PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs

Dijiang Huang, *Senior Member, IEEE*, Satyajayant Misra, *Member, IEEE*,
Mayank Verma, *Member, IEEE*, and Guoliang Xue, *Fellow, IEEE*

***Abstract*—In this paper, we propose a new privacy preservation scheme, named pseudonymous authentication-based conditional privacy (PACP), which allows vehicles in a vehicular ad hoc network (VANET) to use pseudonyms instead of their true identity to obtain provably good privacy. In our scheme, vehicles interact with roadside units to help them generate pseudonyms for anonymous communication. In our setup, the pseudonyms are only known to the vehicles but have no other entities in the network. In addition, our scheme provides an efficient revocation mechanism that allows vehicles to be identified and revoked from the network if needed. Thus, we provide *conditional privacy* to the vehicles in the system, that is, the vehicles will be anonymous in the network until they are revoked, at which point, they cease to be anonymous.**

***Index Terms*—Conditional anonymity, pseudonym, vehicular ad hoc networks (VANETs).**

I. Introduction

VEHICULAR ad hoc networks (VANETs) have recently become a popular direction for research, with specific attention to improving driving experience and road safety [1]. VANETs generally consist of vehicles, infrastructure units such as roadside units (RSUs), and a centralized trusted authority. Each vehicle that is part of a VANET contains an onboard wireless computing unit, which is commonly known as the onboard unit (OBU). Vehicles may communicate with the RSUs, which are online, and with other vehicles in their neighborhood. Recent studies on VANETs have identified several issues, including those in security and privacy, which need to be addressed for widespread adoption.

Security issues in VANETs have been studied in great detail (see [2]–[4]). However, the issue of privacy still has a lot of open questions. With the latest advancement in tracking mechanisms and the potential increase in communication among vehicles, an adversary can track a vehicle by observing its communication and movement patterns. However, if a completely anonymized vehicle turns malicious, then there is no way to identify and revoke it. Thus, a privacy scheme needs to provide privacy to the vehicles while at the same time being able to track and revoke rogue vehicles. In other words, the vehicles in a VANET need *conditional privacy*, that is, the vehicles should have privacy that is contingent on them behaving appropriately in the system. If the vehicle does not perform the protocols correctly or is malicious, then its privacy is revoked, and it can no longer be anonymous. These requirements have served as the motivation for many researchers, leading to the formulation of various schemes, e.g., [5]–[7]. These schemes advocate the use of pseudonym-based approaches for anonymous communication, which helps maintain a vehicle's privacy. Most of the schemes designed for anonymity in VANETs utilize a public key infrastructure (PKI). The RSA-based PKI and the elliptical curve cryptosystem (ECC)-based PKI [8] are two commonly used infrastructures. In general, the ECC-based anonymity schemes are better than the RSA-based schemes because of the smaller key size and lower computation costs [9]. However, all of the existing schemes suffer from a common drawback, that is, the authorities involved in the pseudonym generation process also know the pseudonyms used by the vehicles. Thus, these schemes are not truly anonymous.

Based on the aforementioned presentation, there is a need for a strong privacy-preserving scheme in VANETs that has properties such as low pseudonym generation latency, high scalability, easy revocation, and ability to perform with sparsely distributed RSUs. To achieve these desired properties, our research goal is to design a new anonymity scheme, named pseudonymous authentication with conditional privacy (PACP), for generating pseudonyms. PACP is based on four security requirements: 1) The privacy provided to the vehicles is *conditional* privacy. 2) The construction of PACP is based on pairing [10], which is a mathematical structure based on ECC assumptions. 3) PACP does not rely on storing multiple pseudonym certificates issued from a centralized authority or on providing identity certificates to the RSU for generating on-the-fly pseudonym certificates. Instead, a node generates its pseudonyms with assistance from the RSU in its neighborhood in a way that the RSU gains no information about the node's real identity. 4) In case of any

Manuscript received July 31, 2009; revised August 16, 2010 and March 16, 2011; accepted April 22, 2011. Date of publication August 12, 2011; date of current version September 6, 2011. This work was supported in part by the U.S. Army Research Office under Grant W911NF-09-1-0467, by the National Science Foundation under Grant 0901451, Grant 0942453, and Grant 1029546, and by the Office of Naval Research under the Young Investigator Program Award. The work does not reflect the position or the policy of the federal government. The Associate Editor for this paper was C. T. Chigan.

D. Huang and G. Xue are with the School of Computing, Informatics, and Decision Systems Engineering, Arizona State University, Tempe, AZ 85287 USA (e-mail: dijiang@asu.edu; xue@asu.edu).

S. Misra is with the Department of Computer Science, New Mexico State University, Las Cruces, NM 88003 USA (e-mail: misra@cs.nmsu.edu).

M. Verma is with Brocade Communications, Encinitas, CA 92024 USA (e-mail: verma.mayank@gmail.com).

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

Digital Object Identifier 10.1109/TITS.2011.2156790

dispute, our scheme allows trusted authorities to successfully de-anonymize a misbehaving node to reveal its identity and possibly revoke it with the use of revocation lists (RLs).

The main contribution of this paper is to allow vehicles to generate provably anonymous and computationally efficient pseudonyms to ensure conditional privacy. The presented performance studies and comparisons with other popular anonymity schemes [2], [6] demonstrate that our scheme is effective and efficient.

The rest of this paper is organized as follows. Section II presents the related work. Section III details the system and attack model and provides preliminary definitions. Section IV describes the presented PACP scheme in detail. Section V describes the security and privacy performance analysis. Section VI presents the simulation results that demonstrate the effectiveness of our scheme. Section VII concludes our work and provides directions for future work.

II. Related Work

In the area of security and privacy of VANETs, majority of the research works have focused on authentication to ensure security [2]–[4], [11]. To protect the privacy of vehicles, existing research has mainly focused on location privacy [12], [13] problems, anonymizing sensed data [14], and pseudonym-based schemes to anonymize vehicles' actions [5]–[7]. Previous solutions have shown that, to maintain a vehicle's privacy, pseudonym-based approaches are most effective. However, to thwart privacy-related breaches, frequent change of pseudonyms is essential. The Vehicle Safety Communication (VSC) project [15] was one of the first projects to work on privacy in VANETs. It proposed the use of a list of short-lived pseudonym certificates for guaranteeing privacy through anonymity. Raya and Hubaux [16] proposed a scheme similar to VSC, which required using certificates for vehicle-to-vehicle communication. However, the scheme requires many public key operations and, hence, is expensive for deployment.

Several privacy schemes that use ECC as their fundamental building block have been proposed in the literature. Lu *et al.* [6] proposed an ECC-based scheme, named efficient conditional privacy preservation protocol (ECPP), using bilinear maps to achieve conditional privacy for the vehicles. In ECPP, a vehicle uses multiple anonymous keys obtained from an RSU to prevent its communication from being traced. In addition to the provided anonymity features, the ECPP scheme suffers from three main drawbacks. First, it is not efficient due to two reasons: 1) It has fairly high latency for generation of pseudonym keys by the RSUs, and 2) it requires ubiquitous presence of RSUs to assist vehicles to derive their pseudonyms and corresponding keys at any given road location. Second, ECPP requires that the issued pseudonyms are known to the issuing authorities (i.e., RSUs) beforehand. Since RSUs are distributed in open areas along roads, they are usually vulnerable to physical attacks. Thus, they usually cannot be fully trusted. Third, there is no clear revocation mechanism of using ECPP. Since vehicles can derive their pseudonyms from every RSU, even a compromised one, malicious vehicles cannot be revoked.

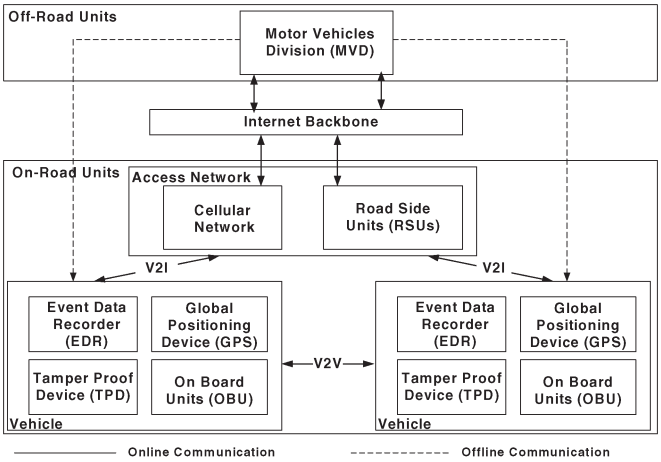


Fig. 1. Network model for VANETs.

