2010

A scalable robust authentication protocol for secure vehicular communications

Lei Zhang
Universitat Rovira I Virgili Tarragona

Qianhong Wu
University of Wollongong

Agusti Solanas
Universitat Rovira I Virgili Tarragona

Josep Domingo-Ferrer
Universitat Rovira I Virgili Tarragona

A scalable robust authentication protocol for secure vehicular communications

Abstract

Existing authentication protocols to secure vehicular ad hoc networks (VANETs) raise challenges such as certificate distribution and revocation, avoidance of computation and communication bottlenecks, and reduction of the strong reliance on tamper-proof devices. This paper efficiently copes with these challenges with a decentralized group-authentication protocol in the sense that the group is maintained by each roadside unit (RSU) rather than by a centralized authority, as in most existing protocols that are employing group signatures. In our proposal, we employ each RSU to maintain and manage an on-the-fly group within its communication range. Vehicles entering the group can anonymously broadcast vehicle-to-vehicle (V2V) messages, which can be instantly verified by the vehicles in the same group (and neighboring groups). Later, if the message is found to be false, a third party can be invoked to disclose the identity of the message originator. Our protocol efficiently exploits the specific features of vehicular mobility, physical road limitations, and properly distributed RSUs. Our design leads to a robust VANET since, if some RSUs occasionally collapse, only the vehicles that are driving in those collapsed areas will be affected. Due to the numerous RSUs sharing the load to maintain the system, performance does not significantly degrade when more vehicles join the VANET; hence, the system is scalable.

Disciplines

Physical Sciences and Mathematics

Publication Details

Zhang, L., Wu, Q., Solanas, A. & Domingo-Ferrer, J. (2010). A scalable robust authentication protocol for secure vehicular communications. IEEE Transactions on Vehicular Technology, 59 (4), 1606-1617.

A Scalable Robust Authentication Protocol for Secure Vehicular Communications

Lei Zhang, Qianhong Wu, Agusti Solanas, *Member, IEEE*, and Josep Domingo-Ferrer, *Senior Member, IEEE*

***Abstract*—Existing authentication protocols to secure vehicular ad hoc networks (VANETs) raise challenges such as certificate distribution and revocation, avoidance of computation and communication bottlenecks, and reduction of the strong reliance on tamper-proof devices. This paper efficiently copes with these challenges with a decentralized group-authentication protocol in the sense that the group is maintained by each roadside unit (RSU) rather than by a centralized authority, as in most existing protocols that are employing group signatures. In our proposal, we employ each RSU to maintain and manage an on-the-fly group within its communication range. Vehicles entering the group can anonymously broadcast vehicle-to-vehicle (V2V) messages, which can be instantly verified by the vehicles in the same group (and neighboring groups). Later, if the message is found to be false, a third party can be invoked to disclose the identity of the message originator. Our protocol efficiently exploits the specific features of vehicular mobility, physical road limitations, and properly distributed RSUs. Our design leads to a robust VANET since, if some RSUs occasionally collapse, only the vehicles that are driving in those collapsed areas will be affected. Due to the numerous RSUs sharing the load to maintain the system, performance does not significantly degrade when more vehicles join the VANET; hence, the system is scalable.**

***Index Terms*—Conditional privacy, information security, protocol design, vehicular ad hoc networks (VANETs).**

I. Introduction

VEHICULAR ad hoc networks (VANETs) are an instance of mobile ad hoc networks that aim to enhance the safety and the efficiency of road traffic. VANETs have a number of distinguishing features and limitations that are related to the very nature of wireless communications and the rapid movement of the vehicles that are involved in those communications. Compared with wired or other wireless networks, VANETs are very dynamic, and their communications are volatile. In such networks, nodes are vehicles that are equipped with communication devices known as on-board units (OBUs), and depending on the applications, OBUs are used to establish communications with other vehicles or roadside units (RSUs) such as traffic lights or traffic signs.

The specific properties of VANETs allow the development of very attractive services such as the so-called *comfort services* that include traffic information, weather information, location of gas stations or restaurants, price information, and interactive communication such as Internet access. Also, it is possible to offer *safety services* such as emergency warnings, lane-changing assistance, intersection coordination, traffic-sign-violation warnings, and road-condition warnings [1]. However, for those new services to make life easier rather than more difficult, they should rely on secure and privacy-preserving protocols that encourage users to participate without fear for their safety or personal privacy.

Consequently, security and privacy are two critical concerns for the designers of VANETs that, if forgotten, might lead to the deployment of vulnerable VANETs. Unless proper measures are taken, a number of attacks could easily be conducted, namely, message content modification, identity theft, false information generation and propagation, etc. The following are examples of some specific attacks.

- If message integrity is not guaranteed, a malicious vehicle could modify the content of a message that is sent by another vehicle to affect the behavior of other vehicles. By doing so, the malicious vehicle could obtain many benefits while keeping its identity unknown. Moreover, the vehicle that originally generated the message would be made responsible for the damage caused.
- If authentication is not provided, a malicious vehicle might impersonate an emergency vehicle to surpass speed limits without being sanctioned.
- A malicious vehicle could report a false emergency situation to obtain better driving conditions (e.g., deserted roads), and if nonrepudiation is not supported, it could not be sanctioned even if discovered.

From the previous examples, it becomes apparent that message authentication, integrity, and nonrepudiation are primary requirements in VANETs. There is a need for mechanisms that provide VANETs with security, i.e., protocols, methods, and procedures that are able to detect whether a message has been

Manuscript received May 21, 2009; revised September 22, 2009. First published December 15, 2009; current version published May 14, 2010. This work was supported in part by the Spanish Government under Project Consolider Ingenio 2010 CSD2007-00004 "ARES" and Project TSI2007-65406-C03-01 "E-AEGIS" and in part by the Chinese National Science Foundation under Project 60970114 and Project 60970116. J. Domingo-Ferrer is also supported in part as an ICREA-Acadèmia researcher by the Institució Catalana de Recerca i Estudis Avançats, Government of Catalonia. The review of this paper was coordinated by Prof. H. Aghvami.

L. Zhang, A. Solanas, and J. Domingo-Ferrer are with the Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, UNESCO Chair in Data Privacy, 43007 Tarragona, Catalonia (e-mail: lei.zhang@urv.cat; agusti.solanas@urv.cat; josep.domingo@urv.cat).

Q. Wu is with the Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, UNESCO Chair in Data Privacy, 43007 Tarragona, Catalonia, with the Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Computer, Wuhan University, Wuhan 430079, China, and also with the University of Wollongong, Wollongong, N.S.W. 2522, Australia (e-mail: qianhong.wu@urv.cat).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2009.2038222

modified by an attacker, determine who is the real sender of a message, and avoid identity theft.

Besides these essential security requirements, privacy is another important issue in VANETs that cannot be forgotten. If the importance of privacy protection measures is underestimated, the privacy of VANET users could be endangered. For example, an eavesdropper could collect messages that are sent by vehicles and track their locations; by doing so, the eavesdropper could infer sensitive users' data such as their residence and their real identities [2]. Note that these privacy problems are similar to the ones of location-based services (cf. [3], [4], and [42] for further details). Nevertheless, privacy in VANETs should be conditional, that is, user-related information such as license plate, current speed, current position, identification number, and the like should be kept private from other users/vehicles in the system while authorized users (e.g., police officers) should have access to it. Usually, the security issues of VANETs are solved by using signature schemes that rely on a public key infrastructure (PKI). Under the PKI solution, each vehicle has a pair of cryptographic keys—a public key and a private key. The private key is kept secret in the vehicle, whereas the public key is bound to a vehicle's identity by means of a certificate, which is issued by a trusted authority (TA). The utilized schemes must be efficient because, according to [5], vehicles should be able to broadcast safety messages every 100–300 ms. Consequently, it is much more critical for authentication to be quick to verify than to generate.

It is easy to see that this simple PKI-based approach does not protect users' privacy since the broadcasting of a message (actually, a message plus the signer's signature on the message plus the signer's certificate) can reveal a vehicle's identity. Therefore, developing a suite of mechanisms to achieve security, high efficiency, and conditional privacy preservation in VANETs is a key research problem that we address in this paper.

A. Related Work

Due to their extraordinary commercial and social potential, VANETs have attracted the attention of industry and academia. In Europe, the CAR 2 CAR Communication Consortium [6] is leading the efforts to create a European industry standard for vehicle-to-vehicle (V2V) communication systems predicated upon wireless local area network components. In the U.S., the Intelligent Transportation Systems Committee, which is sponsored by the IEEE Vehicular Technology Society, has defined the standard for wireless access in vehicular environments (WAVE; see [7]). WAVE is a radio communications system that is intended to provide interoperable wireless networking services for transportation. These services include those recognized for dedicated short-range communications (DSRC) [8] by the U.S. National Intelligent Transportation Systems Architecture [9].

Security and privacy issues in VANETs have recently been studied by many researchers [10]–[12]. Blum and Eskandarian [13] propose a secure communications architecture based on a PKI and a virtual network controlled by cluster heads intended to counter the so-called "intelligent collisions," which are collisions that are intentionally caused by malicious vehicles. This approach produces a remarkable overhead, and the use of cluster heads can create bottlenecks. Gollan and Meinel [14] propose the use of digital signatures along with Global Positioning System technology to securely identify cars, improve the fleet management, and provide new applications for the private and public sectors. Considering the problem from a different point of view, Hubaux *et al.* [15] emphasize the importance of privacy and secure positioning, and propose the use of electronic license plates to identify vehicles. Although they recognize the importance of conditional privacy, they do not provide any specific solution to the problem.

