Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 7978027, 13 pages
https://doi.org/10.1155/2018/7978027

Research Article

Secure Certificateless Authentication and Road Message Dissemination Protocol in VANETs

Haowen Tan[1], **Dongmin Choi**[2], **Pankoo Kim**[1], **Sungbum Pan**[3] and **Ilyong Chung**[1]

[1]*Department of Computer Engineering, Chosun University, 309 Pilmun-daero, Seonam-dong, Dong-gu, Gwangju 61452, Republic of Korea*
[2]*Division of Undeclared Majors, Chosun University, 309 Pilmun-daero, Seonam-dong, Dong-gu, Gwangju 61452, Republic of Korea*
[3]*Department of Electronic Engineering, Chosun University, 309 Pilmun-daero, Seonam-dong, Dong-gu, Gwangju 61452, Republic of Korea*

Correspondence should be addressed to Ilyong Chung; iyc@chosun.ac.kr

Received 17 January 2018; Revised 21 March 2018; Accepted 10 April 2018; Published 20 May 2018

Academic Editor: Ding Wang

As a crucial component of Internet-of-Thing (IoT), vehicular ad hoc networks (VANETs) have attracted increasing attentions from both academia and industry fields in recent years. With the extensive VANETs deployment in transportation systems of more and more countries, drivers' driving experience can be drastically improved. In this case, the real-time road information needs to be disseminated to the correlated vehicles. However, due to inherent wireless communicating characteristics of VANETs, authentication and group key management strategies are indispensable for security assurance. Furthermore, effective road message dissemination mechanism is of significance. In this paper, we address the above problems by developing a certificateless authentication and road message dissemination protocol. In our design, certificateless signature and the relevant feedback mechanism are adopted for authentication and group key distribution. Subsequently, message evaluating and ranking strategy is introduced. Security analysis shows that our protocol achieves desirable security properties. Additionally, performance analysis demonstrates that the proposed protocol is efficient compared with the state of the art.

1. Introduction

Vehicular ad hoc networks (VANETs) are distributed, self-organized wireless networks constructed by vehicles and nearby road-side units (RSUs). The real-time dynamic communication enables efficient and durative information exchange between vehicles and RSUs. Hence, intelligent transportation system (ITS) is achievable with the widely implementation of VANETs [1, 2]. A variety of VANET-based applications, which can be mainly classified into safety-related applications and commercial-oriented applications, not only enhance the driving safety but also provide better driving experience. Typical safety-related applications include emergency vehicle warnings, traffic congestion report, road accident informing, and speed monitoring [3, 4]. Commercial-oriented applications provide convenience service and entertainment applications such as weather forecast, information broadcasting of nearby petrol stations and restaurants, navigation, and Internet access.

In general, a basic VANET consists of three important components: the trusted authority (TA), road-side units (RSUs), and vehicles [5–7]. Considered as both the application provider and key server, TA is responsible for providing various services to vehicles through RSUs. Moreover, pivotal secret key assignment, along with the user management for correlated vehicles, is conducted by TA. The RSUs are deployed by the road sides one after another. Commonly, RSUs are built aside the road in every kilometer. Thus the effective range of VANET system can cover each section of the road. In this case, RSUs are considered as the communication bridge connecting TA and vehicles, which provides timely transmission of vital personal data. To a certain degree, RSUs have the capability of conducting computation and storing essential information in its memories [8]. The vehicle

performs as both terminal customer and information collector. In other words, useful information including traffic congestion and emergency road condition is forwarded to the corresponded RSU. Each vehicle is equipped with an onboard unit (OBU), which conducts all the computation and communication [9, 10]. Compared with regular wireless sensor networks [11], vehicle's high mobility is the unique characteristic of VANETs.

In VANETs, the data exchange between TA and RSUs are via secure wired connection, where the adopted cryptographic strategies guarantee transmission security and message confidentiality. Meanwhile, vehicle-to-vehicle (V2V) communication and vehicle-to-RSU (V2R) communication are conducted through open wireless channel, which employs the dedicated short-range communications (DSRC) [12–14]. On the one hand, the moving vehicle can carry out interactive data exchange with specific RSU through V2R communication. On the other hand, one vehicle is capable of sharing essential messages with other vehicles in its vicinity through V2V communication. In this way, a VANET with high connectivity can be built accordingly [15].

