Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2011, Article ID 716794, 15 pages
doi:10.1155/2011/716794

Research Article

Secure and Efficient Protocol for Vehicular Ad Hoc Network with Privacy Preservation

Hyoung-Kee Choi, In-Hwan Kim, and Jae-Chern Yoo

School of Information and Communication Engineering, Sungkyunkwan University, Seoul 110-745, Republic of Korea

Correspondence should be addressed to Jae-Chern Yoo, yoojc@skku.edu

Received 8 June 2010; Revised 18 August 2010; Accepted 15 September 2010

Academic Editor: Damien Sauveron

Security is a fundamental issue for promising applications in a VANET. Designing a secure protocol for a VANET that accommodates efficiency, privacy, and traceability is difficult because of the contradictions between these qualities. In this paper, we present a secure yet efficient protocol for a VANET that satisfies these security requirements. Although much research has attempted to address similar issues, we contend that our proposed protocol outperforms other proposals that have been advanced. This claim is based on observations that show that the proposed protocol has such strengths as light computational load, efficient storage management, and dependability.

1. Introduction

We are evolving into a society with nearly constant access to the Internet and its vast wealth of information. The key driver of this evolution has been the desire for data sharing through opportunistic contacts in collaborative networks. In this opportunistic environment, the "always-on" assumption is relaxed by allowing data transport even in the absence of a contemporaneous end-to-end path between the source and the destination. This paradigm is a radical departure from the traditional end-to-end communication model pursued in the Internet and falls in the general category of a delay-tolerant network (DTN) [1]. This opportunistic network is distributed and self-organizing in that the control and management are largely up to the individual devices or users. These devices and users are collaborative in the sense that they cooperate to mutually benefit from one another's role in the network in order to maximize the network's utility and possibly to attain a common goal.

This evolution continues even today, and we have witnessed the placement of ad hoc networks in a primary position to represent an opportunistic collaborative network. Forms of this emergent communication paradigm are wide ranging and include low-cost Internet service provision in remote, social-based networks to allow humans to communicate without network infrastructure, pocket-switched networks, underwater networks, or other situations that impose gatekeepers. In particular, we are interested in the vehicular ad hoc network (VANET). In a VANET, vehicles ask to communicate with nearby vehicles with the goal of propagating traffic-related information (referred to as V2V communication) and also seek to communicate with fixed roadside infrastructures (RSUs) as a way to connect to outside networks such as the Internet (denoted as V2I communication). VANETs are expected to greatly enhance drivers' safety and improve the efficiency with which information on local traffic conditions is disseminated. However, the communication model for these versatile networks is unprecedentedly unique compared with other popular networks. Among these unique and challenging features are rapid topological changes in combination with fast-moving vehicles, frequent network fragmentation because of sporadic connectivity, and a small effective network diameter. The latter is because fixed-in-place roadways force the network to operate in an ad hoc manner and behave in ways drastically different from a generic ad hoc network such as the mobile ad hoc network (MANET).

Because a VANET is a special implementation of an opportunistic collaborative network, all VANET applications rely on a trustworthy, secure, and collaborative network

infrastructure to provide correct traffic and road system data. Further, vehicles in the network are expected to behave selflessly and beneficially with other vehicles. However, these naive assumptions about infrastructure and user behavior are difficult to realize in such a highly dynamic and mobile communication environment, and traditional security frameworks are incapable of satisfying the volatile security demands of VANET applications.

Designing a security mechanism for VANET applications deployed in this insecure environment poses numerous unique challenges. First, data and information in the network must be shared efficiently and effectively. Popular districts or even busy streets may involve large numbers of vehicles; the number of messages generated by requests or the need for widespread message distribution can multiply the load of the network far beyond the mere number of vehicles. Some of these messages are so critical that authentication of the sender and a check of message integrity are essential for road safety. Cryptographic algorithms employed in authentication and in the integrity check should be *effective* enough to reduce the overhead in vehicles as well as in a few trusted authorities. The connectivity among vehicles can often be highly transient or a one-time event. Delivering a message may involve long delays of recurrent hops to establish a path to a personal contact on the other side of a VANET while at the same time trust gradually develops as a circle of trusted acquaintances enlarges. Further, many of the envisioned safety and driver-assistance applications pose strict deadlines on their time-sensitive messages. Security mechanisms must take this constraint of *efficiency* into consideration.

The second challenge is to preserve privacy within a secure network. Drivers and passengers value their privacy and are unlikely to adopt applications that require them to forfeit it. It is difficult to satisfy simultaneously these security and privacy challenges. In the course of authentication for security, a vehicle broadcasts considerable information related to its identity and location. Drivers and passengers with malicious intent could take advantage of this freely available information to record and trace individual vehicles. On the other hand, if we attempt to make a vehicle anonymous simply by assigning it a temporary identity, it can only be tracked and recorded for the duration of this assigned identity. Although an adversary might be unable to link several temporary identities to a specific vehicle, a potential side effect of such anonymity might be less reliable information because drivers might tend to spread false messages when there is no risk of being caught.

The third challenge arises from those situations in which drivers argue because of incorrect information broadcast over the network, and an authority must arbitrate the dispute. As far as privacy is concerned, authorities may not be able to assign liability to a vehicle that diffuses bogus messages if there is no link to the identity of the vehicle. Accordingly, the degree of privacy available in a VANET must be relaxed from stringent to *conditional* that user-related private information must be protected while the authorities should be able to reveal the identities of message sender in order for the liability stands. In any case, safety and the liability requirement it entails have top priority and supersede the privacy requirement.

Our goal in this paper is to take significant steps toward designing a security protocol for a VANET that satisfies these three requirements. The issue of how to provide anonymous yet traceable safety message authentication has become a fundamental design requirement in a vehicular network. The basic idea is to sign messages with ephemeral, anonymous, and traceable identities for both network security and user privacy. For effectiveness and efficiency, we adopted proxy signature cryptography [2, 3] to authenticate vehicles and RSUs and directed the RSUs to issue short-lived certificates only for authenticated vehicles. This issuance is authorized by a trusted third party. To use storage efficiently in the vehicle, the RSU maintains a list of revoked vehicles because sometimes the size of this list can grow fairly large. Consequently, mutual authentication between entities in a VANET occurs quickly in the proposed protocol while imposing only minimal additional overhead for management of these new security infrastructures. This form of conditional privacy is also supported with an ephemeral, anonymous, and traceable identity.

The main contributions of this paper are threefold: (1) We define the design requirements for a secure VANET through analysis of the features, strengths, and weaknesses of many security proposals. (2) We propose a protocol for enhanced VANET security of communications not only between vehicles but also between vehicles and RSUs. (3) We evaluate the proposed protocol by measuring delays between VANET components so as to compare the speed of the proposed protocol with other proposals.

The rest of the paper is organized as follows. In Section 2, we survey the features of many VANET security proposals. In Section 3, we analyze, and then define, the system model for a VANET. We also give a brief overview of the system architecture of the proposed protocol. Section 4 details the proposed security protocol for a VANET, followed by a security analysis in Section 5. Section 6 analyzes the performance of the proposed protocol in terms of computational delay, communication delay, and storage overhead. Section 7 presents our conclusions.

2. Related Work

Messages in a VANET contain traffic-related safety information, which makes it critical to preserve the accuracy of messages. Message authentication has been suggested as a way to ensure this accuracy. Historically, Public-Key Infrastructure (PKI) has played a vital role in authenticating such critical messages. Authenticity verification requires a public key for the source and also a certificate of this public key confirmed by the trusted authority (TA). A security weakness begins with this publically available certificate, which includes an owner's ID that can be used to identify vehicles. This disclosure of IDs offers significant threats to privacy in a VANET. The Message Authentication Code (MAC) has been suggested as a promising alternative. This new mechanism is based on symmetric-key cryptography.

Although it dispenses with the need for the certificate, this technique requires a preshared key that limits the scale of the technique. Only a few studies have tackled VANET security and privacy, despite the ultimate importance of these two issues. Those studies that have approached these issues can be categorized largely into three groups: (1) cryptographybased, (2) groupingbased, and (3) unlinkabilitybased.

Fortunately, efficient cryptography exists that can hide the identity of the sender of a message. Group signature [4] and blind signature [5] are examples of such cryptography. Lin et al. proposed a protocol based on a group signature [6]. Group Signature and Identity-based Signature (GSIS) is the name of this protocol. Recipients can verify a message's signature with the group's public key. If the signature is authentic, the recipient can confirm that the sender is a group member but cannot identify a specific person. Although its dispensing with the certificate is considered a GSIS advantage, the GSIS protocol adds a big computational overhead through its requirement to maintain a revocation list (RL). Zhang et al.'s protocol, called a Location Privacy Preserving Authentication Scheme (LPPAS), adopts a blind signature to protect VANET privacy [7]. This prevents vehicles from tracking each other, but it also makes it all but impossible to track faulty vehicles.

