SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks. 2008; **1**:1–13
Published online in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/sec.28

Mobile anonymity of dynamic groups in vehicular networks

Yong Xi*,†, Weisong Shi and Loren Schwiebert
Department of Computer Science, Wayne State University, Detroit, M.I. 48202, U.S.A.

Summary

Vehicular networks are an emerging network to improve safety, efficiency, and convenience of the existing transportation system. In order to preserve privacy in vehicular networks, it is desirable to keep users anonymous. In this paper, we argue that existing approaches, for example, *ring singature* and *anonymous authentication*, are susceptible to intersection attack in vehicular networks, resulting in reduced anonymity, even no anonymity. To quantify the achievable anonymity, we first define a graph-based model called *mobile anonymity* for a general dynamic environment. We show that under this model, anonymity can be achieved on the system level as long as the constructed anonymity graph is strongly connected. We then extend this model into vehicular networks by applying it to ring signature and anonymous authentication in vehicular networks. We propose two strategies, the random (RND) strategy and the latest-preferred (LPR) strategy, and evaluate them *via* simulation using the C3 simulator. The results show that it is promising to apply RND strategy in vehicular networks. Copyright © 2008 John Wiley & Sons, Ltd.

KEY WORDS: mobile anonymity; authentication; vehicular network; location privacy; traffic analysis; anonymity graph

1. Introduction

Each year, over six million crashes occur on U.S. highways, kill more than 42 000 people, injure approximately three million others, and cost more than $230 billion per year. To reduce the number and severity of these crashes, intelligent vehicle initiative (IVI) was launched in 1998. Over the course of 8 years, numerous advanced vehicle safety technologies have grown out of the initiative [1]. For example, to prevent intersection collision, a dynamic warning light has been demonstrated over an intersection if the laser sensor detects an incoming intersecting vehicle in a 2003 national IVI meeting.

An emerging application is vehicle infrastructure integration (VII) planned by the U.S. Department of Transportation (USDOT) in the coming years [2]. Its goal is to provide a communication link between vehicles on the road and between vehicles and roadside infrastructure to improve safety, efficiency, and convenience of the transportation system. In U.S., directed short range communication (DSRC) is the standardized protocol for this communication link, working in the 5.9 GHz band allocated by FCC.

In the U.S., it is expected that the deployment decision for VII will be made in late 2008. Once it is approved, the following coordinated deployments of the communication technologies can be expected: in all

*Correspondence to: Yong Xi, Wayne State University, 5143 Cass Avenue, 431 State Hall, Detroit, M.I. 48202, U.S.A.

†E-mail: yongxi@wayne.edu

vehicles by the automotive industry; and on all major U.S. roadways by the transportation public sector. In the following discussion, we denote the network that is enabled by VII vehicular network.

1.1. Potential Applications

Applications that have been proposed for vehicular networks are roughly categorized into two classes. The first class is safety application. The second class is traffic information application. US National Highway Traffic Safety Administration (NHTSA) and the Vehicle Safety Communications Consortium (VSCC) of Crash Avoidance Metrics Partnership (CAMP) have chosen the following eight high-priority vehicular safety applications [3]: Traffic Signal Violation Warning, Curve Speed Warning, Emergency Electronic Brake Lights, Pre-Crash Warning, Cooperative Forward Collision Warning, Left Turn Assistant, Lane Change Warning, and Stop Sign Movement Assistance.

In literature, various safety applications have been addressed by academic community such as collision avoidance application [4], intersection collision warning [5,6], traffic merging [7], adaptive traffic light [8].

Traffic information applications target improved traffic information dissemination. Examples include TrafficView [9], Self-Organizing Traffic Information System (SOTIS) [10], and parking space finder [11], etc.

1.2. Security Requirements

Both classes of applications exhibit unique characteristics on security and privacy. Safety applications require high-fidelity information being exchanged in real-time. IEEE 1609.2 standard on secure message formats suggests the use of a Public Key Infrastructure [12]. However, as pointed out by Studer *et al*. [13]: 'identification of vehicles is of little importance to VANET safety applications.' 'but location and movement of the signer needs to be verified.' Thus, location information needs to be as precise as possible.

However, the usage of this location is limited to local neighborhood as safety applications rely heavily on single-hop broadcast communication with nearby vehicles and infrastructure [3]. Thus, it is not necessary to expose location information over long distance. To protect location privacy, this location information should be used only within short distance and period. Studer *et al*. proposed an identity-free location verification scheme in Reference [13]. Their protocol is an anonymous protocol since no identity is exposed.

Various traffic information is used to improve transportation system efficiency. Traditional traffic information system uses different sensors, such as inductive loop, fiber optical sensor line, Doppler Radar speed sensor, magnetic sensor, piezoelectric sensor, and traffic video camera, etc. The information collected include vehicle count, vehicle speed, vehicle density, vehicle type, vehicle weight, etc. It should be noted that although there are initial efforts of investigating re-identification of vehicles [14–16], it is only used for travel time estimation in specific road segments and far from pervasive surveillance.

An alternative to in-road sensors is to use a portion of vehicles as 'mobile probes' into traffic flows [17]. This portion of vehicles can be public transportation vehicles, patrol cars, etc. SOTIS [10] generalized this concept by requiring such vehicles participate in a self-organizing *ad hoc* network with Inter-Vehicle Communication. To efficiently distribute traffic information and form a consensus from the information collected, various aggregation techniques have been proposed in References [9,10,18,19], etc. To deal with cheaters, security mechanisms were proposed in References [18,20,21] to perform validation and provide accountability.

To enable the pervasive deployment set in VII, it is desirable to alleviate users' privacy concerns by protecting user anonymity. Although conditional anonymity have been the focus of recent research efforts [22–24], we argue that unconditional anonymity is a useful concept in vehicular networks and can coexist with conditional anonymity.

Ring signature is a cryptographic primitive to provide unconditional anonymity for sending out information. A realization of ring signature in vehicular network has been proposed by Gamage *et al*. for reporting accidents [25]. In a similar way, a realization of anonymous authentication proposed by Sha *et al*. enables the use of interactive protocols with the designated infrastructure [26]. In both schemes, vehicles dynamically share their public keys to construct anonymous proofs. Both schemes integrate with public key infrastructure seamlessly.

However, the anonymity provided in those protocols is computational anonymity. In vehicular networks, both protocols may be susceptible to attacks through traffic analysis. For example, the unique set of public keys used by a vehicle may enable the system to infer its traveling trajectory. The trajectory may expose its

DOI: 10.1002/sec

identity through its starting location or destination. A natural modification is to let a vehicle use different sets of public keys. Even so, its identity may still be narrowed down to the intersection of those sets, thus reducing its anonymity.