As a particular variant of wireless sensor networks, apparently the VANETs suffer from multiple charted and uncharted security attacks [9, 14]. In V2V and V2R communications, the transmitted messages may be eavesdropped, blocked, or even forged by malicious devices. Hence, significant user information is revealed to the attacker accordingly, which compromises the whole VANET and brings severe user privacy disclosure issue [1, 13]. Under this circumstance, proper authentication strategies are required so as to provide security and privacy assurance. Moreover, high mobility feature of the vehicles brings uncertainty to the communication process, which should also be taken into consideration.

Among the aforementioned safety-related applications, road message dissemination is one of the essential functions for VANET [16]. With the assistance of RSUs and remote server, the vehicles of the same VANET could share necessary driving-related information with each other. By analyzing the acquired traffic information of current areas, the driver is able to make better driving decisions such as choosing the best navigation route ahead of time. Furthermore, occurrences of road accidents and traffic jams can be drastically reduced [9]. Thus, the drivers' driving experience is improved.

In VANETs, typical road message management strategies are mainly composed of information collection and dissemination. First, the road messages are reported by the participating vehicles through OBUs [17]. Afterwards, the acquired messages will be processed and then disseminated to the legitimate vehicles. In some VANETs scenarios, TA arranges all the road messages collected from RSUs via wired transmission [18]. Meanwhile, in decentralized VANETs scenarios, most of the computation and storing are done in the RSU side [7], while TA performs as the key generation center (KGC). Consequently, in particular dense scenarios with large amounts of emerging vehicles, the decentralized architecture could reduce the computation overload and storage complexity in TA.

As described above, authentication strategies are necessary during road message dissemination [4, 19]. Furthermore, the characteristic group communication between RSU and vehicles is indispensable, which enables convenient data exchange. In this case, the group key shared between RSU and all the legitimate vehicles is required. Note that the group key distribution should be conducted after mutual authentication [6, 20].

As for message dissemination in practical VANETs occasions, two channels are required [21], namely, the official channel and normal channel. Official channel is provided by governmental agencies, where the broadcast road information is precise and trustworthy. Note that this channel is assumed to be based on real-time monitoring with satellites and road cameras. Thus it is precise and trustworthy. Meanwhile, normal channel is the more ordinary way, where the road information is gathered from normal vehicles. In this case, some of the vehicles are assumed to be benign devices which transmit precise messages, while the rest are negative vehicles [22]. Note that the negative vehicles may report trivial or even false information to the VANET system. For this consideration, with the purpose of guaranteeing the dissemination exactitude, impartial and effective message evaluation mechanism is necessary [23]. For instance, in extreme scenarios with massive road messages to be disseminated, before dissemination, it is necessary for the RSUs to aggregate and evaluate the acquired road messages before dissemination. Hence the RSUs could broadcast in a particular sequence according to the significance and reliability of each message. Urgent and authentic road messages can be broadcast in the first place.

During the message dissemination of the entire VANETs, the accuracy and efficiency of message dissemination closely depend on the participating vehicles [15, 24]. Hence, it is vital to deploy appropriate rewarding strategy so as to motivate the drivers' enthusiasm on reporting [20, 25]. For example, coupons or discounts on certain commodities can be granted to the trustworthy drivers with timely and precise reporting records. In other words, the drivers are encouraged with incentives, which is of great benefit to the entire VANET.

In this paper, we propose a secure certificateless authentication and road message dissemination protocol in vehicular ad hoc networks. Our nontrivial efforts can be summarized as follows:

(i) Secure Certificateless Authentication Scheme for Group Key Distribution. With the purpose of enhancing transmission security, we adopt the bilinear pairing based on elliptic curve into our authentication scheme. Hence, the active vehicles within the effective range can be identified and then allocated with the group key. The proposed scheme yields desirable security properties.

(ii) Road Message Priority Management and Dissemination Mechanism. The encrypted road messages are delivered to the corresponding RSU. The received road message is evaluated based on both the vehicle priority and the assessment. In this way, accuracy and efficiency of the messages dissemination process are provided. Hence, the drivers can timely arrange their routes according to the delivered road information.