A grouping-based protocol has been proposed as a complementary (not a substitute) approach to privacy preservation. The key idea is to hide in a group a vehicle's explicit identity and location. This is a tradeoff of privacy preservation and information accuracy. In Zhang et al.'s protocol [8], a group of k vehicles is formed, all with the same identification. Nearby vehicles cannot tell a vehicle's real identity, only its group identity. Although aggregating traffic-related messages significantly decreases computational overhead, this approach still leaves a lot of room for improvement. Another grouping-based protocol proposed by Sha et al. adopts an authentication algorithm called Group ID-Tree [9]. In this protocol, a vehicle is able to connect to the RSU after proving its membership in a group. Managing group membership, however, leads to additional overhead in this protocol. The protocol proposed by the authors of [10] elects a group leader who then communicates with the RSU on behalf of the group. This protocol also suffers the disadvantage of the overhead associated with the RL management required to authenticate group membership.

A solution suggested as a third approach breaks this linkability along with the messages. Because linkability is caused by the same certificate being used repeatedly, the new approach uses a concept of ephemeral in issuing identifications and certificates. This approach leaves the identification in the message open to public access, but identifications, the two messages from the same vehicle are different. Raya and Hubaux protocol, called Huge Anonymous Certificate (HAP), installs a large number of certificates—about 43,800—in advance and randomly selects one of them to sign a message [11]. The authors of [12] proposed a protocol similar to HAP, the exception being its use of a short-lived anonymous certificate. Although these two protocols are impressive in protecting privacy, the overhead associated with storing certificates and revocation lists leaves room for improvement. In [13], Zhang et al. proposed another protocol for a VANET based on Identity-Based Encryption (IBE) cryptography [14]. A vehicle's identification is set to its public key, and the vehicle keeps changing its ID quickly to avoid being tracked. To efficiently generate a private key paired with the vehicle's short-lived ID, the TA's master secret is distributed securely among vehicles and saved in a tamper-proof device in each vehicle. This protocol is regarded as making a huge step toward reducing overhead in cryptographic operations. However, administrators are unlikely to adopt systems that require them to abandon their master keys. Lu et al.'s protocol, called Efficient Conditional Privacy Preservation Protocol (ECPP), sought to solve the storage requirement by using the RSU to manage the vehicle's certificate [15]. At the time of authentication, the RSU issues only ephemeral certificates for valid vehicles, eliminating the need for vehicles to manage the certificates and RL. Our work complements this ECCP work by providing another fully designed protocol to furnish a secure VANET environment.

3. System Model

Some design decisions were made in the course of building the system model. These decisions were made after taking into consideration both practical implementation and performance issues.

3.1. System Design Considerations. In V2I communication, messages are vulnerable to interception and manipulation by adversaries seeking to harm vehicles and networks. There also is the possibility that adversaries may impersonate the RSU to deliver wrong or false information to vehicles to disrupt communication. Another risk is impersonation of a legitimate vehicle as a means to access paid services illegally. Mutual authentication is essential to ensure that only authorized entities are allowed to access the network.

V2V communication contains such traffic-related information as traffic conditions, road safety, local danger warnings, and a vehicle's own behavior (e.g., emergency braking). Thus, the sharing of this information with other vehicles is not a concern. However, because the information contains safety-critical messages, an imposter could jeopardize both vehicles and road safety. Whereas the confidentiality of messages may be relaxed in V2V communication, the integrity of such messages remains essential. In addition, the source of the information must be identified before it is made available to the vehicles. This is because an integrity check can only ensure that a message is intact, not that it is accurate. Source authentication surely adds value to the protocol by elevating the level of trustworthiness of the message.

Exchange of private information is hard to avoid in the implementation of secure communications. Anonymity would allow resolution of some of the tension between authentication and privacy. This anonymity, however, should be conditional, given that there are requests by authorities and law enforcement that require that anonymity be overridden. In a continuing sense, the real identity of a vehicle should be traced and revealed by authorized personnel if the source of information is demanded in a dispute.

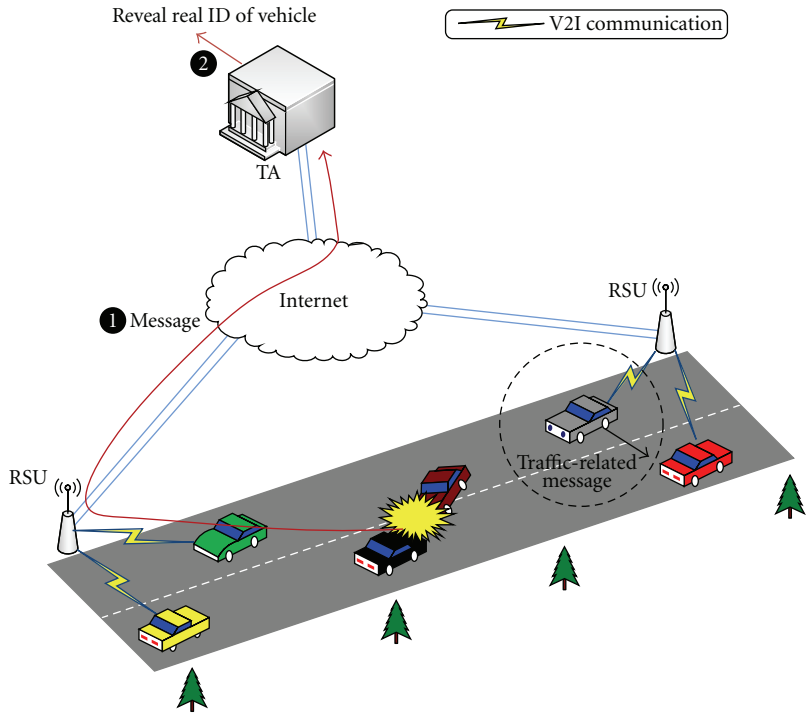

Figure 1: Vehicular network architecture.

A vehicle's misbehavior can result in the TA revoking its authorization to participate in the network. In order to isolate vehicles whose participation has been banned, the TA maintains a list of such vehicles and advertises the revocation list (RL) periodically in the network. The management of the RL is quite expensive in the context of the system operator. A vehicle searches the RL to determine if the source of the information is listed before using the traffic-related message. A vehicle must either save the RL in its own storage or check with other authorities. As the number of vehicles on the RL increases, a vehicle incurs either storage or bandwidth overhead.

3.2. Vehicular Network Architecture. Figure 1 illustrates the vehicular network architecture, which consists of three network entities: the TA, the immobile RSU at the roadside, and a vehicle.

An RSU is a gateway to a VANET, connecting a vehicle to the Internet. Traffic associated with V2I communication must go through this gateway. The RSU assists the TA in disputes in efficiently revoking vehicles and in tracking the real ID of vehicles. RSUs can be assumed to have absolute and relative locations that in most cases are fixed and thus often known or can be inferred straightforwardly.

A vehicle is a subject of communication and periodically broadcasts traffic-related messages of two kinds of information: (1) the vehicle's current condition, including its geographical position, current time, direction of movement, and speed; (2) traffic-related information such as traffic conditions, road accidents, and unusual traffic events. Each vehicle is equipped with a Global Positioning System (GPS). This device provides accurate time and positioning information to the vehicle.

A user can be the owner and/or the driver of the vehicle or, in general, any passenger. The association of vehicles and users is typically many-to-many; however, at each point in time only one user can operate a vehicle. For the rest of this discussion, we make the simplifying assumption that the user is the vehicle operator. Also, we do not distinguish between users and vehicles in any aspect of authentication. Vehicles in this model are equipped with tamper-resistant trusted components (TCs). The role of TCs is to protect the vehicle's cryptographic material and their use.

The TA generates cryptographic key materials for the RSU and the vehicle and delivers these keys to them over a secure channel. The TA also manages the list of vehicles whose participation has been revoked, periodically updates the list, and advertises the list to the network in order to isolate vehicles on the list. If a message sent by a vehicle creates a problem on the roadway, the TA is responsible for tracing and identifying the source of the message to resolve the dispute. We made two assumptions for the TA: (1) the TA is trusted by all parties in the system and (2) secure channels are established between the TA and RSUs and between the TA and vehicles using the transport layer security (TLS) protocol.