III. System Overview

Here, we present the system assumptions, the network model, the attack model, and some mathematical models used by our solutions.

A. Assumptions

We assume that all vehicles are registered with a central trusted authority (TA), i.e., the Motor Vehicles Division (MVD), before they are approved for driving on the road. Registration of a vehicle includes registration of the vehicle's license plate number, identity, owner's address, and any other information needed to uniquely identify the vehicle and its owner. Since the MVD is assumed to be trusted and cannot be compromised, the initial security parameters and keys are issued by the MVD. RSUs are not fully trusted since they are usually exposed in open unattended environments, which are subject to physical breaches. However, we assume that the functions of RSUs are monitored and that their compromise can be detected in a bounded time period. Consequently, at a given time, very few RSUs are compromised. Because RSUs can be compromised, we assume that the security keys and corresponding identity information cannot be directly generated by RSUs. Other vehicles are not trusted.

B. Network Model

The network model for our anonymity scheme is shown in Fig. 1. It comprises on- and off-road units. The on-road units consist of the vehicles, the RSUs, and the communication network. The RSUs are managed and regularly monitored by a local transportation department office such as the MVD. The RSUs and the MVD are connected via the Internet. Existence of a central trust authority such as the MVD helps expedite revocation as all RSUs can contact it for updated vehicle RLs. Each vehicle is assumed to be equipped with an OBU, which is a tamper-proof device (TPD) that stores the secret information, an event data recorder (EDR), and a Global Positioning System.

The RSUs and the vehicles are equipped with network cards that can provide support for the dedicated short-range communication (DSRC) [17] service or WiFi access, hence enabling high-data-transfer rates with minimal latency. Vehicles and the nearby RSUs are assumed to be time synchronized, which can be used to validate the expiration date of a pseudonym.

C. Attack Model

The attackers in a VANET may be classified as either *internal attackers* or *external attackers*. External attackers are powerful attackers that can observe and analyze the traffic in the network. They are not part of the system; hence, they cannot decrypt the messages, but they can obtain related information from the messages and use it for traffic and data analysis. We assume that the external attackers are more powerful than the vehicles or the RSUs; however, their powers are bounded. Usually, it takes multiple colluding external attackers to observe the whole system. Internal attackers are compromised vehicles. Internal attackers are potent as well since they are part of the system and have access to shared secrets.

Here, we present all possible attack scenarios in a VANET. An attacker can (a) modify or replay existing messages, (b) inject fake messages, (c) impersonate a legitimate node (RSU or vehicle), (d) compromise an RSU or a vehicle, or (e) perform a denial-of-service attack. The attacks may be performed by a single attacker or a group of colluding attackers. We note that, of the aforementioned attacks, attacks (c), (d), and (e) are those that result in loss of privacy. In our study, we do not consider attack (e) as they have been addressed in [18]. Our scheme handles the rest of the attack scenarios and ensures that the anonymity of communication is preserved. In the following section, we present our scheme PACP in detail.

D. Background Concepts

We first formally define the term conditional privacy.

Definition 1—Conditional Privacy: Given a set of vehicles $\mathcal{V} = \{V_1, \ldots, V_m, \ldots, V_p\}$, a set of RSUs $\mathcal{R} = \{R_1, \ldots, R_q\}$, and a trusted MVD, the conditional privacy of a vehicle V_m ensures that its real identity is only known to the MVD. If the vehicle is identified as compromised or malicious, then its privacy can be revoked by the MVD, and its identity will be known to other vehicles and RSUs. □

Here, we present some concepts that form the basis for the design of our PACP scheme and the proof of its security. Our protocol uses bilinear mapping, which uses pairing-based construction to map a pair of elements in a given group to another element in the same or a different group. The following definition states some properties of bilinear mapping.

Definition 2—Properties of Bilinear Mapping: Given two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ with same order p, where $p = q^n$, q is prime and $n \in \mathbb{Z}^+$, $\mathbb{G}_1$ is an additive group, and $\mathbb{G}_2$ is a multiplicative group, the bilinear mapping $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ satisfies three properties.

1) *Bilinearity:* The mapping $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is said to be *bilinear* if $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$, $\forall P, Q \in \mathbb{G}_1$ and $\forall a, b \in \mathbb{Z}_p^*$, where $\mathbb{Z}_p^* = [1, \ldots, p-1]$.
2) *Nondegeneracy:* If $\hat{e}(P, Q) = 1$ for all $Q \in \mathbb{G}_1$, then $\hat{e}(P, P)$ is a generator of $\mathbb{G}_2$, and P is the identity element in $\mathbb{G}_1$.

TABLE I
NOTATIONS USED IN PACP

Notation	Description
ID	The identity of the vehicle.
R_i	The identity of RSU R_i (also its public key).
S_{R_i}	The private key of RSU R_i.
R_{TH}	The threshold value of the RSU.
$Cert_{R_i}$	Identity-based Certificate of RSU R_i.
$SIG(\mathcal{M}; K)$	ECC-based signature of $\mathcal{M}$ using key K.
P_{MVD}	The public key of the MVD.
S_{MVD}	The private key of the MVD.
$\mathcal{M}$	Message.
$\mathcal{C}$	Ciphertext.

TABLE II
PUBLICLY KNOWN SYSTEM PARAMETERS

$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$	Mapping from an additive group $\mathbb{G}_1$ to a multiplicative group $\mathbb{G}_2$.
$P \in \mathbb{G}_1$	P is a generator of $\mathbb{G}_1$.
$P_{MVD} = \alpha P$	Public key of MVD.
$H : \mathbb{G}_1 \rightarrow \{0,1\}^n$ $H_1 : \mathbb{G}_2 \rightarrow \{0,1\}^n$ $H_2 : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$	H, H_1, H_2 are publicly known hash functions.

3) *Computability:* The bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ can be efficiently computed.

□

Definition 3—Elliptical Curve Discrete Logarithmic Problem (ECDLP): Given $P, Q \in E(\mathbb{F}_q)$, find the value of λ, if it exists, such that $Q = \lambda P$. □

The ECDLP had been proved to be a hard problem [19].

IV. Pseudonymous Authentication-Based Conditional Privacy

Here, we present our PACP scheme that provides pseudonym-based anonymity to vehicles in VANETs. Before presenting our scheme in detail, we first give a general overview. A vehicle that uses our PACP scheme registers with the motor vehicle department using its identity and gets a ticket. It uses the ticket to communicate with an RSU in its neighborhood to obtain tokens. The tokens are used by the vehicle to generate pseudonyms for anonymous broadcast communication with other vehicles. In what follows, we will present the scheme in detail. Table I illustrates the notations used in the presentation of our scheme.

A. System Setup

The scheme uses a set of publicly known system parameters $\texttt{params} = \langle \mathbb{G}_1, \mathbb{G}_2, e, P, H, H_1, H_2 \rangle$, which are stored in each vehicle by the MVD at the time of registration. The detailed explanation of parameters is given in Table II. The MVD generates its public key as $P_{\mathrm{MVD}} = \alpha P$, where $\alpha \in \mathbb{Z}_p^*$ is the private key of the MVD.

Our scheme uses the identity-based encryption (IBE) scheme proposed by Boneh and Franklin [20] for secure communication. All signatures generated in our scheme utilize the BLS short signature scheme proposed by Boneh *et al.* because of

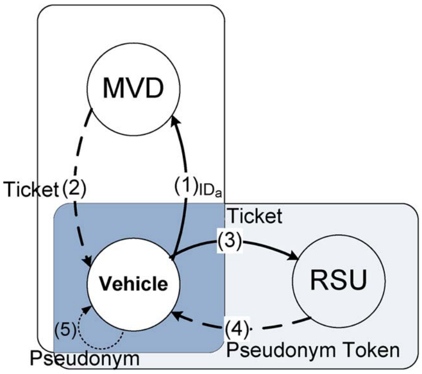


Fig. 2. State transition diagram for pseudonym generation in PACP.

its efficiency and low computation cost [21]. In the following section, we present our PACP scheme in detail.

