

Trustworthy Privacy-Preserving Car-Generated Announcements in Vehicular Ad Hoc Networks

Vanesa Daza, Josep Domingo-Ferrer, *Senior Member, IEEE*, Francesc Sebé, and Alexandre Viejo

Abstract—Vehicular ad hoc networks (VANETs) allow vehicle-to-vehicle communication and, in particular, vehicle-generated announcements. Provided that the trustworthiness of such announcements can be guaranteed, they can greatly increase the safety of driving. A new system for vehicle-generated announcements is presented that is secure against external and internal attackers attempting to send fake messages. Internal attacks are thwarted by using an endorsement mechanism based on threshold signatures. Our system outperforms previous proposals in message length and computational cost. Three different privacy-preserving variants of the system are also described to ensure that vehicles volunteering to generate and/or endorse trustworthy announcements do not have to sacrifice their privacy.

Index Terms—Privacy, protocol design, secret sharing, security, threshold signatures, vehicular communications.

I. INTRODUCTION

A MOBILE ad hoc network (MANET) is formed by mobile nodes that are connected in a self-organized way without an underlying hierarchical infrastructure. In the special case where the mobile nodes are embedded in vehicles, the MANET is called a vehicular ad hoc network (VANET).

VANETs permit a vehicle to automatically warn nearby vehicles about its movements (e.g., braking and lane change) to avert dangerous situations. These *alert messages* only require a limited dissemination range (less than 100 m) but have very strong real-time requirements (they must be processed very quickly).

VANETs also allow a car to send *announcement messages* about road conditions (e.g., traffic jams and accidents) to other vehicles so that the latter can take advantage of that information to select routes, avoiding troublesome points. Such announcement messages require a longer dissemination range. However, their requirement of real-time processing is much less strict than in the case of alerts so that advanced cryptography can be used to make such messages secure and trustworthy. This paper focuses on announcements.

Privacy is a key aspect in VANETs. The fact that a vehicle is equipped with communication capabilities should not result

in profiling its driver's habits (e.g., locations visited and driving pattern) any easier. Indeed, as noted in [1], a lot can be inferred on the driver's personality if the whereabouts and the driving pattern of a car can be tracked. There are two layers of privacy: *anonymity* and *unlinkability*. A system preserves anonymity when it does not require the identity of its users to be disclosed. Unlinkability is stronger than anonymity and refers to the fact that different interactions of the same user with the system cannot be related. Unlinkability prevents user tracking and profiling.

Security in car-generated announcements sent over a VANET is fundamental. It is particularly important that the system does not permit an intruder (external attacker) or a dishonest driver (internal attacker) to attack integrity by either inserting fake announcements or modifying announcements sent by others. Tampered announcements could seriously disrupt traffic or cause dangerous situations for other vehicles.

Security against insertion of fake announcements by external attackers is easy to achieve using well-known cryptographic authentication techniques (digital signatures or message authentication codes). Such techniques require the sender of a message to access some secret key material only available to legitimate registered users—and therefore unavailable to external attackers.

Dealing with internal attackers is a thornier issue. The reason is that legitimate system users, and thus internal attackers, have access to the secret key material required to send authenticated fake messages (for instance, to announce a false traffic jam with the aim of diverting traffic from a certain area where some kind of crime is being committed). Countermeasures against fake messages from internal attackers fall into two classes: *a posteriori* and *a priori*.

A. A Posteriori Countermeasures

A posteriori countermeasures consist of taking punitive actions against users who have been proven to have originated fake messages (e.g., the offenders can be banished from the network). These countermeasures in anonymous systems require the presence of a trusted third party able to revoke the key material of such dishonest users. This way, they will be excluded from the system.

Digital signatures have extensively been used in most of the protocols that offer *a posteriori* countermeasures: from plain digital signatures [2]–[5] until more sophisticated distributed signatures, such as group signatures in [6] or ring signatures in [7]. References [7] and [8] also consider ID-based ring signatures.

Manuscript received October 25, 2007; revised May 28, 2008. First published July 25, 2008; current version published April 22, 2009. This work was supported in part by the Spanish Government through Projects TS12007-65406-C03-01 "E-AEGIS" and CONSOLIDER INGENIO 2010 CSD2007-00004 "ARES" and in part by the Government of Catalonia under Grant 2005 SGR 00446. The review of this paper was coordinated by Dr. W. Zhuang.

The authors are with the UNESCO Chair in Data Privacy, Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, 43007 Tarragona, Spain (e-mail: vanesa.daza@urv.cat; josep.domingo@urv.cat; francesc.sebe@urv.cat; alexandre.viejo@urv.cat).

Digital Object Identifier 10.1109/TVT.2008.2002581

B. A Priori Countermeasures

A priori countermeasures attempt to prevent the generation of fake messages. In this approach, a message is not considered valid unless it has been endorsed by a number of vehicles above a certain threshold. Those vehicles must be in a position to confirm what is reported in the message; for a traffic jam announcement, other jammed vehicles are potential endorsers (automatically or after intervention of their drivers); for an “icy road” message, nearby vehicles whose traction system has detected slippery ground can be automatic endorsers. This approach is based on the assumption that most users are honest, and therefore, they will not endorse any message containing false data.

Under this approach, the risk that a collusion of dishonest vehicles reaches the size necessary to generate fake messages always exists. The natural strategy against collusions is to choose a threshold sufficiently high to render successful collusions unlikely. However, this threshold should not be so high that it prevents honest vehicles from sending true announcements in situations with a low density of vehicles.

The *a priori* approach is compatible with driver privacy: since false announcements are thwarted without resorting to punitive actions, unconditional vehicle anonymity is allowable (in contrast, *a posteriori* countermeasures assume that offenders are identified and punished).

The use of an honest majority to prevent generation of fake messages has previously been proposed in [9]–[12]. A brief discussion of those papers is given next.

In [9], a framework is presented to validate received data in VANETs. In this approach, a vehicle receives alerts from different neighbors and compares them to infer the correctness of a certain event. This scheme suffers from high communication overhead due to the lack of aggregation techniques. In addition, the proposed framework has not been empirically tested. Reference [10] presents a contribution that remains quite vague: VANET security issues are identified, some security primitives are enumerated, but no complete protocol is actually described. In [11], a system that evaluates the plausibility of received danger warnings is proposed. This system estimates the trustworthiness of a reported hazard by taking a vote on the received danger messages. The paper provides a simulative analysis of different voting schemes, but privacy remains unaddressed, and security is not completely covered. Finally, [12] describes a detailed protocol deployable in real VANET environments (the authors show this via simulation), which systematically deals with security threats and reduces communication overhead by aggregating messages.

According to the aforementioned discussion, [12] seems the most competitive scheme in the literature on the *a priori* approach; thus, we concentrate on it in what follows. That paper presents three variants offering *a priori* countermeasures against fake messages: *concatenated signatures*, *onion signatures*, and *hybrid signatures*.

In the variant based on *concatenated signatures*, a vehicle generates an announcement and sends it, its signature, and its public-key certificate to a nearby car, which will endorse it by computing its own signature on it. This new signature and

the corresponding public-key certificate will be appended to the frame that will be retransmitted to the next vehicle. An announcement is considered valid after it has been endorsed by at least the number of vehicles determined by the threshold. This approach has several drawbacks.