In reality, a VANET can have multiple regional TAs, and each TA is responsible for a given region (e.g., state or province). Other candidates for the TA role are automobile manufacturers. In any of the two cases, the different TAs will have to be cross certified so that vehicles from different regions or different manufacturers can authenticate each

other. These regional TAs will share their public keys and IDs with one another, and the size of a region is carefully controlled so as to allocate to a TA a manageable number of RSUs and vehicles. At the time of registration, a vehicle receives that vehicle's home TA public key and home ID in its region. Authentication in a foreign TA can be done by exchanging a vehicle's home and foreign TA information. For simplicity, we present a protocol that has only one TA in its system.

3.3. Cryptography Model. Authenticating two parties must have a channel to certify each party's identity. The traditionally popular key exchange algorithm, Diffie-Hellman, is vulnerable to a man-in-the-middle attack because two parties without any auxiliary channels cannot ascertain each other's identity. One of the popular forms of the channel is a common trusted authority (TA); this TA brokers authentication by certifying each party's identity. Hence, it requires that authentication be supported by at least three entities in the network without any weaknesses associated with this effort.

In an opportunistic collaborative network, however, it is hard to imagine that an on-line TA will be constantly available. During a rush hour, the number of vehicles may grow suddenly and quickly, generating numerous authentication requests to a few TAs. These TAs cannot respond in a timely manner because both the system and communication channels are overloaded. Hence, it is frequently impractical for vehicles to interact directly with each such TA to gain authentication.

Delegation of authorities has been suggested as a solution to the intermittently available TA and the occurrence of a single point of failure. A user (the delegator) grants some of her capability to another user (the delegate) in such a way that the delegate can act on behalf of the delegator. A receiver can simultaneously verify both the delegator's acknowledgement and delegation. This concept of delegation is a common practice in various circumstances and applications; examples of the practice include distributed computing [16, 17], grid computing [18], electronic commerce [19], and mobile communications [20].

The main issue in delegation of authorities is the nature of the credentials given to the delegate and how the delegate can obtain these credentials. A delegator could enable a delegate to act on her behalf by giving the delegate the appropriate credentials (e.g., a password or a private key). This simple approach has at least one significant weakness It introduces an increased risk of the credentials being compromised and abused. The more controlled approach is *delegation with warrant* [21]; that is, the delegator issues a temporary credential by signing her warrant with a secret. The warrant may include a validity interval, a list of identities which these credentials are entitled to, and/or other restrictions imposed by the delegator.

We introduced this concept of delegation into our framework by adopting a proxy signature. Vehicles and RSUs implement the proxy signature as a way to receive the TA's credentials. These credentials are used to authenticate vehicles and RSUs even if the TA is not available to assist authentication. These credentials are ephemeral, so that the vehicle and the RSU are responsible for renewing the credential before its validity expires. The compromised credentials are soon useless because of their temporary nature. Because at any one time the authentication authority of only a single TA is distributed to individual vehicles and RSUs, the risk of failed authentication because a TA is unavailable decreases substantially. At the same time, the load imposed on each TA is lessened, even at peak periods.

4. Proposed Mechanism

Our proposed protocol consists of four phases: setup, registration, V2I communication, and V2V communication. Table 1 lists the notations used throughout this paper to describe our proposed protocol.

4.1. System Setup Phase. The TA first generates a set of basic parameters for cryptography that is, $(q, G_1, G_2, G_T, e, P_1, P_2)$. Let G_1 and G_2 be two cyclic additive groups and G_T be a cyclic multiplicative group of the same prime order q, that is, $|G_1| = |G_2| = |G_T| = q$. Let P_1 be a generator of G_1, P_2 a generator of G_2, and e a bilinear map $e : G_2 \times G_2 \rightarrow G_T$. The TA chooses the master key $\in Z_q^*$, and computes $Y_1 = sP_1 \in G_1$ and $Y_2 = sP_2 \in G_2$ as its public keys. The TA also chooses three cryptographic hash functions $H_1 : (0,1)^* \rightarrow Z_q^*$, $H_2 : (0,1)^* \rightarrow G_2^*$, $H_3 : G_T^* \rightarrow (0,1)^*$. All public parameters published by the TA are $(q, G_1, G_2, G_T, e, P_1, P_2, Y_1, Y_2, H_1, H_2, H_3)$.

4.2. Registration Phase. The vehicle and the RSU are required to register themselves with the TA in order to receive private information for a proxy signature [22] and IBE cryptography [14]. A vehicle receives two kinds of information from the TA; pseudo-ID and the parameters required to implement a proxy signature. The RSU also receives from the TA the necessary parameters for the proxy signature and its private key. In order to prevent a vehicle from impersonating the RSU by using the TA's delegation and vice versa, the vehicle and the RSU are assigned to different groups (e.g., G_1 and G_2) in elliptic curve cryptography. This phase must precede the deployment of a vehicle and RSU into communication. The registration phase comprises two registrations for the vehicle and RSU, respectively. Algorithm 1 elaborates the registration procedure for the vehicle and RSU from the perspective of the TA.

4.2.1. Vehicle Registration. Vehicle V_i sends its identity ID_V to the TA and negotiates with the TA for a proper delegated period T_{Exp} for the proxy signature. Then, the TA performs the following steps to generate proxy parameters for V_i.

(1) Generate pseudo-ID of V_i PID_V and set warrant $W_V = (\mathrm{PID}_V, T_{\mathrm{Exp}})$.

(2) Choose a random number $a_1 \in Z_q^*$ and compute a delegated key pair (U_V, σ_V) as illustrated in (1). U_V is

Table 1: Notations and descriptions.

Notation	Descriptions
G_1, G_2	Cyclic additive groups
G_T	A cyclic multiplicative group
P_1, P_2	Generators of the cyclic additive group G_1, G_2
s	Master key of the TA
$Y_1 = sP_1,\ Y_2 = sP_2$	Public keys of the TA
e	A bilinear map $G_2 \times G_2 \rightarrow G_T$
q	The order of groups G_1, G_2, and G_T
W_i	Warrant of vehicle or RSU i
CERT_i	Short-lived anonymous certificate of vehicle i
d_i/Q_i	Private/public key of RSU i-based IBE
x_i/Y_i	Short-lived private/public key of vehicle i
σ_i/U_i	Delegated private/public key of vehicle or RSU i
SK_{ij}	Session key between vehicle i and RSU j

Data: Vehicle and RSU send their IDs to TA for registration
Result: Parameters for proxy signature
(1) **begin**
(2) **If** ID is vehicle's **then**
(3) Choose pseudo ID PID_V
(4) Set $W_V = (\text{PID}_V, T_{\text{Exp}})$
(5) Compute $U_V = H_1(W_V)P_1 + a_1P_1 \in G_1$ and $\sigma_V = -sH_1(U_V) - a_1 \in Z_q^*$
(6) Store the duplet $(\text{ID}_V, \text{PID}_V, W_V, \sigma_V)$
(7) **return** $(\text{PID}_V, U_V, W_V, \sigma_V)$
(8) **else if** ID is RSU's **then**
(9) Set $W_R = (\text{ID}_R, T_{\text{Exp}})$ and $\text{LID}_R = (\text{ID}_R, L_R)$
(10) Compute $U_R = H_1(W_R)P_2 + a_2P_2 \in G_2$, $\sigma_R = -sH_1(U_R) - a_2 \in Z_q^*$ and $Q_R = H_2(\text{LID}_R) \in G_2$ and $d_R = sQ_R \in G_2$
(11) Store $(\text{LID}_R, W_R, U_R, \sigma_R)$
(12) **return** $(\text{LID}_R, W_R, U_R, \sigma_R, d_R)$
(13) **end**
(14) **end**

Algorithm 1: Registration from TA's perspective.

a delegated public key, and σ_V is a delegated private key

$$U_V = H_1(W_V)P_1 + a_1P_1 \in G_1,$$
$$\sigma_V = -sH_1(U_V) - a_1 \in Z_q^*. \tag{1}$$

(3) Store duplet $(\text{ID}_V, \text{PID}_V, W_V, \sigma_V)$ in the database for future use.

(4) Return $(U_V, \text{PID}_V, W_V, \sigma_V)$ to V_i through the secure channel.