B. PACP Protocols

In our scheme, pseudonym generation for a vehicle requires three types of entities, namely, the vehicle, the MVD, and the RSU. The interaction between these three entities is shown in Fig. 2. A vehicle V_a provides the required identity information to the MVD as part of the registration process. Then, the MVD issues V_a a ticket. The ticket uniquely identifies V_a; however, it does not reveal V_a's true identity. When moving on the road, V_a authenticates itself with the nearest RSU and obtains a pseudonym token. Then, V_a uses the token to generate its pseudonyms. Here, we must note that the RSU only provides the credential (i.e., signature) and restrictions (i.e., a time stamp) for the vehicle to generate its pseudonyms, and it does not learn any private information of the vehicle. As a result, the RSU is unaware of the vehicle's true identity, which is mapped to the pseudonym that the vehicle will generate using the token. We note that the RSU can map a ticket to a pseudonym token and the generated pseudonym. However, this mapping cannot review the real identity of the vehicle. The only information possessed by the RSU is the token, which will be used in the revocation phase. We will discuss more about the resultant improvement in security in the security analysis section. Our system consists of three building blocks, namely, *registration, generation*, and *extraction*. Each block is a protocol in itself. In what follows, we present the three protocols.

1) Registration Protocol: The registration procedure requires V_a to be physically present at the MVD. The vehicle registers with the MVD and obtains a ticket δ_a. The MVD loads δ_a and `params`, i.e., the system parameters, into the vehicle's TPD. Algorithm 1 illustrates the complete registration process executed by the MVD.

Algorithm 1: Registration Protocol executed by the MVD

```
Require: $\mathrm{ID}_a$.
1:Choose a random number $\mathrm{rnd} \in \mathbb{Z}_p^*$.
2:Use $H_2$ to compute $S_a = H_2(\mathrm{ID}_a, \mathrm{rnd}) \in \{0,1\}^n$, and $S_a$
  is $V_a$'s private key.
3:Compute ticket $\delta_a = S_a P \in \mathbb{G}_1$ and sign $\delta_a$ with $S_{\mathrm{MVD}}$
  to obtain $\mathrm{SIG}(\delta_a; S_{\mathrm{MVD}})$, and $\delta_a$ is $V_a$'s public key.
4:Store the mapping $\mathrm{map}_{\mathrm{MVD}}^a = \langle \delta_a, \mathrm{ID}_a \rangle$ in the database.
5:Store the 3-tuple $Q_a = \langle \delta_a, \mathrm{SIG}(\delta_a; P_{\mathrm{MVD}}), S_a \rangle$ with
  params in the vehicle's OBU.
```

Identity ID_a is the true identity of vehicle V_a, and S_a is the master secret key of V_a. We note that ticket δ_a does not reveal any information about V_a. However, in case of misconduct, the MVD can obtain ID_a by looking up the mapping $\mathrm{map}_{\mathrm{MVD}}^a$ (line 4), which is stored in a hash table in its database, in $\mathcal{O}(1)$ time. The signature performed by the MVD (line 5) utilizes the lightweight BLS scheme [21]. The MVD signs δ_a with its private key. The 3-tuple Q_a is V_a's private information that is stored in the OBU and can only be modified by the MVD. Once V_a has successfully obtained δ_a, it can initiate anonymous communication on the road.

2) Generation Protocol: After obtaining a ticket δ_a from the MVD, V_a has to communicate with a nearby RSU(s), e.g., R_i, to generate pseudonyms. R_i periodically broadcasts its identity certificate Cert_{R_i} derived from the MVD, where R_i serves as both the identity and the public key for the RSU. Table III illustrates this procedure, which is known as the generation protocol. Vehicle V_a creates the 3-tuple Δ_a by concatenating its ticket, the signature of the ticket, and a symmetric key $K_{(a,i)}$. For encryption, the vehicle uses the IBE scheme with R_i as the ID to generate $\mathcal{C}$. When R_i receives $\mathcal{C}$, it uses its private key S_{R_i} to decrypt $\mathcal{C}$ and then verifies $\mathrm{SIG}(\delta_a; S_{\mathrm{MVD}})$ using P_{MVD}. On successful verification, R_i computes a pseudonym token $\tau_{(a,i)}$. RSU R_i also obtains expiration time $t_{(a,i)}$ for the token. It then creates the message

$$\mathcal{M} = \left\langle \tau_{(a,i)}, t_{(a,i)}, \mathrm{SIG}\left(\tau_{(a,i)}, t_{(a,i)}; S_{R_i}\right), \gamma_{(a,i)} \right\rangle$$

which is also shown in Table III. R_i encrypts it using secret key $K_{(a,i)}$ in $\mathcal{C}$ and transmits it to V_a as $\mathcal{C}'$. RSU R_i also stores the mapping between the ticket and the tuple $(\mathrm{map}_{R_i}^a)$ in a hashed map for $\mathcal{O}(1)$ time retrieval. Vehicle V_a decrypts $\mathcal{C}'$ and generates its pseudonym by using $\tau_{(a,i)}$. Encryption and decryption in the generation protocol are symmetric.

Our scheme allows V_a to obtain multiple tokens from a single RSU by using the same ticket δ_a. In this setup, $\tau_{(a,i)}^k$ represents the kth token issued to vehicle V_a by R_i. Token $\tau_{(a,i)}^k$ is used by V_a in the extraction protocol to generate the kth pseudonym. The value of k is upper bounded by a threshold value R_{TH}, which is a tunable system parameter. The value of R_{TH} determines the extent of anonymity, with higher values of R_{TH}, resulting in a higher number of pseudonyms and, thus, better anonymity. We do not perform analysis to obtain the best value for R_{TH} under different settings. However, we note that it is easy to calculate an R_{TH} value for a given anonymity requirement based on a threshold on the probability of correct identification of a token.

3) Extraction Protocol: A vehicle V_a uses the extraction protocol, which is illustrated in Algorithm 2 to generate a pseudonym. Let V_a obtain n tokens from RSU R_i. As illustrated in the protocol, V_a chooses one of the n tokens. Without loss of generality, let this token be $\tau_{(a,i)}^j$. The value $\gamma_{(a,i)}^j$ (which is obtained from R_i) is the private key component of $\tau_{(a,i)}^j$.

TABLE III
SCHEMATIC OF THE GENERATION PROTOCOL INVOLVING V_a AND R_i

Vehicle V_a		R_i
1. Generate a key $K_{(a,i)}$		
2. Select $x, \ell \in Z_P$, create the tuple: $\Delta_a = \langle \delta_a, SIG(\delta_a; S_{MVD}), K_{(a,i)})\rangle$, $SIG(\Delta_a; S_a)$		
3. Encrypt Δ_a using R_i as the key to generate $\mathcal{C}$		
4. $\mathcal{C}, SIG(\Delta_a; S_a)$	→	5. Decrypt $\mathcal{C}$ and verify the signature using keys S_{R_i} and δ_a, respectively.
		6. Verify $SIG(\delta_a; S_{MVD})$ by using P_{MVD}.
		7. If(Verification == Successful)
		7.1 Choose random number $\gamma_{(a,i)} \in \mathbb{Z}_P^*$.
		7.2 Compute $\tau_{(a,i)} = \gamma_{(a,i)}\delta_a$.
		7.3 Generate $SIG(\tau_{(a,i)}, t_{(a,i)}; S_{R_i})$.
		7.4 Create $\mathcal{M} = \langle \tau_{(a,i)}, t_{(a,i)}, SIG(\tau_{(a,i)}, t_{(a,i)}; S_{R_i}), \gamma_{(a,i)}, Cert_{R_i}\rangle$.
		7.5 Store the mapping map$_{R_i}^a = \langle \tau_{(a,i)}, \delta_a\rangle$.
		7.6 Encrypt $\mathcal{M}$ using symmetric key $K_{(a,i)}$ to obtain $\mathcal{C}'$.
8. Obtain $\mathcal{C}'$	←	7.7 $\mathcal{C}'$
		9. Else discard $\mathcal{C}$.
10. Decrypt $\mathcal{C}'$ using $K_{(a,i)}$ to obtain $\mathcal{M}$		
11. Verify $SIG(\tau_{(a,i)}, t_{(a,i)}; S_{R_i})$ using P_{R_i}		
12. If(Verification == Successful)		
12.1 Accept and store $\mathcal{M}$.		
13. Else discard $\mathcal{M}$.		