To the best of our knowledge, there are a few articles that consider both security and conditional privacy preservation in VANETs. In this line, a foundational proposal is given by Raya and Hubaux [5]. The authors use anonymous certificates to hide the real identities of users.[1] Although anonymous certificates do not contain any publicly known relationship to the true identities of the key holders, privacy can still be invaded by logging the messages containing a given key and tracking the sender until her identity is discovered (e.g., by associating her with her residence).[2] To avoid this attack, the way in which anonymous certificates are used should be modified so that an observer cannot track the owner of the keys. A natural way to do so, which is proposed in [5], consists of storing a number of anonymous certificates (as well as the corresponding private/public key pairs) in a vehicle so that the vehicle can use different key pairs and avert traceability. However, depending on the key change frequency, which can vary according to the current speed of the vehicle, vehicles will have to store a large number of pairs. Thus, the secure distribution of keys, key management, and storage become very complex; hence, this type of scheme should be avoided for the sake of practicality.

With the aim to overcome the limitation of prestoring a large number of anonymous certificates, Lin *et al.* [16] presented Grey Systems and Intelligent Services (GSIS), which is a conditional privacy-preserving vehicular communications protocol based on group signatures [17], [18] and ID-based signatures [19]. The main advantage of using group signature schemes is that they guarantee the unlinkability of the messages because group members can anonymously sign on behalf of the group. In the GSIS protocol, a single membership manager who issues secret member keys for vehicles is used. Unfortunately, this approach cannot effectively cope with the exclusion of compromised vehicles from the system. The solutions proposed by Lin *et al.* [16] to deal with compromised vehicles seem to be insufficient. The first option is to update the group public key pair for all nonrevoked vehicles. That entails a considerable overhead. The second option, which is called verifier-local revocation (VLR), is similar to the traditional certificate revocation list (CRL) scheme. Since the signature verification time linearly grows with the number of revoked vehicles, the VLR procedure becomes very time-consuming and inefficient when the number of revoked vehicles grows.

Lu *et al.* [20] proposed an alternative way to overcome the limitation of prestoring a large number of anonymous

[1]Note that even when anonymous certificates are used, TAs can trace the real identity of users.

[2]This attack is possible due to the linkability "property" of the messages.

certificates while preserving conditional privacy. They assume that vehicles and RSUs are able to collaborate actively. Each vehicle issues a request for a short-time anonymous certificate from an RSU when the vehicle is passing by the RSU and obtains an anonymous certificate after running a two-round protocol. Since a vehicle should change the anonymous certificate quite often to avert linkability of the messages, it should frequently interact with RSUs. Such a frequent interaction may affect the efficiency of the VANET. This short-lived anonymous certificate (i.e., a pseudonym) needs to be sent and forwarded to verifiers for validating messages from the anonymous originator. It is also worth mentioning the schemes in [21] and [22], which also rely on RSUs. In [21], the method of mix zones is used to enhance the anonymity of vehicles. However, this scheme still relies on preloading a large set of anonymous certificates in each vehicle. In [22], by exploiting a keyed hash message authentication code, a scheme with low communication overhead is proposed for secure vehicle communication. This scheme requires a vehicle to obtain a symmetric key from an RSU using a key agreement protocol. To protect its privacy, the vehicle should use different public keys to communicate with the RSUs. Hence, the vehicle still needs to preload a certain number of anonymous certificates. As to robustness, the schemes in [21] and [22] fully rely on RSUs. If an RSU collapses, then these schemes will no longer work.

Recently, by using ID-based cryptography [19] to avoid complicated certificate management, Zhang *et al.* [23] have designed an efficient conditional privacy-preserving protocol for vehicular communications. Their approach relies on tamper-proof devices that are embedded in the vehicles. The system's master key is stored in those tamper-proof devices so that pseudoidentities can be generated locally. Storing the system's master key in each vehicle may expose the system to powerful attackers and unpredictable risks, even if the storage devices are assumed to be tamper proof. Those expensive tamper-proof devices can prevent attackers from reading the secrets that are physically stored in them. However, since the system's master key will be involved in local computations, the attacker has the chance to measure the energy (or time) consumed by the computations and the emitted electronic radiation, which contains information about the secret. With this information and by means of statistical methods, the attacker can launch powerful key extraction attacks such as side-channel attack [24], [25], which are well known in cryptography. Although the side-channel attack may be expensive to regular users, it is attractive and practical to organized criminals since, once the master key is extracted, they have full control over the system.

B. Our Contribution

We observe that existing privacy-preserving protocols for securing VANETs must face several challenges such as efficient certificate distribution and revocation, avoidance of computation and communication bottlenecks, and reduction of the strong dependence on tamper-proof devices. This paper addresses these challenges by exploiting the features of vehicular mobility, road limitations, and densely distributed RSUs. We propose a decentralized authentication protocol,[3] which, unlike the existing proposals, uses RSUs to maintain an on-the-fly generated group within their communication range, which is normally much longer than the V2V communication range. Vehicles can anonymously broadcast V2V messages that can be verified by other vehicles in the group and neighboring groups.

In our system, vehicles only request a new secret member key when 1) they pass by an RSU for the first time or 2) when their existing secret member keys expire. Since each vehicle only verifies messages from vehicles that have moved into the range of the same RSU and its neighbors, it can easily check whether the anonymous sender was revoked with the help of those RSUs and does not need to retrieve the revocation list from a remote centralized authority. This greatly reduces the certificate management overhead. Compared with the millions of vehicles in a VANET, the number of active vehicles within a range of a single RSU is much smaller. Hence, the system will not suffer from computation and communication bottlenecks. Although each party in our system needs a secret member key, the system's master key is only known and stored by a centralized authority, rather than being stored in each tamper-proof device that is embedded in vehicles. Furthermore, our system is robust since, if some RSUs occasionally collapse, only vehicles that are moving in those areas will be affected, and our protocol can still work with slight changes. Due to the numerous RSUs sharing the load to maintain the system, its performance does not significantly degrade when more vehicles join the VANET; hence, the system is scalable.

The remainder of this paper is organized as follows. Section II gives some preliminaries, including the network model, the security requirements, and the concepts of signcryption, group signature, and bilinear maps. Our efficient conditional privacy-preserving protocol is explained in Section III. In Section IV, the security of our protocol is examined. The performance of our protocol is evaluated in Section V. Finally, Section VI gives the conclusion.

II. Preliminaries

A. Network Model

Fig. 1 illustrates the network model that will be used later. It consists of a TA, a tracing manager (TM), RSUs, and vehicles.

- TA: The responsibility of the TA is to issue digital certificates for vehicles and RSUs. Also, it maintains a CRL containing the certificates of revoked vehicles. The TA is assumed to be completely trustable, hard to compromise, and powerful, i.e., with sufficient computation and storage capacity.
- TM: When the content of a safety message broadcast by a vehicle is found to be false, the TM should be able to determine the vehicle's real identity.

[3]The protocol is still centralized in the system setup stage for enrolling vehicles. The term "decentralized authentication" refers to the group authentication being maintained by each distributed RSU to achieve robustness and scalability, rather than by a centralized authority, as in most existing protocols employing group signatures.

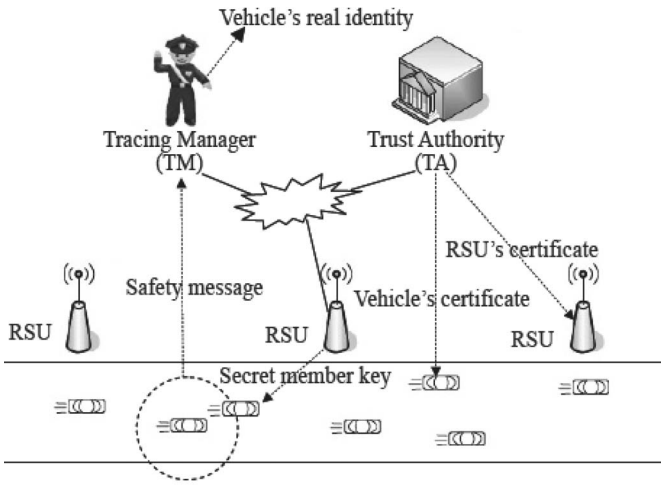

Fig. 1. Network model.

- RSU: RSUs are densely distributed in the roadside. In our protocol, RSUs are used to issue secret member keys to vehicles and assist the TM to efficiently track the real identity of a vehicle from any safety message.
- Vehicle: Vehicles move along the roads, sharing collective environmental information contained in safety messages or requesting secret member keys from RSUs. OBUs are assumed to be embedded in each vehicle. By using OBUs, vehicles can communicate with each other as well as with the RSUs. The communication among them is based on the DSRC protocol.

B. Security Requirements

In this paper, we consider several security requirements [5], [16] in two communication scenarios: 1) confidential communication between a vehicle and an RSU and 2) V2V communication. The first scenario has three security requirements: *confidential communication*, *message authentication*, and *privacy protection*; the second scenario should satisfy *message authentication*, *privacy protection*, and *anonymity revocability*. The detailed descriptions of the above requirements follow.