V_i accepts the delegated key pair (U_V, σ_V) if the following equation holds. The vehicle's delegated private key σ_V was created by the TA using the TA's master secret key s as follow:

$$H_1(W_V)P_1 = \sigma_V P_1 + H_1(U_V)Y_1 + U_V. \tag{2}$$

Correctness of (2). A verifier can be assured validation of the delegated key pair by confirming the inclusion of Y_1 in the equation.

$$\begin{aligned} &\sigma_V P_1 + H_1(U_V)Y_1 + U_V \\ &\quad = -sH_1(U_V)P_1 - a_1P_1 + sH_1(U_V)P_1 + U_V \\ &\quad = -a_1P_1 + U_V \\ &\quad = H_1(W_V)P_1. \end{aligned} \tag{3}$$

Table 2: Authentication and generation of short-lived anonymous certificate in V2I communication.

	Vehicle V_i		RSU R_j
(1)	M=($W_V, U_V, r_1P_1, \text{PID}_V, Y_V, TS_V$) Sign $M \Rightarrow (K, w)$ and Encrypt M and $(K, w) \Rightarrow (L, S)$	$\xrightarrow{(L,S)}$	
(2)			Decrypt (L, S) and verify (K, w) Compute session Key SK_{VR} Issue the CERT_V
		$\xleftarrow{C, r_2}$	Encrypt $(r_1, T_{\text{cert}}, \text{CERT}_V, TS_R) \Rightarrow C$
(3)	Generate session key SK_{VR} Decrypt C with SK_{VR} Check r_1 and verify CERT_V		

4.2.2. RSU Registration. At the outset, RSU R_j sends its identity ID_R and location information L_R to the TA. The TA selects a proper delegated period T_{Exp} for the proxy signature and performs the following steps to generate proxy parameters for R_j.

(1) Set warrant $W_R = (\text{ID}_R, T_{\text{Exp}})$ and location ID $\text{LID}_R = (\text{ID}_R, L_R)$, respectively.

(2) This step is very similar to the second step in vehicle registration. The TA generates a delegated key pair (U_R, σ_R) for the RSU.

(3) Compute a public key $Q_R = H_2(\text{LID}_R) \in G_2$ and private key $d_R = sQ_R \in G_2$ of the RSU based on IBE cryptography.

(4) Store duplet $(\text{LID}_R, W_R, U_R, \sigma_R)$.

(5) Return $(\text{LID}_R, W_R, U_R, \sigma_R, d_R)$ to R_j through the secure channel.

R_j's verification for the delegated key pair (U_R, σ_R) is the same as the one in the vehicle. Extension to the RSU from (2) should be straightforward.

4.3. V2I Communication Phase. V_i must be authenticated by the RSU before any connection to the Internet occurs. Further, in order to avoid counterfeit RSUs, V_i also must authenticate the RSU. Once mutual authentication is successful, the vehicle and RSU share a session key SK_{VR}, and vehicle V_i owns its own short-lived anonymous certificate. The session key prevents messages transmitted between the vehicle and the RSU from being disclosed to other vehicles. The short-lived anonymous certificate notarizes V_i's public key to sign messages delivered in V2V communication. Table 2 shows message exchanges for authentication and generation of short-lived anonymous certificates in V2I communication.

Step 1. When vehicle V_i comes into communication range of the RSU R_j, V_i is able to acquire the identification of R_j (ID_R) from the RSU's beacon message. This vehicle measures the location information of R_j (L_R) by using its GPS to generate the location ID of R_j, $\text{LID}_R = (\text{ID}_R, L_R)$ and compute the public key of R_j, $Q_R = H_2(\text{LID}_R)$. V_i generates a random number $r_1 \in Z_q^*$ and computes $r_1P_1 \in G_1$ for the selection of a session key SK_{VR} used in V2I communication. V_i also selects a random number $x_V \in Z_q^*$ for its short-lived private key and a corresponding public key $Y_V = x_VP_1 \in G_1$ for signing messages in V2V communication. This short-lived key pair is carefully designed to be only effective in the region between the current and next RSU. The vehicle forms a message as shown in (4) by including parameters required to authenticate the vehicle to the RSU

$$\begin{aligned} M &= (W_V, U_V, r_1P_1, Y_V, TS_V), \\ M_1 &= (W_v, TS_v) \in Z_q^*, \\ M_2 &= (U_v, r_1P_1, Y_v) \in G_1. \end{aligned} \tag{4}$$

TS_V is a timestamp chosen by the vehicle to prevent this message from being reused. This authentication message is signed by the vehicle. V_i generates a random number $k_1 \in Z_q^*$ and then signs the message with its delegated private key σ_V based upon the proxy signature. The signature of the messages is (K, w), and (5) shows the computation of the signature as follow:

$$\begin{aligned} K &= k_1P_1 \in G_1, \\ w &= \sigma_V - k_1H_1(K \| M) \in Z_q^*. \end{aligned} \tag{5}$$

Sending this signature in clear text subjects the vehicle to disclosure of private information and provides an easy means for location tracking. Hence, the authentication message and its signature are encrypted with the RSU's public key based on IBE cryptography. V_i generates a second random number $k_2 \in Z_q^*$, encrypts the message and its signature as shown in (6), and sends encrypted message (L, S) to the RSU as follow:

$$\begin{aligned} L &= k_2P_2 \in G_2, \\ S_1 &= (M_1, w) \oplus H_3\left(e(Q_R, Y_2)^{k_2}\right) \in Z_q^*, \\ S_2 &= (M_2, K) \oplus wP_1 \in G_1, \\ S &= (S_1, S_2). \end{aligned} \tag{6}$$

Step 2. The RSU decrypts the encrypted message from the vehicle with its private key $d_R = sQ_R$ as shown in.

$$\begin{aligned} S_1 \oplus H_3(e(d_R, L)) &= (W_v, TS_v, w) \in Z_q^*, \\ S_2 \oplus wP_1 &= (U_v, r_1P_1, Y_v, K) \in G_1, \\ M &= (W_v, U_v, r_1P_1, Y_v, TS_v). \end{aligned} \tag{7}$$

Subsequently, the RSU validates the expiration time in the warrant and checks if PID_V is on the RL. If these two verifications are successful, the RSU validates V_i 's proxy signature (K, w) with the TA's public key Y_1 as shown in.

$$wP_1 + U_V + H_1(U_V)Y_1 + H_1(K\|M)K = H_1(W_V)P_1. \tag{8}$$

Successful validation in (8) leads to authentication of the vehicle by the RSU and then to generation of the short-lived anonymous certificate for the vehicle's short-lived public key Y_V. The expiration time for this certificate T_{Cert} should be chosen with great care. An optimal expiration time would be when the vehicle comes within range of the next RSU. In determining the expiration time, the RSU must consider the distance to the next RSU in the vehicle's direction of travel, the number of vehicles on the road, driving speed, and so on. To generate the short-lived anonymous certificate, the RSU selects a random number $n \in Z_q^*$ and computes three parameters c, N, and z, according to (9). More specifically, (9) illustrates the RSU's proxy signature for a vehicle's short-time public key Y_V and T_{Cert} as follow:

$$\begin{aligned} c &= H_1(Y_V\|T_{\mathrm{Cert}}), \\ N &= nP_2 \in G_2, \\ z &= \sigma_R - nH_1(N\|c) \in Z_q^*. \end{aligned} \tag{9}$$

The short-lived anonymous certificate is set to $\mathrm{CERT}_V = ((z\|N\|c), W_R, U_R)$. A set of parameters $(W_R, \mathrm{CERT_V}, \mathrm{SK_{VR}}, \mathrm{PID_V})$ is saved in the RSU for the purpose of assisting the TA in tracing the real identity of a vehicle. Note that this certificate is signed by the RSU with the RSU's delegated private key σ_R on behalf of the TA. Note also that anyone can validate this certificate with the TA's public key Y_2. Finally, the RSU generates a random number $r_2 \in Z_q^*$ and computes the session key $\mathrm{SK}_{VR} = r_1r_2P_1 \in G_1$ for V2I communication. Another authentication message is formed by the RSU with the parameters of $(r_1P_1, T_{\mathrm{Cert}}, \mathrm{CERT}_V, TS_R)$ and sent, along with the RSU's contribution toward the session key r_2, to the vehicle after the encryption of the authentication message with session key SK_{VR}. TS_R is another timestamp selected by the RSU.