Successful completion of the extraction protocol outputs a pseudonym PN$^j_{(a,i)}$ for V_a, as shown in the algorithm. The vehicle can use pseudonym PN$^j_{(a,i)}$ to perform anonymous communication. Certificate Cert$_{R_i}$ is part of the pseudonym to allow another vehicle that receives pseudonym PN$^j_{(a,i)}$ from V_a to verify V_a's authenticity by verifying the signature.

Algorithm 2: Extraction Protocol performed by V_a

```
1:Randomly selects $\tau^j_{(a,i)}$ $(1 \leq j \leq n)$.
2:Chooses a random value $r^j_a \in \mathbb{Z}^*_p$.
3:Computes $\sigma^j_a = r^j_a S_a$.
4:PN$^j_{(a,i)} = \langle \sigma^j_a P, \tau^j_{(a,i)}, t^j_{(a,i)}$, SIG$(\tau^j_{(a,i)}, t^j_{(a,i)}; S_{R_i})$,
  Cert$_{R_i}\rangle$ is the pseudonym, and $\tau^j_{(a,i)}$ is the public key.
5:Stores $S^j_{(a,i)} = \gamma^j_{(a,i)} S_a$ as the private key.
```

C. Anonymous Communication in PACP

Here, we illustrate anonymous communication using PACP. We use two vehicles, namely, V_a and V_b, for our illustration. Consider a scenario where V_a needs information about the road conditions. V_a sends a broadcast request for the information using its pseudonym PN$^j_{(a,i)}$. Vehicle V_b that has the information uses pseudonym PN$^j_{(a,i)}$ to encrypt it in a message and sends it to V_a. On receiving the encrypted message, V_a decrypts the message using private key $S^j_{(a,i)}$. In another scenario, vehicle V_a can itself initiate a road conditions broadcast. When V_a broadcasts a message with road conditions in its vicinity, other vehicles can use the public key of its pseudonym $\tau^j_{(a,i)} = \gamma^j_{(a,i)} S_a P$ to verify the BLS signature generated by V_a using private key $\gamma^j_{(a,i)} S_a$. In what follows, we describe the encryption and decryption procedures.

Algorithm 3: Encryption Protocol performed by V_b

```
Require: Pseudonym PN$^j_{(a,i)}$ of $V_a$ and message $\mathcal{M}$.
1:Verify SIG$(\tau^j_{(a,i)}, t_{(a,i)}; S_{R_i})$ and compute $\lambda^j_{(a,i)} =$
  $e(\tau^j_{(a,i)}, \sigma^j_a P)$.
2:Choose $k \in \{0,1\}^n$ randomly.
3:Compute $\rho = H_2(k, \mathcal{M})$.
4:Compute ciphertext as
  $\mathcal{C} = \langle H(\rho P) \oplus (\lambda^j_{(a,i)})^k, e(P, \sigma^j_a P)^k, \mathcal{M} \oplus$
  $H_1(e(\sigma^j_a P, H(\rho P) P))\rangle$.
5:Transmit $\mathcal{C}$ to $V_a$.
```

Encryption Protocol: Algorithm 3 illustrates the encryption protocol used by V_b to send a message to V_a. Vehicle V_b receives the pseudonym of V_a and first verifies signature SIG$(\tau^j_{(a,i)}, t_{(a,i)}; S_{R_i})$ to ensure that V_a is a genuine member of the system and has been authenticated by an RSU. For verification, V_b first verifies Cert$_{R_i}$ using P_{MVD} and then uses R_i from Cert$_{R_i}$ to verify signature SIG$(\tau^j_{(a,i)}, t_{(a,i)}; S_{R_i})$. If verification is successful, V_b computes

$$\lambda^j_{(a,i)} = e\left(\tau^j_{(a,i)}, \sigma^j_a P\right).$$

To encrypt the plain-text message $\mathcal{M} \in \{0,1\}^n$ for V_a with pseudonym PN$^j_{(a,i)}$, V_b performs Steps 2–4 of Algorithm 3. Symbol $\oplus$ stands for the XOR operation.

Decryption Protocol: To decrypt ciphertext $\mathcal{C}$ sent by V_b, V_a performs the decryption protocol given in Algorithm 4. We denote ciphertext $\mathcal{C}$ using the tuple $\mathcal{C} = \langle U, V, W\rangle$, where $U = H(\rho P) \oplus (\lambda^j_{(a,i)})^k$, $V = e(P, \sigma^j_a P)^k$, and $W = \mathcal{M} \oplus H_1(e(\sigma^j_a P, H(\rho P) P))$. The protocol is fairly self-explanatory. The decryption of $\mathcal{C}$ is done using private key $S^j_{(a,i)}$.

Algorithm 4: Decryption Protocol performed by V_a

```
Require: $C = \langle U, V, W \rangle$, $S^j_{(a,i)}$.
Compute $\Gamma^j_{(a,i)} = U \oplus V^{S^j_{(a,i)}}$.
Retrieve $\mathcal{M}' = W \oplus H_1(e(\sigma^j_a P, \Gamma^j_{(a,i)} P))$.
```

Now, we will show the correctness of the encryption and decryption protocols. We first demonstrate the correctness of hash operation H_1 that is used in the encryption and decryption protocols (see Algorithms 3 and 4). To prove the correctness of the encryption and decryption protocols, we need to show that XOR-ing of W with $H_1(e(\sigma^j_a P, \Gamma^j_{(a,i)} P))$ recovers message $\mathcal{M}$, as shown in the equation at the bottom of the page. From the preceding derivations, we have

$$H_1\left(e\left(\sigma^j_a P, \Gamma^j_{(a,i)} P\right)\right) = H_1\left(e\left(\sigma^j_a P, H(\rho P) P\right)\right). \tag{1}$$

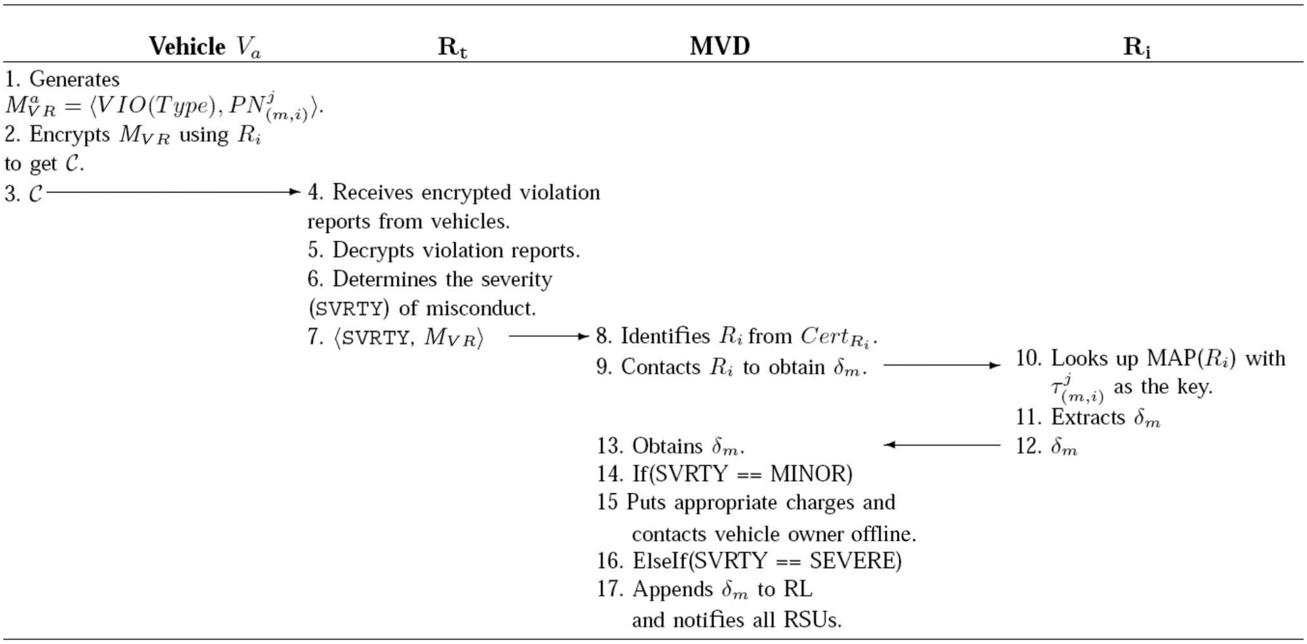
Using (1), it is easy to prove that XOR-ing W with $H_1(e(\sigma^j_a P, \Gamma^j_{(a,i)} P))$ recovers message $\mathcal{M}$. We note that, in [20], Boneh and Franklin proved that the hash functions in the *FullIndent* scheme are secure against the chosen ciphertext attack under the random oracle model. Hash function H_1 that is used in the PACP scheme possesses this property. Next, we present the revocation protocol.