- 1) It does not offer unlinkability since different signatures made by the same user can be linked through the public key that verifies them. Anonymity is, however, feasible by using pseudonyms.
- 2) Announcement generation is delayed due to the sequential communication pattern (the delay is proportional to the number of endorsing vehicles).
- 3) It requires the verifier to check several signatures upon receiving an announcement (as many verifications as vehicles have endorsed the message). These verifications involve checking the validity of public-key certificates and probably revocation lists as well.

Therefore, there is room for improvement both in terms of privacy and efficiency (communication and computation costs).

The variants based on onion signatures and hybrid signatures are similar and designed to reduce the overall message length. Both variants use the so-called *oversignatures*; instead of appending its signature, each new endorsing car signs the signature by the previous endorsing car (this is called oversigning). In an oversignature, a verifier can check the last endorser’s signature but not the signatures by the previous endorsers. Since this is a serious design flaw, we will only consider the *concatenated signatures* variant for comparison in the rest of this paper.

C. Contribution and Plan of This Paper

In this paper, a proposal is presented following the *a priori* protection paradigm that reduces the verification cost of endorsed messages to one signature verification. Three different privacy-preserving variants of the system are also described to ensure that vehicles volunteering to generate and/or endorse trustworthy announcements do not have to sacrifice their privacy (anonymity and unlinkability). Section II gives some brief background on secret sharing and threshold signatures. Section III presents the new protocol and three privacy-preserving variants of it, which are eventually combined in a compound protocol. Section IV studies the proposed protocol using simulations. Finally, Section V contains some concluding remarks.

II. BACKGROUND

This section gives some minimalistic cryptographic background needed to understand the rest of this paper.

A. Secret Sharing

A secret sharing scheme is a method by means of which a special figure, called a dealer, distributes a secret s among a set $\mathcal{P} = \{P_1, \dots, P_n\}$ of n players. The dealer secretly sends to each player P_i his share s_i of the secret s in such a way that only authorized subsets can recover the secret.

A (t, n) -threshold secret sharing scheme is a particular case in which authorized subsets are those composed of at least

t players. Shamir's threshold secret sharing scheme [13] gives a solution to this problem. Indeed, let \mathbb{Z}_q be a finite field with $q > n$ and $s \in \mathbb{Z}_q$ be the secret to be shared. The dealer picks a polynomial $p(x)$ of degree at most $t - 1$ at random, whose free term is the secret s , that is, $p(0) = s$. The polynomial $p(x)$ can be written as $p(x) = s + \sum_{j=1}^{t-1} a_j x^j$, where $a_j \in \mathbb{Z}_q$ has randomly been chosen.

Each player P_i is assigned a known value $\alpha_i \in \mathbb{Z}_q$. Then, the dealer privately sends to player P_i his share $s_i = p(\alpha_i)$, for $i = 1, \dots, n$.

Therefore, a set $A \subset \mathcal{P}$ of at least t players can recover the secret $s = p(0)$ by interpolating the set of shares they hold, i.e.,

$$s = p(0) = \sum_{P_i \in A} s_i \lambda_i^A = \sum_{P_i \in A} s_i \left(\prod_{P_j \in (A \setminus P_i)} \frac{-\alpha_j}{\alpha_i - \alpha_j} \right).$$

Values λ_i^A are called the Lagrange coefficients. It can be proven that less than t players cannot obtain any information about the secret s .

B. Threshold Signatures

Digital signatures allow to send authenticated and nonrepudiable messages. The message sender is required to have a public/private key pair. Signature generation is an algorithm that takes as input the message m and the sender's private key SK . Its output is the signature $\sigma(m)$ on m . Signature verification is performed by the receiver. Its algorithm takes as input the message m , its signature $\sigma(m)$, and the sender's public key PK . It outputs "yes" or "no" to reflect the validity of $\sigma(m)$. A valid signature convinces the receiver about the integrity of m and is taken as a proof that the message was generated by the authentic sender (the only party knowing SK).

A (t, n) -threshold signature distributes the signing operation among a group of n participants. Each participant in a distributed signature scheme is given a share SK_i of the secret key SK in such a way that to sign a message, every participant computes a partial signature $\sigma_i(m)$ using his share of the secret key. Then, any set of at least t participants can compute a valid signature $\sigma(m)$ on the message by combining their partial signatures. The resulting signature is equivalent to the one that results in the nondistributed case (it is also verifiable using PK). A distributed signature scheme is said to be noninteractive if every participant can compute his partial signature on a message m without interacting with the rest of participants. Signatures in [14]–[17] are examples of noninteractive threshold signature schemes.

For the sake of concreteness, we next recall an efficient threshold signature scheme, namely, the one in [15], which is a distributed version of the signature scheme by Boneh, Lynn, and Shacham (BLS [18]). Both schemes work over Gap Diffie–Hellman (GDH) groups—see original papers for more details. In a nutshell, these signature protocols based on pairings are quite efficient as the signing process only requires hash operations and modular exponentiations, and the verification process requires two pairing computations. In [19], a fast implementation of the Tate pairing computation was given, and the

BLS signature scheme was compared with a Rivest–Shamir–Adleman (RSA) signature on a Pentium III processor at 1 GHz. Using RSA with a modulus length $|n| = 1024$ bits and a private exponent length $|d| = 1007$ bits, signing and verifying took 7.90 and 0.4 ms, respectively. Using the BLS signature with elliptic curves over $\mathbb{F}_{3^{97}}$, signatures were 160 bits long (which yields a similar security as the aforementioned 1024-bit RSA signature), and signing and verifying took 3.57 and 53 ms, respectively. Thus, there exist threshold signatures with reasonable computational cost.

Let \mathbb{G} be a GDH group, $g = \langle \mathbb{G} \rangle$ be a generator of the group, and p be the order of the group. Using methods described in [20], every participant P_i obtains a share SK_i . The set of shares realizes a (t, n) -threshold access structure, that is, t parties can retrieve the secret key SK , whereas less than t cannot obtain any information on the secret key. The retrieval process can be performed by means of Lagrange interpolation and also yields the matching public key $PK = g^{SK}$. To sign a message m , a participant P_i computes his partial signature as $\sigma_i(m) = \mathcal{H}(m)^{SK_i}$ (\mathcal{H} is a public one-way collision-free hash function whose input is a string of arbitrary length and whose output is an element in $\mathbb{G} \setminus \{1\}$) and broadcasts $\sigma_i(m)$. After a set A of at least t participants has broadcast their partial signatures $\sigma_i(m)$ for message m , a standard signature σ for the message can be computed as

$$\sigma(m) = \prod_{i \in A} \sigma_i(m)^{\lambda_i^A} = \mathcal{H}(m)^{\sum_{i \in A} \lambda_i^A SK_i} = \mathcal{H}(m)^{SK}$$

where λ_i^A are the Lagrange coefficients.

C. Privacy in Secret Sharing

In short, an anonymous secret sharing scheme is one where participants can cooperate in the retrieval of the secret while keeping their identity undisclosed (anonymity) and without successive cooperations by the same participant being linkable (unlinkability). Shamir's (t, n) -threshold secret sharing scheme described in Section II-A does not offer unlinkability: Each Lagrange coefficient corresponds to a certain participant P_i and, even if that correspondence is kept secret for anonymity (i.e., by using the underlying α_i as pseudonyms), successive cooperations by the same participant can be linked because the Lagrange coefficient of the participant appears every time. Anonymous secret sharing schemes in the literature present a very high cost that limits their practical applicability [21].