Correctness of (7) *Consider that:*

$$\begin{aligned} &S_1 \oplus H_3(e(d_R, L)) \\ &\quad = (W_v, TS_v, w) \oplus H_3\left(e(Q_R, Y_2)^{k_2}\right) \oplus H_3(e(sQ_R, k_2P_2)) \\ &\quad = (W_v, TS_v, w) \oplus H_3\left(e(Q_R, Y_2)^{k_2}\right) \oplus H_3\left(e(Q_R, sP_2)^{k_2}\right) \\ &\quad = (W_v, TS_v, w) \oplus H_3\left(e(Q_R, Y_2)^{k_2}\right) \oplus H_3\left(e(Q_R, Y_2)^{k_2}\right) \\ &\quad = (W_v, TS_v, w). \end{aligned} \tag{10}$$

Correctness of (8). The RSU verifies the signature of message M by confirming the inclusion of Y_1 in the following equation:

$$\begin{aligned} &wP_1 + U_V + H_1(U_V)Y_1 + H_1(K\|M)K \\ &\quad = \sigma_V P_1 - k_1H_1(K\|M)P_1 + U_V + H_1(U_V)Y_1 \\ &\qquad + k_1H_1(K\|M)P_1 \\ &\quad = \sigma_V P_1 + U_V + H_1(U_V)Y_1 \\ &\quad = -sH_1(U_V)P_1 - a_1P_1 + U_V + sH_1(U_V)P_1 \\ &\quad = -a_1P_1 + U_V \\ &\quad = H_1(W_V)P_1. \end{aligned} \tag{11}$$

Step 3. The vehicle should be able to obtain the session key by calculating $\mathrm{SK}_{VR} = r_1r_2P_1 \in G_1$. Further, the vehicle should be able to decrypt the authentication message with this session key. For authentication of the RSU, the vehicle compares r_1P_1 in the decrypted authentication message with r_1P_1 that has been known since Step 1. Given that these two values are the same, the vehicle can now authenticate the RSU. The vehicle computes (12) with the goal of validating the effectiveness of the short-lived anonymous certificate given by the RSU. Because the TA's public key is used in the validation, if this equation holds, the vehicle can assure the certificate as follows:

$$zP_2 + U_R + H_1(U_R)Y_2 + H_1(N\|c)N = H_1(W_R)P_2. \tag{12}$$

At this point mutual authentication between the vehicle and RSU is successful, and messages in the V2I communication are secured by the session key. The vehicle will repeat this mutual authentication with the RSUs along the highway route and update the short-lived anonymous certificate frequently to mask its identity to other vehicles.

Note that the session key in the channel between the vehicle and the RSU is created using the Elliptic Curve Diffie-Hellman (ECDH) algorithm. A derivative of the key generation mechanism based on Diffie-Hellman is subject to a man-in-the-middle attack. However, because messages related to the session key generation are encrypted and signed, the proposed protocol is invulnerable to such attacks.

4.4. V2V Communication Phase. Traffic-related messages need to be shared by as many vehicles as possible. The

Elliptic Curve Digital Signature Architecture (ECDSA) [23] is employed to sign messages in V2V communication. When signing, the source vehicle uses its short-lived private key x_V. The verifying vehicle uses the source vehicle's short-lived public key Y_V, which is notarized by the short-lived anonymous certificate CERT_V.

Signing Messages. A vehicle generates a random number $b \in Z_q^*$ and computes B, r, and t, according to the following:.

$$B = bP_1 = (x_A, y_A) \in G_1,$$
$$r = x_A \bmod q, \tag{13}$$
$$t = b^{-1}(H_1(\text{INFO}) + x_V \cdot r) \bmod q.$$

Traffic-related information is denoted as INFO, and its signature is created using ECDSA is (r, t). The vehicle forms a message as shown in (14) to broadcast the information. Included are the information, its signature, the sending vehicle's public key, its expiration time, and the public key certificate

$$M = [\text{INFO} \| (r, t) \| (Y_V, T_{\text{Cert}}) \| \text{CERT}_V] \tag{14}$$

Verifying Messages. When vehicles receive a broadcast message, they verify it as follows.

(1) Check the valid period of CERT_V. If it is overdue, drop the message.

(2) Verify CERT_V with the TA's public key $Y_2 = sP_2 \in G_2$ through (12) in V2I communication.

(3) Verify the signature by computing (15). If equation $x'_A \bmod q = r$ holds, the traffic-related information can be accepted

$$u_1 = H_1(M) \cdot t^{-1} \bmod q,$$
$$u_2 = r \cdot t^{-1} \bmod q, \tag{15}$$
$$K = u_1 P_1 + u_2 Y_V = (x'_A, y'_A).$$

5. Security Analysis

We subjected our proposed protocol to a security analysis. We contend that our protocol supports all security requirements demanded for V2I and V2V communication.

5.1. Mutual Authentication. The vehicle's delegated private key σ_V was created with the TA's master key, and the vehicle sends a message requesting authentication after signing the message with σ_V, based on a proxy signature. The RSU may validate the signature with the TA's public key Y_1. If the signature proves authentic, the RSU can authenticate the vehicle. For authentication in the other direction, the RSU proves knowledge of r_1P_1 in a message requesting authentication (see the message in (4)). Note that the message requesting authentication is encrypted with the RSU's IBE public key, $Q_R = H_2(\text{LID}_R)$ (refer to the encryption in (6)). Only the RSU with a valid IBE private key $d_R = sQ_R$ can decrypt the message. Because the TA creates the RSU's IBE private key, if the vehicle correctly confirms r_1P_1, then the vehicle can safely authenticate the RSU.

5.2. Source Authentication. The vehicle attaches its public key, signature, and certificate to all broadcast information as shown in (14). Nearby vehicles use (12) to examine the effectiveness of the short-lived anonymous certificate and then verify the signature with the sender's short-lived public key Y_V. If the test is successful, nearby vehicles can confirm the source of the information because the certificate is ultimately signed by the TA. This is true because the RSU used the proxy signature to create the short-lived anonymous certificate on behalf of the TA. Further, because the RSU checks the TA's RL before issuing the short-lived anonymous certificate, nearby vehicles can be assured that the sending vehicle is not among those on the list. Although revocation is possible at any time, a vehicle's certificate is updated frequently because of its short lifetime. The vehicle renews its certificate either on its timed expiration or on movement to a new RSU region.

5.3. Anonymity. The vehicle generates a random identity PID_V and uses this identity for future communication. Only the TA can link the random identity of the vehicle to its real identity. A vehicle's real identify can be revealed upon a request from authorities.

Nearby vehicles cannot recognize the identity of the source because messages do not contain an identity. A nearby vehicle may track the source vehicle by comparing the vehicle's public key and certificate. However, such keys and certificates are renewed every time the vehicle comes within range of a new RSU. Hence, the ability of other vehicles to track a vehicle is possible only for a short period that occurs in a small section near each RSU. Further, in case the vehicle sends its PID_V to the RSU to request authentication, this message requesting authentication is encrypted by the RSU's public key. An adversary has no way to acquire the RSU's private key, which was created by the TA by using its master secret. Hence, a vehicle's real and randomly assigned identities are safe.

5.4. Movement Tracking Avoidance. An RSU generates short-lived anonymous certificates without regard to a vehicle's real identity. This hidden identity prevents a communication from disclosing a vehicle's location. However, if a series of RSUs are compromised, an adversary may be able to track one vehicle through its temporary identity. Even then, however, the vehicle's real identity would never be revealed.

5.5. Data Confidentiality and Integrity. In V2I communication, the vehicle and the RSU share the session key SK_{VR} immediately after mutual authentication. Afterward, all subsequent messages are encrypted with the session key for confidentiality and appended by the Message Authentication Code (MAC) for message authentication. In V2V communication, public traffic information does not require

encryption. However, because of the importance of this traffic information to safety, authentication is required to prevent manipulation and tampering that might jeopardize drivers. A vehicle signs messages with a short-lived private key x_V, as shown in (13). Nearby vehicles can verify these messages through the sending vehicle's short-lived public key Y_V, which is certified by anonymous certificate CERT_V. (15) illustrates message verification with the short-lived public key.

5.6. Prevention of an RSU Replication Attack. When a vehicle sends V2I messages before the session key is set, the vehicle encrypts the message with the RSU's public key $Q_R = H_2(\text{LID}_R)$. Because the encryption is based on IBE cryptography, the RSU's identification LID_R becomes the public key. LID_R is the concatenation of ID_R and L_R, where ID_R is the real identity of a RSU, and L_R is the geographic location measured by the GPS. Once the RSU is compromised and relocated, the RSU's geographic location would change and the RSU's public key as understood by vehicles also would change accordingly. In such a situation, the RSU would not be able to decrypt the message and, further, would not be able to respond to a vehicle's requests. As a result, this replication attack is no longer valid.

5.7. Prevention from Message Replay Attack. Timestamps TS_V and TS_R are embedded for mutual authentication in messages exchanged in V2I communication. If the time information included in the timestamp of the message is questionable, the vehicle and RSU will simply drop the message. In terms of a continuum, V2V messages contain traffic-related information, including the current time. By checking whether a message arrives within the allowable time window, a replay attack can be diagnosed and thwarted.