In this paper, we set out to investigate the achievable anonymity by the above mentioned unconditional anonymity schemes in vehicular networks. We propose that vehicles on the road cooperatively share their public keys so that the sets of public keys used by different vehicles have a great probability to intersect. We derive the necessary conditions to preserve anonymity and show by simulation that without any strong synchronization protocol, anonymity can still be very well preserved given properly chosen parameters at each vehicle. Assume that drivers are selfish, they will tend to choose the proper parameters. Thus, the anonymity across the system will be very well preserved. To facilitate discussion, we propose to use *mobile anonymity* to denote the achievable anonymity. Note that *mobile anonymity* is not computational anonymity. It is rather a system-level anonymity.

The paper is organized in the following way. Section 2 discuss related work. Ring signature and anonymous authentication in vehicular networks are briefly reviewed in Section 3. We define the generalized *Mobile Anonymity* in Section 4. In Section 5, we discuss its application to anonymous authentication in vehicular networks. Section 6 presents our simulation results. We conclude our paper in Section 7.

2. Related Work

2.1. Privacy in Vehicular Networks

The privacy in vehicular networks is roughly categorized into two classes: implicit location privacy and explicit location privacy. Implicit location privacy deals with location information disclosure through the authentication [27–31]. The main principal in preserving the implicit location privacy is to use different credentials at different locations and break the mobile path into unlinkable segments.

Raya and Hubaux design a key changing algorithm to preserve anonymity and minimize the storage costs of the public keys [28]. Dötzer introduces another layer of authentication thus separates service usage from identity [29]. Choi *et al*. propose a two tier of hash chain-based pseudonyms to obscure the vehicles' identities [30]. In Reference [31], Sampigethaya *et al*. focus more on the system issues.

In the above cases, the location information of each vehicle is intact. It is rather the identity associated with a specific location that is protected. Explicit location privacy instead protects the location information [32,33]. The location information of one vehicle is mixed into location information from a group of vehicles. Hoh *et al*. [32] shuffles location samples from different vehicles within a local area so that a trajectory cannot be correctly identified [32]. Gedik and Liu propose a k-anonymity model in which a message from one vehicle is mixed with at least $k-1$ messages chosen from a minimal bounding box [33].

In References [27,28,34,35], system design, attack models, and general security mechanisms, and protocols are discussed. Recently, a number of research efforts have been focusing on identity management in vehicular networks as it appears to be a central issue in security and privacy in vehicular networks. To provide unlinkability in vehicular networks, pseudonymity was proposed and investigated in References [36–39]. Group signature presents an ideal candidate to provide security, accountability, and privacy at the same time in vehicular networks [22–24]. Another approach based on key-escrow was proposed in Reference [40]. These are promising methods to provide conditional anonymity. Crescenzo *et al*. proposed several interesting anonymity notions in Reference [41]. Their anonymity notions are also conditional, based on the ability to access sensitive information. We investigate unconditional anonymity, which can be applied with specific applications.

2.2. Anonymous Authentication

Several anonymous authentication schemes have been proposed in recent years [42–46]. Reference [43] enables a user to demonstrate its membership in an arbitrary subset. The identify of the user can be revealed with an escrow key. References [42,44,46] instead provide total anonymous authentication protocols in which nobody can reveal users' identities. In Reference [42], the anonymity is unconditional. In References [44,46], the anonymity is unconditional only if the anonymous credentials is used less than a constant times. In the above work, the group is centrally constructed and distributed to users. Reference [45] proposes an anonymous identification protocol in an *ad hoc* group that is formed through mutual agreement among a group of users. These protocols focus on computational anonymity. They can be adapted into vehicular network by combining with the result in this paper.

2.3. Mobile Anonymity

In Reference [47], Kong *et al.* used the term mobile anonymity in investigating the impact of different network behaviors to communication anonymity in mobile *ad hoc* networks. They also discussed the possible disclosure of location privacy through communication pattern. Our target is to preserve identity anonymity when the source of the communication is known and protect its location privacy when it moves through the road network. We do not try to conceal the communication itself.

3. Background

In this section, we give a brief overview of the two mentioned protocols providing unconditional anonymity in vehicular networks. These two protocols assume the existence of Public Key Infrastructure (PKI) in vehicular networks, which most likely will be deployed to establish trust in vehicular networks. For example, Electronic Chassis Number (ECN) and Electronic License Plate (ELP) [28] are two identities issued by the manufacturer and the government, respectively.

3.1. Ring Signature Protocol

Gamage *et al.* proposed an identity-base ring signature for vehicular networks [25]. For reference purpose, we briefly repeat their approach below. In their approach, the trusted Key Generation Center (KGC) selects two secure hash function $H(\cdot)$ and $H_0(\cdot)$ such that $H : \{0, 1\}^* \rightarrow G_1$ and $H_0 : \{0, 1\}^* \rightarrow Z_q^*$, where G_1 is an additive cyclic group of prime order q for some large prime q. The KGC randomly chooses a secret value $x \in_R Z^*$ and keeps it as its master secret key and computes the corresponding public key as $P_{pub} = xP$ where P is a generator of G_1. G_2 is a multiplicative cyclic group of prime order q for the same large prime q.

There is a bilinear pairing $\hat{e} : G_1 \times G_1 \rightarrow G_2$ that satisfies the following properties:

- Bilinearity: $\forall P, Q, R \in G_1, \hat{e}(P + Q, R) = \hat{e}(P, R) \hat{e}(Q, R)$ and $\hat{e}(P, Q + R) = \hat{e}(P, Q)\hat{e}(P, R)$.
- Non-degeneracy: $(\exists P, Q \in G_1$ such that $\hat{e}(P, Q) \neq 1))$
- Computability: $\hat{e}(P, Q) \forall P, Q \in G_1$ can be computed efficiently.

It is assumed that the Bilinear Diffie–Hellman (BDH) problem in $\langle G_1, G_2, \hat{e}\rangle$ of given a tuple $\langle P, aP, bP, cP\rangle$ for some $a, b, c \in Z_q^*$ then the computing of $\hat{e}(P, P)^{abc} \in G_2$ is computationally intractable to be true. The KGC publishes the system-wide parameters $\langle q, G_1, G_2, H(\cdot), H_0(\cdot), \hat{e}(\cdot, \cdot), P, P_{pub}\rangle$.

Each vehicle has a public key $Q_{\text{ID}} = H(\text{ID})$, which is generated by applying secure hash function H over its identity ID. Each vehicle obtains its secret key from KGC by submitting its ID. The KGC calculates the vehicle's secret $S_{\text{ID}} = xQ_{\text{ID}}$ where x is KGC's master secret key.

To sign a message, the vehicle takes its neighbor set $L = \{\text{ID}_1, \text{ID}_2, \cdots, \text{ID}_n\}$, with itself being indexed at s $(1 \leq s \leq n)$. It then uses the following steps to sign the message m.