Note that if the secret sharing scheme underpinning a threshold signature protocol is not anonymous, the resulting threshold signature is either linkable (successive partial signatures by a participant can be linked) or requires a trusted third party and is thus unsuitable for a VANET.

III. OUR PROPOSAL

In this section, a new system for secure announcements in VANETs is presented. It uses digital signatures to prevent external attackers from being able to inject false messages and follows the *a priori* approach to thwart fake announcements

sent by internal attackers. An announcement will only be considered valid if it has been endorsed by at least t different vehicles.

A. Nonprivate Protocol

For clarity, let us begin with a protocol that can offer anonymity but not unlinkability.

- *Setup:* During this stage, the carmakers set up a (t, n) -threshold signature scheme, where n is the maximum number of vehicles allowable in the VANET. To do this, the carmakers must agree on a polynomial of degree $(t - 1)$ that will be evaluated at points α_i , for $i = 1$ to n . The range of n points is partitioned into several subranges, each of which is assigned to a carmaker. The number n can be very large without scalability problems. Next, a public key PK and n shares SK_i , $i = 1, \dots, n$, of the secret key SK are generated. Each vehicle P_i is equipped with the public key PK and its secret key share SK_i ; the share SK_i is held in a smart card plugged into the vehicle (tamper resistance is assumed for the card in what follows). When the hash value $\mathcal{H}(m)$ of a message is input, the smart card returns a partial signature on that hash value, that is, $\sigma_i(m) = \mathcal{H}(m)^{SK_i}$. Anonymity is obtained by not linking SK_i with the identity of the vehicle; this makes sense for other reasons too because, smart cards being removable, several smart cards each holding a different secret key share could alternatively be used with the same vehicle (like several cards can be used with a cell phone).
- *Announcement generation:* When a vehicle P_i wishes to send an announcement m , P_i computes the partial signature $\sigma_i(m)$ and broadcasts m and $\sigma_i(m)$. An announcement should only reach vehicles that are close enough to the originating vehicle to be able to check the validity of the announced condition. Since they do not need to reach distant points, announcement messages are not relayed by VANET nodes, and they travel only up to the range of the broadcast technology used (even if a maximum range of 1000 m for car-to-car communication with the Dedicated Short-Range Communication protocol is reported in [22], typical ranges from 300 to 500 m on highways and about 100 m in cities are mentioned in [23]).
- *Announcement endorsement:* If vehicle P_j receives an announcement m (together with the partial signature on it by the announcement originator P_i) and wishes to endorse m , then P_j computes its own partial signature $\sigma_j(m)$ on m and broadcasts $\mathcal{H}(m)$ and $\sigma_j(m)$ to return them to P_i , where $\mathcal{H}()$ is the same hash function used in the signature computation. As in announcement generation, messages with partial signatures are not relayed.
- *Signature composition:* The vehicle P_i that generated an announcement stores m and the partial signatures on m it receives (partial signatures on m are identifiable by the hash $\mathcal{H}(m)$ they carry). Once P_i has collected t different partial signatures on m , it can compute a standard signature $\sigma(m)$ and broadcast it along with m .
- *Announcement reception and verification:* Vehicles in the VANET will only consider as trustworthy those announce-

ments carrying a standard signature that can be verified using the public key PK . The use of the threshold signature scheme provides vehicles with the assurance that such a standard signature can only have been computed if at least t vehicles have endorsed m by computing their partial signature on it. These messages, containing a standard signature, will be relayed by VANET nodes. This way, they will reach distant vehicles, which will benefit from the information in the messages.

The reason for keeping SK_i in a smart card is to prevent the vehicle driver from learning SK_i ; otherwise, t colluding drivers could recover the secret key SK , which would allow any single one of them to sign messages that would be accepted as trustworthy without any endorsement.

In any case, the choice of t is a tradeoff between security and availability. On one hand, t should be high enough so that the probability of there being t or more within-range colluding vehicles who could validly endorse fake messages is reasonably low (security). On the other hand, t should not be so high that finding $t - 1$ additional within-range endorsers is too difficult for an honest announcement generator (availability).

The problem with the aforementioned protocol is that it lacks privacy and, more precisely, unlinkability. This is due to the fact that signature composition requires computing Lagrange coefficients (see Section II-A). Computation of such coefficients requires, in turn, knowledge of the value α_i assigned to each vehicle P_i having contributed a partial signature. Certainly, it can be assumed, and it is assumed that the correspondence between P_i and α_i is withheld (α_i is used as a pseudonym for vehicle P_i), which provides anonymity. However, different partial signatures generated by the same vehicle P_i all use α_i ; thus, they are linkable. Therefore, unlinkability is not achieved.

B. Cost Analysis of the Nonprivate Protocol

In this section we compare the cost of our aforementioned nonprivate protocol with the cost of the concatenated signatures protocol in [12]. Both protocols are nonprivate; so, the comparison is fair. In the next sections, the cost is analyzed in terms of announcement length, announcement generation time, and announcement verification time.

1) *Announcement Length:* In the concatenated signatures protocol in [12], authenticated announcements contain as many signatures and public key certificates as endorsing vehicles; that is, their length is $O(t)$. In our proposal, both the partially signed announcements and the completely signed announcements contain a single signature; that is, the length of announcements is $O(1)$.

Since the aforementioned comparison in O -notation may be misleading for small values of t , we next compare both proposals by taking the constant terms into account. We assume that [12] uses the concatenated signatures protocol with the RSA public key cryptosystem with 1024-bit moduli (thus, digital signatures will be 1024 bits long). Let us consider that the information that is announced is a bits long. The concatenated signatures protocol in [12] requires one signature and one public key certificate from t different signers. We will consider that a digital certificate contains an RSA public key (barely longer

than the 1024-bit modulus if a short public exponent is used), the owner's pseudonym (which could be a 64-bit serial number), and a signature by the Certification Authority (1024 bits). According to that, the total length of an announcement in [12] is $a + t \cdot (3 \cdot 1024 + 64)$ bits. For example, if four endorsing vehicles are required ($t = 4$), this scheme yields an announcement length of $a + 12544$ bits. With the same assumptions, our proposal has a constant announcement length of $a + 160$ bits (we are using the BLS signature scheme). As t grows, the advantage of using our system increases.

2) *Announcement Generation Time*: In [12], vehicles sequentially contribute with their signature to endorse an announcement. This means that a valid message generation takes at least the time necessary for a message to perform $t - 1$ hops plus the time required to compute t digital signatures. This is an $O(t)$ cost. Let j be the time (in milliseconds) necessary for a message to perform one hop. According to the signature generation time reported in Section II-B, a valid message generation in [12] using the RSA cryptosystem with 1024-bit public keys takes $7.90 \cdot t + (t - 1) \cdot j$ ms.

In our protocol, vehicles can endorse a message in parallel. Thus, the delay due to data transmission required to generate a valid message is fixed to the time to perform two hops (one from the generator to within-range endorsers and another from endorsers to the generator) plus the time to compute two BLS signatures. This time is $2 \cdot (j + 3.57)$ ms.

After t endorsement messages have been collected in our protocol, a standard signature is composed by the vehicle originating a message at an $O(t)$ cost (the cost of computing a standard signature from t partial signatures). As can be seen in Section II-B, the cost of this operation is dominated by the exponentiation of each partial signature to its corresponding Lagrange coefficient. The cost of each exponentiation is similar to the cost of computing one digital signature (also consisting of one exponentiation). Thus, the composition time is approximately $t \cdot 3.57$ ms.