(iii) Security and Performance Analysis. The formal security analysis is provided, involving some necessary proofs on resistance to the existing malicious attacks. Furthermore, performance analysis emphasizing the transmission overload and computation cost is hereby presented.

The remainder of this paper is organized as follows. Section 2 provides brief description of the related research achievements. Section 3 introduces some necessary preliminary works and the designed system model in order for the reader to obtain better understanding of this topic. Section 4 presents the proposed secure certificateless authentication scheme in detail. Section 5 describes the proposed road message dissemination scheme. Section 6 demonstrates the security analysis. Section 7 displays the performance analysis. The conclusion is drawn in Section 8.

2. Related Work

In order to provide enhanced authentication and secure transmission in VANETs, various cryptographic techniques have been deployed in existing researches [2, 3, 6, 16, 26–28]. In 2009, Studer et al. [3] developed a hybrid VANET authentication mechanism (VAST) based on the elliptic curve digital signature algorithm (ECDSA) [29] and TESLA [30] with the purpose of providing fast and extensible authentication and nonrepudiation. Subsequently, emphasizing group authentication and conditional privacy, Zhang et al. [26] proposed a scalable decentralized group authentication protocol, where certain vehicle is able to verify anonymous messages from neighboring vehicles. Motivated by chameleon hash signature based on elliptic curve, in 2011, Huang et al. [27] designed pseudonymous authentication-based conditional privacy protocol (PACP), which adopts the pseudonyms for anonymous communication. Similarly, ABAKA [6] with batch verification was proposed by Huang et al. After that, Lu et al. [28] presented a dynamic privacy-preserving key management scheme (DIKE) enabling both vehicle anonymous authentication and double-registration detection. Guo et al. [2] designed a privacy-preserving anonymous authentication protocol with vehicle unlinkability and authority trackability in 2014, where high efficiency and desired security properties can be achieved accordingly. Afterwards, multiple authentication and group key management protocols in VANETs have been designed recently [8, 31].

Specifically, identity-based encryption, which was first presented by Shamir [33] for certificate management of KGC, has been widely implemented in VANETs authentication protocols. In 2007, Lin et al. [34] combined group signature with identity-based cryptography in the proposed GSIS protocol. Hence, appropriate traceability toward specific vehicle is achieved. After that, Zhang et al. [15] designed an identity-based batch signature verification scheme in VANETs, where multiple signatures can be simultaneously verified in one RSU. Nevertheless, this scheme suffers from replay attack [35]. Subsequently, Sun et al. [5] constructed an identity-based security framework in order to address the misbehavior issue in VANET system. In 2012, Shim [9] developed an identity-based conditional privacy-preserving authentication scheme (CPAS) supporting fast batch verification. However, the proposed protocol is vulnerable to modification attack [36]. Another signature scheme for VANETs, named EIBS [37], was proposed in 2015, where the RSUs perform as the certificate verifiers in order to decrease the computation overload in TA side. Moreover, the anonymity of the legitimate vehicle is provided by using pseudo identity instead of real identity. Hence, the vehicle privacy is preserved. Aiming to decrease the computational complexity, He et al. [10] designed an identity-based conditional privacy-preserving authentication scheme in VANETs. With relatively limited computation and communication requirements, the proposed protocol is suitable for practical VANETs applications.

With the purpose of addressing the key escrow issue in identity-based public key cryptography system (ID-PKC), certificateless public key cryptography (CL-PKC) was first introduced by Al-Riyami and Paterson [38] in 2003. In CL-PKC design, the private partial keys are, respectively, generated by the semitrusted key generation center (KGC) and the user itself. Multiple certificateless authentication protocols were proposed afterwards [25, 39]. Thereafter, Li and Wang [17] presented a fast certificateless authentication scheme (RCS) employing bilinear pairing, where particular vehicles are selected as the assistance to the relevant RSUs. In this case, the transmission overload can be alleviated. Afterwards, Xiong and Qin proposed a certificateless encryption scheme and another certificateless signature scheme with efficient revocation against short-term key exposure in [40]. In 2016, Peng [1] designed an anonymous authentication protocol based on certificateless signature scheme, which provides conditional privacy and mutual authentication.