(1) Choose $U_i \in_R G_1$, compute $h_i = H_0(m\|L\|U_i) \forall i \in \{1, \cdots, n\}\backslash\{s\}$
(2) Choose $r'_s \in_R Z_q^*$ and compute $U_s = r'_s Q_{\text{ID}_s} - \sum_{i \neq s}\{U_i + h_i Q_{\text{ID}_i}\}$
(3) Compute $h_s = H_0(m\|L\|U_s)$ and $V = (h_s + r'_s)S_{\text{ID}_s}$
(4) Output the signature on m as $\sigma = \left\{ \bigcup_{i=1}^{n}\{U_i\}, V \right\}$ and L

To verify a message (m, L, σ), the steps are:

(1) Compute $h_i = H_0(m\|L\|U_i) \forall i \in \{1, \cdots, n\}$.
(2) Check whether $\hat{e}\left(P_{pub}, \sum_{i=1}^{n}(U_i + h_i Q_{\text{ID}_i})\right) = \hat{e}(P, V)$ and
(3) Accept the signature if the result is true. Otherwise, reject the signature.

Gamage *et al.* propose to use the protocol for anonymous accident reporting. For example, a vehicle driver may anonymously inform the authorities of other vehicles present at a scene of accident without the fear of reprisals from other vehicle drivers.

3.2. Anonymous Authentication Protocol

We consider the application of anonymous authentication [42] to vehicular networks. In the anonymous authentication protocol, a vehicle does not prove its exact identity. It rather proves its membership in a group. The authentication protocol is depicted in Figure 1.

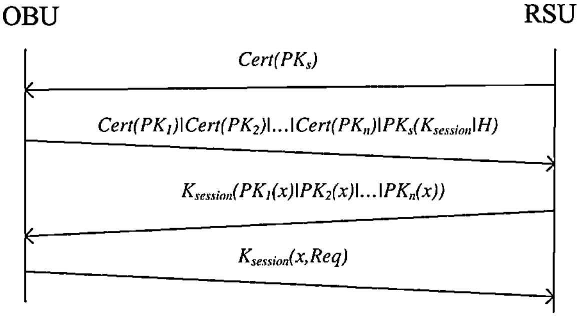

OBU
RSU
$Cert(PK_s)$
$Cert(PK_1)|Cert(PK_2)|\ldots|Cert(PK_n)|PK_s(K_{session}|H)$
$K_{session}(PK_1(x)|PK_2(x)|\ldots|PK_n(x))$
$K_{session}(x,Req)$

Fig. 1. The basic anonymous authentication protocol.

DOI: 10.1002/sec

In Figure 1, RSU refers to a road-side unit providing services. OBU refers to a on-board unit in a vehicle that implements our protocol. | means concatenation of data fields in a message. The rest of the notations are summarized below.

Cert(PK_s)	Certificate of road-side unit (RSU)
PK_s	Public key of RSU
PK_i	Public keys used by a on-board unit (OBU) $1 \leq i \leq n$
$PK_i(x)$	Use public key PK_i to encrypt x
K_{session}	A symmetric session key chosen by OBU
H	Secure hash of the message Cert(PK_1)|Cert(PK_2)| $\cdots$ |Cert(PK_n)
Req	The service request from OBU

A vehicle dynamically collects other public keys along its traveling course. It uses those public keys as its own group members in the anonymous authentication protocol in order to use some services anonymously.

All the public/private keys are issued and signed by a central authority (CA). RSU regularly broadcasts its certificate Cert(PK_s) so that it can be recognized as a legitimate service provider. An OBU verifies this certificate by using the public key of CA. It sends the certificates Cert(PK_1), Cert(PK_2), $\cdots$, Cert(PK_n) it has, including its own, to the RSU along with a session key K_{session}. The session key and the hash of the certificates H are signed with the public key of RSU to provide confidentiality of the session key and to protect message integrity. RSU verifies all the public keys it received and builds a challenge by encrypting a common secret x with each one of the public keys. The challenge is encrypted with the session key to conceal it from other vehicles. OBU then decrypt the common secret x. It sends the secret along with the service request back to RSU.

The two protocols share the same characteristics. First, both of them are based on public key cryptography. Second, both of them are leader free. The construction of the group is *ad hoc* and requires no interaction among vehicles. Third, the anonymity is the number of public keys a vehicle has used. Due to this, we do not differentiate them in the subsequent sections.

3.3. Intersection Attack

The above two protocols provide computational anonymity for each single usage of the protocols. The anonymity of each single usage is guaranteed by the computation intractability of the underlying public key cryptography. However, when they are applied to vehicular network and used multiple times by a single vehicle, the location privacy of the vehicle may be violated. Furthermore, the vehicle may lose its anonymity. For example, assuming the set of public keys that are used by a vehicle is fixed, this set may be unique among all the vehicles. Thus, it may be used by an adversary as its quasi-identifier. If it is used multiple times during a single itinerary, the trajectory of the vehicle will be observed by the adversary. This breach of location privacy may lead to loss of anonymity. For example, if the vehicle is observed leaving a residential address in the early morning, it belongs to the resident at this address with high probability.

Allowing dynamic sets of public keys to be used is the focus of this paper. However, the use of dynamic sets of public keys may be susceptible to intersection attacks. For example, on a freeway without any exit, two sets of public keys, one used at a upstream location, the other used at a downstream location later, have high probability of coming from one vehicle. In this case, the identity of the vehicle is narrowed down to the intersection of both sets, which is smaller than either one of them. Applying this approach to enough number of such sets, the identity of the vehicle is revealed.

Essentially, the loss of anonymity is due to that additional information about the vehicle is available. We believe that this is common when anonymous protocols are applied in vehicular networks. In the examples given above, the connection between different sets is made through implicit location information. In this paper, we limit our discussion of the additional information to this implicit location information. The investigation of the impact of other kind of information to anonymity should be equally interesting. We leave it as future work. Starting from the next section, we derive the necessary conditions to protect anonymity when dynamic sets of public keys are used across the vehicular network with implicit location information.

4. Mobile Anonymity

In dynamically constructing a group, different members of the group may not have a consistent view of the group membership. This is due to two reasons. One reason is that the use of group members at each vehicle is decided by each vehicle. Different vehicles may use different group members. The other reason is that different vehicles may hear a new vehicle at different time. This issue is not specific to vehicular networks. It applies to general mobile scenarios in which different users come and go. Thus, we term the anonymity in a mobile scenario *Mobile Anonymity*.

DOI: 10.1002/sec

Mobile Anonymity is significantly different from static anonymity. First, the group changes much faster than a static anonymity group. Second, the group size is often limited due to limited range of choices for group members.

In order to cope with the inconsistency among group members, we use a graph model to check its effect on the overall anonymity. We define an *anonymity graph* for a dynamic group as the following.