The overall generation time with our protocol is $2 \cdot (j + 3.57) + t \cdot 3.57$ ms. This expression can be rewritten as $2 \cdot j + (t + 2) \cdot 3.57$ ms. This is a shorter time than the time required in [12]. As t grows, the advantage of using our system increases.

3) *Announcement Verification Time*: In [12], announcement verification requires checking t signatures and t public key certificates. If certificates are subject to revocation, there is an additional cost related to checking certificate revocation lists (even this cost is not explicitly mentioned in [12]). In any case, the verification cost is $O(t)$.

In our protocol, an announcement is verified by checking one signature. Since the public key PK used for verification is always the same and is stored in the smart card by the carmaker, its validity does not need to be checked. This is an $O(1)$ cost.

Let us now consider the constant terms for greater accuracy. Assume that the RSA and BLS signature schemes are used by [12] and our proposal, respectively. Section II-B details the signature verification time for each signature scheme. This way, announcement verification in [12] takes $2 \cdot 0.4 \cdot t$ ms (the verifier checks the certificate and message signatures sent by each endorsing vehicle). The same operation using our protocol takes 53 ms. Therefore, with those assumptions, our proposal

TABLE I
COST BREAKDOWN AS A FUNCTION OF THE THRESHOLD t
OF THE NONPRIVATE PROTOCOL IN [12] AND THE
NONPRIVATE PROTOCOL IN THIS PAPER

	Protocol [12]	Our protocol
Announcement length	$O(t)$	$O(1)$
Announcement generation time	$O(t)$	$O(t)$
Announcement verification time	$O(t)$	$O(1)$

outperforms [12] only when $t \geq 67$. In practice, t will be usually less than 67 so that [12] will normally be faster than our protocol as far as the computation involved in signature verification goes.

Nonetheless, if the time and communication needed to check certificate revocation lists was taken into account, our proposal would be more efficient, because in [12], a certificate revocation list may need to be checked for each certificate to be verified.

4) *Summary of Cost Analysis*: Table I summarizes the cost of both protocols as a function of the threshold t . The strong points of our proposal are that the following is constant: announcement length and announcement verification time.

If a more accurate analysis of the constant terms is performed (which is necessary when t is small), it turns out that our system still yields shorter announcements and faster announcement generation than [12]. Announcement verification, on the contrary, is faster with [12] at least for the usual (small) values of t .

However, if the cost of checking certificate revocation lists is considered in announcement verification, the picture dramatically changes. Indeed, [12] requires verifying t certificates, which may require checking certificate revocation lists t times. This may be very long as it involves not only computation but also communication. In our proposal, the validity of PK does not need checking, as previously explained in this paper. Thus, when the cost of checking certificate revocation is included, our proposal is also more efficient for announcement verification.

C. Group-Based Private Protocol

In this section, a modification of the previous protocol is described to provide unlinkability. The modification mainly affects the setup phase.

- *Setup*: The n vehicles that form the VANET are divided into r groups, with each group consisting of n/r vehicles (for simplicity, it is assumed that parameters n and r are chosen so that r divides n , but suitable rounding can be used in the general case). The carmakers set up a (t, r) -threshold signature scheme. During this generation, a public key PK and r shares SK_j , $j = 1, \dots, r$, of the secret key SK are generated (one share for each group). Each carmaker keeps a copy of each of the r shares. Each manufactured vehicle P_i is randomly assigned by the carmaker to a group j ; then, it is equipped with the public key PK and the secret key share SK_j assigned to its group (as aforementioned, SK_j is held in a smart card plugged to the vehicle).

This modification causes vehicles belonging to the same group to be assigned the same secret key share. This way, partial signatures cannot be related to a single vehicle but to any member of its group. If groups are large enough, this protocol

provides unlinkability. On the other side, a valid signature $\sigma(m)$ must now be generated not only by any t vehicles but also by vehicles belonging to at least t different groups.

Security, Privacy, and Availability: Parameters t and r of the group-based protocol have an impact on security against fake messages, on privacy, and on availability.

The threshold t should be set high enough so that the probability of there being t or more colluding vehicles who could validly endorse false announcements is reasonably low.

For a choice of t , parameter r must be chosen considering the tradeoff between unlinkability and availability.

- *Unlinkability:* The group size $g := n/r$ must be large enough so that linkability at the group level (which cannot be avoided) does not imply linkability at the vehicle level.
- *Availability:* The number of groups r must be large enough so that, given an announcement, finding t endorsing vehicles from different groups is easy. Thus, $r \gg t$.

By construction, this proposal has the same cost as the nonprivate protocol (see Section III-A).

D. Extended Group-Based Private Protocol

In the previous group-based protocol, it may be difficult in some cases to find a value for r striking a balance between unlinkability and availability. This is the case when the VANET is sparse or consists of an actual number n' of vehicles much less than the maximum allowable number n . Since the group size cannot be too small if unlinkability is to be preserved, the number r of groups has to be small. In those conditions, finding t within-range endorsing vehicles from different groups may be quite challenging.

A solution to mitigate the problem caused by a small r is to use d different threshold signature schemes so that if t within-range endorsing vehicles from different groups cannot be found for the first scheme, they are sought for the second scheme, and so on. The modified setup, announcement generation, endorsement, and signature composition phases are given in the list that follows.

- *Setup:* The n vehicles that form the VANET are divided into r groups, as shown in Section III-C. The carmakers set up d different (t, r) -threshold signature schemes. For $k = 1$ to d , the k th scheme consists of a public key PK^k and r shares SK_j^k , $j = 1, \dots, r$ (one share per group). Each carmaker keeps a copy of all r shares for all d signature schemes. For $i = 1, \dots, n$, each manufactured vehicle P_i is equipped with the public keys (PK^1, \dots, PK^d) and the secret key shares $(SK_{i_1}^1, \dots, SK_{i_d}^d)$, where $i_k \in_R \{1, \dots, r\}$ is the group randomly assigned by the carmaker to P_i for the k th threshold signature scheme. As aforementioned, all secret key shares are held in a smart card.

The only variation in the extended group-based protocol with respect to the previous protocols (nonprivate, group-based) in what concerns the announcement generation, endorsement, and signature composition steps is that now messages in those steps must include a field specifying which threshold signature scheme among the d possible signature schemes is being used in a particular execution.

Announcement generation, endorsement, and signature composition are attempted for the first threshold signature scheme, as shown in Section III-C. If, after a predefined timeout, partial signatures from t different groups have not been collected, announcement generation and endorsement are restarted for the second threshold signature scheme. The process stops when a threshold signature scheme is found, for which endorsements from t different groups can be collected. In the worst case, all d threshold signatures schemes can fail.

Storage requirements at the vehicles are increased. In this case, each vehicle stores d key shares and d public keys (compared to one share and one public key in the previous proposal).

E. Semiprivate Protocol for Sparse VANETs

The protocol in Section III-D is not without drawbacks. Even with d different threshold signature schemes, collecting endorsement from t different groups may fail in very sparse VANETs. A way to circumvent the aforementioned problem is to drop groups but to keep several threshold signature schemes for privacy. The modified protocol is now given in the list that follows.