Furthermore, as the crucial and unique feature of VANETs, message dissemination has been studied due to its promising advantages in both safety-related and commercial-oriented applications. Focusing on commercial advertisements dissemination, Tseng et al. [7] adopted Reed-Solomon Code in the incentive scheme through interactions between vehicles. Similarly, a cooperative message authentication scheme [18] is developed to alleviate the verification overload in the RSU side, where the legitimate vehicles are responsible for message verification in the vicinity. Thereafter, in order to achieve high reliability and low dissemination delay at the same time, density-aware emergency message extension protocol (DEEP) [22] is constructed. As illustrated, emergency warning messages can be timely delivered to all the vehicles within the operating range, which could drastically improve driving safety. As one of the significant services offered by VANETs, RSU-assisted navigation is studied by Chim et al. in [20]. In the assumption, the real-time road conditions are used to compute a better route for the requesting vehicles. The privacy of the drivers can be protected with the advantages of anonymous credential. In [23], Milojevic and Rakocevic developed a location-aware data aggregation mechanism for real-time observation and efficient message dissemination. The communication cost is minimized with the use of intelligent passive clustering and adaptive broadcasting. For improving the accuracy of the delivered message, the aggregated information is arranged by real-time spatiotemporal database refreshing. Recently, Liu et al. presented a cloud-assisted message downlink dissemination scheme (CMDS)

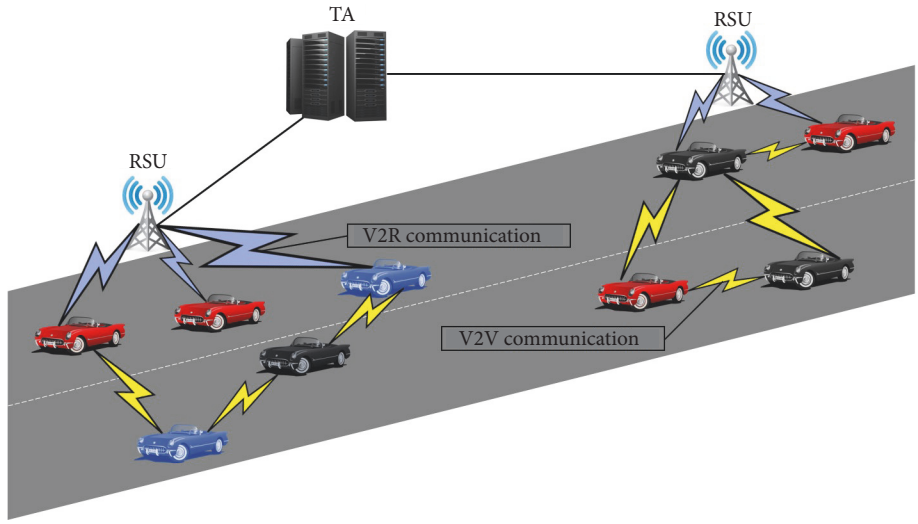

Figure 1: System Model.

under a developed VANET-cellular heterogeneous framework combining cloud computing [21, 41].

3. Model Definition and Preliminaries

In this section, some necessary preliminaries are introduced with the purpose of facilitating the readers' understanding, including the definition of bilinear pairing and hash function. Subsequently, the corresponding notations, the system model, and network assumptions are illustrated.

3.1. Bilinear Pairing. Let $\mathbb{G}_{\mathcal{O}}$ and $\mathbb{G}_{\mathcal{N}}$ be two additive cyclic groups of a large prime order $\mathcal{P}$. A map function $\hat{e} : \mathbb{G}_{\mathcal{O}} \times \mathbb{G}_{\mathcal{O}} \rightarrow \mathbb{G}_{\mathcal{N}}$ is a bilinear pairing if it satisfies the three properties below:

(1) Bilinear: for $\forall M, N \in \mathbb{G}_{\mathcal{O}}$ and $\forall a, b \in \mathbb{Z}^*_{\mathcal{P}}$, there is $\hat{e}(aM, bN) = \hat{e}(M, N)^{ab}$. In addition, for $\forall M, N, Y \in \mathbb{G}_{\mathcal{O}}$, there are $\hat{e}(M + N, Y) = \hat{e}(M, Y)\hat{e}(N, Y)$ and $\hat{e}(M, N + Y) = \hat{e}(M, N)\hat{e}(M, Y)$.