- *Confidential communication*. When a vehicle communicates with an RSU, only that vehicle and that RSU are aware of the information exchange. In our protocol, this implies that vehicles send a request to an RSU for a secret member key without being detected by other vehicles and secretly receive a secret member key from the RSU.
- *Message authentication*. If a message has been modified after being sent, this modification is observable by a legitimate receiver. In addition, if the message has never been modified, it confirms to the legitimate receiver that the message is from a legitimate entity.
- *Privacy protection*. As mentioned above, privacy is an important concern in VANETs. In this paper, we consider the following two cases.

1) If the communication takes place between vehicles and RSUs, privacy means that an eavesdropper cannot decide whether two different messages come from the same vehicle.
2) If the communication is between vehicles, privacy means that deciding whether two different valid messages were generated by the same vehicle is computationally hard for everyone except the TM.

- *Anonymity revocability*. The TM has the ability to retrieve the real identity of dishonest vehicles that are sending fake messages to other vehicles to disrupt traffic.

C. Signcryption

Our protocol uses a signcryption scheme and a group signature scheme. The signcryption scheme is used to help a vehicle to secretly receive a secret member key from an RSU. Signcryption [26] is a public-key primitive that has the ingredients of both digital signature and data encryption. A signcryption scheme allows a sender to simultaneously sign and encrypt a message. An attractive point is that it takes less computational time and has lower message expansion rate than the sign-then-encrypt procedure [26].

The basic requirement for a signcryption scheme is that it should satisfy the properties of *message confidentiality* and *signature unforgeability*.

- *Message confidentiality*. This allows the communicating parties to preserve the secrecy of their exchanges. This property can be used to fulfill the *confidential communication* requirement in VANETs.
- *Signature unforgeability*. A signcryption scheme offering nonrepudiation prevents the sender of a signcrypted message from repudiating her signature. This can fulfill the *message-authentication* requirement in VANETs.

Privacy is an important concern in VANETs. The signcryption scheme should also satisfy the *ciphertext anonymity* property that is defined by Boyen [27]. *Ciphertext anonymity* captures the property that the ciphertext must contain no information in the clear that identifies the sender or the recipient of the message.

- *Ciphertext anonymity*. A ciphertext should look anonymous to everyone but the actual recipient. The identities of both the sender and the recipient of the ciphertext should stay hidden from third parties. The *privacy-protection* requirement in VANETs can be satisfied by this property.

The signcryption scheme in [28] is shown to satisfy *message confidentiality*, *signature unforgeability*, and *ciphertext anonymity*. In this paper, we employ this signcryption scheme to help a vehicle to safely receive secret member keys from RSUs.

D. Group Signature

In our system, after receiving a secret member key from an RSU, each vehicle can anonymously send messages on behalf of the group maintained by this RSU by using a group signature scheme. Group signatures [18] allow the members of a group to sign on behalf of the group. Everyone can verify the signature with a group public key, while no one can know the identity of the signer except the group manager.[4] Furthermore, it is

[4]In case of a dispute, a designated group manager can reveal the actual identity of the signer.

computationally hard to decide whether two different signatures were issued by the same member. In this paper, we employ a group signature scheme to secure V2V communications.

Due to the security requirements of VANETs, the group signature scheme employed should satisfy the following properties.

- *Unforgeability*. Only the group members can sign messages on behalf of the group. This fulfills the *message authentication* requirement in VANETs.
- *Unlinkability*. Deciding whether two different valid signatures were computed by the same group member is computationally hard for anyone except the group manager. This can deal with the *privacy-protection* requirement in VANETs.
- *Traceability*. The group manager is always able to open a valid signature and identify the signer. In this paper, the TM acts as the group manager, and it can use this property to address the *anonymity revocability* requirement in VANETs.

E. Bilinear Maps

Recently, bilinear maps have been extensively investigated to build efficient schemes [29]–[33]. Our protocol is also implemented with bilinear maps. Thus, we briefly review them.

Let G_1, G_2, and G_T be three multiplicative groups of prime order q. Let g_1 denote a generator of G_1, g_2 be a generator of G_2, and ψ be a computable isomorphism from G_2 to G_1, with $\psi(g_2) = g_1$. A mapping $e : G_1 \times G_2 \longrightarrow G_T$ is called bilinear mapping if it satisfies the following properties.

1) Bilinearity: $e(u^a, v^b) = e(u, v)^{ab}$ for all $u \in G_1, v \in G_2$, $a, b \in Z_q^*$.
2) Nondegeneracy: $e(g_1, g_2) \neq 1$.
3) Computability: There exists an efficient algorithm to compute $e(u, v)$ for any $u \in G_1, v \in G_2$.

ψ can be a trace map as described in [31], and when $G_1 = G_2$ and $g_1 = g_2$, ψ can be the identity map.

Computational co-Diffie-Hellman (co-CDH) problem: Given (g_1^a, g_2^b) for unknown $a, b \in Z_q^*$, compute g_1^{ab}.

p-strong Diffie-Hellman (p-SDH) problem: The p-SDH problem in (G_1, G_2) is defined as follows: Given a $(p+2)$-tuple $(g_1, g_2, g_2^s, g_2^{s^2}, \ldots, g_2^{s^p})$ as input, output a pair $(g_1^{1/(s+x)}, x)$ where $x \in Z_q$.

Decision linear problem in G_1: Given u, v, h, u^a, v^b, and $h^c \in G_1$ as input, output "yes" if $a + b = c$ and "no" otherwise.

Our protocol employs the signcryption scheme defined in [28] and the group-signature scheme defined in [34]. The security of the signcryption is based on the hardness of the co-CDH problem, and the security of the group-signature scheme in [34] is based on the hardness of the p-SDH problem and the decision linear problem.

III. Robust and Scalable Protocol

Here, we propose a concrete robust and scalable protocol for VANETs. This protocol employs the signcryption scheme defined in [28] and the group signature scheme proposed in [34] as building blocks. The signcryption scheme is used to help a vehicle to secretly obtain a secret member key from an RSU, and the group signature scheme is used for V2V communications.

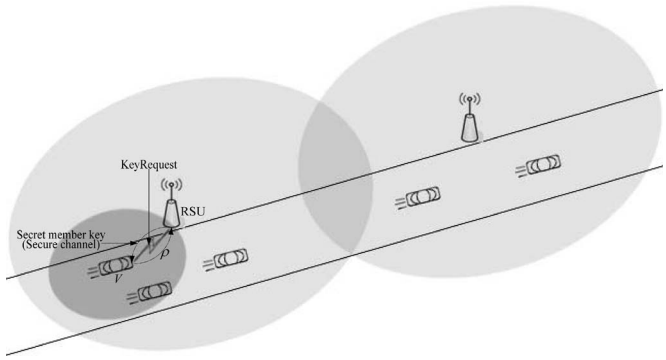

Fig. 2. Basic ideas in the decentralized protocol.

A. Basic Ideas

Here, we outline the basic ideas in our decentralized privacy-preserving authentication protocol to secure vehicular communications. Fig. 2 illustrates those basic ideas.

In our system, we let each RSU maintain an on-the-fly generated group consisting of vehicles that occasionally enter the RSU's communication range. The RSU will periodically broadcast its own certificate and its neighbor RSUs' certificates to the vehicles within its range. When a vehicle V passes by an RSU, if it is the first time it sees this RSU or if the vehicle's current secret member key has expired, the vehicle V and the RSU will run a KeyRequest protocol. V sends a signcrypted message ρ to the RSU to request a secret member key. When the RSU receives the request, first, it de-signcrypts the message ρ to obtain the plaintext m (which includes a session key, a timestamp, the certificate of V, and a signature) and checks whether V is entitled to obtain a secret member key (i.e., an anonymous group certificate), according to certain security policies to be detailed in specific implementations. If V satisfies the security criteria, a secure channel between V and the RSU will be opened, and a secret member key that is generated by the RSU will be sent back to the vehicle V through the secure channel. After receiving the secret member key, V can anonymously sign with a group signature scheme any V2V messages during its stay within the range of the RSU. These signed messages can be verified by other vehicles in the areas that are covered by the current and neighboring RSUs. Most messages are about regular driving status information and do not need to be forwarded. In case of important messages, after verifying them, vehicles can sign again and forward them to other vehicles in the areas covered by the current RSU and its neighbors. This will allow important messages to be disseminated to the whole VANET.

As claimed in Section I-B, this local processing of messages by the RSUs within the range results in increased efficiency and robustness. As to efficiency, since each vehicle only verifies messages from vehicles that move into the range of the same RSU and its neighbors, it can easily check whether the anonymous sender was revoked with the help of the neighboring RSUs and does not need to retrieve the revocation list from

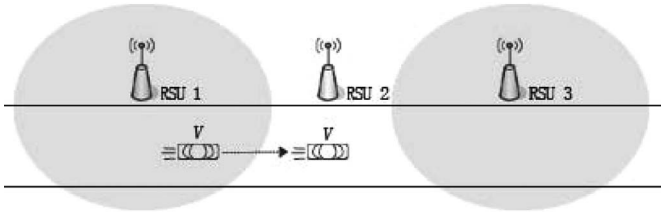

Fig. 3. Collapsed RSU 2.

a remote centralized authority. Regarding robustness, if some RSUs collapse, only vehicles entering the areas of those RSUs will be affected, and our protocol can still work with slight changes. For instance, as shown in Fig. 3, assume that vehicle V has obtained the secret member key from RSU 1 and that it is now in the cover range of RSU 2, which has collapsed. In this case, V can still use the secret member key from RSU 1 to sign the messages before it can join the group maintained by RSU 3, and RSU 1/3 only needs to broadcast a notification and the certificates of RSU 3/1 in its area as well. This mechanism may slightly decrease the security of the VANET in the case that a vehicle cannot get the up-to-date certificates of nearby RSUs (this problem can be alleviated by requesting the updated certificates from other vehicles using a multihop mechanism).

