $\mathbb{T}_i$, the AS uses GKeyGen to generate a group public key pk_i and uses GJoin to generate a set of group member secret keys $(sk_i^1, sk_i^2, \cdots, sk_i^n)$ where n is the number of vehicles in the system. A secret key sk_i^j will be used by vehicle V_j during the time interval $\mathbb{T}_i$. Group member secret keys $(sk_0^j, sk_1^j, sk_2^j, \cdots)$ will be used by V_j during the corresponding time intervals $(\mathbb{T}_0, \mathbb{T}_1, \mathbb{T}_2, \cdots)$. The keys sk_i^j for all i and j are kept confidential for future use.

Vehicle Registration. In addition to Step 3 of the basic scheme, our privacy-aware scheme requires the AS to: 1) generate the keys to be used by V for MEA^+; and 2) install MEA^+, GSign, GVerify in V, and securely send V with the keys generated from the previous step and $(pk_0, pk_1, pk_2, \cdots)$.

Reputation Retrieval. When a vehicle V_b drives into the proximity of a wireless communication interface during a time interval $\mathbb{T}_i$, whose beginning time is denoted by t_i, it retrieves its reputation as follows: 1) V_b and the AS execute MEA^+ to establish an encrypted and mutually authenticated channel; 2) upon retrieving (r, V_b, t_i) from the RS, the AS computes $(r_i', r_{i+1}', \cdots, r_{i+m}')$ until $r_{i+m+1}' < \Psi$ where $r_{i+k}' = r \cdot \mathsf{TimeDiscount}(t_{i+k} - t_i)$ (in other words V_b is considered as reputable for the time intervals $\mathbb{T}_i, \cdots, \mathbb{T}_{i+m}$); and 3) the AS sends V_b in the encrypted and mutually authenticated channel $(sk_i^b, \cdots, sk_{i+m}^b)$.

Message Broadcast. V_b broadcasts a message m as follows: 1) V_b identifies the current time interval, say $\mathbb{T}_i$, from its clock; 2) V_b uses GSign and sk_i^b, which corresponds to $\mathbb{T}_i$, to generate a signature θ on (m, i), forms a *message tuple* $M = (m, i, \theta)$, and then broadcasts M; 3) Upon receiving M, a receiving vehicle V_r immediately identifies the current time interval $\mathbb{T}_j$ from its clock. 4) V_r checks if $j = i$. If so then V_r uses GVerify and pk_i, which corresponds to $\mathbb{T}_i$, to verify θ. Upon successful verification, V_r considers V_b to be reputable, and the message m to be reliable. The message tuple M is stored for future possible feedback reporting. If $j \neq i$ or the verification fails then V_r does not consider V_b to be reputable, and discards M.

Feedback reporting. Feedback is reported as follows: 1) V_r and the AS execute MEA^+ to establish an encrypted and mutually authenticated channel, and V_r sends f, M to the AS via the channel; 2) the AS uses Open and pk_i to open M, in order to retrieve signer V_b, and sends the RS the tuple (f, V_b, V_r). The rest remains the same as the basic scheme.

Vehicle Revocation. In our privacy-aware scheme the AS revokes malicious vehicles by no longer providing them with new group member secret keys in the future.

In our scheme a reputation credential of V_b at time interval $\mathbb{T}_i$ is represented by a group member secret key: $\{r_i' : AS \mapsto V_b\} = sk_i^b$ if $r_i' \geq \Psi$. TOA^+ is realised by GS: $\mathsf{TOA}^+\{V_b : m, (r_i' \geq \Psi) : AS\} = (m, i, \theta)$ where $\theta = \mathsf{GSign}_{sk_i^b}(m, i))$. This gives a recipient assurance that m originated from a reputable (but unidentified) vehicle.

B. Privacy Analysis

In this section we analyse *anonymity* and *unlinkability* of our privacy-aware scheme. We focus on three protocols: reputation retrieval, message broadcast, and feedback reporting, since only in these protocols does a vehicle transmit data and thus potentially suffer in a privacy breach.

During reputation retrieval or feedback reporting, since the channel is protected by MEA^+, the anonymity and unlinkability of all data sent by a vehicle is protected against all entities except for the AS. During message broadcast, θ is generated by using a group signature scheme, which protects anonymity and unlinkability against all entities except for the AS.