5.8. Tracking a Disputed Message. In the case of a disputed message, warrant information can be found in the certificate, $W_R = (\text{ID}_R, T_{\text{Exp}})$, and ID_R can be used to identify which RSU issued a specific certificate. In the corresponding RSU, one can find a vehicle's pseudo-ID PID_V in the tuple of vehicle information, $(W_R, \text{CERT}_V, \text{SK}_{VR}, \text{PID}_V)$. PID_V is then sent to the TA to find the real identity of the vehicle. The TA extracts ID_V associated with PID_V from the database, where another tuple of information is saved $(\text{ID}_V, \text{PID}_V, W_V, \sigma_V)$.

Table 3 compares the five protocols discussed earlier in terms of their capability to fulfill security and privacy requirements. Only the proposed protocol supports both V2I and V2V communication in the VANET.

6. Performance Evaluation

We evaluated the performance of our proposed protocol with respect to delays in mutual authentication in V2I communication and delays in signing and verifying messages in V2V communication. After these measurements, we compared the proposed protocol with other popular protocols in the VANET with respect to the same metrics.

6.1. Delay in V2I Communication. Delay overhead in the V2I communication comprises computational delay and communication delay. The communication delay is by definition the round-trip time (RTT) between communicating entities. The computational delay in V2I communication starts the moment a vehicle requests authentication from the RSU and accumulates until the RSU returns the short-lived anonymous certificate to the vehicle. Delay itself is a function of many parameters in this measurement. In particular, we are interested in measuring delay in the two most influential parameters. These are the delay associated with a point multiplication over an elliptic curve and the delay of a pairing operation. Let us denote these two types of delay as PM and PR, respectively. We adopted the experiment used in [24], which observed the processing time for PM and PR as measured in running on an Intel Pentium IV 3.0 GHZ machine. Our measurements showed that single operations of PM and PR took about 0.6 and 4.5 milliseconds, respectively. We did not account for any other operations, such as one-way hash, because processing time for those operations, 2 microseconds, is so small as to be negligible in the computation.

We compared the computational expenses for the three protocols described in Section 2: ECPP [15], LPPAS [7], and the proposed protocol. Because the number of messages required to complete mutual authentication differs from protocol to protocol, we compared them in terms of the computational expense in each message. Table 4 shows the computational expense for each message up to the sixth message. In order to distinguish operations in the vehicle, the RSU and the TA, cells in the table have different backgrounds. The computational delays of LPPAS for the first two messages are left empty in Table 4. This is because these two messages are formed without involving PM and PR operations.

Although ECPP and LPPAS comprise four and six messages, respectively, the proposed protocol requires only two messages to complete mutual authentication. Because the proposed protocol requires fewer messages to complete authentication, the delay associated with traveling between its authentication entities is less.

Figure 2 shows the computational delays of the three protocols in completing authentication (communication delay is not included). The delay taken by each operation as shown in Table 4 is modeled by its average value. The delays of operations done by the three entities are summed and plotted in Figure 2. It takes 15 milliseconds and 34.2 milliseconds, respectively, in the proposed protocol and in ECPP. The proposed protocol is faster than ECPP because it entails fewer messages and also because the protocol is designed to use less expensive operations. The computational delay of LPPAS in authentication is three milliseconds. This is the fastest among the three protocols because the protocol operates by dispensing with anonymous certificates. However, the overall delay of LPPAS would exceed the other two protocols because of its long communication delay.

LPPAS requires three round trips, but the proposed protocol and ECPP require only one and two round trips, respectively, to complete authentication. The TA is not involved in authentication in either the ECPP or the proposed

Table 3: Comparison of the five protocols with respect to fulfillment of security and privacy requirements.

	System requirements	GSIS [6]	LPPAS [7]	HAP [11]	ECPP [15]	Our protocol
V2I	Mutual authentication	X	O	X	O	O
	Confidentiality and integrity	X	O	X	X	O
	Privacy	X	O	X	O	O
V2V	Source authentication	O	X	O	O	O
	Providing message integrity	O	X	O	O	O
	Privacy	O	X	O	O	O
Traceability		O	X	O	O	O
Efficient revocation		X	X	X	O	O

Table 4: Computational expenses to form each message. The table shows the comparison for up to the sixth message. Although ECPP and LPPAS need four and six messages, respectively, the proposed protocol requires only two messages to complete mutual authentication. Note that cells in the table have different backgrounds to distinguish the nodes in which these operations are computed. Single operations of PM and PR took about 0.6 and 4.5 milliseconds, respectively.

	1	2	3	4	5	6
ECPP	2 PM*	PR†	PR + PM*	4 PR + 9 PM†	—	—
Our Protocol	PR + 4 PM*	PR + 6 PM†	—	—	—	—
LPPAS	—*	—†	PR*	2 PR‡	PR*	PR‡

*Vehicle. †RSU. ‡TA.

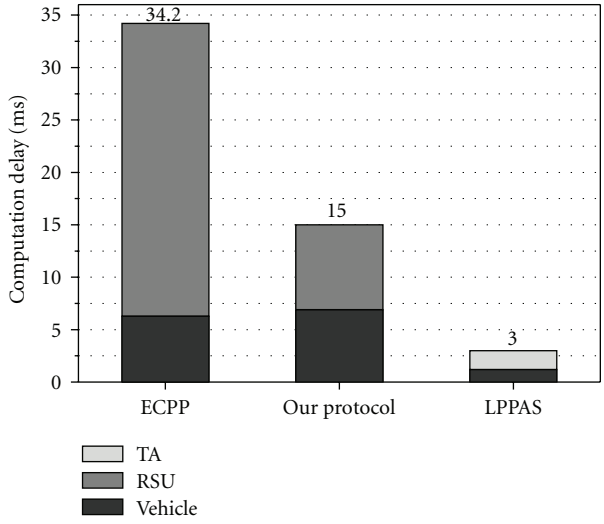

Figure 2: Comparison of computational delays of the three protocols. The delays in operation by the three entities are summed and plotted.

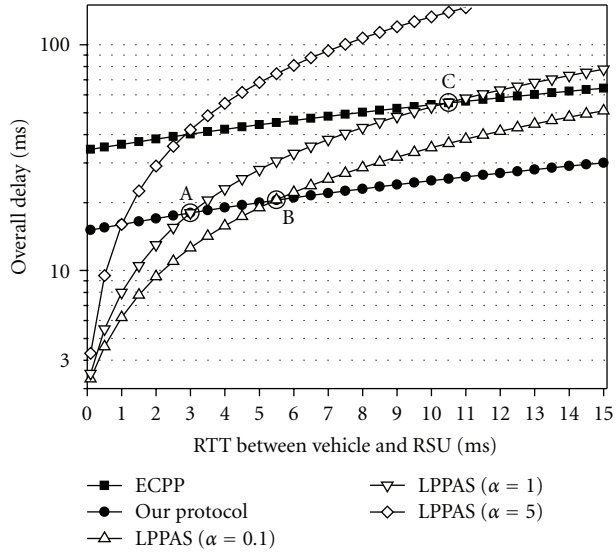

Figure 3: Delays of the three protocols with respect to the RTT between a vehicle and the RSU. The RTT between the RSU and the TA is determined by multiplication of α to RTT between the vehicle and the RSU.

protocol because the RSU is authorized to act as the TA. On the other hand, authentication messages in LPPAS must travel back and forth to the TA three times. In general, the distance between an RSU and the TA is a lot longer than the one between a vehicle and the RSU. Moreover, the communication delay typically is greater than the computational delay. ECPP and the proposed protocol can authenticate quickly because neither requires travel to the TA.

Figure 3 compares the overall delay of the three protocols with respect to the RTT between a vehicle and an RSU. The RTT varies from zero to 15 milliseconds. The RTT between a RSU and a TA in LPPAS is determined by the multiplication of α to the RTT between a vehicle and a RSU. The three different values of α for LPPAS are plotted in: 0.1, 1, and 5. At short RTTs, LPPAS has the least overall delay. However, as the RTT lengthens, the inversion of the delay among the protocols occurs at points that include A, B, and C as shown in Figure 3. For instance, at an RTT of 3 milliseconds (marked as A), the LPPAS delay exceeds that of the proposed protocol with $\alpha = 1$. We speculate that 10 milliseconds is a typical value of the RTT between a vehicle and an RSU.

With this figure of 10 milliseconds, the proposed protocol is the fastest of the three in terms of overall delay.