We note that, in the early stages of VANET deployment, RSUs may not be densely distributed. They are more likely to be deployed in metropolitan areas that suffer from heavy traffic. It seems reasonable to assume that there will be some sporadic RSUs in the early stage of VANETs, although the density of RSUs might not be very high. In this case, a measure that is similar to that in the above paragraph can be used to alleviate the dependence of RSUs. Finally, if the density of vehicles in an area is extremely low, similarly to the centralized group signature-based protocol in [16], our protocol can also be used as a centralized authentication scheme.

B. Concrete Protocol

Here, we describe our robust and scalable protocol for secure vehicular communication in detail. Our protocol consists of five stages: *system setup*, *key issuance*, *re-key issuance*, *signing*, *batch verification*, and *tracing*.

Before describing our protocol, we first explain the notation that is used to simplify the description.

TA	viewed as an electronic counterpart of the traffic administration office in the real world. The TA owns the system's master key, which is used to issue digital certificates for vehicles and RSUs. It also maintains a CRL, which contains the certificates of the revoked vehicles;
TM	instantiated by the traffic police. It is able to trace the identity of a vehicle having generated a certain safety message;
R_i	ith RSU. The responsibility of an RSU in our protocol is to issue secret member keys for vehicles;
V_i	ith vehicle;
ID_{V_i}	identity of V_i;
TP	timestamp;
$Cert_{R_i}$	certificate of R_i;
$Cert_{V_i}$	certificate of V_i;
$E_K(\cdot)/D_K(\cdot)$	encryption/decryption algorithm of a symmetric key encryption scheme, where K is a key that specifies the particular transformation of plaintext into ciphertext during encryption, or *vice versa* during decryption;
SK	session key that will be used as the key of $E_K(\cdot)/D_K(\cdot)$;
$\|$	message concatenation operation;
SM	safety message. The format of a safety message that is sent by a vehicle is shown in Table I.

TABLE I
FORMAT OF A SAFETY MESSAGE: FIELDS AND LENGTHS

Group ID	Payload	Timestamp	Signature
2 bytes	100 bytes	4 bytes	368 bytes

The group ID is used to identify to which group a vehicle belongs, and its length is 2 B. Position, current time, direction, speed, acceleration/deceleration, traffic events, etc., of a vehicle are included in the message payload. According to [35], the length of a payload is 100 B. We add the timestamp into a safety message to prevent the message replay attack. The last field is the signature of the first three parts of the safety message. The length of a signature in our protocol is 368 B (we will elaborate on that later). Therefore, the total message length is 474 B.

Now, we describe the *system setup*, *key issuance*, *re-key issue*, *signing*, *batch verification*, and *tracing* stages of our protocol in detail.

1) System Setup: At this stage, the TA generates the parameters for the whole system by using the TAKeyGen algorithm. Using the TMKeyGen algorithm, the TM generates its private and public keys. Similarly, each RSU or vehicle generates its private and public keys by using RKeyGen or VKeyGen.

- TAKeyGen: TA proceeds as follows.
  1) Select G_1, G_2, g_1, g_2, ψ, e.
  2) Choose cryptographic hash functions $H_1 : \{0,1\}^* \longrightarrow G_1$, $H_2 : \{0,1\}^* \longrightarrow \{0,1\}^f$, $H_3 : \{0,1\}^* \longrightarrow Z_q^*$, and $E_K(\cdot)/D_K(\cdot)$.
  3) Publish the system parameters as $params = (G_1, G_2, g_1, g_2, \psi, e, H_1 \sim H_3, E_K(\cdot)/D_K(\cdot))$, where f is the total length of the messages to be signcrypted. $params$ are prestored in the TM and in each R_i, V_i.
- TMKeyGen: Randomly select $h \in G_1^*$, $x, y \in Z_q^*$, and set $u, v \in G_1$ such that $u^x = v^y = h$. The TM's public key is $g_{TM} = (h, u, v)$. The private key of TM is $s_{TM} = (x, y)$. TM's public key is prestored in each R_i, V_i.
- RKeyGen: Select $\zeta_i \in Z_q^*$ at random, and compute $w_i = g_2^{\zeta_i}$. The private/public keys of an RSU R_i are ζ_i / w_i, and the corresponding certificate of R_i is $Cert_{R_i}$.
- VKeyGen: Choose a random $\xi_i \in Z_q^*$, and compute $pk_{V_i} = g_2^{\xi_i}$. The vehicle V_i's private/public keys are ξ_i / pk_{V_i}, whereas $Cert_{V_i}$ is the V_i's certificate.

Note that the certificates of vehicles and RSUs are issued by the TA.

2) Key Issuance: In this stage, a vehicle joins a group that is maintained by an RSU. An RSU is assumed to be more powerful than a vehicle, and its communication range is assumed to be longer. RSUs are distributed in the roadside, and they broadcast their certificates and the ones of their adjacent RSUs. When V_i passes by R_i, if V_i is already a member of the current group that is maintained by R_i, then R_i does nothing. Otherwise, V_i requests a secret member key from R_i by using the KeyRequest protocol.

- KeyRequest: This is an interactive protocol run between V_i and R_i. V_i has private/public keys ξ_i/pk_{V_i} and certificate $Cert_{V_i}$; R_i has private/public keys ζ_i/w_i and certificate $Cert_{R_i}$. This protocol employs the signcryption scheme described in [28] and consists of three steps.
  1) At this step, V_i takes as input SK, TP, $Cert_{V_i}$, and ξ_i to generate a signcrypted message and sends the signcrypted message to R_i. To do this, V_i does the following.
     a) Choose a session key SK.
     b) Select a random $r \in Z_q^*$, and compute $s = g^r$, $\sigma = H_1(SK\|Cert_{V_i}\|TP\|s\|w_i\|\psi(w_i^r))^{\xi_i}$, and $\varphi = (SK\|TP\|Cert_{V_i}\|\sigma) \oplus H_2(s\|w_i\|\psi(w_i^r))$.
     c) Send $\rho = (s, \varphi)$ to R_i.
  2) After receiving $\rho = (s, \varphi)$ from V_i, R_i first designcrypts ρ to get the plaintext. It checks the validity of the signature and the certificate in the plaintext. If they are valid, a secure channel between R_i and V_i is opened. Through this secure channel, a secret member key will be returned to V_i. The concrete procedure is as follows.
     a) Compute the plaintext $(SK\|TP\|Cert_{V_i}\|\sigma) = \varphi \oplus H_2(s\|w_i\|s^{\zeta_i})$.
     b) Check the validity of $Cert_{V_i}$. If it is invalid, "abort"; otherwise, extract pk_{V_i} from $Cert_{V_i}$.
     c) Verify the signature by checking $e(\sigma, g_2) \stackrel{?}{=} e(H_1(SK\|Cert_{V_i}\|TP\|s\|w_i\|s^{\zeta_i}), pk_{V_i})$. If the check is satisfied, using ζ_i, generate a tuple (η_i, θ_i): select $\theta_i \in Z_q^*$, and set $\eta_i = g_1^{(1/\zeta_i+\theta_i)}$. Otherwise, "abort."
     d) Compute $\kappa = E_{SK}((TP\|\eta_i\|\theta_i))$ and send κ to V_i.
     e) Store $(Cert_{V_i}, \eta_i)$ to R_i's database.
  3) When V_i receives κ from R_i, it computes $(TP'\|\eta_i\|\theta_i) = D_{SK}(\kappa)$. If $TP = TP'$, V_i accepts the secret member key (η_i, θ_i), where TP is the timestamp that is used by V_i in the first step.

Note that, to further enhance the anonymity of a vehicle and reduce the frequency of interaction between vehicles and RSUs, we can let several seriate RSUs (e.g., all the RSUs along the same street) to share the same private/public key.

3) Re-Key Issuance: A vehicle V_i can revoke its certificate $Cert_{V_i}$ for several reasons, e.g., when its private key has been stolen. If this happens, to ensure the security of the VANET, the RSUs whose databases contain $Cert_{V_i}$ should update their private/public keys, as well as their certificates. Specifically, if an RSU R_i finds that there is a certificate $Cert_{V_i}$ on the CRL and $(Cert_{V_j}, \eta_j)$ on R_i's database such that $Cert_{V_i} = Cert_{V_j}$, R_i runs the following ReKey protocol.