(2) Nondegeneracy: for $\exists M, N \in \mathbb{G}_{\mathcal{O}}$, there is $\hat{e}(M, N) \neq 1$.

(3) Computability: for $\forall M, N \in \mathbb{G}_{\mathcal{O}}$, there is an efficient algorithm to compute $\hat{e}(M, N)$.

In order to prove the security of our schemes, the following intractable problems are briefly presented as

(1) discrete logarithm problem (DLP): for $\forall M, N \in \mathbb{G}_{\mathcal{O}}$, it is difficult to find an integer $a \in \mathbb{Z}^*_{\mathcal{P}}$, such that $M = aN$ holds;

(2) computational Diffie-Hellman problem (CDHP): for $\forall M, aM, bM \in \mathbb{G}_{\mathcal{O}}$, it is difficult to compute abM;

(3) decisional Diffie-Hellman problem (DDHP): for $\forall M, aM, bM, cM \in \mathbb{G}_{\mathcal{O}}$ and $\forall a, b, c \in \mathbb{Z}^*_{\mathcal{P}}$, it is difficult to decide whether $c = ab \bmod \mathcal{P}$ holds;

(4) pairing inversion problem (PIP): for a pairing $\hat{e}$ and $\forall c \in \mathbb{Z}^*_{\mathcal{P}}$, it is difficult to find $M, N \in \mathbb{G}_{\mathcal{O}}$, such that $\hat{e}(M, N) = c$ holds.

3.2. Hash Function. A one-way hash function is considered to be secure if the following properties can be satisfied [42]:

(1) Inputting a message x of arbitrary length, it is easy to compute a message digest of a fixed length output $h(x)$.

(2) Given y, it is difficult to compute $x = h^{-1}(y)$.

(3) Given x, it is computationally infeasible to find $x' \neq x$ such that $h(x') = h(x)$ holds.

3.3. Notations. The notations and the brief description are listed in Notations.

3.4. System Model. The structure of VANET system of our design is shown in Figure 1, where the whole VANET system is composed of three entities: the trusted authority (TA), the road-side units (RSUs), and the vehicles. Descriptions of these entities are, respectively, illustrated below.

Trusted Authority (TA) is a trustworthy management center in charge of all the involving RSUs and vehicles. The vital system operations, including vehicle registration, assignment, and secret key generation, are all conducted by TA. Additionally, TA stores the significant user data in its memory. Hence, TA is assumed to have adequate storage and computing capability. Moreover, performing as both the trustworthy verifier and key generation center, TA is infeasible to be compromised by the adversaries. Thus various services can be securely presented to the designated vehicles. In this case, the group key is necessary for secure message exchange.

Road-side units (RSUs) are vital VANET infrastructure implemented at the roadside, which perform as the sole intermediaries between TA and vehicles. RSUs are responsible for verifying the vehicles. Furthermore, the group key issued by TA will also be delivered by RSUs. Note that RSUs are assumed to have adequate storage in order to manage the acquired data. Hence, in our scheme, the gathered road messages are stored and managed in RSUs. In general, RSUs are connected with TA in a secure wired way. However, since

the RSUs are placed along the roadside far from TA, it is possible that these RSUs may be physically compromised. In this case, the stored user information may be illegally acquired [20]. For this consideration, the RSUs are assumed to be semitrusted devices.

Vehicles are referred to as terminal users of the VANET system. It is designed to be both service receiver and information collector. In other words, with the implemented OBU, each vehicle is able to receive the broadcasting messages. Meanwhile, the vehicle reports real-time road information to RSU wirelessly. In this case, it is essential to adopt effective cryptographic strategies in order to guarantee the secure transmission. Furthermore, each vehicle is equipped with a tamper-proof device (TPD), where the corresponding secrets and derived group key are stored. In our system model, each driver is relevant to certain vehicles during the registration to TA. Every time when the driver activates the vehicles, his/her fingerprint and the assigned certification card are verified. This way, the driver and the correlative vehicle are closely connected. Consequently, for better description, the driver, the OBU, and the vehicle are considered the same entity in this paper.