- *Setup:* The carmakers set up d' different (t, n) -threshold signature schemes. Like in the nonprivate protocol of Section III-A, but for each signature scheme in this protocol, the range of n points corresponding to possible vehicles is partitioned into several subranges, each of which is assigned to a carmaker. For $k = 1$ to d' , the k th scheme consists of a public key PK^k and n shares SK_i^k , $i = 1, \dots, n$ (one share per vehicle). For $i = 1, \dots, n$, each vehicle P_i is equipped with the public keys $(PK^1, \dots, PK^{d'})$ and the secret key shares $(SK_i^1, \dots, SK_i^{d'})$, with share SK_i^k being obtained by evaluating the polynomial of the k th scheme at point α_i^k , where α_i^k is assumed to belong to the subrange of the carmaker of P_i for the k th scheme.
- *Announcement generation:* When a vehicle P_i wishes to send an announcement m , P_i randomly selects one of the d' threshold signature schemes, e.g., scheme k . One can assume that the selection is performed by the smart card in the vehicle so that the selected k is beyond the user's control. Then, P_i computes its partial signature $\sigma_i^k(m)$ on m and broadcasts the announcement and its partial signature. This solution also requires messages to include a field indicating which signature scheme k is being used.
- *Announcement endorsement:* If vehicle P_j receives the announcement m (together with the partial signature on it by the announcement originator P_i) and wishes to endorse m , P_j uses the k th threshold scheme to compute its own partial signature $\sigma_j^k(m)$ on m and broadcasts $\mathcal{H}(m)$ and $\sigma_j^k(m)$, where $\mathcal{H}()$ is the same hash function used in the signature computation.
- *Signature composition:* The vehicle P_i that generated an announcement stores m and the partial signatures on m it receives (partial signatures on m are identifiable by the hash $\mathcal{H}(m)$ they carry). Once P_i has collected t different partial signatures on m , it can compute a standard signature $\sigma^k(m)$ and broadcast it along with m .

- *Announcement reception:* Vehicles in the VANET will only consider as trustworthy those announcements carrying a standard signature that can be verified using a public key PK^k in the set $(PK^1, \dots, PK^{d'})$.

The aforementioned semiprivate protocol requires vehicles to store d' shares and d' public keys.

Security, Privacy, and Availability: As in the previous protocols, the threshold t is the parameter controlling security against insertion of fake announcements.

Unlinkability is related to parameter d' , which is the number of threshold signature schemes set up by the carmaker for this protocol. Provided that the threshold signature scheme is randomly selected, the probability that two successive participations by P_i can be linked is $1/d'$ (this happens if the same threshold signature scheme is selected in both cases). Thus, unlinkability improves with respect to the nonprivate protocol (Section III-A), but it is worse than in the group-based or extended group-based protocols (Section III-C and D, respectively). However, the advantage is increased availability in that there are no constraints on the t vehicles that must endorse an announcement (any t vehicles will do), so that the endorsement process is easier in very sparse VANETs with really few vehicles per area unit.

A way to improve unlinkability is by taking a large d' , which does not affect the announcement verification time. This is different from what happens in the extended group-based protocol if parameter d is increased: there, the signature schemes are tried one after the other until a valid signature is obtained or the d schemes have been tried; thus, a large d may result in longer verification times.

F. Compound Protocol

The protocol in Section III-E can be used as a fallback for the protocol in Section III-D, which, in turn, is a fallback for the protocol in Section III-C. The idea is that vehicles can be set up for all three protocols by the carmaker. The first option to be tried is the group-based protocol. If traffic sparseness is such that partial signatures from t different groups cannot be collected for a certain announcement before a fixed timeout, then the protocol in Section III-D is used. If this does not work either, the protocol Section III-E can be used to get limited unlinkability without increasing the difficulty of collecting endorsements with respect to the nonprivate protocol. According to that, a compound protocol combining the protocols in Sections III-C–E can be specified, as shown in the list that follows.

- 1) Initially, the group-based protocol of Section III-C is used. Note that this protocol is a particular case of the extended group-based protocol, where there is only one (t, n) -threshold signature scheme in use. Thus, hereafter, we will consider this step as a part of the next step, where the extended group-based protocol is used. (In what follows, we will only refer to the extended group-based protocol and the semiprivate protocol. This also applies to the simulation results, which will be presented in Section IV.)
- 2) If a complete signature cannot be constructed before a certain timeout, the extended group-based system of

Section III-D is launched. Construction of a complete signature by means of d different (t, n) -threshold signature schemes is attempted. The timeout in use depends on the value t (the number of different partial signatures required to compute a standard signature). For each unit increase of threshold t , the timeout increases by β ms. Each of the d signature schemes is tried in sequence until a complete signature is constructed or the timeout expires; thus, at most $d \times \text{timeout}$ ms are spent on the extended group-based system.

- 3) If the extended group-based system does not work either, the semiprivate protocol (see Section III-E) is tried.

Compound Setup Phase: The compound protocol is composed of three schemes. In previous sections, we have presented the setup phase for each of these schemes. We next explain the compound setup phase when deploying such a system in a real environment.

Let us consider the coexistence of m carmakers in a certain area. The i th carmaker produces v_i hundreds of thousands of vehicles per year. According to the European Environment Agency [24], the EU-15 area had about 170 millions of vehicles in 2004. Although the carmakers produce $v_1 + \dots + v_m$ hundreds of thousands of new cars each year, there is also a large quantity of old vehicles that are eliminated in the same period. Therefore, the size of the vehicle fleet in a certain area does not undergo a strong increase from year to year. The value n is the maximum number of vehicles allowable in the system covering the area. The only assumption on n is that it cannot be greater than the cardinality of the group used to construct the BLS signature scheme. For cryptographic security reasons, this cardinality should be at least 2^{160} . Thus, we can set a value for n close to this upper limit. Such a huge n ensures that we will never run out of key shares. As it can be seen in Section II, a huge n can be used without any negative impact on the system performance.

Our system requires a governmental authority GA in the geographical area of deployment to ensure a correct setup phase. Note that this authority is no longer needed when executing the compound protocol. The only role of the authority is to coordinate share distribution among the vehicles produced by different carmakers. This way, GA establishes d signature schemes and the number r of groups of vehicles in the area. According to that, each signature scheme generates r shares. Each share is linked to one group. Additionally, GA partitions the n possible vehicles into several subranges, each of which is assigned to a carmaker. It also establishes d' different threshold signature schemes. Each one generates n shares. Note that a certain carmaker receives the shares that correspond to its assigned subrange of n .

Now, let us consider that a certain vehicle P_i is manufactured. This car has to be set up by its carmaker for both extended group-based and semiprivate protocols. This process has individually been explained in Sections III-D and E.

We next summarize it in the list that follows.

- *Extended group-based protocol:* For each signature scheme $k = 1, \dots, d$, P_i is randomly assigned by the carmaker to a group j_k (where $j_k \in \{1, \dots, r\}$), and it is equipped with the share corresponding to group j_k .