- ReKey: This protocol consists of the following steps.
  1) R_i first runs RKeyGen to generate a new private/public key pair ζ_i'/w_i' and the corresponding certificate $Cert'_{R_i}$. After this step, the public key of the group maintained by R_i is updated to w_i'.
  2) Then, R_i broadcasts within its communication range its new certificate and a lifetime (during this lifetime, both the new certificate and the old certificate of R_i are considered valid).
  3) When a vehicle V_i receives the above messages from R_i, it should launch the KeyRequest protocol that is used in the *Key Issuance* stage to request a fresh secret member key corresponding to the new public key w_i' of R_i.

4) Signing: As mentioned above, if a vehicle directly broadcasts a message M (in this paper, $M =$ Group ID$\|$ Payload$\|$Timestamp) with no secure mechanism, VANETs may suffer from some serious attacks. To avoid or detect those attacks and simultaneously protect the privacy of users, we use the group signature scheme proposed by Ferrara *et al.* [34]. Before sending a message M, V_i first signs it by using the following VBSign algorithm.

- VBSign: Let $(\eta_i\|\theta_i)$ be V_i's secret member key. V_i computes the group signature π_{V_i} on M as follows.
  1) Randomly select $\alpha, \beta \in Z_q^*$ and compute
$$\begin{cases} T_1 = u^\alpha \\ T_2 = v^\beta \\ T_3 = \eta_i h^{(\alpha+\beta)} \\ \gamma_1 = \theta_i \alpha \\ \gamma_2 = \theta_i \beta. \end{cases}$$
  2) Select r_α, r_β, r_θ, r_{γ_1}, $r_{\gamma_2} \in Z_q^*$ at random and compute
$$\begin{cases} R_1 = u^{r_\alpha} \\ R_2 = v^{r_\beta} \\ R_3 = e(T_3, g_2)^{r_\theta} e(h, w_i)^{-r_\alpha - r_\beta} e(h, g_2)^{-r_{\gamma_1} - r_{\gamma_2}} \\ R_4 = T_1^{r_\theta} u^{-r_{\gamma_1}} \\ R_5 = T_2^{r_\theta} v^{-\gamma_2}. \end{cases}$$
  3) Compute $c = H_3(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$.
  4) Compute
$$\begin{cases} s_\alpha = r_\alpha + c\alpha \\ s_\beta = r_\beta + c\beta \\ s_\theta = r_\theta + c\theta_i \\ s_{\gamma_1} = r_{\gamma_1} + c\gamma_1 \\ s_{\gamma_2} = r_{\gamma_2} + c\gamma_2. \end{cases}$$
  5) Output the group signature $\pi_{V_i} = (T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5, s_\alpha, s_\beta, s_\theta, s_{\gamma_1}, s_{\gamma_2})$.

5) Batch Verification: A vehicle may receive many safety-related messages from other vehicles in a very short time. Before accepting these safety messages, it should first verify their validity by checking the signatures of the safety messages. As remarked in [36], fast validation of vehicular messages is crucial for a wide deployment of VANETs in practice. To meet this requirement, we use a batch-verification technique similar

to the one shown in [36] and [37]. When a vehicle receives safety messages from other vehicles in the group maintained by R_i whose public key is w_i, it runs the following VBVerify algorithm to check the validity of these safety messages.

- VBVerify: Assume that a vehicle should verify n safety messages at the same time. Let $\pi_j = (T_{1,j}, T_{2,j}, T_{3,j}, R_{1,j}, R_{2,j}, R_{3,j}, R_{4,j}, R_{5,j}, s_{\alpha,j}, s_{\beta,j}, s_{\theta,j}, s_{\gamma_1,j}, s_{\gamma_2,j})$ be the signature on the message M_j in the jth safety message. For each $j = 1, \ldots, n$, first compute

$$c_j = H_3(M_j, T_{1,j}, T_{2,j}, T_{3,j}, R_{1,j}, R_{2,j}, R_{3,j}, R_{4,j}, R_{5,j})$$

and take random width-w nonadjacent forms (w-NAFs, [37]) $\delta_1, \ldots, \delta_n$. Batch verify the following bilinear-map-based equation:

$$\prod_{j=1}^{n} R_{3,j}^{\delta_j} \stackrel{?}{=} e\left(\prod_{j=1}^{n}\left(T_{3,j}^{s_{\theta,j}\delta_j} h^{\left(-s_{\gamma_1,j}-s_{\gamma_2,j}\right)\delta_j} g_1^{-c_j\delta_j}\right), g_2\right) \cdot e\left(\prod_{j=1}^{n}\left(h^{(-s_{\alpha,j}-s_{\beta,j})\delta_j} T_3^{c_j\delta_j}\right), w_i\right).$$

Then, verify the validity of the following nonbilinear map equations:

$$\begin{cases} u^{s_{\theta,j}} \stackrel{?}{=} T_{1,j}^{c_j} \\ v^{s_{\beta,j}} \stackrel{?}{=} T_{2,j}^{c_j} R_{2,j} \\ T_{1,j}^{s_{\theta,j}} u^{-s_{\gamma_1,j}} \stackrel{?}{=} R_{4,j} \\ T_{2,j}^{s_{\theta,j}} v^{-s_{\gamma_2,j}} \stackrel{?}{=} R_{5,j} \end{cases}$$

by picking random w-NAFs [37] $\varrho_{1,1}, \ldots, \varrho_{1,n}; \varrho_{2,1}, \ldots, \varrho_{2,n}; \varrho_{3,1}, \ldots, \varrho_{3,n}; \varrho_{4,1}, \ldots, \varrho_{4,n}$ and batch verifying $\prod_{j=1}^{n} (u^{s_{\theta,j}\varrho_{1,j}} T_{1,j}^{-c_j\varrho_{1,j}} v^{s_{\beta,j}\varrho_{2,j}} T_{2,j}^{-c_j\varrho_{2,j}} R_{2,j}^{-\varrho_{2,j}} T_{1,j}^{s_{\theta,j}\varrho_{3,j}} u^{-s_{\gamma_1,j}\varrho_{3,j}} R_{4,j}^{-\varrho_{3,j}} T_{2,j}^{s_{\theta,j}\varrho_{4,j}} v^{-s_{\gamma_2,j}\varrho_{4,j}} R_{5,j}^{-\varrho_{4,j}}) \stackrel{?}{=} 1$. Finally, accept the safety messages if and only if all checks succeed.

Bilinear map operation is the most time-consuming operation in the above VBVerify algorithm. Using the batch-verification technique requires only two (rather than $2n$) bilinear map operations. In addition to saving in bilinear map computation, the above batch verification performs approximately 4.8 times faster than the individual verifications [37].

6) Tracing: Malicious entities (vehicles) may exist in VANETs. They may send fake messages to other vehicles to influence the traffic. If this happens, the TM can disclose the identity of the actual sender by invoking the following Open algorithm.

- Open: This algorithm is used by the TM to trace a signature that is included in a safety message. Let $\pi_{V_i} = (T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5, s_\alpha, s_\beta, s_\theta, s_{\gamma_1}, s_{\gamma_2})$ be a valid signature on M_i under an RSU's public key w_i (according to the group ID in M_i, the TM can download the public key of the corresponding RSU from the TA). The TM proceeds as follows.
  1) Recover the vehicle's η_i as $\eta_i = T_3/(T_1^x \cdot T_2^y)$.
  2) Get $(Cert_{V_i}, \eta_i)$ from the RSU's database.
  3) Extract ID_{V_i} from $Cert_{V_i}$.

IV. Security Analysis

Here, we analyze the security of the proposed protocol. We will show that our protocol meets all the security requirements described in Section II-B.

We first consider the scenario of a confidential communication between a vehicle and an RSU. It can be divided into two phases.

- The first is the vehicle-to-RSU communication phase. This scenario has three security requirements: *confidential communication*, *message authentication*, and *privacy protection*. In this phase, a vehicle V_i that wants to join a group maintained by R_i first selects a session key, generates a ciphertext ρ by using a signcryption scheme that takes as input the session key, a timestamp TP, etc., and then, V_i sends ρ to R_i. Since the signcryption scheme we choose satisfies the *message confidentiality*, *signature unforgeability*, and *ciphertext anonymity* properties that provide *confidential communication*, *message authentication*, and *privacy protection*, respectively, it is easy to see that the communications in this phase meet the desired security requirements in VANETs.
- The second phase is the RSU-to-vehicle communication. This scenario also has three security requirements: *confidential communication*, *message authentication*, and *privacy protection*. In this phase, R_i first extracts the secret member key (η_i, θ_i) for V_i, then uses the session key SK received from V_i and the symmetric-key encryption algorithm $E_{SK}(\cdot)$ to encrypt $(TP\|\eta_i\|\theta_i)$ and get the ciphertext κ, and finally sends the ciphertext κ to V_i. Since only V_i knows the corresponding session key, only V_i can decrypt $(TP'\|\eta_i\|\theta_i)$ from κ. Therefore, the *confidential communication* requirement is guaranteed. Furthermore, the session key is only used once. Hence, *privacy protection* is also satisfied. After getting $(TP'\|\eta_i\|\theta_i)$, V_i checks $TP \stackrel{?}{=} TP'$. This is used to fulfill the *message-authentication* requirement.

Finally, we turn to the V2V communication scenario. The security requirements of *message authentication*, *privacy protection*, and *anonymity revocability* should hold in this scenario. Here, the group signature scheme is used in our protocol, and the group signature has the *unforgeability*, *unlinkability*, and *traceability* properties, which ensure *message authentication*, *privacy protection*, and *anonymity revocability*, respectively. Hence, the desired security requirements for this scenario are naturally fulfilled.