D. Revocation Protocol

Revocation is a critical issue for an anonymous communication system. In VANETs, revocation is required to prevent malicious vehicles from launching security attacks against legitimate vehicles. Fig. 3 shows our revocation protocol.

If a vehicle has performed a violation, other vehicles in its vicinity would have observed the violation and will report the violator to the nearest RSU. The reporting vehicles will use the pseudonym of the violating vehicle to identify it. The violation events are recorded by the EDR of the vehicles. The EDR of a reporting vehicle V_a instructs the OBU to create a violation report (M^a_{VR}). The OBU creates $M^a_{\mathrm{VR}} = \langle \mathrm{VIO(Type)}, \mathrm{PN}^j_{(m,i)} \rangle$, where $\mathrm{VIO(Type)}$ is the type of violation, and $\mathrm{PN}^j_{(m,i)}$ is the pseudonym used by the alleged malicious vehicle V_m. Designing the violation message is trivial; hence, we do not discuss it in this paper. When V_a enters the communication range of an RSU, the message (M^a_{VR}) is encrypted using the RSU's identity and transmitted to it. All vehicles reporting the event will report their violation report to the nearest RSU. For instance, let the RSU closest to V_a be denoted by R_t. Vehicle V_a and other vehicles in the vicinity send their violation report to R_t. RSU R_t decrypts all messages received from the vehicles (including V_a) and determines the severity of the violation by analyzing the messages. Then, RSU R_t sends pseudonym $\mathrm{PN}^j_{(m,i)}$ used by V_m to the MVD for revocation. The MVD identifies RSU R_i that had given V_m the token by using Cert_{R_i} contained in the pseudonym. The MVD contacts R_i and obtains δ_m, i.e., the vehicle's ticket, from R_i. The MVD then looks up the mapping $\mathrm{map}^m_{\mathrm{MVD}}$ and extracts ID_m the identity of vehicle V_m using the ticket. Once V_m is identified, the MVD transmits the ticket of V_m to all the RSUs in the network in the form of an updated RL. If R_t is compromised in the presented revocation protocol, in which it may collude with V_m, then V_m cannot be revoked. However, we note that an easy fix to this problem is to have the reporting vehicle transmit revocation reports to multiple RSUs. Since we assume that only a few RSUs can be compromised, as long as one revocation report reaches the MVD, the malicious vehicle V_m can be identified. If a vehicle V_m is in the RL, then the RSUs do not help it in generating tokens for anonymous

$$\begin{aligned}
H\left(e\left(\sigma^j_a P, \Gamma^j_{(a,i)} P\right)\right) &= H_1\left(e\left(\sigma^j_a P, \left(U \oplus V^{S^j_{(a,i)}}\right) P\right)\right)\\
&= H_1\left(e\left(\sigma^j_a P, \left(\underbrace{H(\rho P) \oplus (\lambda_j)^k}_{U} \oplus \underbrace{e\left(P, \sigma^j_a P\right)^{k S^j_{(a,i)}}}_{V^{S^j_{(a,i)}}}\right) P\right)\right)\\
&= H_1\left(e\left(\sigma^j_a P, \left(H(\rho P) \oplus (\lambda_j)^k \oplus e(P,P)^{k\gamma^j_{(a,i)} S_a \sigma^j_a}\right) P\right)\right)\\
&= H_1\left(e\left(\sigma^j_a P, \left(H(\rho P) \oplus e\left(\tau^j_{(a,i)}, \sigma^j_a P\right)^k \oplus e(P,P)^{k\gamma^j_{(a,i)} S_a \sigma^j_a}\right) P\right)\right)\\
&= H_1\left(e\left(\sigma^j_a P, \left(H(\rho P) \oplus e\left(\gamma^j_{(a,i)} \delta_a, \sigma^j_a P\right)^k \oplus e(P,P)^{k\gamma^j_{(a,i)} S_a \sigma^j_a}\right)\right) P\right)\\
&= H_1\left(e\left(\sigma^j_a P, \left(H(\rho P) \oplus e\left(\gamma^j_{(a,i)} S_a P, \sigma^j_a P\right)^k \oplus e(P,P)^{k\gamma^j_{(a,i)} S_a \sigma^j_a}\right)\right) P\right)\\
&= H_1\left(e\left(\sigma^j_a P, \left(H(\rho P) \oplus e(P,P)^{k\gamma^j_{(a,i)} S_a \sigma^j_a} \oplus e(P,P)^{k\gamma^j_{(a,i)} S_a \sigma^j_a}\right) P\right)\right)\\
&= H_1\left(e\left(\sigma^j_a P, H(\rho P) P\right)\right)
\end{aligned}$$



1. Generates $M^a_{VR} = \langle VIO(Type), PN^j_{(m,i)}\rangle$.
2. Encrypts M_{VR} using R_i to get $\mathcal{C}$.
3. $\mathcal{C}$ →
4. Receives encrypted violation reports from vehicles.
5. Decrypts violation reports.
6. Determines the severity (SVRTY) of misconduct.
7. $\langle$SVRTY, $M_{VR}\rangle$ →
8. Identifies R_i from $Cert_{R_i}$.
9. Contacts R_i to obtain δ_m. →
10. Looks up MAP(R_i) with $\tau^j_{(m,i)}$ as the key.
11. Extracts δ_m
12. δ_m
13. Obtains δ_m.
14. If(SVRTY == MINOR)
15 Puts appropriate charges and contacts vehicle owner offline.
16. ElseIf(SVRTY == SEVERE)
17. Appends δ_m to RL and notifies all RSUs.

Fig. 3. Schematic of the revocation protocol. Vehicle V_m is the vehicle to be revoked, and V_a is the reporting vehicle.

communication. This effectively revokes V_m once its current pseudonyms expire. In a more proactive mechanism, the RSUs can broadcast the pseudonym of V_m to the other vehicles to incorporate revocation. The revocation cost is negligible since checking is performed between an RSU and the MVD, which we assume to be connected using the Internet.

V. Performance Assessments of Security and Privacy

Here, we first analyze the security and anonymity strength of our PACP scheme with reference to the attack scenarios presented in Section III-C. Then, we compare the security performance between PACP and ECPP.

A. Security and Anonymity Analysis

In the PACP scheme, signature and encryption are fundamental security protections to counter modification, eavesdropping, replay, and injection and impersonation attacks. To modify a message sent by vehicle V_b to vehicle V_a, the adversary has to decrypt the message, modify it, and then encrypt it using V_a's pseudonym. To decrypt the message, the adversary needs the private key corresponding to the pseudonym of V_a, which is not available to the adversary, thus making it impossible to modify the message. Without going into the details, we note that replay attacks can be easily prevented with the use of authentication and sequence numbers. Using PACP, an external attacker cannot generate a valid signature using other vehicles' pseudonym. As a result, it cannot inject fake messages into the system.

Theorem 1: The PACP scheme is semantically secure against the impersonation attack.

Proof: Our proof is based on sematic security. In general, a semantic security proof assumes that the attackers are passive. The sematic security proof is usually done by reducing the solution to a well-known hard problem, such as the ECDLP used in this paper.