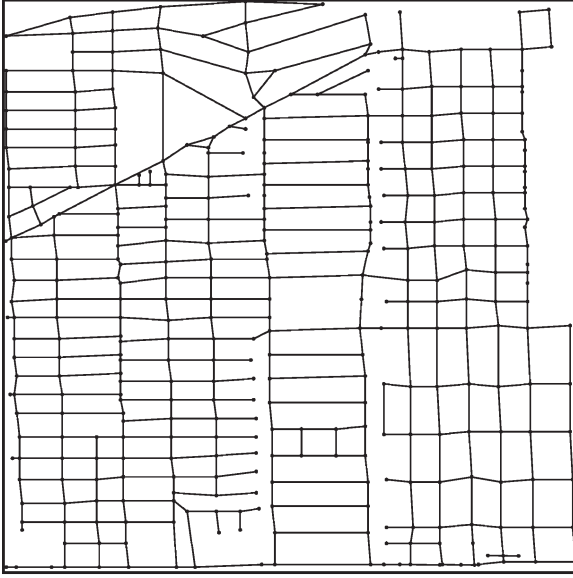


Fig. 1. Simulation scenario.

- *Semiprivate protocol*: P_i is equipped with shares $(SK_i^1, \dots, SK_i^{d'})$, where the share SK_i^w is obtained by evaluating the polynomial of the w th scheme at point α_i^w , which is assumed to belong to the subrange of the carmaker of P_i .

The compound setup phase we have presented relies on the assumption that an authority GA exists, which coordinates share distribution. An open problem is to devise a compound setup phase that can work when no GA is available.

IV. SIMULATION

Our scheme for secure vehicle-generated announcements over VANETs was simulated in a realistic environment, where the range of car-to-car broadcasts was assumed to be 100 m (the worst-case urban range according to [23]).

The goal of our simulations is to observe the performance of the compound protocol explained in Section III-F. This protocol requires a timeout that depends on values β and t . In our simulations, we have fixed β to 50 ms. According to that, $t = 4$ represents a timeout of 200 ms.

A. Simulation Setup

The network simulator *ns-2* [25] was used. The VANET scenario was built using the scenario generator presented in [26]. The road network considered covered an area of $2.4 \text{ km} \times 2.4 \text{ km}$ and is shown in Fig. 1.

In our simulations, the primary indicator examined is the probability for a certain announcement to get validated. An announcement is validated when its standard signature is constructed from t different partial signatures generated by t different cars. Those vehicles can belong to t different groups or to only one group, depending on whether the extended group-based protocol or the semiprivate protocol is used.

A second indicator taken into account is the average number of different (t, n) -threshold signature schemes, which are used

when applying the extended group-based protocol. This indicator determines the time needed to validate the announcements.

Both indicators are essential to evaluate whether our scheme is usable in real VANETs.

In Section IV-B, the optimal values for the parameters used in our system are studied. The goal of that study is to select the values for parameters based on the two indicators previously stated for a wide range of vehicle densities. When the system is running, parameter values cannot be easily modified; thus, a parameter choice must be made which works well under several road conditions. The lessons learned from the simulations are summarized in Section IV-C.

The results given in what follows are average values obtained from 100 executions performed for each parameter choice.

B. Parameter Selection

Vehicle density is expressed in vehicles per square kilometer. This value is changed by varying the total number of vehicles in the scenario represented in Fig. 1.

Let t stand for the minimum number of vehicles needed to validate an announcement. Each vehicle should belong to a different group when using the extended group-based protocol. Under the semiprivate protocol, there are no group constraints.

Table II shows the average probability p_1 of a certain announcement to be validated using the extended group-based protocol for fixed r and several values of t . The value i indicates the average number of different threshold signature schemes tried (each one is used until a timeout occurs) to validate the announcement with the extended group-based protocol. When the number of different threshold signature schemes tried for a certain announcement reaches the number d of available schemes without the announcement being validated under any of them, the semiprivate protocol is launched. We have set $d = 3$ given the values i obtained in preliminary simulations. This will be further explained in the following discussion.

The value p_2 is the average probability of validating the announcement under the semiprivate protocol when the extended group-based protocol fails. Note that the semiprivate protocol is a tolerable fallback for low vehicle densities. For higher vehicle densities, the probability p_1 of successful validation with the extended group-based protocol is already very high; therefore, the instances in which the semiprivate protocol is used as a fallback are very difficult instances (e.g., very sparse locations); this explains the near-zero p_2 values for higher densities. In addition, the N/A value for p_2 means that there was no need to call the semiprivate protocol. We have set $d' = 20$ as the number of different threshold signature schemes available in the semiprivate protocol; this should yield a good tradeoff between unlinkability and implementation cost in the vehicles.

The results in Table II are given as a function of vehicle density and the minimum number of validating groups t . For this experiment, the number of groups of vehicles was set to $r = 10$. The dependence on this value r will be studied in Table III.

It can be observed in Table II that both validation probabilities p_1 and p_2 decrease as t increases, no matter whether the VANET is sparse or dense. This is not surprising because

TABLE II
AVERAGE VALIDATION PROBABILITY p_1 AND AVERAGE NUMBER i OF DIFFERENT THRESHOLD SIGNATURE SCHEMES TRIED FOR THE EXTENDED GROUP-BASED PROTOCOL FOR CONSTANT NUMBER OF GROUPS $r = 10$. AVERAGE VALIDATION PROBABILITY p_2 FOR THE SEMIPRIVATE PROTOCOL WHEN THE EXTENDED GROUP-BASED PROTOCOL FAILS. RESULTS ARE GIVEN AS A FUNCTION OF VEHICLE DENSITY AND THE MINIMUM NUMBER OF VALIDATING VEHICLES t

Vehic. dens.	$t = 4$			$t = 5$			$t = 6$		
	p_1	i	p_2	p_1	i	p_2	p_1	i	p_2
6.94	0.48	1.67	0.07	0.24	1.81	0.12	0.00	N/A	0.04
8.68	0.64	1.69	0.02	0.33	1.74	0.05	0.04	2.00	0.04
12.15	0.70	1.25	0.01	0.40	1.80	0.04	0.20	1.60	0.11
15.62	0.72	1.22	0.00	0.44	1.70	0.04	0.36	1.85	0.10
17.36	0.76	1.17	0.00	0.68	1.59	0.09	0.52	1.57	0.08
24.31	0.94	1.14	0.00	0.76	1.53	0.02	0.72	1.67	0.11
31.25	0.96	1.13	0.00	0.92	1.17	0.00	0.81	1.51	0.05
38.19	0.96	1.09	0.00	0.94	1.08	0.00	0.89	1.48	0.00
45.14	1.00	1.00	N/A	0.94	1.09	0.00	0.92	1.33	0.00
52.08	1.00	1.00	N/A	1.00	1.00	N/A	0.96	1.26	0.00

TABLE III
AVERAGE VALIDATION PROBABILITY p_1 FOR THE EXTENDED GROUP-BASED PROTOCOL AND AVERAGE VALIDATION PROBABILITY p_2 FOR THE SEMIPRIVATE PROTOCOL WHEN THE EXTENDED GROUP-BASED PROTOCOL FAILS; THE AVERAGE GROUP SIZE g IS ALSO SHOWN. RESULTS ARE GIVEN AS A FUNCTION OF VEHICLE DENSITY AND NUMBER OF GROUPS r FOR CONSTANT THRESHOLD $t = 4$