V. Performance Evaluation

Here, we evaluate the performance of our protocol by comparing it with the up-to-date protocols GSIS [16] and efficient conditional privacy preservation (ECPP) [20], which offer similar security and privacy properties.

A. Transmission Overhead of Safety Messages

According to DSRC [8], a vehicle sends each message with a time interval from 100 to 300 ms, and the minimal data rate in DSRC is 6 Mb/s (for safety messaging, it is typically 12 Mb/s).

TABLE II
RSU SERVICE EFFICIENCY

	T_V	T_R	Rounds
ECPP	3 ms $(5\tau_e)$	10.2 ms $(2\tau_m, 2\tau_e)$	2
Our Protocol	1.8 ms $(3\tau_e)$	10.2 ms $(2\tau_m, 2\tau_e)$	1

In the following, we will consider two scenarios. Our analyses show that our protocol is practical in both scenarios.

First, we consider a six-lane two-way highway, each lane being 3 m wide. We assume uniform presence of vehicles, with an intervehicle space of 30 m. Vehicles are in movement and transmit DSRC safety messages every 300 ms over a 300-m communication range. According to [5], a vehicle can hear at most 120 vehicles per 300 ms, which amounts to a system throughput of 1.45 Mb/s $[(120 \times 3.33 \times 474 \times 8)/(1024 \times 1024)$ Mb/s$]$. This throughput is much smaller than 6 Mb/s.

Second, we consider the same highway, but this time, vehicles are very slow or even stopped (i.e., a congestion scenario). The vehicles are separated by 5 m (including the vehicle length). Each vehicle transmits a safety message over a range of 15 m every 100 ms. In the worst case [5], a vehicle can hear at most 36 other vehicles per 100 ms. Hence, we have the maximal throughput 1.30 Mb/s $[(36 \times 10 \times 474 \times 8)/(1024 \times 1024)$ Mb/s$]$, which is also smaller than the minimum bandwidth available of 6 Mb/s.

B. RSU Service Efficiency

Here, we compare the RSU service efficiency (the cost for a vehicle to receive a secret member key or a short-time anonymous certificate from an RSU) of our protocol with the ECPP protocol.

According to the execution time results shown in [38], the measured processing time[5] for one bilinear map operation τ_m is about 4.5 ms, and the time for one point exponentiation τ_e is about 0.6 ms. In the sequel, we denote by T_V the computation overhead of a vehicle and by T_R the computation overhead of an RSU.

From Table II, regarding the computational cost, we can find that the RSU service efficiency of our protocol is slightly better than the efficiency of the ECPP protocol in [20]. In addition, our protocol is round efficient. To obtain a secret member key from an RSU, our protocol requires only one round, whereas the ECPP requires two rounds (for a short-time anonymous certificate). A two-round protocol causes more delays than a single-round one. Sometimes, a vehicle may pass by an RSU at a very high speed. Hence, if a two-round protocol is used, the vehicle may not receive the secret member key or the short-time anonymous certificate in time.

C. Computation Overhead on Signature Verification

Here, we compare the computational overhead of signature verification in our protocol with that in ECPP and GSIS (V2V communication scenario).

[5]For a Miyaji, Nakabayashi, and Takano (MNT) curve [39] of embedding degree $k = 6$ and 160-bit q and an implementation run on an Intel Pentium IV 3.0-GHz machine.

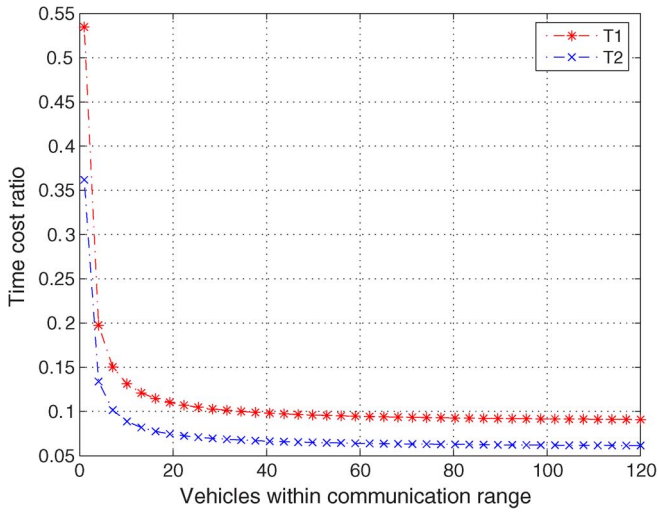

Fig. 4. Time-efficiency ratio $T1 = T_o/T_E$ and $T2 = T_o/T_G$.

With our protocol, to verify n safety messages (essentially, to verify n signatures in n safety messages) from the same group, the required time cost is

$$T_o = 2\tau_m + \frac{14n\tau_e}{4.8} = 2 \times 4.5 + \frac{14n \times 0.6}{4.8} \text{ ms}.$$

Generally, a vehicle may receive safety messages from at most two groups. The required time cost to verify n safety messages from two different groups is

$$T_o' = 4\tau_m + \frac{14n\tau_e}{4.8} = 4 \times 4.5 + \frac{14n \times 0.6}{4.8} \text{ ms}.$$

With ECPP, to verify n safety messages, the time cost is $T_E = 3n\tau_m + 11n\tau_e = 3n \times 4.5 + 11n \times 0.6$ ms. With GSIS, the time cost of verifying n safety messages increases with the number of revoked certificates of vehicles in the revocation list. It is fair to compare our protocol with GSIS when the revocation list is empty. In this case, the computational time of signature verification of GSIS is $T_G = 5n\tau_m + 12n\tau_e = 5n \times 4.5 + 11n \times 0.6$ ms. Fig. 4 shows the time-cost ratio $T1 = T_o/T_E$ and $T2 = T_o/T_G$. Fig. 5 shows the time-cost ratio $T3 = T_o'/T_E$ and $T4 = T_o'/T_G$.

From Figs. 4 and 5, it is apparent that the computational overhead of the signature verification of our protocol is always much lower than that in [16] and [20]. This advantage of our protocol is more obvious when the number of vehicles within the communication range grows. In VANETs, vehicles broadcast safety messages every 100–300 ms to other vehicles. This way, a vehicle may receive lots of safety messages from other vehicles in a very short period of time. Hence, the efficiency of the signature verification is vital when the number of vehicles within the communication range is high. In [16], the group signature can only be verified one by one, whereas in [20], before verifying a signature from a vehicle, one should first verify the short-time anonymous certificate of the vehicle. In contrast, in our protocol, no short-time anonymous certificates are required, and the batch-verification technique is used. This largely improves the efficiency of our signature verification.

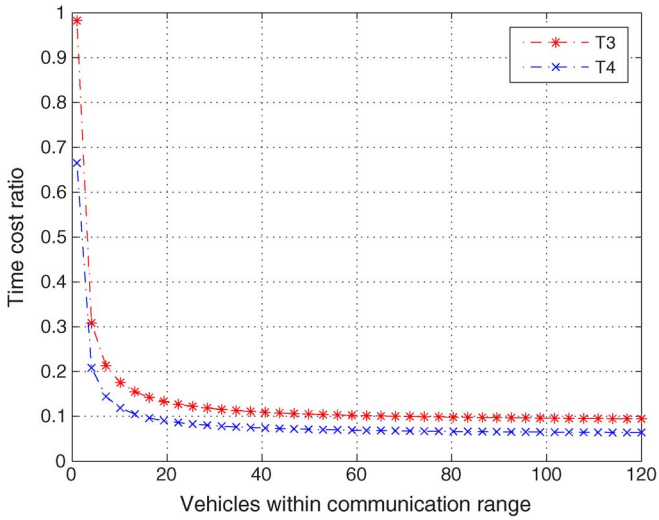

Fig. 5. Time-efficiency ratio $T3 = T'_o/T_E$ and $T4 = T'_o/T_G$.

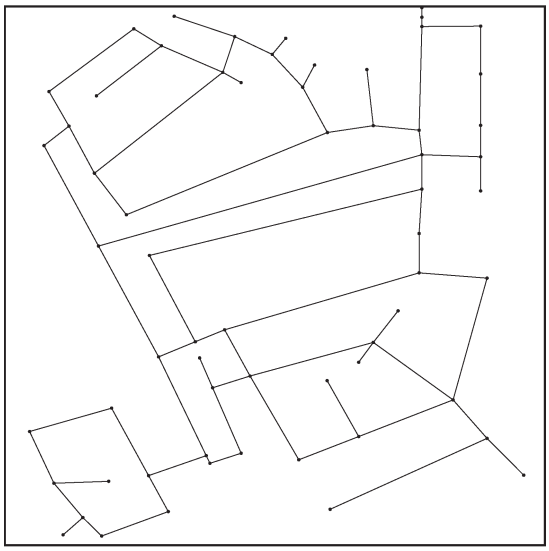

Fig. 6. Road scenario corresponding to a square area of size 1×1 km^2.