C. Robustness of Our Privacy-aware Scheme

Observe that our privacy-aware scheme still features the same robustness as the basic scheme against adversaries. First, an adversary is not able to impersonate an existing vehicle (just as in the basic scheme). In addition, an adversary is also not able to forge a legitimate broadcast message. This is because all group member signing keys are transmitted to vehicles via encrypted channels, and external adversaries are thus unable to obtain a valid group member secret key. In addition, all approaches that can be used in the basic scheme to prevent internal adversaries conducting reputation manipulation can also be used in our privacy-aware scheme.

V. Discussion

A. Communication and Computational Overheads

In our proposed scheme, the main communication overhead is the signature θ. If we use the closely scrutinised Boneh-

Boyen-Shacham (BBS) group signature scheme [4], then θ can be 192 bytes (128 bytes if an additional assumption holds) with the security level approximately equivalent to 128-byte RSA signature [4]. The main computational overhead is the generation and verification of θ, in which the most expensive operations are one and two pairing operations, respectively. One pairing operation takes 3.6ms on an Athlon XP 2 GHz using code written in C++ [2], meaning that generating and verifying θ takes approximately 3.6ms and 7.2ms, respectively. With the similar security level, the signatures in [13] take 96 bytes, and signing and verification take 2.1ms and 8.6ms, respectively. Thus, the computational cost is comparable between the two schemes while the communication cost of our scheme is greater.

B. Multiple Reputation Levels

Note that our privacy-aware scheme only supports a binary reputation. It can easily be extended to support multiple reputation levels with minimal modifications: Suppose there are m reputation values $[\Psi_1, \Psi_2, \cdots, \Psi_m]$ where $\Psi_k < \Psi_{k+1}$. During scheme initialisation, the AS will generate m group public keys for each time interval $\mathbb{T}_i$, denoted by $pk_{i,1}, \cdots, pk_{i,m}$. The AS will also generates m sets of group member secret keys $(sk^1_{i,1}, \cdots, sk^n_{i,1}, sk^1_{i,2}, \cdots, sk^n_{i,2}, \cdots sk^1_{i,m}, \cdots, sk^n_{i,m})$ for time interval $\mathbb{T}_i$. During reputation retrieval if a vehicle V_b has a time-discounted reputation $r'_i \geq \Psi_k$ for a time interval $\mathbb{T}_i$, then V_b will be provided with the group member secret keys $(sk^b_{i,k}, sk^b_{i,k+1}, \cdots, sk^b_{i,m})$. During message broadcast, V_b uses a group member secret key $sk^b_{i,k}$ to generate a signature θ on a message m, and form a message tuple $M = (m, i, k, \theta)$. A receiving vehicle learns i, k from M, and uses the group public key $pk_{i,k}$ to verify θ. Upon successful verification, V_r believes that the reputation of V_b is Ψ_k.

C. Secret Key Retrieval via an Un-encrypted Channel

In our scheme sk^j_i has to be transmitted via an encrypted channel, which imposes a constraint. This can be removed if we use the BBS scheme [4]. In this scheme a group public key includes g_1, g_2, two generators of (multiplicative) cyclic groups G_1, G_2 of prime order p, respectively, and $g_1 = \psi(g_2)$ for a computable isomorphism ψ from G_2 to G_1. A group member secret key for member j is (A_j, x_j) where $A_j = g_1^{1/(\gamma + x_j)}$, $\gamma \in \mathbb{Z}_p$ is a secret of the signature authority, and $x_j \in \mathbb{Z}_p$ is only known to j and the signature authority.