3.5. Network Assumption. As illustrated in Figure 1, TA manages all the operative RSUs of the VANET system through wired communication. Various safe strategies deployed for TA-RSU communication guarantee the security of the key data exchange. Therefore, the vehicle secret keys can be securely delivered to the correlative RSUs. However, it is possible that some RSUs are compromised physically since they are far from the TA. In this way, the distributed vehicle secret keys are illegally acquired by the adversaries, which could damage both the VANET system and the user privacy. Considered as semitrusted devices, it is not appropriate for the RSUs to manage all the vehicle-related secret keys. As a result, we assume in this paper the TA-RSU communication channel is safe for data transmission, while the RSU itself may be damaged, which results in vehicle information disclosure.

Two types of wireless communication are displayed in the proposed system model, including the vehicle-to-vehicle communication (V2V) and the vehicle-to-RSU communication (V2R). Due to the inherent wireless transmission characteristics, both V2V and V2R communication suffer from charted and uncharted attacks. In a nutshell, the V2V communication is used for information sharing and cooperative data processing between the neighboring vehicles. While the V2R communication emphasizes longitudinal message acquisition and feedback between vehicle and RSU. Note that in our scheme the operative vehicles safely exchange messages with RSUs on road condition using the derived group key.

4. Proposed Secure Certificateless Authentication Scheme

In a nutshell, two principal factors are taken into consideration in this paper: the secure authentication and road message management mechanism, which will be, respectively, discussed in two sections. In this section, we describe the proposed secure certificateless authentication scheme between RSU and vehicles. The proposed scheme can be clarified into three different phases, including *initialization phase*, *authentication phase*, and *group key distribution phase*. Accordingly, some nontrivial preparations are made in the initialization phase. Subsequently, verification on the vehicles is conducted in the following authentication phase. Finally, the generated group key is allocated to the legitimate vehicle.

Our design adopts the certificateless encryption strategy based on elliptic curve cryptography (ECC). Note that the corresponding public keys have been previously revealed to the devices. Meanwhile, the confidential information is assigned to vehicle during registration. Based on this, the adopted cryptographic techniques are available, which could provide adequate security assurance for the VANET system. Emphasizing the authentication between RSU and vehicle, we describe our scheme in the scenario involving single RSU and single vehicle. Note that the scheme for regular VANET scenarios with multiple RSUs and vehicles is similar.

4.1. Initialization Phase. Necessary preliminary works are conducted in the initialization phase, which can be generally classified into user registration and key information allocation. It is desirable that each vehicle should register to TA first. After that, TA assigns the secret information to the corresponding vehicle. Moreover, TA stores the drivers' personal information such as the car plate number, the contact information, and the address. Let $Q_{\mathscr{H}}$ be the generator of a cyclic additive group $\mathbb{G}_{\mathscr{H}}$ and id be the unique identifier for vehicle. Additionally, TA adopts secure hash functions $h : \{0,1\}^* \times \mathbb{G}_{\mathscr{H}} \to \mathbb{Z}^*_{\mathscr{P}}$, where $\mathbb{Z}^*_{\mathscr{P}}$ is defined as a nonnegative integer set less than the large prime number $\mathscr{P}$. Hence, TA generates the secret key R_{id} for each vehicle illustrated as

$$R_{id} = h\left(id, Q_{\mathscr{H}}\right), \tag{1}$$

which is allocated to the relevant vehicle after user registration. Note that the secret keys of all the registered vehicles are securely stored in TA's database. At the same time, TA chooses a random integer $s_{\mathrm{RSU}} \in \mathbb{Z}^*_{\mathscr{P}}$ as the RSU private key. Let $\mathbb{G}_1$ be the cyclic additive group generated by P with the order q. Hence the RSU public key can be computed according to

$$Q_{\mathrm{RSU}} = s_{\mathrm{RSU}} P. \tag{2}$$

It is worth noting that the RSU public key Q_{RSU}, the generator P, the hash function h, and $\mathbb{G}_1$ will be published to all the devices, while the private key s_{RSU} is kept secret during the entire process.