Definition 1. *An anonymity graph $G = (V, E)$ is a directed graph.*

1. *V is the vertex set. Each vertex corresponds to a vehicle that is participating in the group.*
2. *The edges in E are constructed in the following way. For each vehicle V_i, if it uses V_j as its group member, there is a directed edge from V_j to V_i in E.*
3. *Each vertex V_i has a true identity which is represented with V_i. Each vertex V_i is also marked with a sequence of identities that can be assigned to it.*

Note that an anonymity graph is only used as an analysis tool. Each vertex in G has a true identity that corresponds to the vehicle it represents. To an outside observer, the true identities of vertices and the edges are not known. An outside observer can only deduce the identity of a vertex from the set of identities it uses.

In this section, we generalize the concept of *Mobile Anonymity* under an ideal model in which each vehicle sends exactly one request. In Section 5, we apply this model to vehicular networks by considering some real issues. For example, one vehicle cannot be at two locations at the same time. Thus, two requests at two different locations at almost the same time are clearly from two vehicles.

Under this graph model, a static group is mapped to a complete graph since each vehicle will be used by all the other vehicles. It provides maximum anonymity where every identity is used by every other vehicle. Clearly, anonymities for different members are closely related with each other. In the following, we define *group anonymity* to characterize this relationship among group members in a dynamic group.

Definition 2. *The group anonymity $\mathcal{K}(G)$ of an anonymity graph G is defined by the number of possible ways to assign identities to vehicles. A valid assignment $\mathcal{A}(G)$ has the following properties:*

1. *Each vertex has exactly one identity assigned to it.*
2. *Each identity is assigned to exactly one vertex.*
3. *The identities that can be assigned to a vertex V_i are V_i and the true identities of those vertices that have outbound edges to V_i.*

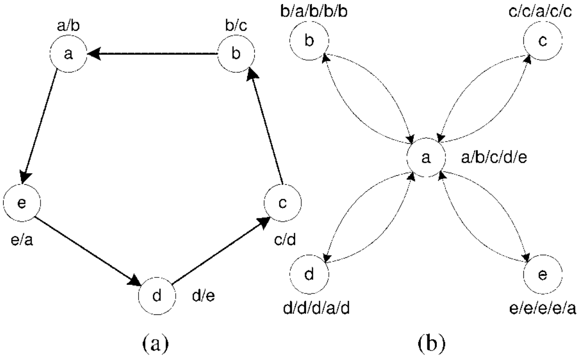


Fig. 2. Anonymities of dynamic groups. (a) Example 1, (b) Example 2.

If u is assigned to v in $\mathcal{A}(G)$, we write $u \rightarrow v \in \mathcal{A}(G)$.

Similarly, we define individual anonymity.

Definition 3. *The individual anonymity $\mathcal{I}(v)$ of a vertex v in an anonymity graph is defined by the number of identities that can be assigned to v.*

We use two examples in Figure 2 to illustrate the above concepts. In Figure 2, possible assignments of identities to each vehicle are marked next to each vehicle. The group anonymity in Example 2(a) is two because there are two possible ways to assign identities: $(a \rightarrow a, b \rightarrow b, c \rightarrow c, d \rightarrow d, e \rightarrow e)$ and $(b \rightarrow a, c \rightarrow b, d \rightarrow c, e \rightarrow d, a \rightarrow e)$. Similarly, the group anonymity in Example 2(b) is five. In the following discussion, we use anonymity for group anonymity when the context is specifically about a group. Notice that group anonymity does not necessarily equal to the individual anonymity for each member. In Example 2(b), only a has anonymity 5. The rest have anonymity 2.

Lemma 1. *A vertex v can be assigned exactly those inbound identities that are in the strongly connected component $\mathcal{SCC}(v)$ it belongs to.*

Proof. First, we prove that those inbound identities that are not in the strongly connected component cannot be assigned to v.

Assume that $u \notin \mathcal{SCC}(v)$ and u is assigned to v. We divide the vertices in G into two sets. One set A is the set of vertices whose identities have been assigned to. The other set U is the set of vertices whose identities are to be determined. We start with putting v into A.

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/sec

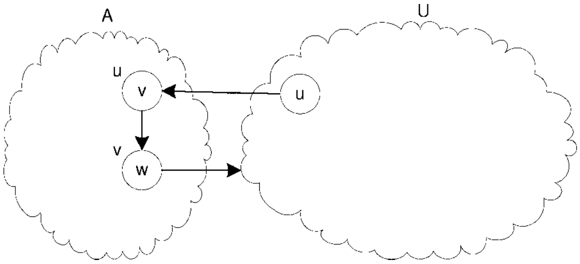


Fig. 3. Assigning identities.

Now v has to be assigned to one of the vertices in U according to definition 2.

There are two choices to assign v. If v is assigned to u, v and u form a strongly connected component with two vertices. If v is assigned not to u but to w, we remove w from U and put it into A as illustrated in Figure 3. Now w has to be assigned to some vertex in U. This process continues until we assign an identity to u and u is put into A. Apparently, v can reach u following the above path. Thus, $u \in \mathcal{SCC}(v)$. This contradicts with our assumption $u \notin \mathcal{SCC}(v)$. Thus, those inbound identities that are not in $\mathcal{SCC}(v)$ cannot be assigned to v.

Then we prove that there is at least one unique assignment that assigns each of those inbound identities in $\mathcal{SCC}(v)$ to v.

For any anonymity graph G, there is always an assignment that assigns each identity to its owner. For each inbound identity u of v in $\mathcal{SCC}(v)$, we generate a unique assignment in the following way. At first assign each identity to its owner. Within $\mathcal{SCC}(v)$, there must be a simple cycle containing u and v. Then just shift all the identities along the direction of the cycle to create the new assignment.

Apparently, when u is different, the assignment is also different since v takes different identities. Thus, the generated assignment is unique. □

We have the following Corollaries immediately.

Corollary 1. *The individual anonymity $\mathcal{I}(v) > 1$ if and only if v belongs to a strongly connected component with more than one vertices.*

Proof. This is apparent since $\mathcal{I}(v)$ is exactly the number of inbound identities that can be assigned to v. □

Corollary 2. *The group anonymity has the following properties:*

1. *A vehicle whose identity is not used by other vehicles does not contribute to $\mathcal{K}$. It should be removed from the dynamic group.*
2. *A vehicle which does not use any identity from other vehicles does not contribute to $\mathcal{K}$. It should also be removed from the dynamic group.*

Proof. In both scenarios, the vehicle does not belong to a strongly connected component with more than one vertices. Its individual anonymity is thus 1. It should not be included in the dynamic group. □

Corollary 3. *The group anonymity $\mathcal{K}(G)$ is the product of group anonymities of strongly connected components of G.*

Proof. From Lemma 1, group anonymities among strongly connected components of G are independent. The number of ways to assignment identities are thus product of the number of ways to assign identities to strongly connected components of G. □

Since group anonymity is basically the product of group anonymities of strongly connected components, we focus on the group anonymity of a strongly connected graph in the following. In order to facilitate our discussion, we define *assignment graph* of an anonymity graph as the following:

Definition 4. *An assignment graph $\mathcal{M}_{\mathcal{A}}(G) = (V', E')$ of an anonymity graph $G = (V, E)$ represents one assignment $\mathcal{A}$ of identities to vertices, where*

$$V' = V \tag{1}$$

$$E' = \{\overrightarrow{uv} : \overrightarrow{uv} \in E, u \rightarrow v \in \mathcal{A}\} \tag{2}$$

Due to Definition 2*, it has the following property: the in-degree and out-degree of a vertex v are either* $(0, 0)$ *or* $(1, 1)$.