To perform an impersonation attack, the adversary must be able to derive the secret, i.e., S_a, owned by a legitimate vehicle V_a. To assess the security strength of the PACP scheme, we use the fact that the ECDLP is computationally hard. The proof of hardness of ECC is also based on the fact that the ECDLP is computationally hard. We show that either the adversary cannot attack a building block of the PACP scheme or those that it can attack are semantically secure. The registration protocol cannot be compromised by the adversary as it is performed offline, whereas the extraction protocol cannot be compromised by an adversary as it has no message exchanges.

We now consider the encryption protocol. An adversary cannot impersonate a legitimate noncompromised vehicle V_a as the message encrypted using V_a's pseudonym cannot be decrypted without using V_a's private key, which the adversary does not possess. Since k is randomly chosen, ρ is also random. Consequently, the contents of $\mathcal{C}$ are random for the adversary.

The generation and decryption protocols are the only protocols that an adversary could attack to break down the system. In what follows, we show that these protocols are semantically secure.

- *Generation protocol:* The adversary will want to attack the generation protocol to obtain S_a. However, even if the adversary compromises an RSU R_i and obtains ticket δ_a $(= S_aP)$, obtaining S_a from δ_a is at least as hard as solving the ECDLP. Hence, it cannot obtain the true identity of V_a. In addition, if V_a uses multiple tickets obtained from the MVD, every time it interacts with R_i, it can use a randomly chosen ticket; thus, the ticket itself cannot lead to the compromise of V_a's secret S_a. The communication between an uncompromised RSU and V_a is also secure since the traffic is protected by the encryption using $K_{(a,i)}$. In addition, $\gamma_{(a,i)}$ is random, making $\mathcal{C}'$ random as well.

- *Decryption protocol:* Parameters P, $\sigma_a^j P$, and $\tau_{(a,i)}^j$ are publicly known. To decrypt a message, the adversary attempts to reduce $\tau_{(a,i)}^j$ to obtain $S_{(a,i)}^j$ (corresponding private key). Another direction of attack may be for the adversary to attempt to unmask the XOR value $H_1(e(\sigma_a^j P, H(\rho P)P))$ associated with the message. The adversary cannot generate the private key as it is equivalent to solving the ECDLP. In addition, the adversary cannot unmask the hash value because the unmasking operation requires the computation of a pairing on $H(\rho P)P$ and $\sigma_a^j P$. In addition, the adversary also does not possess $\mathcal{M}$ and random number k. All these ensure that the adversary cannot decrypt the message.

This proves that the PACP scheme is semantically secure and the attackers cannot derive any secrets of vehicle V_a. As a result, the adversary cannot use a pseudonym for vehicle V_a to generate a valid signature for impersonation attacks. ■

Theorem 2: PACP is secure against colluding attacks to discover the vehicle's identity.

Proof: The goals of using pseudonyms are twofold: 1) preventing attackers from linking actions from the same vehicle and 2) preventing attackers from discovering the real identity of the vehicle (or discover the private key). Preventing attackers (including colluding attackers) from linking actions performed by the same vehicle can be achieved by using multiple pseudonyms for each communication session, road segment, or time period. This can be achieved by deriving multiple pseudonyms from RSUs, which has been proposed by many previous solutions. PACP can achieve a similar level of anonymity using the same approaches. However, the trust model of using PACP is different from previous solutions, as we will discuss in Section V-B. Preventing attackers from discovering the real identity of a vehicle has been discussed in Theorem 1. Thus, PACP achieves its desired anonymity properties. ■

B. Comparative Study With ECPP

Now, we compare the security of our PACP scheme with the ECPP scheme [6]. We compare PACP with ECPP as both of them aim to achieve anonymous and unlinkable communication for the vehicles and both are based on ECC. ECPP provides mutual authentication between RSUs and vehicles, and its protocol that generates the anonymous keys forms the basis for anonymity. ECPP has been demonstrated (using the hardness of the ECDLP) to be secure against impersonation and compromised RSUs. In PACP, the generation algorithm uses the same basis for anonymity. We have proved in Theorem 1 that it is computationally hard for the adversary to compromise the generation protocol or impersonate either the vehicle or the RSU. The ECPP protocol aims at designing a secure privacy protocol for transmission of safety messages while at the same time allowing for fast revocation of the malicious vehicles. PACP provides the same security and privacy features with a faster revocation mechanism. Particularly, the search for the malicious vehicles in the RSUs and the MVD's databases has an asymptotic time complexity of $\mathcal{O}(M)$, in comparison with $\mathcal{O}(M \log N)$ for ECPP, where M is the number of vehicles to be revoked, and N is the total number of vehicles. This is due to the use of hash maps to store two mappings between the token and the ticket at the RSU, and the ticket and the ID at the MVD, which allow $\mathcal{O}(1)$ lookup for each revoked vehicle.

The operation model is different in that the pseudonym generation of PACP is done by the vehicles, which is better than their generation at the RSUs, as is done in ECPP. This puts less burden on an RSU and allows it to be more effective in handling denser traffic. The aforementioned analysis shows that PACP will scale better than ECPP.

VI. Evaluation Results and Analyses

Here, we present our evaluation results. The schemes proposed in the literature can be broadly categorized into those based on elliptical curve cryptography and those based on RSA. We compare our PACP protocol with the best schemes in each category. The schemes we compare with are the elliptical-curve-based VANET standard named ECIES [22], the ECPP scheme [6], and the RSA-based schemes in [11]. In Theorem 1, we proved that our PACP protocol is secure against the presented attack scenarios. Here, we show that our protocol can be implemented in current generation vehicular networks and that it admirably performs in comparison with the existing schemes. We compare the schemes on the basis of average latency experienced at the RSUs for pseudonym generation, the time taken to perform the encryption and decryption protocols that ensure anonymity, and the running time complexity of revocation. The latency experienced at the RSU has to be as small as possible because high latency results in a few number of vehicles obtaining their tokens in a given time period. Not all schemes can be compared with PACP on the aforementioned comparison criteria. For the latency measurements, we compare with ECPP; for encryption and decryption, we compare with the ECIES- and RSA-based schemes; and for complexity analysis of revocation, we compare with the ECPP scheme. For the RSA-based schemes, the basic building block is RSA; hence, instead of comparing with each scheme, we compare PACP with only RSA.

All the schemes were implemented on our simulator written in C++. We do not use currently available simulators for VANETs because the results of the performance measurements are independent of the simulator used. For the elliptical curve and pairing operations, we used the Pairing-Based Cryptography (PBC) Library [23]. We also used the Crypto++ 5.4 Library [24] for the ECIES implementation, as well as routines such as the SHA-1 hash function. For ECC and pairing, we used the Type-A curve defined in the PBC library with the default parameters [23].

All our implementations were done on a 2-GHz machine with 2-GB memory, running Cygwin 1.5.25–15 [25] with the gcc version 3.3. All the results of analyses were averaged over 1000 randomized simulation runs. For RSA and ECC, we chose key sizes of 1024 and 160 bits, respectively, to ensure the same level of security.

Table IV presents the time taken to execute basic operations such as signing, encryption, and decryption for the various

TABLE IV
EXECUTION TIME OF BASIC OPERATIONS PER BLOCK

Notation	Time (ms)	Description
Signature generation & verification time		
T^{SG}_{RSA}	27.78	RSA signature generation.
T^{SV}_{RSA}	0.91	RSA signature verification.
T^{SG}_{BLS}	28.1	BLS signature generation.
T^{SV}_{BLS}	14.86	BLS signature verification.
Encryption & decryption time		
T^{E}_{RSA}	0.91	RSA encryption.
T^{D}_{RSA}	28.22	RSA decryption.
T^{E}_{IBE}	23.8	IBE encryption.
T^{D}_{IBE}	7.4	IBE decryption.
T^{E}_{ECIES}	30.30	ECIES encryption.
T^{D}_{ECIES}	20.41	ECIES decryption.
T^{E}_{PACP}	25.0	PACP encryption.
T^{D}_{PACP}	8.5	PACP decryption.
PACP protocol time		
T^{REG}_{PACP}	42.3	Registration protocol.
$T^{GEN–User}_{PACP}$	23.8	User in generation protocol.
$T^{GEN–RSU}_{PACP}$	58.86	RSU in generation protocol.
T^{EXT}_{PACP}	21.8	User in extraction protocol.
Miscellaneous time		
T_{pmul}	8.5	One point multiplication in $\mathbb{G}_1$.
T_{pair}	7.3	One pairing operation.