Vehic. dens.	$r = 8$			$r = 10$			$r = 15$			$r = 20$		
	p_1	p_2	g	p_1	p_2	g	p_1	p_2	g	p_1	p_2	g
6.94	0.33	0.08	5.0	0.48	0.07	4.0	0.54	0.01	2.7	0.56	0.00	2.0
8.68	0.38	0.05	6.2	0.64	0.02	5.0	0.66	0.03	3.3	0.66	0.00	2.5
12.15	0.52	0.04	8.7	0.70	0.01	7.0	0.76	0.00	4.7	0.74	0.00	3.5
15.62	0.67	0.00	11.2	0.72	0.00	9.0	0.76	0.00	6.0	0.88	0.00	4.5
17.36	0.71	0.00	12.5	0.76	0.00	10.0	0.88	0.00	6.7	0.93	0.00	5.0
24.31	0.86	0.00	17.5	0.94	0.00	14.0	0.96	0.00	9.3	0.99	0.00	7.0
31.25	0.93	0.00	22.5	0.96	0.00	18.0	1.00	N/A	12.0	1.00	N/A	9.0
38.19	0.94	0.00	27.5	0.96	0.00	22.0	1.00	N/A	14.7	1.00	N/A	11.0
45.14	0.97	0.00	32.5	1.00	N/A	26.0	1.00	N/A	17.3	1.00	N/A	13.0
52.08	1.00	N/A	37.5	1.00	N/A	30.0	1.00	N/A	20.0	1.00	N/A	15.0

validation is “easier” for smaller t ; however, the price paid is that for smaller t , the trustworthiness of a validated message is lower. Following this argument, it is also expected that for very sparse networks (vehicle density of 6.94) and high t values (for instance, $t = 6$), the extended group-based protocol is unable to validate a single announcement; in fact, not even the semiprivate protocol properly works in that setting ($p_2 = 0.04$ for a vehicle density of 6.94). As a tradeoff between trustworthiness and availability, it is suggested to take $t = 4$ or $t = 5$, depending on the desired trustworthiness level for the announcements. In fact, $t = 5$ is the highest reasonable value because, although $t = 6$ works fine for dense VANETs (vehicle density above 38.19), it does not for medium-density ($p_1 = 0.52$ for a density of 17.36) and sparse VANETs. Since a threshold that properly works under several road conditions must be chosen, it is better to select $t < 6$. In what follows, $t = 4$ is taken.

Simulation shows that the average number i of different threshold signature schemes tried by the extended group-based protocol decreases when the vehicle density increases and increases when the threshold t increases. All in all, usually $i \leq 2$ whenever validation is successful, which is the usual outcome for medium- to high-density VANETs and moderate threshold ($t = 4$). For very sparse networks, validation mainly relies on the semiprivate protocol; so, we can choose the number d of signature schemes for the extended group-based protocol by considering only medium- to high-density VANETs. Thus, a choice of $d = 3$ is fair enough and is assumed in what follows;

this implies that at most $3 \times \text{timeout}$ milliseconds are spent on the extended group-based protocol (as aforementioned, for $t = 4$, we consider $\text{timeout} = 200$ ms; so, the overall time spent on the extended group-based protocol is 600 ms).

Table III shows the average probability p_1 of a certain announcement being validated using the extended group-based protocol for fixed t and several values of r . If this protocol fails, the semiprivate fallback is launched. The value p_2 represents the average probability of validating a message with the semiprivate protocol when the extended group-based protocol fails. Finally, the value g represents the average group size. All results are given as a function of vehicle density and the number of groups of vehicles r . A value of r that works fine for very different vehicle densities must be set. In addition, r must be chosen considering the tradeoff between unlinkability and availability (see related discussion in Section III-C): The value r should be greater than t to guarantee availability (i.e., so that finding t endorsing vehicles from different groups is easy). However, a big r implies that the group size g is small ($g := n/r$). This way, the unlinkability of a certain vehicle is poor. In contrast, for a small r , the unlinkability of a certain vehicle is very high, but the validation probability decreases. Table III reflects the availability problems of the system in very sparse VANETs when a certain unlinkability level is demanded. More specifically, we can observe that with a vehicle density of 6.94 and an average group size $g = 5.0$ (which occurs when $r = 8$), the probability p_1 of a certain announcement to be validated is 0.33. Note that larger group sizes (which imply $r \ll 8$) will

yield worse availability results. When availability problems arise, the system resorts to the semiprivate protocol (which is less good in terms of privacy, unless d' is extremely high).

According to the aforementioned considerations, $r = 10$ is taken as a reasonable tradeoff between unlinkability and availability for all vehicle densities.

Note: As mentioned in Section III-C, unlinkability is proportional to the group size g . One might object that the average group size in the simulations is small, which is true because the small geographical area considered ($2.4 \text{ km} \times 2.4 \text{ km}$) can only accommodate a small number of vehicles. However, the purpose of the simulation is to evaluate the validation probability, which is independent of the group size (it only depends on the threshold t , the number of groups r , and the vehicle density). In a real scenario (e.g., the EU-15 area with 170 million vehicles mentioned in Section III-F-1), the same t and r values used in the simulations can be employed, which will result in a very large group size g guaranteeing high unlinkability.

C. Lessons Learned From the Simulation

The probability of successful validation depends on the threshold t , the number of groups r , and the vehicle density, regardless of the group size. For a fixed density, the greater r with respect to t , the higher the success probability. The closer r is to t , the lower the success probability.

All simulations performed reflect that with the parameter selection used ($t = 4$, $r = 10$, and $d = 3$), our proposal provides message trustworthiness and vehicle unlinkability under different road conditions. Results show that our scheme performs best in medium- to high-density VANETs (densities from 12.15 to 52.08). Nevertheless, it also works fair enough in very sparse environments.

- For a vehicle density 6.94, our scheme achieves a success probability $p_1 = 0.48$ in announcement validation with the extended group-based protocol. In the cases when this protocol fails, the semiprivate protocol works with a probability $p_2 = 0.07$.
- For a vehicle density 8.68, the success probability with the extended group-based protocol increases to $p_1 = 0.64$. The semiprivate protocol used as a fallback earns an additional $p_2 = 0.02$.

The low success in validation for sparse VANETs should be put into context. In an area with very low traffic, it is often less critical to get announcements on road conditions, as there is hardly anyone who can benefit from them.

V. CONCLUSION

In this paper, a new system has been presented for secure vehicle-generated announcements on VANETs that relies on *a priori* measures against internal attackers (vehicles in the VANET sending fake messages). Due to the use of threshold signatures, our system outperforms previous proposals in message length and computational cost.

However, it would be very unfair if vehicles and drivers volunteering to cooperate in generating trustworthy announcements could be tracked and saw their privacy diminished. Three

different variants of the system have been proposed to achieve unlinkability without losing trustworthiness: The first variant is a special case of the second variant and is better suited to dense VANETs, whereas the second and third variants can be used as fallbacks for sparse VANETs. This naturally leads to combining the three variants in a compound protocol.

ACKNOWLEDGMENT

The authors would like to thank Ú. González-Nicolás for programming the required simulations. The authors are with the UNESCO Chair in Data Privacy, but they are solely responsible for the views expressed in this paper, which do not necessarily reflect the position of UNESCO nor commit that organization.