Lemma 2. *In any assignment graph $\mathcal{M}(G)$ of an anonymity graph G, a vertex v is either isolated or belongs to a simple cycle.*

Proof. From Definition 4, if the in-degree and out-degree of v is $(0, 0)$, v is isolated. If the in-degree and out-degree of v is $(1, 1)$, following the construction procedure illustrated in the proof for Lemma 1, v belongs to a simple cycle. □

Theorem 1. *Let $\mathcal{VCC}(G)$ be the number of vertex-disjoint cycle covers of an anonymity graph G, then:* $\mathcal{K}(G) = \mathcal{VCC}(G)$

Proof. From Lemma 2, each assignment graph is a vertex-disjoint cycle cover of an anonymity graph G. Thus, the number of assignments is the number of vertex-disjoint cycle covers. □

DOI: 10.1002/sec

In Figure 2(b), $\mathcal{I}(a)$ is the same as $\mathcal{K}(G)$. Thus, if the identity of a is exposed, the rest of the graph has no anonymity. We define *anonymity criticality* as the criticality of individual vertex in determining the group anonymity. The formal definition is as follows:

Definition 5. *The anonymity criticality $\mathcal{C}(v)$ of vertex v in an anonymity graph G is defined as*

$$\mathcal{C}(v) = \frac{\mathcal{I}(v)}{\mathcal{K}(G)} \tag{3}$$

It has the following properties:

1. $0 < \mathcal{C}(v) \leq 1$
2. *The greater $\mathcal{C}_v$, the more critical v in determining $\mathcal{K}_G$.*

For a complete anonymity graph G, $\mathcal{C}_v = 1/(|G| - 1)!$.

5. Application of Mobile Anonymity to Vehicular Networks

We consider the following dynamic group construction scenario in vehicular networks. Then, we discuss the application of the general *Mobile Anonymity* model to vehicular networks.

We illustrate the application of *Mobile Anonymity* in Figure 4. There are three vehicles a, b, c in Figure 4. Vehicles a, b, and c made a request at time T_1 using (a, b), at time T_2 using (b, c), at time T_3 using (b, c), respectively, where $T_1 < T_2 < T_3$. Spd is the maximal speed of a vehicle in this scenario.

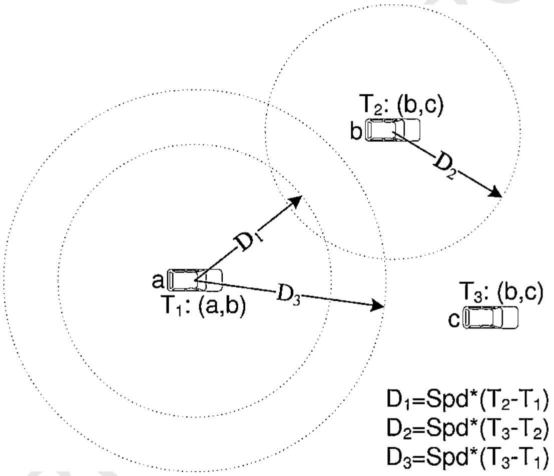


Fig. 4. Anonymity in vehicular networks.

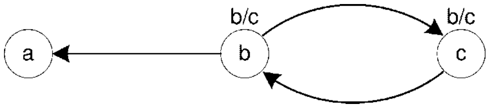


Fig. 5. Anonymity graph of Figure 4.

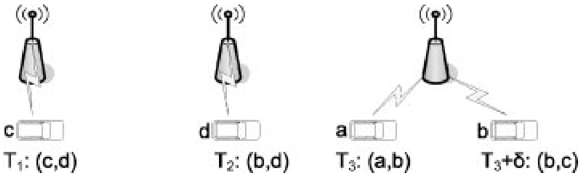


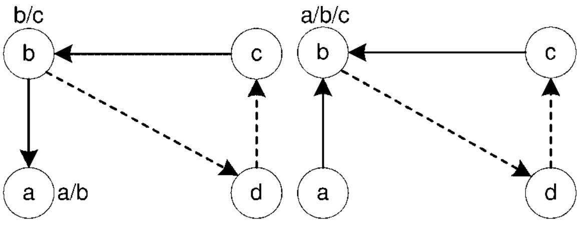
Fig. 6. Local anonymity in vehicular networks.

At time T_2, b is outside the possible reach of a. At time T_3, c is outside the possible reach of both a and b. Thus, a, b, and c can be identified as different vehicles. Its anonymity graph is shown in Figure 5. According to Corollary 1, a has no anonymity while the anonymities of both b and c are two.

Figure 6 illustrates an example in which two vehicles a and b cannot be told apart. In Figure 6, the three RSUs are separated far enough that the requests made at T_1, T_2, and T_3 can be clearly identified as requests from different vehicles. However, since δ is very small, the request from a at T_3 and the request from b at $T_3 + \delta$ cannot be reliably distinguished as from two different vehicles.

Figure 7(a) is its anonymity graph. According to Corollary 1, a should have no anonymity. However, it is also possible that b made both requests. The resulting anonymity graph would be shown in Figure 7(b). In Figure 7(b), a is hidden since it did not make any request.

In the above examples, we use the assumption that two vehicles using the same certificate can only be reliably told apart when they are over some distance away within a short period. This is essentially based on the speed limit of a vehicle in a vehicular network. The algorithm is listed in Figure 8. There may be other mechanisms to differentiate between two vehicles. However,



(a) (b)

Fig. 7. Local anonymity graph of Figure 6. (a) Real graph, (b) possible graph.

DOI: 10.1002/sec

```
Input: two requests $i = (Loc_i, T_i)$ and
       $j = (Loc_j, T_j)$
Output: $true/false$ whether the two requests
        can be told apart
$len$ ← the length of the shortest path between
$Loc_i$ and $Loc_j$
$deltat$ ← the time difference between $T_i$ and
$T_j$
if $len/delta$ is greater than the speed limit
then
    return $true$
else
    return $false$
end
```

Fig. 8. Function distinct (*i*, *j*).

our approach can be applied similarly with other mechanisms by substituting the function in Figure 8. Hence, we only consider the speed limit in this paper.

As a vehicle travels through the road network, the set of certificates collected by it keeps changing over time. The anonymity graph thus changes over time. To deal with this dynamic, we construct a vertex for each request, instead of for each vehicle. We also extend the generalized anonymity graph to represent each request as illustrated in Figure 9.