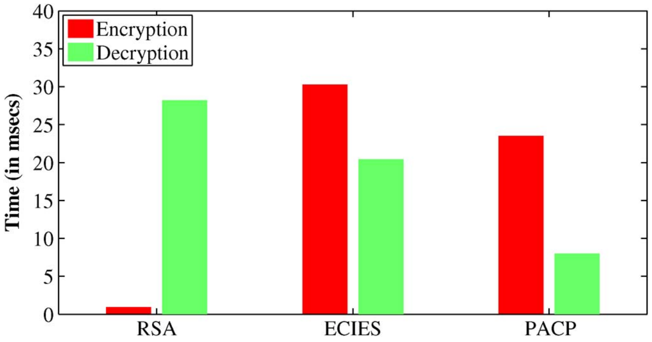


Fig. 4. Protocol comparison.

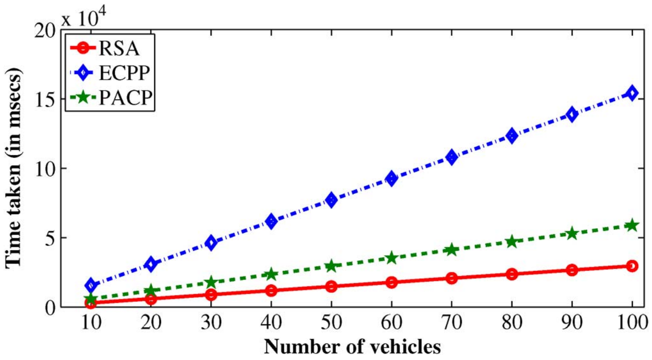


Fig. 5. Protocol latency comparison.

schemes. All the timings reported in Table IV are averaged over 1000 randomized runs.

Fig. 4 shows the time taken by RSA (RSA-based schemes), ECIES, and our PACP scheme to perform encryption and decryption. We ignore the other aspects of the corresponding protocols as they will take negligible time in comparison. The RSA protocol is much faster in comparison with ECIES and PACP in encryption; this is because in RSA, encryption generally uses a small prime number for exponentiation, which is very fast. The ECC scheme on which ECIES and PACP are based does not have this advantage; hence, the running time of encryption is higher in ECIES and PACP. We note that the performance of encryption in PACP is, on average, 18% better than that in ECIES. This is because the PACP protocol uses only two pairings and one-point multiplication operation, whereas ECIES uses three-point multiplications and one expensive map-to-point operation to provide the same level of security. For decryption, RSA has the worst execution time of the three schemes. Here, PACP outperforms RSA by 71.65% and ECIES by 60.80%, taking only 8 ms for decryption. In VANETs, having a small decryption time is highly desirable as it reduces the protocol overhead at the vehicles receiving the message. A smaller decryption time allows the vehicles receiving a message to decrypt the message faster, hence allowing more time for an appropriate response. The ciphertext size is similar for each of the presented solutions. However, PACP has the least payload size in comparison with the other schemes. This is because PACP uses the BLS signature scheme [26], in which the authors showed that a BLS signature of length 154 bits has security comparable with a 320-bit digital signature algorithm or a 320-bit elliptic curve digital signature algorithm.

Fig. 5 shows the comparison between the total time taken by an RSU for token generation when the RSA-based, ECPP, and PACP schemes are used. We study the total time for token generation at the RSU because it is also an overhead of the anonymity protocols, and the lower the total time required, the more desirable the protocol. The number of vehicles communicating with the RSU was increased from 10 to 100, and for each vehicle, ten tokens were requested. As we have pointed out before, low latency at the RSU is desirable as it allows more vehicles to obtain tokens from the RSU. The latency at the RSU for the generation of a single token using each of the three schemes is given as $T^l_{\mathrm{RSA}} = 29.6$ ms, $T^l_{\mathrm{ECPP}} = 154.3$ ms, and $T^l_{\mathrm{PACP}} = 58.86$ ms. For RSA, T^l_{RSA} is dominated by the sum of the time taken by the RSU to verify the vehicle's identity certificate, the time required to sign the new pseudonym, and, finally, the time required to encrypt the pseudonym with the public key of the vehicle. For ECPP, the latency is computed as the total time taken by the RSU to perform 13-point multiplication and six pairing operations [6]. The time consumed by other operations such as random number generation is ignored. In our PACP scheme, the latency is the sum of the time taken by the RSU to decrypt the message, verify the signature of the ticket, perform a point multiplication, and generate the signature of the token. The time taken for performing symmetric key encryption is negligible. We ignore the time taken for communication between the vehicle and the RSU, as our objective is to demonstrate the latency of computation of the tokens. The communication latency does not depend on our scheme but instead depends on factors such as the number of vehicles communicating with the RSU, the number of tokens per vehicle, and the medium-access control protocol. This latency affects all protocols in the same way.

From the figure, it is clear that the RSA-based solutions have the least latency, followed by the PACP and ECPP schemes.

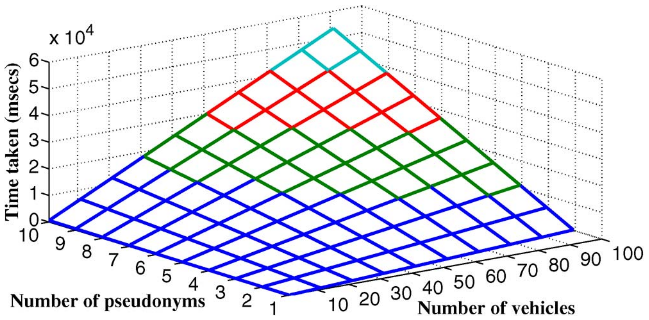


Fig. 6. Protocol latency analysis of PACP.

The reason for low latency in RSA is because of the efficiency of the public key operations for encryption.

However, the RSA-based schemes have their own drawbacks. First, the decryption at the vehicle is generally very slow and, hence, may not be applicable in a practical setting. Second, and more importantly, the existing RSA-based schemes do not provide the same level of security as PACP. In these schemes, when an RSU issues a pseudonym, it also gets to know the pseudonym. If the RSU is compromised, all the pseudonyms issued by the RSU will be known to the attacker. As a result, the attacker can easily track all the vehicles that use the pseudonyms issued by the compromised RSU. In comparison, in our PACP scheme, the pseudonyms are unknown to the RSUs; hence, PACP provides improved security. When compared with the popular ECPP scheme, our PACP scheme has less than half the latency. This is because of the use of fewer pairing and multiplication operations. Hence, PACP is more secure and efficient when compared with the existing RSA-based schemes and ECPP in terms of RSU latency. Fig. 6 shows the time taken by a single RSU for token generation when the number of vehicles increases from 1 to 100 and the number of pseudonyms required by each vehicle increases from 1 to 10. With an increase in the number of vehicles or the number of pseudonyms, the latency at the RSU increases because the RSU has to generate more tokens. We note that our scheme scales pretty well. Even when the number of vehicles is 100 and the number of pseudonyms required is 10, the latency for pseudonym generation is less than 60 s.

Fig. 7 shows the comparison of the time taken by an RSU and the MVD to search for a vehicle to revoke it from the system. We compare our scheme with the ECPP scheme as it is the only scheme in the literature that studies node revocation in any significant detail. In our PACP scheme, the MVD and the RSUs take much less time to search the revoked node, in comparison with that in the ECPP scheme. This is because of the difference in the asymptotic complexity of search operation as discussed in Section IV-C. Hence, our scheme is faster.

The simulation results and the security analyses demonstrate the effectiveness and efficiency of our PACP scheme. Our scheme has a protocol latency that is comparable to the faster schemes based on RSA while having much lower search and revocation times when compared with the ECPP scheme; this shows that it will scale well with the increase in the number of vehicles in the network. Hence, PACP provides high security and better scalability.

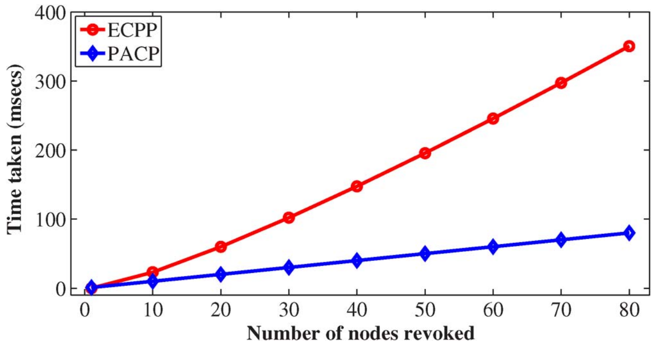


Fig. 7. Comparison of search times for revocation.