6.2. Delay in V2V Communication. We mainly use computational delay to compare the performance of the protocols in V2V communication. Unlike V2I communication in which messages in different protocols may follow different paths and consequently create communication delays that differ significantly from protocol to protocol, the length of the delay in V2V communication should be almost constant. This is because messages are delivered among vehicles irrespective of protocols. The computational delay in V2V communication consists mostly of two operations that is, signing and verifying traffic-related messages.

We have selected three other popular protocols in the VANET for comparison of computational delays. The three are ECPP [15], GSIS [6], and BLS [25, 26]. We did not include LPPAS in this comparison because LPPAS does not define V2V communication. Table 5 compares the computational delays of the four protocols. ECPP and the proposed protocol must verify a certificate before the use of a public key for signature verification. It takes 4 PM for certificate verification and 2 PM for message verification, resulting in a total of 6 PM for signature verification in the proposed protocol. In ECPP, the same delay is required for certificate verification, but the message verification takes 9 PM + 3 PR. Group signature-based BLS and GSIS dispense with the certificate because all group members agree on the group key. Consequently, these two can avoid the additional overhead associated with certificate validation. It takes 8 PM + 5 PR and 2 PR, respectively, to verify a single message in GSIS and BLS. In particular, BLS is quite effective in verifying multiple messages because of its capability for parallel verification. Hence, while verifying a single message takes 2 PR, verifying n messages takes $(n + 1)$ PR. In contrast, ECPP, GSIS, and the proposed protocol iterate one-message verification n times for the same number of message verifications. BLS's advantage does not work for signing multiple messages, and thus all of the four protocols should repeat a single message signature n times.

The above discussion is illustrated in Figures 4 and 5 by depicting the comparison of delays in signing and verifying messages, respectively, as the number of messages increases. In signing n messages, as the number of messages increases, the delay in GSIS increases more steeply than in the other protocols (see Figure 4). In other words, these protocols, except GSIS, perform very similarly in signing. In verification, the proposed protocol is the fastest, with BLS second (see Figure 5). Although BLS is effective in verifying multiple messages, the proposed protocol outperforms BLS because of an efficient design that employs less expensive operations, that is, 6 PM versus 2 PR per message. The operational delays in signing and verifying a message are summed together and compared in Figure 6. The message signing delays in ECPP, BLS, and the proposed protocol are 0.6 milliseconds. The proposed protocol and BLS require 3 and 9 milliseconds, respectively, to verify a message. The delay in BLS is three times the delay of the proposed protocol.

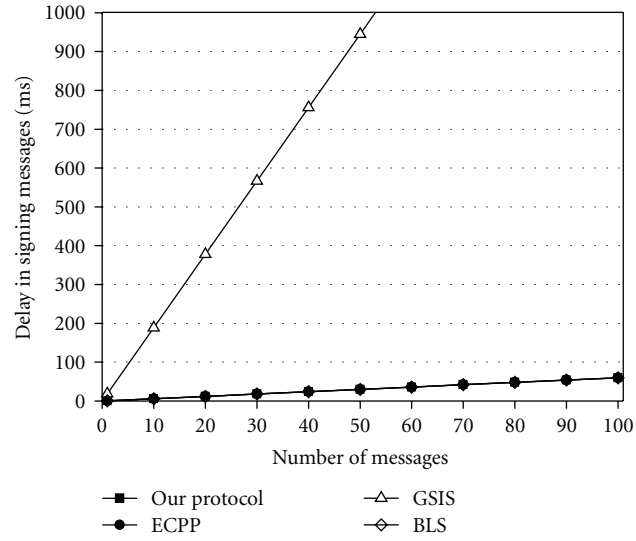

Figure 4: Delay in signing messages with respect to the number of messages.

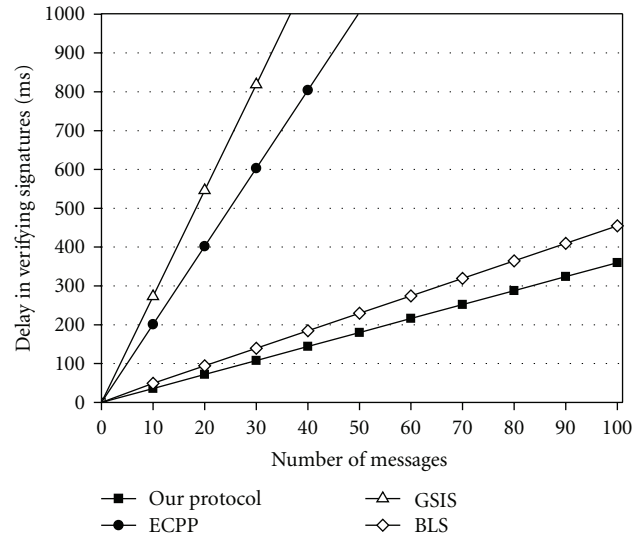

Figure 5: Delay in verifying messages with respect to the number of messages.

The robustness of the protocol—that is, its capability to deliver traffic-related messages with unpredictable variations in the network condition—represents another interesting aspect of performance evaluation. According to the Dedicated Short Range Communications (DSRCs) standard [27], vehicles broadcast safety messages at intervals between 100 and 300 milliseconds. We drove vehicles that sent messages at 300-millisecond intervals. As the number of vehicles and messages increased, some protocols began to drop messages because they were incapable of decrypting messages fast enough. We want to compare the robustness of the protocols by introducing a service rate, which is defined as a ratio of

Table 5: Comparison of computational delays of the four protocols in signing messages and verifying signatures.

	Signing a message	Signing n messages	Verifying a single signature	Verifying n signatures
Our protocol	PM	nPM	6 PM	6 nPM
ECPP	PM	nPM	11 PM + 3 PR	11 nPM + 3 nPR
GSIS	9 PM + 3 PR	9 nPM + 3 nPR	8 PM + 5 PR	8 nPM + 5 nPR
BLS	PM	nPM	2 PR	$(n + 1)$ PR

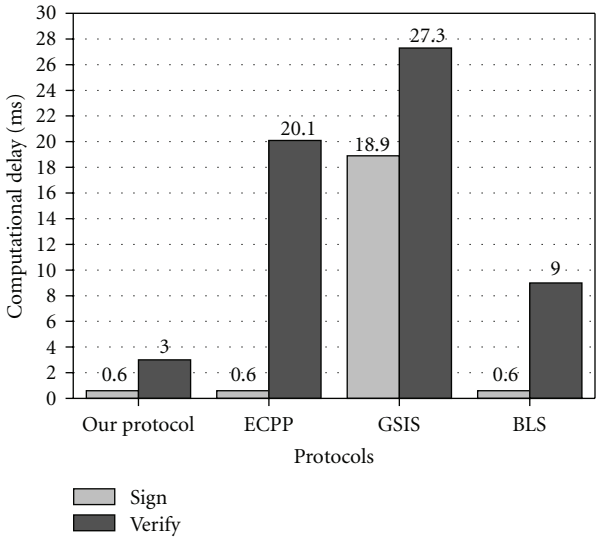

Figure 6: Comparison of computational delay to sign and verify a message.

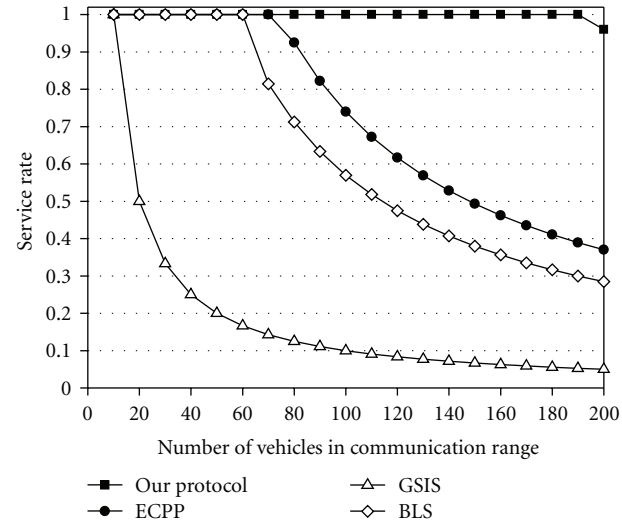

Figure 7: Comparison of service rates of four protocols with 15 percent of group membership changes.