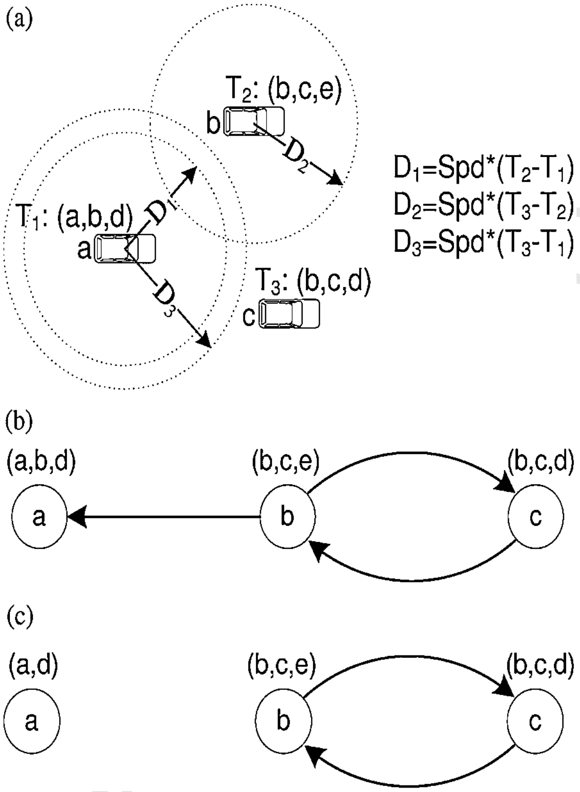


Fig. 9. Extended request-based anonymity graph. (a) Scenario, (b) anonymity graph, (c) reduced anonymity graph.

In Figure 9(a), vehicles *d* and *e* are used by vehicles *a* and *c*, and *b*, respectively. They are not present in the graph due to the hidden scenario illustrated in Figure 6. Figure 9(b) shows its extended anonymity graph, in which we mark each vertex with its associated request information. Figure 9(c) is its reduced form. Since *a* does not belong to the strongly connected component with *b*, *b* will be removed from the set of identities used by *a*.

We use the algorithm in Figure 10 to construct the extended anonymity graph.

```
Input: set of requests $R$ made at different
       RSUs sorted in the ascending order of
       occurrence
Output: the extended anonymity graph
initialize vertex set $V = []$
initialize edge set $E = []$
foreach Request $r = (v_r, c_r) \in R$ do
    insert $r$ into $V$
    update the location and time of the vehicle
    with certificate $v_r$ that initiated $r$
    // update out-edges
    foreach Request $l$ that used $v_r$ in the past
    do
        if $Distinct(l, r)$ is true then
            insert $\overrightarrow{rl}$ into $E$
        end
    end
    // update in-edges
    foreach Certificate $c \in$ certificate set $c_r$
    do
        $l$ ← last request made by $v_c$ that owns
        $c$
        if $Distinct(l, r)$ is true then
            insert $\overrightarrow{lr}$ into $E$
        end
    end
end
return $G = (V, E)$
```

Fig. 10. Extended anonymity graph construction.

DOI: 10.1002/sec

6. Simulation Evaluation

We run simulations to evaluate the effectiveness of different strategies in preserving anonymity. The simulation is completed in C3 simulator [48]. C3 is based on scalable wireless *ad hoc* network simulator (SWANS) [49].

The simulation scenario is set up as the following. We used a lattice road network to simulate a local road network. The size of the network is 7.5× 7.5 km^2. Each street block is 250 × 250 m^2. There are totally 100 simulated vehicles. All vehicles are equipped with OBUs. There are totally 16 simulated RSUs that form a 4 × 4 equal distance grid in the network. We assume that a vehicle makes one request at each RSU. The simulation is run for 20 min. The average vehicle speed is 10 m/sec, which is about 22 miles/h.

We evaluate the following certificate usage strategies by vehicles.

1. **Random strategy (RND)**. In this strategy, each vehicle randomly chooses some fixed number of certificates to use.
2. **Latest-preferred strategy (LPR)**. In this strategy, each vehicle always chooses certificates that were received most recently.

The use of RND is to look at how anonymity can be achieved given that each vehicle may behave differently. In our implementation, we require a vehicle to choose at least one other certificate randomly. Also, a vehicle chooses as many as certificates with a specified upper limit. The use of LPR is for comparison under a non-random strategy.

For a vehicle to anonymously distribute its certificate, the broadcasting protocol is similar with the authentication protocol. Instead of just broadcasting its own certificate, a vehicle broadcasts a group of certificates. The broadcasting protocol is more relaxed than the authentication protocol. There is no need for the originator to prove its possession of any private key since certificates are signed by CA.

Although at the beginning, a vehicle would have to broadcast only its own certificate. However, there is no reliable way to tell whether a vehicle is broadcasting its own certificate or just another certificate. Thus, we do not investigate this case in the following simulation.

6.1. Properties of Anonymity Graph

We present the properties of the constructed anonymity graph in the simulation. The specified upper limit for the number of certificates is varied between 2 and 10. For each upper limit, we run the configuration 10 times. For each run, we run Algorithm 10 to construct its anonymity graph. For each configuration, we record the sample mean and sample standard deviation of the sizes of the largest components in the 10 runs. The result is shown in Figure 11.

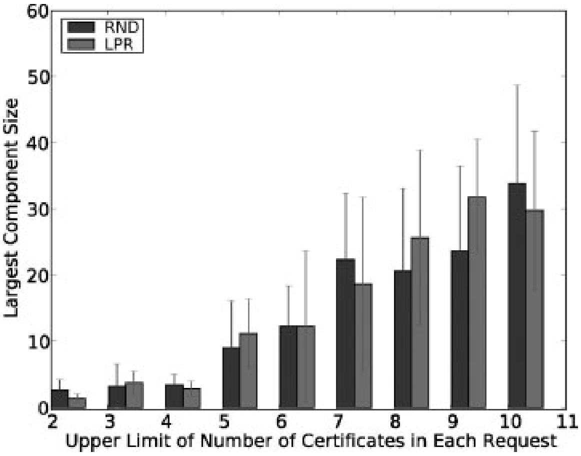


Fig. 11. Largest component size.

The size of the largest component increases as the number of certificates increases. This is due to that the increased number of certificates creates more edges in the anonymity graph. We do not observe any significant difference between the two strategies. This shows that LPR is not effective in overcoming the randomness in the network. In the subsequent sections, we present only the results obtained with RND. The results obtained with LPR are similar.