REFERENCES

- [1] F. Dötzer, *Privacy Issues in Vehicular Ad Hoc Networks*, vol. 3856. New York: Springer-Verlag, 2006, pp. 197–209.
- [2] M. Raya, P. Papadimitratos, and J.-P. Hubaux, “Securing vehicular communications,” *Wireless Commun.*, vol. 13, no. 5, pp. 8–15, Oct. 2006.
- [3] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” *J. Comput. Secur.—Special Issue on Security of Ad Hoc and Sensor Networks*, vol. 15, no. 1, pp. 39–68, Jan. 2007.
- [4] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, “Eviction of misbehaving and faulty nodes in vehicular networks,” *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.
- [5] F. Armknecht, A. Festag, D. Westhoff, and K. Zeng, “Cross-layer privacy enhancement and non-repudiation in vehicular communication,” in *Proc. 4th WMAN*, Bern, Switzerland, Mar. 2007.
- [6] J. Guo, J. P. Baugh, and S. Wang, “A group signature based secure and privacy-preserving vehicular communication framework,” in *Proc. Mobile Netw. Veh. Environ.*, 2007, pp. 103–108.
- [7] X. Lin, X. Sun, P.-H. 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.
- [8] C. Gamage, B. Gras, and A. S. Tanenbaum, “An identity-based ring signature scheme with enhanced privacy,” in *Proc. IEEE SecureComm Conf.*, 2006, pp. 1–5.
- [9] P. Golle, D. Greene, and J. Staddon, “Detecting and correcting malicious data in VANETs,” in *Proc. 1st ACM Int. Workshop Veh. Ad Hoc Netw.*, 2004, pp. 29–37.
- [10] B. Parno and A. Perrig, “Challenges in securing vehicular networks,” in *Proc. ACM Workshop Hot Topics Netw.*, 2005.
- [11] B. Ostermaier, F. Dötzer, and M. Strassberger, “Enhancing the security of local danger warnings in VANETs—A simulative analysis of voting schemes,” in *Proc. 2nd Int. Conf. Availability, Rel. Security*, 2007, pp. 422–431.
- [12] M. Raya, A. Aziz, and J.-P. Hubaux, “Efficient secure aggregation in VANETs,” in *Proc. 3rd Int. Workshop VANET*, 2006, pp. 67–75.
- [13] A. Shamir, “How to share a secret,” *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.
- [14] V. Shoup, “Practical threshold signatures,” in *Proc. Advances Cryptology—Eurocrypt*, 2000, vol. 1807, pp. 207–220.
- [15] A. Boldyreva, “Threshold signatures, multisignatures and blind signatures based on the Gap-Diffie–Hellman-group signature scheme,” in *Proc. Public Key Cryptography*, 2003, vol. 2567, pp. 31–46.
- [16] P. A. Fouque and J. Stern, “Fully distributed threshold RSA under standard assumptions,” in *Proc. Asiacrypt*, 2001, vol. 2248, pp. 310–330.
- [17] I. Damgård and M. Krawczyk, “Practical threshold RSA signatures without a trusted dealer,” in *Proc. Advances Cryptology—Eurocrypt*, 2001, vol. 2045, pp. 152–165.
- [18] D. Boneh, B. Lynn, and H. Shacham, “Short signatures from the Weil pairing,” in *Proc. Advances Cryptology—Asiacrypt*, 2001, vol. 2248, pp. 514–532.
- [19] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott, “Efficient algorithms for pairing-based cryptosystems,” in *Proc. Advances Cryptology—Crypto*, 2002, vol. 2442, pp. 354–368.
- [20] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, “Robust threshold DSS signatures,” in *Proc. Advances Cryptology—Eurocrypt*, 1996, vol. 1070, pp. 354–371.

- [21] C. Blundo and D. R. Stinson, "Anonymous secret sharing schemes," *Discrete Appl. Math.*, vol. 77, no. 1, pp. 13–28, 1997.
- [22] N. M. Rabadi and S. M. Mahmud, "Performance evaluation of IEEE 802.11a MAC protocol for vehicle intersection collision avoidance system," in *Proc. CCNC*, 2007, pp. 54–58.
- [23] I. Berger, "Standards for car talk," *IEEE The Institute*, vol. 31, no. 1, p. 1 and p. 6, Mar. 2007.
- [24] Eur. Environ. Agency. [Online]. Available: <http://www.eea.europa.eu>
- [25] *The Network Simulator—ns*. [Online]. Available: http://nsnam.isi.edu/nsnam/index.php/Main_Page
- [26] A. K. Saha and D. B. Johnson, "Modeling mobility for vehicular ad hoc networks," in *Proc. 1st Int. Workshop VANET*, 2004, pp. 91–92.



Vanesa Daza received the M.Sc. degree in mathematics from the University of Barcelona, Barcelona, Spain, in 1999 and the Ph.D. degree in mathematics from the Technical University of Catalonia, Barcelona, in 2004.

She joined a crypto-based security company as a Senior Researcher. Afterward, she held a post-doctoral position with the CRISES Research Group, Rovira i Virgili University, Tarragona, Spain, where she is currently a Lecturer. She has authored more than 30 papers published in international journals

and conference proceedings. She is the holder of two international patents. Her research interests are mainly related to distributed cryptography and its applications.



José Domingo-Ferrer (SM'02) received the M.Sc. degree in mathematics from the Universidad Nacional de Educación a Distancia, Madrid, Spain, and the M.Sc. and Ph.D. degrees (with honors) in computer science from the Autonomous University of Barcelona, Bellaterra, Spain, in 1988 and 1991.

He is a Full Professor of computer science with Rovira i Virgili University, Tarragona, Spain, where he holds the UNESCO Chair in Data Privacy. In 2004, he was a Visiting Fellow with Princeton University, Princeton, NJ. He has been the Coordinator

of the EU FP5 project CO-ORTHOGONAL and of several Spanish- and U.S.-funded research projects. He currently coordinates the CONSOLIDER "ARES" team on security and privacy, which is one of Spain's 34 strongest research teams. He has authored more than 200 publications, one of which became an ISI highly cited paper in early 2005. He is the holder of three patents. His fields of activity are data privacy, data security, and cryptographic protocols.

Prof. Domingo-Ferrer has chaired or cochaired nine international conferences and has served on the program committees of more than 60 conferences on privacy and security. He is a Co-Editor-in-Chief of the *Transactions on Data Privacy*. He is an Associate Editor of three international journals. He was a corecipient of a research prize from the Association of Telecom Engineers of Catalonia in 2003. He was also a recipient of the Outstanding Graduation Award from the Autonomous University of Barcelona in 1988 and The Outstanding Young Person (TOYP) Award from the Junior Chambers of Catalonia in 2004.



Francesc Sebé received the M.Sc. degree in computer engineering from Rovira i Virgili University, Tarragona, Spain, in 2001 and the Ph.D. degree in telematics engineering from the Technical University of Catalonia, Barcelona, Spain, in 2003.

He is currently an Associate Professor of telematics engineering with Rovira i Virgili University. In 2004, he was a Visiting Researcher with the Laboratoire d'Analyse et d'Architecture des Systèmes, Centre National de la Recherche Scientifique (LAAS-CNRS), Toulouse, France. He has participated

in several European- and Spanish-funded research projects. He has authored more than 50 international publications. His fields of interest are cryptography and information privacy.

Prof. Sebé was a corecipient of a research prize from the Association of Telecom Engineers of Catalonia in 2003.



Alexandre Viejo received the M.Sc. degree in computer engineering from Rovira i Virgili University, Tarragona, Spain, in 2005, the Master's degree in telematics engineering from the Technical University of Catalonia (UPC), Barcelona, Spain, in 2007, and the Master's degree in computer engineering and security from Rovira i Virgili University, where he is currently working toward the Ph.D. degree in computer engineering.

His research interests are in cryptography and information privacy.