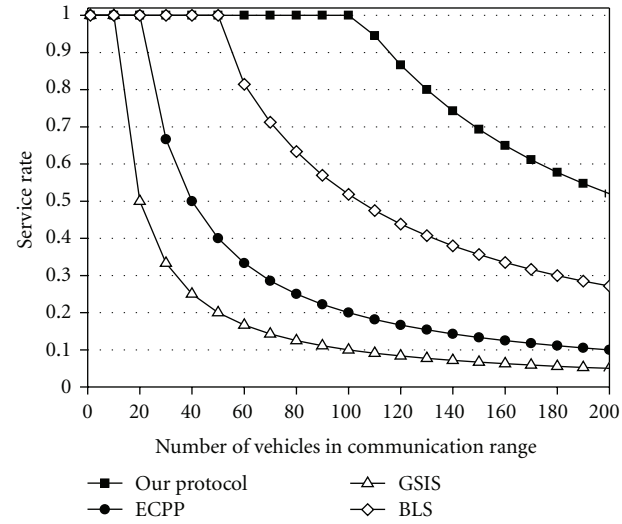

Figure 8: Comparison of service rates of four protocols with 70 percent of group membership changes.

the number of delivered messages to the number of incoming messages in a given time as follow:

$$\text{Serivce Rate} = \frac{\text{The number of delivered messages}}{\text{The number of incoming messages}}. \quad (16)$$

The higher the service rate, the more robust a protocol.

Further, the dynamics of group membership may affect the robustness of a protocol. Verification of a certificate for a vehicle happens at the first introduction of this vehicle into a network controlled by one RSU. The later verification can be skipped after the first successful verification as long as this vehicle stays within this network (of course, before the timeout). Frequent changes in group membership may result in vehicles verifying certificates of source vehicles for almost all messages. This case can be observed typically at highway interchanges and at the intersections of busy streets. On the other hand, if the dynamics of membership change are rather static, such as when a group of vehicles move in one direction on a highway, the vehicles need only to verify certificates once for each vehicle in the group regardless of the number of messages.

Figures 7 and 8 compare the service rate of the four protocols at 15 percent and 70 percent membership changes, respectively, within a given time. As the number of vehicles increases, the service rate begins to drop from one, despite different starting points, protocol by protocol. As group membership changes more frequently (i.e., from 15 percent to 70 percent), ECPP and the proposed protocol drop messages for a smaller number of vehicles; for example, 190 vehicles for ECPP and 100 vehicles for the proposed protocol. However, as for GSIS and BLS, which dispense with the certificate, the service rates do not change significantly as the percentage of membership changes. The service rate

Table 6: Comparison of storage overhead in four protocols.

	Our protocol	ECPP	GSIS	HAP
Storage overhead	—	—	n	mn

for ECPP is higher than that of BLS in Figure 7. However, in Figure 8, BLS's service rate is higher than that of ECPP because ECPP takes a significant amount of time to verify certificates. In both figures, our proposed protocol scores the highest service rate in terms of the total number of vehicles served.

6.3. Storage Overhead in Vehicles. Table 6 shows a comparison of storage overhead in the four selected protocols. They are ECPP, GSIS, HAP, and the proposed protocol. Storage overhead is minimal in both ECPP and the proposed protocol because a vehicle has no RL to maintain. An RSU inquires of a TA, where the RL is actually maintained, to check if a vehicle's public key remains valid. An RSU then creates short-lived anonymous certificates for only those vehicles positively acknowledged by a TA. In GSIS, the size of the storage increases linearly with the number of vehicles. In HAP, each vehicle has multiple anonymous certificates. If we denote the number of anonymous certificates in the vehicle to m, then the size of the storage increases by mn as the number of vehicles n increases. In addition, because the RL must be updated periodically, traffic associated with updating the RL may impose an additional type of overhead.

7. Conclusion

Securing a vehicular network is an ill-defined problem, and most systems available for the VANET do not combine efficiency, security, and traceability. They tend to do well in one quality or two qualities, but not three. We initiated our research in an effort to determine whether a vehicular network could be designed that would satisfy all three qualities at the same time. The basic idea is to sign messages with ephemeral, anonymous, and traceable identities for network security. We adopted proxy signature cryptography to authenticate vehicles and RSUs and to delegate the RSU to issue short-lived certificates only for authenticated vehicles. This issuance is authorized by the TA. To use storage efficiently in the vehicle, the RSU maintains the RL on behalf of vehicles. The experimental results demonstrated that even within a harsh communication environment, our protocol significantly improved the security, privacy, and efficiency of a VANET.

References

[1] K. Fall, "A delay-tolerant network architecture for challenged Internets," in *Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '03)*, pp. 27–34, 2003.

[2] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation," in *Proceedings of the 3rd ACM Conference on Computer and Communications Security (CCS '96)*, pp. 48–56, March 1996.

[3] T. Okamoto, M. Tada, and E. Okamoto, "Extended proxy signatures for smart cards," in *Proceedings of the 2nd InternationalWorkshop on Information Security*, vol. 1729 of *Lecture Notes in Computer Science*, pp. 773–773, Kuala Lumpur, Malaysia, November 1999.

[4] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Proceedings of the 24th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '04)*, vol. 3152 of *Lecture Notes in Computer Science*, pp. 41–55, Santa Barbara, Calif, USA, 2004.

[5] D. Chaum, "Blind signatures for untraceable payments," in *Proceedings of the International Conference on Advances in Cryptology (CRYPTO '82)*, Lecture Notes in Computer Science, pp. 191–203, Santa Barbara, Calif, USA, 1982.

[6] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[7] C. Zhang, R. Lu, P.-H. Ho, and A. Chen, "A location privacy preserving authentication scheme in vehicular networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '08)*, pp. 2543–2548, April 2008.

[8] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks," in *Proceedings of the IEEE International Conference on Communications (ICC '08)*, pp. 1451–1457, May 2008.

[9] K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang, "Adaptive privacy-preserving authentication in vehicular networks," in *Proceedings of the International Workshop on Vehicle Communication and Applications*, pp. 1–8, October 2006.

[10] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: robust location privacy scheme for VANET," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1569–1589, 2007.

[11] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[12] U.S. Department of Transportation, "National highway traffic safety administration," Vehicle Safety Communications Project, Final Report, April 2006.

[13] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proceedings of the 27th IEEE Communications Society Conference on Computer Communications (INFOCOM '08)*, pp. 816–824, April 2008.

[14] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '01)*, Lecture Notes in Computer Science, pp. 213–229, Santa Barbara, Calif, USA, 2001.

[15] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communications," in *Proceedings of the 27th IEEE Communications Society Conference on Computer Communications (INFOCOM '08)*, pp. 1903–1911, April 2008.

[16] M. Gasser and E. McDermott, "An architecture for practical delegation in a distributed system," in *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 20–30, May 1990.

[17] B. C. Neuman, "Proxy-based authorization and accounting for distributed systems," in *Proceedings of the 13th IEEE*

International Conference on Distributed Computing Systems, pp. 283–291, May 1993.

[18] I. Foster, C. Kesselman, G. Tsudik, and S. Tuecke, "A security architecture for computational grids," in *Proceedings of the 5th ACM Conference on Computer and Communications Security (CCS '98)*, pp. 83–92, San Francisco, Calif, USA, November 1998.

[19] T. Okamoto, M. Tada, and E. Okamoto, "Extended proxy signatures for smart cards," in *Proceedings of the 2nd InternationalWorkshop on Information Security*, vol. 1729 of *Lecture Notes in Computer Science*, pp. 247–258, Kuala Lumpur, Malaysia, November 1999.

[20] R. Lu, X. Dong, and Z. Cao, "Designing efficient proxy signature schemes for mobile communication," *Science in China Series F*, vol. 51, no. 2, pp. 183–195, 2008.

[21] S. Kim, S. Park, and D. Won, "Proxy signature, revisited," in *Proceedings of the Information and Communications Security*, vol. 1334 of *Lecture Notes in Computer Science*, pp. 223–232, 1997.

[22] C. Tang and D. O. Wu, "An efficient mobile authentication scheme for wireless networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1408–1416, 2008.

[23] V. Kapoor, V. S. Abraham, and R. Singh, "Elliptic curve cryptography," *Ubiquity*, vol. 9, no. 20, pp. 1–8, 2008.

[24] M. Scott, "Efficient implementation of cryptographic pairings," http://ecrypt-ss07.rhul.ac.uk/Slides/Thursday/mscott-samos07.pdf.

[25] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt '01)*, vol. 2248, pp. 514–532, Gold Coast, Australia, December 2001.

[26] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Proceedings of the 22nd Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt '03)*, vol. 2656 of *Lecture Notes in Computer Science*, pp. 416–432, Warsaw, Poland, May 2003.

[27] "Dedicated Short Range Communications (DSRC)," http://vii.path.berkeley.edu/1609_wave/.