By using the BBS scheme, the AS generates a group public key pk_0 and, for each vehicle V_j, a group member secret key $sk^j_0 = (A^j_0, x_j)$ where $A^j_0 = g_1^{1/(\gamma + x_j)}$. The AS also assigns each time interval $\mathbb{T}_i$ a random value $h_i \in G_1 \backslash \{g_1^{-1}\}$. The AS then derives pk_i from pk_0: the g_1 element of pk_i equals $g_1 \cdot h_i$, and other elements remain the same as those of pk_0. Note that there always exists a computable isomorphism ψ_i from G_2 to G_1 such that $g_1 \cdot h_i = \psi_i(g_2)$. The AS also computes a value $h_i^{1/\gamma + x_j}$ for each sk^j_i. During vehicle registration the AS sends sk^b_0 to V_b in an encrypted channel. During reputation retrieval the AS sends $h_i^{1/\gamma + x_b}$ to V_b in plaintext if $r'_i \geq \Psi$. Then V_b computes $A^b_i = A^b_0 \cdot h_i^{1/\gamma + x_b}$, and forms $sk^b_i = (A^b_i, x_b)$.

VI. Conclusion

In this paper we proposed an abstraction of the scheme in [13], and layered on top of it a privacy-aware announcement scheme.

References

[1] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A practical and provably secure coalition-resistant group signature scheme. In *Proceedings of Crypto 2000*, volume 1880 of *LNCS*, pages 255–270. Springer, 2000.

[2] P. Barreto, B. Libert, N. McCullagh, and J.J. Quisquater. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In *Proceedings of ASIACRYPT 2005*, volume 3788 of *LNCS*, pages 515–532. Springer, 2005.

[3] M. Blum and S. Goldwasser. An efficient probabilistic public-key encryption scheme which hides all partial information. In *Proceedings of Crypto 1985*, volume 196 of *LNCS*, pages 289–299. Springer, 1985.

[4] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *Proceedings of Crypto 2004*, volume 3152 of *LNCS*, pages 41–55. Springer, 2004.

[5] D. Chaum and E. van Heyst. Group signatures. In *Proceedings of Eurocrypt 1991*, volume 547 of *LNCS*, pages 257–265. Springer, 1991.

[6] L. Chen, S.L. Ng, and G. Wang. Threshold anonymous announcement in VANETs. *IEEE Journal on Selected Areas in Communications*, 29(3):605–615, 2011.

[7] V. Daza, J. Domingo-Ferrer, F. Sebé, and A. Viejo. Trustworthy privacy-preserving car generated announcements in vehicular ad hoc networks. *IEEE Transaction on Vehicular Technology*, 58(4):1876 – 1886, 2009.

[8] F. Dötzer, L. Fischer, and P. Magiera. VARS: a vehicle ad hoc network reputation system. In *Proceedings of the 6th IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks*, volume 1, pages 454–456, 2005.

[9] J.R. Douceur. The sybil attack. In *Proceedings for the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02)*, pages 251–260, 2002.

[10] A. Festag, P. Papadimitratos, and T. Tielert. Design and performance of secure geocast for vehicular communication. *IEEE Transactions on Vehicular Technology*, 59(5):2456–2471, 2010.

[11] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.

[12] G. Kounga, T. Walter, and S. Lachmund. Proving reliability of anonymous information in VANETs. *IEEE Transactions on Vehicular Technology*, 58(6):2977–2989, 2009.

[13] Q. Li, A. Malip, K.M. Martin, S.L. Ng, and J. Zhang. A reputation-based announcement scheme for VANETs. *IEEE Transactions on Vehicular Technology*, 2012. To appear.

[14] U.F. Minhas, J. Zhang, T. Tran, and R. Cohen. Towards expanded trust management for agents in vehicular ad hoc networks. *International Journal of Computational Intelligence Theory and Practice*, 5(1):3–15, 2010.

[15] M. Raya, A. Aziz, and J. Hubaux. Efficient secure aggregation in VANETs. In *Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks*, pages 67–75. ACM, 2006.

[16] R.K. Schmidt, T. Leinmüller, E. Schoch, A. Held, and G. Schäfer. Vehicle behavior analysis to enhance security in VANETs. In *Proceedings of the 4th Workshop on Vehicle to Vehicle Communications (V2VCOM)*, 2008.

[17] I. Teranishi, J. Furukawa, and K. Sako. k-times anonymous authentication. In *Proceedings of Asiacrypt 2004*, volume 3329 of *LNCS*, pages 308–322. Springer, 2004.

[18] Q. Wu, J. Domingo-Ferrer, and U. González-Nicolás. Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications. *IEEE Transactions on Vehicular Technology*, 59(2):559–573, 2010.