Figure 12 shows the percentage of non-isolated vertices at different speed limits given to Algorithm 8. In the *distinct* case, we intentionally assign −1.0 to speed limit so that every request can be seen as

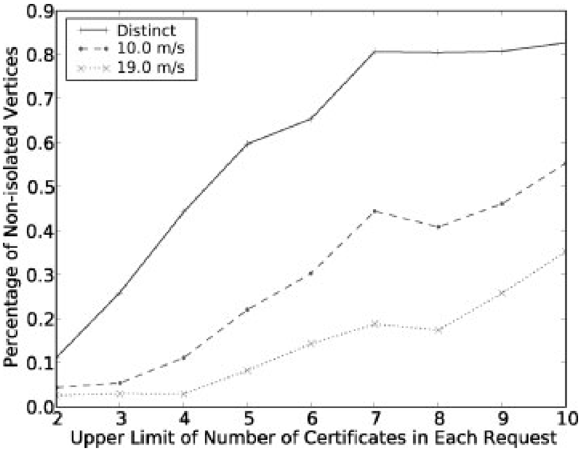


Fig. 12. Percentage of non-isolated vertices.

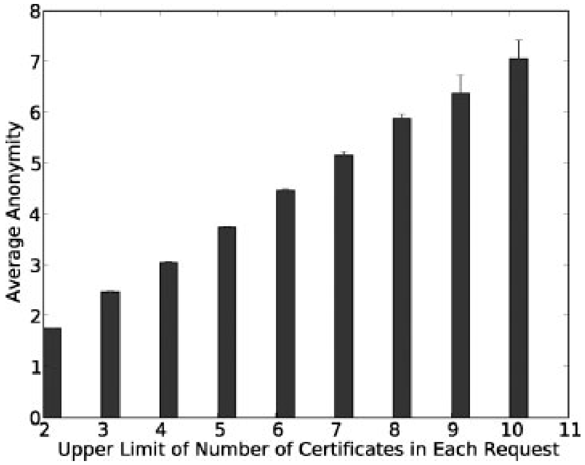


Fig. 13. Average anonymity.

distinct. In this case, given 10 certificates are used in each request, the anonymity graph is almost strongly connected. This shows that the use of more certificates will help preserve anonymity even a RDM strategy is used. This is a property of RDM graphs. An RDM graph is almost connected when its average vertex degree is over a threshold.

6.2. Anonymity of Each Request

The reduced anonymity graph in Figure 9(c) shows that a vehicle can still have anonymity even it does not belong to a strongly connected component. Figure 13 shows the average anonymity for different number of certificates. It almost grows linearly with the number of certificates.

Figure 14 shows the average number of requests that do not have any anonymity. When vehicles use only one other certificate in each request, a significant portion of requests can be identified due to that the mutual use of each other's certificate between two vehicles is unlikely due to RDM picking. However, even in this case, only about 24 per cent of requests are exposed. Although there are very few requests exposed when the number of certificate is larger, we have verified that no request is exposed if we increase the minimal number of certificates required in each request. We omit its display here due to that all the numbers are zeros.

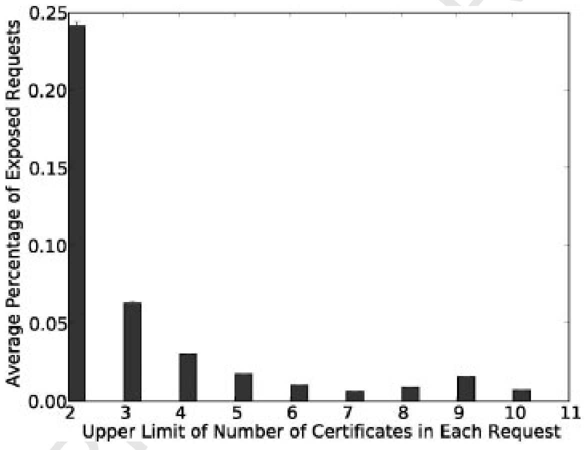


Fig. 14. Average percentage of exposed requests.

The simulation results clearly support using a large number of certificates in each request. The anonymity of each request in an extended anonymity graph comes from two parts. On the one hand, a larger set of certificates increases the probability of the request belonging to a strongly connected component. On the other hand, the number of requests not distinguishable will also increase with a larger set of certificates.

7. Conclusions

In this paper, we investigated providing unconditional anonymity in vehicular networks. We proposed a *Mobile Anonymity* model as its general model and constructed anonymity graph as its analysis tool. Under this model, we proved that anonymity can be obtained if and only if a vehicle belongs to a strongly connected component in the anonymity graph. We also proposed group anonymity as a measurement of the quality of a group in preserving anonymity. We then proved that group anonymity is the number of cycle covers in the anonymity graph.

The general *Mobile Anonymity* is extended when it is applied to a vehicular network. The extended model takes into account practical issues like mechanisms to reliably differentiate multiple vehicles. The proposed extension can also incorporate other similar mechanisms besides the one that was discussed.

We investigated the performance of two certificate usage strategies on preserving anonymity by simulation. The simulation results reveal that the LPR strategy is not significantly different from RDM strategy. The results also show that it is promising to use the RDM strategy with anonymous authentication in vehicular networks.

References

1. Saving lives through advanced vehicle safety technology: intelligent vehicle initiative final report. [Online]. Available: http://www.itsdocs.fhwa.dot.gov/JPODOCS/REPTS_PR/14153_files/ivi.pdf