D. Simulation

Here, by using NS-2 [40], we carry out some simulations to evaluate the average message delay and message loss rate to determine the practical performance of our protocol. In our simulations, the road scenario that is considered covers an area of 1×1 km^2 and is shown in Fig. 6. The vehicles were generated at random, and their average speed was 56 km/h, which is typical in urban areas. The communication range of each vehicle is from 10 to 300 m. The channel bandwidth bound is 6 Mb/s, and the packet size is 474 B (see Section III-B). For each experiment, the simulation time is 200 s. In addition, since the communication range of an RSU is much longer than the one of a vehicle, for most cases, a vehicle only verifies safety messages from the members in the same on-the-fly group. As shown in Section V-C, to verify n safety messages, the required time cost is $T_o = 2 \times 4.5 + (14n \times 0.6/4.8)$ ms.

The average message delay D_{msg} is defined as follows [36]: $D_{\text{msg}} = (1/L_{\mathbb{D}}) \sum_{\ell \in \mathbb{D}} ((1/M_{\ell_\rightarrow}) \sum_{m=1}^{M_{\ell_\rightarrow}} (T_{\overrightarrow{\text{sgn}}}^{\ell_m} + (1/K_\ell) \sum_{k=1}^{K_\ell} (T_{\overrightarrow{\text{trnsmsn}}}^{\ell_m k} + \sum_{j=1}^{\lceil MAD/\tau \rceil} j P_{m,j} \tau)))$, where $\mathbb{D}$ is the sample district in the simulation, $L_{\mathbb{D}}$ is the number of vehicles in $\mathbb{D}$, $M_{\ell_\rightarrow}$ is the number of messages sent by vehicle ℓ, K_ℓ is the number of vehicles within a one-hop communication range of vehicle ℓ, $T_{\overrightarrow{\text{sgn}}}^{\ell_m}$ is the time taken by vehicle ℓ to sign message m, $T_{\overrightarrow{\text{trnsmsn}}}^{\ell_m k}$ is the time taken to transmit message m from vehicle ℓ to vehicle k, τ is the time period taken to perform a batch verification, and MAD is the maximum allowable delay for end-to-end message transmissions. According to [41], MAD is 100 ms. $P_{m,j} = v_{m,j}/V_m$, where V_m is the total number of vehicles processing m among the K_ℓ vehicles, and $v_{m,j}$ is the number of vehicles processing m in the interval $((j-1)\tau, j\tau]$ for $j\tau \le MAD$. Clearly, we have $V_m = \sum v_{m,j}$.

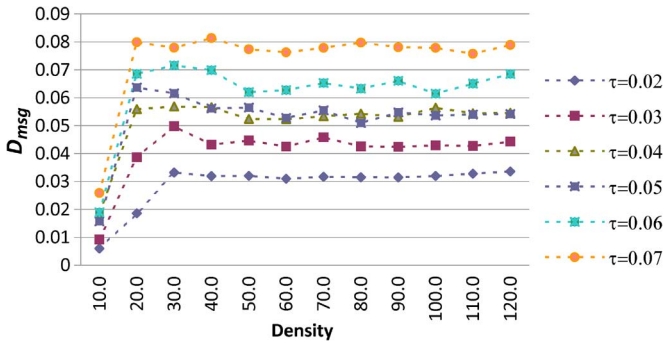

Fig. 7. Impact of authentication on the message delay.

The average message delay D_{msg} reflects the average time latency for a message to be processed and must be smaller than MAD. Fig. 7 shows the relationship between D_{msg}, the vehicle density, and the batch-verification period τ. From this figure, one can see that, for a fixed vehicle density, D_{msg} increases with τ. For a fixed τ, in the case of a very low density, D_{msg} sharply grows when the vehicle density is increased from $10/\text{km}^2$ to $30/\text{km}^2$. However, the delay stabilizes for vehicle densities above $30/\text{km}^2$. These experimental results seem to contradict the intuition that the delay will keep increasing as more messages will be received for verification. We observe that such a stable curve is due to the fact that most received messages can be verified in a batch, and the average message delay does not increasingly grow for a larger density. We also note that, for all combinations of different densities and batch-verification intervals, the average message delay is lower than $MAD = 100$ ms, which implies that our protocol works well for various traffic environments.

When the arriving messages surpass the processing capacity of the vehicle in a batch-verification period, some messages cannot be verified, which results in message loss due to the authentication mechanism. The average message loss (introduced by cryptographic operations) rate can be computed as follows:

$$R_{\text{loss}} = 1 - \frac{1}{L_{\mathbb{D}}} \sum_{v_i \in \mathbb{D}} \frac{n_\tau}{n_{v_i}}$$

where n_τ is the maximum number of messages that a vehicle can verify in a given batch period τ, and n_{v_i} is the number of messages that a vehicle v_i receives to verify in a given batch period τ. If $n_{v_i} \le n_\tau$, then $n_\tau/n_{v_i} = 1$.

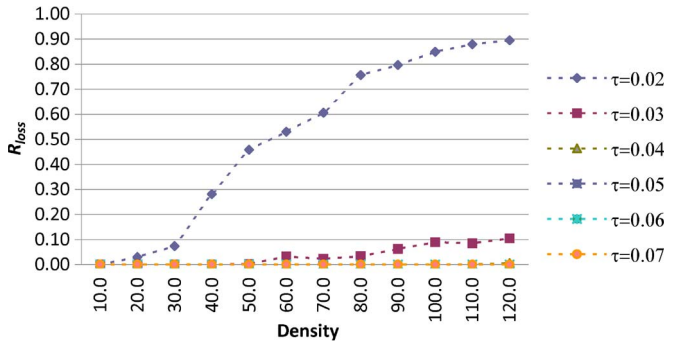

Fig. 8. Impact of authentication on the message loss rate.

Fig. 8 shows that, when $\tau = 0.02$ and 0.03 s, R_{loss} increases as the vehicle density grows, and when $\tau \geq 0.04$ s, R_{loss} is almost 0 for a density between $0/\text{km}^2$ and $120/\text{km}^2$. This is because when τ is small, only a few messages are received in a batch period, and the advantage of batch verification is not well exploited; when τ and the vehicle density grow, the messages received in τ also grow. However, the arriving message growth rate cannot surpass the message processing capacity, which also grows with τ.

From the results illustrated in Figs. 7 and 8, one may find that there is a conflict between the average message delay D_{msg} and the average message loss rate R_{loss}. We expect low average message delay, as lower latency implies that vehicles can take less time to respond to the traffic environment changes. To obtain lower average message delay, the batch-verification interval τ should be as small as possible. However, if τ is too small, some messages cannot be verified, and the average message loss rate grows. Hence, a balance point has to be found, and from Figs. 7 and 8, $\tau = 0.05$ s might be an ideal balance point.

VI. Conclusion

A number of challenges such as efficient certificate distribution and revocation, avoidance of computation and communication bottlenecks, and reduction of the strong dependence on tamper-proof devices arise in existing protocols for securing VANETs. We have proposed a new privacy-preserving authentication protocol that efficiently addresses those challenges by considering the special features of vehicular mobility, road limitations, and densely distributed RSUs in VANETs. In our system, each RSU maintains an on-the-fly-generated group within its communication range in which vehicles can anonymously generate V2V messages and verify anonymous V2V messages from other vehicles. Vehicles generating false/bogus messages can be traced by a third party. Our scheme has been shown to be robust, scalable, and practical. Furthermore, it clearly outperforms state-of-the-art alternatives in the case of dense traffic.

Acknowledgment

The authors would like to thank Ú. González-Nicolaś for the simulation. The authors are with the UNESCO Chair in Data Privacy, but their views do not necessarily reflect the position of the UNESCO nor make any commitments for that organization.