VII. Conclusion and Future Work

In this paper, we have proposed a novel PACP protocol for the vehicles in VANETs. Our protocol not only provides the desired level of anonymity to the vehicles but also is efficient in computation and storage. It also performs better than other state-of-the-art schemes. In the future, we would like to evaluate PACP on a large-scale VANET testbed with varying vehicle mobility models.

References

[1] J. Blum, A. Eskandarian, and L. Hoffman, "Challenges of intervehicle ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 5, no. 4, pp. 347–351, Dec. 2004.

[2] M. Raya and J. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Security*, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[3] C. Zhang, R. Lu, X. Lin, P. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. IEEE INFOCOM*, Apr. 2008, pp. 246–250.

[4] H. Zhu, X. Lin, R. Lu, P. Ho, and X. Shen, "AEMA: An aggregated emergency message authentication scheme for enhancing the security of vehicular ad hoc networks," in *Proc. IEEE ICC*, May 2008, pp. 1436–1440.

[5] J. Hubaux and S. Luo, "The security and privacy of smart vehicles," *IEEE Security Privacy*, vol. 2, no. 3, pp. 49–55, May/Jun. 2004.

[6] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE INFOCOM*, Apr. 2008, pp. 1229–1237.

[7] P. Papadimitratos, A. Kung, J. Hubaux, and F. Kargl, "Privacy and identity management for vehicular communication systems: A position paper," in *Proc. Workshop Standards Privacy User-Centric Identity Manage.*, Zurich, Switzerland, Jul. 2006.

[8] I. Blake, G. Seroussi, and N. Smart, *Advances in Elliptic Curve Cryptography*. Cambridge, U.K.: Cambridge Univ. Press, 2005, ser. London Mathematical Society Lecture Note Series 317.

[9] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.

[10] I. Blake, V. Murty, and G. Xu, "Refinements of Miller's algorithm for computing the Weil/Tate pairing," *J. Algorithms*, vol. 58, no. 2, pp. 134–149, Feb. 2006.

[11] M. Raya, P. Papadimitratos, and J. Hubaux, "Securing vehicular communications," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 8–15, Oct. 2006.

[12] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[13] A. Wasef and X. Shen, "PPGCV: Privacy preserving group communications protocol for vehicular ad hoc networks," in *Proc. IEEE ICC*, May 2008, pp. 1458–1463.

[14] H. Xie, L. Kulik, and E. Tanin, "Privacy-aware traffic monitoring," *IEEE Trans. Intell. Transp. Syst.*, vol. 11, no. 1, pp. 61–70, Mar. 2010.

[15] U.S. Department of Transportation, National Highway Traffic Safety Administration, Vehicle Safety Communications Project—Final Rep., Apr. 2006. [Online]. Available: http://www.nhtsa.gov/DOT/NHTSA/NRD/Multimedia/PDFs/Crash%20Avoidance/2005/CAMP3scr.pdf

[16] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proc. 3rd ACM Workshop Security Ad Hoc Sens. Netw.*, 2005, pp. 11–21.

[17] C. Cseh, "Architecture of the Dedicated Short-Range Communications (DSRC) protocol," in *Proc. 48th IEEE VTC*, May 1998, vol. 3, pp. 2095–2099.

[18] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication," *J. Commun. Netw.*, vol. 11, no. 6, pp. 574–588, 2009.

[19] A. Menezes, S. Vanstone, and T. Okamoto, "Reducing elliptic curve logarithms to logarithms in a finite field," in *Proc. 23rd Annu. ACM STOC*, 1991, pp. 80–89.

[20] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. 21st Annu. Int. Cryptology Conf. Adv. Cryptology*, 2001, pp. 213–229.

[21] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," in *Proc. Asiacrypt*, vol. 2248, *LNCS*, 2001, pp. 514–532.

[22] *Unapproved IEEE Draft Trial-Use Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages Replaced by Approved Draft*, IEEE Std. P1609.2/D7, 2006.

[23] Pairing-Based Cryptography Library. [Online]. Avaialble: http://crypto.stanford.edu/pbc/

[24] Crpto++ Library 5.5.2: A Free C++ Class Library of Cryptographic Schemes. [Online]. Avaialble: http://www.cryptopp.com/

[25] Cygwin: Linux Environment Emulator for Windows. [Online]. Available: http://www.cygwin.com/

[26] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *J. Cryptol.*, vol. 17, no. 4, pp. 297–319, 2004.

Dijiang Huang (M'00–SM'11) received the B.S. degree from Beijing University of Posts and Telecommunications, Beijing, China, in 1995 and the M.S. and Ph.D. degrees from the University of Missouri-Kansas City in 2001 and 2004, respectively.

In 2005, he joined Arizona State University, (ASU), Tempe, as an Assistant Professor. He is currently an Associate Professor with the School of Computing, Informatics, and Decision Systems Engineering, ASU. His current research interests are computer networking, security, and privacy. His research has been supported by federal agencies, including the National Science Foundation, the Office of Naval Research (ONR), the Air Force Research Laboratory, and the U.S. Army Research Office.

Prof. Huang is an Editor of the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS and an Associate Editor of the *Journal of Network and Systems Management*. His recent conference services include being a Technical Program Committee Cochair of the 2011 IEEE Globecom Communication and Information System Security Symposium and a Symposium Cochair of the 2012 Mobile Computing and Vehicle Communications of the International Conference on Computing, Networking, and Communications. He was a recipient of the 2010 ONR Young Investigator Award.

Satyajayant Misra (M'04) received the integrated M.Sc. (Tech.) information systems and M.Sc. (Hons.) physics degrees from Birla Institute of Technology and Science, Pilani, India, in 2003 and the Ph.D. degree in computer science from Arizona State University, Tempe, in 2009.

He is currently an Assistant Professor with the Department of Computer Science, New Mexico State University, Las Cruces. His research interests include algorithm and protocol design for security, privacy, reliability, and efficient energy harvesting in wireless networks.

Prof. Misra serves on the Editorial Board of the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS. He has served on the Executive Committee of the 2011 IEEE Communications Society Conference on Sensor, Mesh, and Ad Hoc Communications and Networks and on the Technical Program Committee of several conferences. He will serve as the Vice Chair for Information Systems for the 2012 IEEE Conference on Computer Communications.

Mayank Verma (M'06) received the M.S. degree from Arizona State University, Tempe, in 2008.

He is currently a Security and Networking Engineer with Brocade Communications, Encinitas, CA.

Guoliang Xue (M'96–SM'99–F'11) received the B.S. degree in mathematics and the M.S. degree in operations research from Qufu Normal University, Qufu, China, in 1981 and 1984, respectively, and the Ph.D. degree in computer science from the University of Minnesota, Minneapolis, in 1991.

He is currently a Professor of computer science and engineering with Arizona State University, Tempe. He has been continuously supported by federal agencies, including the National Science Foundation (NSF) and the U.S. Army Research Office. His research interests include survivability, security, and resource allocation issues in networks, ranging from optical networks to wireless mesh and sensor networks. He has published more than 180 papers in the aforementioned areas.

Prof. Xue is an Associate Editor of the IEEE/ACM TRANSACTIONS ON NETWORKING and *IEEE Network Magazine*, as well as an Editorial Advisory Board Member of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. He served as an Associate Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and of the *Computer Networks* journal. His recent conference services include being a Technical Program Committee Cochair of the 2010 IEEE Conference on Computer Communications, a Symposium Cochair of the 2009 IEEE International Conference on Communications, and a General Cochair of the 2008 IEEE International Conference on High Performance Switching and Routing. He is a Distinguished Lecturer of the IEEE Communications Society. He was a recipient of the NSF Research Initiation Award in 1994, the Best Paper Award at the IEEE Global Communications Conference in 2007, and the Best Paper Runner-up Award at the IEEE International Conference on Network Protocols in 2010.