2. Vehicle infrastructure integration. [Online]. Available: http://www.its.dot.gov/vii/docs/vii_factsheet.pdf
3. Robinson C, Caminiti L, Caveney D, Laberteaux K. Efficient coordination and transmission of data for cooperative vehicular safety applications. In *Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks*, 2006.
4. ElBatt T, Goel SK, Holland G, Krishnan H, Parikh J. Cooperative collision warning using dedicated short range wireless communications. In *Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks*, 2006.
5. Miller R, Huang Q. An adaptive peer-to-peer collision warning system. In *Vehicular Technology Conference (Spring)*, 2002.
6. Doğan A, Korkmaz G, Liu Y, *et al*. Evaluation of intersection collision warning system using an inter-vehicle communication simulator. In *The 7th International IEEE Conference on Intelligent Transportation Systems*, 2004.
7. Wang Z, Kulik L, Ramamohanarao K. Proactive traffic merging strategies for sensor-enabled cars. In *Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc Networks*, 2007.
8. Gradinescu V, Gorgorin C, Diaconescu R, Cristea V, Iftode L. Adaptive traffic lights using car-to-car communication. In *Vehicular Technology Conference (Spring)*, 2007.
9. Nadeem T, Dashtinezhad S, Liao C, Iftode L. Trafficview: traffic data dissemination using car-to-car communication. *ACM SIGMOBILE Mobile Computing and Communications Review* 2004; **8**: 6–19.
10. Wischhof L, Ebner A, Rohling H. Information dissemination in self-organizing intervehicle networks. *IEEE Transactions on Intelligent Transportation Systems* 2005; **6**: 90–101.
11. Caliskan M, Graupner D, Mauve M. Decentralized discovery of free parking places. In *Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks*, 2006, pp. 30–39.
12. IEEE 1609.2: Trial-use standard for wireless access in vehicular environments-security services for applications and management messages, 2006.
13. Studer A, Luk M, Perrig A. Efficient mechanisms to provide convoy member and vehicle sequence authentication in VANETs. In *Proceedings of 3rd International Conference on Security and Privacy in Communication Networks (SecureComm'07)*, September 2007.
14. Sun C, Arr G, Ramachandran RP. Vehicle reidentification as method for deriving travel time and travel time distributions: investigation. *Transportation Research Record*, Vol. 1826, 2003; pp. 25–30.
15. Sun CC, Arr GS, Ramachandran RP, Ritchie SG. Vehicle reidentification using multidetector fusion. *IEEE Transactions on Intelligent Transportation Systems* 2004; **5**: 155–164.
16. Oh C, Ritchie SG, Jeng S-T. Anonymous vehicle reidentification using heterogeneous detection systems. *IEEE Transactions on Intelligent Transportation Systems* 2007; **8**: 460–469.
17. Srinivasan KK, Jovanis PP. Determination of number of probe vehicles required for reliable travel time measurement in urban network. *Transportation Research Record*, Vol. 1537, 1996; pp. 15–22.
18. Golle P, Greene D, Staddon J. Detecting and correcting malicious data in VANETs. In *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks*, 2004; pp. 29–37.
19. Lochert C, Scheuermann B, Mauve M. Probabilistic aggregation for data dissemination in VANETs. In *Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc Networks*, 2007; pp. 1–8.
20. Raya M, Aziz A, Hubaux J-P. Efficient secure aggregation in VANETs. In *Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks*, 2006; pp. 67–75.
21. Picconi F, Ravi N, Gruteser M, Iftode L. Probabilistic validation of aggregated data in vehicular ad-hoc networks. In *Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks*, 2006; pp. 76–85.
22. Lin X, Sun X, Ho P-H, Shen X. GSIS: a secure and privacy preserving protocol for vehicular communications. *IEEE Transactions on Vehicular Technology* 2007; **56**: 3442–3456.
23. Guo J, Baugh JP, Wang S. A group signature based secure and privacy-preserving vehicular communication framework. In *Proceedings of the Mobile Networking for Vehicular Environments (MOVE) Workshop in Conjunction with IEEE INFOCOM*, 2007; pp. 103–108.
24. Calandriello G, Papadimitratos P, Lloy A, Hubaux J-P. Efficient and robust pseudonymous authentication in VANET. In *Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc Networks*, 2007.
25. Gamage C, Gras B, Crispo B, Tanenbaum AS. An identity-based ring signature scheme with enhanced privacy. In *Proceedings of Securecomm and Workshops*, 2006; pp. 1–5.
26. Sha K, Xi Y, Shi W, Schwiebert L, Zhang T. Adaptive privacy-preserving authentication in vehicular networks. In *Proceedings of IEEE International Workshop on Vehicle Communication and Applications*, 2006.
27. Hubaux J, Čapkun S, Luo J. The security and privacy of smart vehicles. *IEEE Security and Privacy* 2004; **4**(3): 49–55.
28. Raya M, Hubaux J-P. The security of VANETs. In *Proceedings of the 3rd ACM workshop on Security of Ad Hoc and Sensor Networks*, November 2005.
29. Dötzer F. Privacy issues in vehicular ad hoc networks. In *Proceedings of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks*, September 2005.
30. Choi J, Jakobsson M, Wetzel S. Balancing auditability and privacy in vehicular networks. In *Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks*, October 2005.
31. Sampigethaya K, *et al*. Caravan: providing location privacy for VANET. In *Embedded Security in Cars (ESCAR)*, November 2005.
32. Hoh B, Gruteser M. Protecting location privacy through path confusion. In *IEEE/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm)*, September 2005.
33. Gedik B, Liu L. Location privacy in mobile systems: a personalized anonymization model. In *Proceedings of the 25th International Conference on Distributed Computing Systems*, June 2005.
34. Zarki M, Mehrotra S, Tsudik G, Venkatasubramanian N. Security issues in a future vehicular network. In *Proceedings of EuroWireless 2002*, February 2002.
35. Parno B, Perrig A. Challenges in securing vehicular networks. In *Proceedings of Workshop on Hot Topics in Networks (HotNets-IV)*, November 2005.
36. Schoch E, Kargl F, Leinmüller T, Schlott S, Papadimitratos P. Impact of pseudonym changes on geographic routing in VANETs. In *Proceedings of the European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS)*, 2006.
37. Fonseca E, Festag A, Baldessari R, Aguiar R. Support of anonymity in VANETs—putting pseudonymity into practice. In *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, March 2007.
38. Gerlach M, Güttler F. Privacy in VANETs using changing pseudonyms—ideal and real (poster presentation). In *Proceedings of the 65th IEEE Vehicular Technology Conference VTC2007-Spring*, 2007; pp. 2521–2525.
39. Buttyán L, Holczer T, Vajda I. On the effectiveness of changing pseudonyms to provide location privacy in VANETs. In *Proceedings of the European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS)*, 2007.
40. Laurendeau C, Barbeau M. Secure anonymous broadcasting in vehicular networks. In *Proceedings of the 32nd IEEE Conference on Local Computer Networks*, 2007.
41. di Crescenzo G, Zhang T, Pietrowicz S. Anonymity notions for public-key infrastructures in mobile vehicular networks. In

DOI: 10.1002/sec

Proceedings of the 1st IEEE International Workshop on Mobile Vehicular Networks (MoVeNet 2007), 2007.

42. Schechter S, Parnell T, Hartemink A. Anonymous authentication of membership in dynamic groups. In *Proceedings of the Third International Conference on Financial Data Security and Digital Commerce*, January 1999.
43. Boneh D, Franklin MK. Anonymous authentication with subset queries (extended abstract). In *ACM Conference on Computer and Communications Security*, 1999; pp. 113–119.
44. Teranishi I, Furukawa J, Sako K. k-times anonymous authentication (extended abstract). In *ASIACRYPT*, 2004; pp. 308–322.
45. Dodis Y, Kiayias A, Nicolosi A, Shoup V. Anonymous identification in ad hoc groups. In *EUROCRYPT*, 2004; pp. 609–626.
46. Nguyen L, Safavi-Naini R. Dynamic k-times anonymous authentication. In *ACNS*, 2005; pp. 318–333.
47. Kong J, Hong X, Sanadidi M, Gerla M. Mobility changes anonymity: mobile ad hoc networks need efficient anonymous routing. In *Proceedings of the 10th IEEE Symposium on Computers and Communications*, 2005.
48. Choffnes DR, Bustamante FE. An integrated mobility and traffic model for vehicular wireless networks. In *Proceedings of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks*, September 2005.
49. Barr R. An efficient, unifying approach to simulation using virtual machines, Ph.D. Dissertation, Cornell University, 2004.

DOI: 10.1002/sec