References

[1] L. Wischhof, A. Ebner, and H. Rohling, "Information dissemination in self-organizing intervehicle networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 6, no. 1, pp. 90–101, Mar. 2005.
[2] P. Karger and Y. Frankel, "Security and privacy threats to ITS," in *Proc. 2nd World Congr. Intell. Transp. Syst.*, 1995, vol. 5, pp. 2452–2458.
[3] A. Solanas, J. Domingo-Ferrer, and A. Martínez-Ballesté, "Location privacy in location-based services: Beyond TTP-based schemes," in *Proc. 1st Int. Workshop PiLBA*, 2008, pp. 12–23.
[4] A. Solanas and A. Martínez-Ballesté, "A TTP-free protocol for location privacy in location-based services," *Comput. Commun.*, vol. 31, no. 6, pp. 1181–1191, Apr. 2008.
[5] M. Raya and J. Hubaux, "Securing vehicular *ad hoc* networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, Jan. 2007.
[6] Car 2 Car Communication Consortium. [Online]. Available: http://www.car-to-car.org/
[7] *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments*, IEEE Std. 1609.2-2006, 2006.
[8] *Dedicated Short Range Communications (DRSC) Home*. [Online]. Available: http://www.leearmstrong.com/Dsrc/DSRCHomeset.htm
[9] *National ITS Architecture*. [Online]. Available: http://www.iteris.com/itsarch/index.htm
[10] V. Daza, J. Domingo-Ferrer, F. Sebé, and A. Viejo, "Trustworthy privacy-preserving car-generated announcements in vehicular *ad hoc* networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 4, pp. 1876–1886, May 2009.
[11] M. Raya, A. Aziz, and J.-P. Hubaux, "Efficient secure aggregation in VANETs," in *Proc. 3rd Int. Workshop VANET*, 2006, pp. 67–75.
[12] M. Raya and J. Hubaux, "The security of vehicular *ad hoc* networks," in *Proc. 3rd ACM Workshop SASN*, 2005, pp. 11–21.
[13] J. Blum and A. Eskandarian, "The threat of intelligent collisions," *IT Prof.*, vol. 6, no. 1, pp. 24–29, Jan. 2004.
[14] L. Gollan and C. Meinel, "Digital signatures for automobiles, Institut für Telematik e.V, Trier, Germany, Tech. Rep., 2002. [Online]. Available: http://www.hpi.uni-potsdam.de/fileadmin/hpi/FG_ITS/papers/DigitalSignaturesAuto02.pdf
[15] J. Hubaux, S. Ćapkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security Privacy*, vol. 2, no. 3, pp. 49–55, May 2004.
[16] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.
[17] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Advances in Cryptology—CRYPTO*, vol. 3152, *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 2004, pp. 41–55.
[18] D. Chaum and E. van Heijst, "Group signatures," in *Advances in Cryptology—Eurocrypt 1991*, vol. 576, *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 1991, pp. 257–265.
[19] A. Shamir, "Identity based cryptosystems and signature schemes," in *Advances in Cryptology—CRYPTO*, vol. 196, *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 1984, pp. 47–53.
[20] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE INFOCOM*, 2008, pp. 1229–1237.
[21] J. Freudiger, M. Raya, and M. Feleghhazi, "Mix zones for location privacy in vehicular networks," in *Proc. ACM Workshop WiN-ITS*, 2007.
[22] C. Zhang, X. Lin, R. Lu, and P. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in *Proc. IEEE ICC*, May 19–23, 2008, pp. 1451–1457.
[23] C. Zhang, R. Lu, X. Lin, P. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. IEEE INFOCOM*, 2008, pp. 246–250.
[24] P. C. Kocher, "Timing attacks on implementations of Diffie–Hellman, RSA, DSS, and other systems," in *Advances in Cryptology—CRYPTO 1996*, vol. 1109, *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 1996, pp. 104–113.
[25] F. Standaert, T. Malkin, and M. Yung, "A unified framework for the analysis of side-channel key recovery attacks," in *Advances in Cryptology—Eurocrypt*, vol. 5479, *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 2009, pp. 443–461.
[26] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) $\ll$ cost(signature) + cost(encryption)," in *Advances in Cryptology—CRYPTO*, vol. 1294, *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 1997, pp. 165–179.
[27] X. Boyen, "Multipurpose identity-based signcryption: A Swiss army knife for identity-based cryptography," in *Advances in Cryptology—CRYPTO*, vol. 2729, *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 2003, pp. 383–399.

[28] C. Li, G. Yang, D. Wong, X. Deng, and S. Chow, "An efficient signcryption scheme with key privacy," in *Proc. EuroPKI*, vol. 4582, *Lecture Notes in Computer Science*, 2007, pp. 78–93.
[29] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology—CRYPTO*, vol. 2139, *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 2001, pp. 213–229.
[30] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Advances in Cryptology—Eurocrypt*, vol. 2656, *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 2003, pp. 416–432.
[31] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," in *Proc. Asiacrypt*, vol. 2248, *Lecture Notes in Computer Science*, 2001, pp. 514–532.
[32] J. Camenisch, S. Hohenberger, and M. Pedersen, "Batch verification of short signatures," in *Advances in Cryptology—Eurocrypt*, vol. 4515, *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 2007, pp. 246–263.
[33] L. Zhang and F. Zhang, "A new certificateless aggregate signature scheme," *Comput. Commun.*, vol. 32, no. 6, pp. 1079–1085, Apr. 2009.
[34] A. Ferrara, M. Green, S. Hohenberger, and M. Pedersen, "Practical short signature batch verification," in *Proc. CT-RSA*, vol. 5473, *Lecture Notes in Computer Science*, 2009, pp. 309–324.
[35] U.S. Department of Transportation, *Vehicle Safety Communications Project*, Nat. Highway Traffic Safety Admin., Apr. 2006. Final Rep., App. H: WAVE/DSRC Security.
[36] Q. Wu, J. Domingo-Ferrer, and Ú. González-Nicolás, "Balanced trustworthiness, safety and privacy in vehicle-to-vehicle communications," *IEEE Trans. Veh. Technol.*, to be published. DOI: 10.1109/TVT.2009.2034669.
[37] J. Cheon and J. Yi, "Fast batch verification of multiple signatures," in *Public-Key Cryptography—PKC*, vol. 4450, *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 2007, pp. 442–457.
[38] M. Scott, Efficient Implementation of Cryptographic Pairings. [Online]. Available: http://ecrypt-ss07.rhul.ac.uk/Slides/Thursday/mscott-samos07.pdf
[39] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," *IEICE Trans. Fundam.*, vol. E84-A, no. 5, pp. 1234–123, 2001.
[40] The Network Simulator—ns. [Online]. Available: http://www.isi.edu/nsnam/ns/
[41] European Parliament, *Legislative Resolution on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection With the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)0438 C6-0293/2005 2005/0182(COD))*, 2005.
[42] D. Lin, E. Bertino, R. Cheng, and S. Prabhakar, "Location privacy in moving-object environments," *Trans. Data Privacy*, vol. 2, no. 1, pp. 21–46, 2009.

Lei Zhang received the B.S. and M.S. degrees in applied mathematics and computer engineering from Nanjing Normal University, Nanjing, China, in 2004 and 2008, respectively. He is currently working toward the Ph.D. degree with the CRISES Research Group and the UNESCO Chair in Data Privacy, Department of Computer Science and Mathematics, Universitat Rovira i Virgili, Tarragona, Catalonia.

His fields of activity include information security, cryptography, data privacy, and network security.

Qianhong Wu received the M.Sc. degree in applied mathematics from Sichuan University, Sichuan, China, and the Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2001 and 2004, respectively.

Since then, he has been an Associate Research Fellow with the University of Wollongong, Wollongong, Australia, an Associate Professor with Wuhan University, Wuhan, China, and a Senior Researcher with the Universitat Rovira i Virgili, Tarragona, Catalonia. His research interests include cryptography, information security and privacy, and ad hoc network security. He has been a main researcher or project holder/coholder for more than ten Chinese-, Australian-, and Spanish-funded projects. He has authored over 60 publications and served on the program committees of several international conferences on information security and privacy.

Dr. Wu is a member of the International Association for Cryptologic Research.

Agusti Solanas (M'06) received the B.Sc. and M.Sc. (with honors, i.e., Outstanding Graduation Award) degrees in computer engineering from Universitat Rovira i Virgili (URV), Tarragona, Catalonia, in 2002 and 2004, respectively, and the Diploma of Advanced Studies (Master) and Ph.D. degrees with honors (*cum laude*) in telematics engineering from the Technical University of Catalonia, Barcelona, Spain, in 2006 and 2007, respectively.

He is currently a Researcher with the CRISES Research Group and the UNESCO Chair in Data Privacy and a Tenure-Track Lecturer with the Department of Computer Science and Mathematics, URV. His fields of activity include data privacy, data security, and artificial intelligence, specifically clustering and evolutionary computation. He is a participant researcher in the Consolider Ingenio 2007 project. Also, he has participated in several Spanish-funded and Catalan-funded research projects. He has authored over 60 publications and has delivered several talks. He has served as the chair, a program committee member, and a reviewer for several conferences and journals.

Dr. Solanas is a member of several scientific organizations such as the Association for Computing Machinery, the International Association for Cryptologic Research, and the Sigma Xi Scientific Research Society. He is also a member of the IEEE Graduates of the Last Decade and volunteers as an Editorial Assistant for the IEEE GOLDRush Newsletter. He is currently a member of the board of the IEEE Spain Section.

Josep Domingo-Ferrer (SM'02) received the M.Sc. and Ph.D. degrees (with honors, i.e., Outstanding Graduation Award) in computer science from the Universitat Autònoma de Barcelona, Barcelona, Spain, in 1988 and 1991, respectively. He also received the M.Sc. degree in mathematics from Universidad Nacional de Educación a Distancia, Madrid, Spain.

In 2004, he was a Visiting Fellow with Princeton University, Princeton, NJ. He is currently a Full Professor of computer science and an Institució Catalana de Recerca i Estudis Avançats (ICREA) Académia Researcher with the Universitat Rovira i Virgili, Tarragona, Catalonia, where he holds the UNESCO Chair in Data Privacy. He is the holder of three patents and has authored over 230 publications, one of which became an Institute for Scientific Information highly cited paper in early 2005. He has been the coordinator of European Union Fifth Framework Programme project Co-Orthogonal and of several Spanish and U.S.-funded research projects. He currently coordinates the Consolider "ARES" team on security and privacy: one of Spain's 34 strongest research teams. His fields of activity include data privacy, data security, and cryptographic protocols.

Dr. Domingo-Ferrer was a recipient of three research awards and four entrepreneurship awards, among which is the ICREA Académia Research Prize from the Government of Catalonia. He has chaired or cochaired nine international conferences and has served on the program committees of over 80 conferences on privacy and security. He is a Coeditor-in-Chief of the *Transactions on Data Privacy* and an Associate Editor of three international journals.