Now we assume that the registered vehicle approaches the working range of a fixed RSU. If certain vehicle wants to receive services from the VANET system, identification and key assignment are essential. In this assumption, the vehicle chooses $s_v \in \mathbb{Z}^*_{\mathscr{P}}$ as its partial private key. Then the corresponding partial public key Q_v is defined as

$$Q_v = s_v P, \tag{3}$$

where P is the system parameter as mentioned above. Subsequently, $\langle Request, Q_v, id \rangle$ are delivered to RSU.

After deriving the partial public key Q_v, RSU requests TA for the secret key R_{id} of vehicle id. Let $H : \{0,1\}^* \times \mathbb{G}_1 \to \mathbb{G}_1$

denote the secure hash function. Related computations can be conducted for partial key generation as follows:

$$\begin{aligned} Q_{id} &= H\left(id, Q_{\mathrm{RSU}}\right) \\ C &= R_{id} s_{\mathrm{RSU}} Q_{id}. \end{aligned} \tag{4}$$

Thereafter, the generated C is delivered to vehicle. Hence the vehicle derives the partial private key s_u according to

$$s_u = R_{id}^{-1} C = s_{\mathrm{RSU}} Q_{id}. \tag{5}$$

At this point, the public key set for vehicle can be displayed as $\langle Q_v, id\rangle$. Meanwhile, the relevant private key set is defined as $\langle s_v, s_u\rangle$. Note that the two partial private keys are, respectively, decided by RSU and vehicle. In other words, RSU has no access to s_v, so that the privacy protection based on certificateless cryptography is achieved even if RSU is compromised by attackers.

4.2. Authentication Phase. After initialization, RSU conducts authentication on the requesting vehicle. In certain time point t, we assume that vehicle starts to use the road message service. Then the following computation is conducted:

$$Q_1 = tQ_v = ts_v P, \tag{6}$$

which combines the current time with the partial public key. In addition, let $\mathbb{G}_2$ be the cyclic group of prime order s and $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ be the bilinear pairing operator. Hence the vehicle gets the intermediate value Q_{id} by

$$Q_{id} = H\left(id, Q_{\mathrm{RSU}}\right), \tag{7}$$

where the vehicle identity id and RSU public key Q_{RSU} are known to vehicle. Subsequently, two necessary parameters r and v are generated as

$$\begin{aligned} r &= \hat{e}\left(Q_{\mathrm{RSU}}, Q_{id}\right) \\ v &= h\left(t \parallel r, R_{id}\right), \end{aligned} \tag{8}$$

where R_{id} is the secret key previously allocated to vehicle in the initialization. Accordingly, the signature U is generated based on

$$U = tvs_v Q_{id} + s_u. \tag{9}$$

At this point, vehicle sends $\langle id, t, v, U\rangle$ to the RSU. In the RSU side, the validity of the received t and v will be verified first. Then RSU computes whether

$$r \stackrel{?}{=} \frac{\hat{e}\left(P, U\right)}{\hat{e}\left(Q_1, Q_{id}\right)^v} \tag{10}$$

holds. The correctness is elaborated as follows:

$$\begin{aligned} \frac{\hat{e}\left(P, U\right)}{\hat{e}\left(Q_1, Q_{id}\right)^v} &= \frac{\hat{e}\left(P, tvs_v Q_{id} + s_u\right)}{\hat{e}\left(tQ_v, Q_{id}\right)^v} \\ &= \frac{\hat{e}\left(P, h\left(t \parallel r, R_{id}\right) ts_v Q_{id} + s_{\mathrm{RSU}} Q_{id}\right)}{\hat{e}\left(Q_v, tQ_{id}\right)^{h(t\parallel r, R_{id})}} \\ &= \frac{\hat{e}\left(P, h\left(t \parallel r, R_{id}\right) ts_v Q_{id} + s_{\mathrm{RSU}} Q_{id}\right)}{\hat{e}\left(ts_v P, tQ_{id}\right)^{h(t\parallel r, R_{id})}} \\ &= \frac{\hat{e}\left(P, h\left(t \parallel r, R_{id}\right) ts_v Q_{id} + s_{\mathrm{RSU}} Q_{id}\right)}{\hat{e}\left(P, ts_v Q_{id}\right)^{h(t\parallel r, R_{id})}} \\ &= \frac{\hat{e}\left(P, h\left(t \parallel r, R_{id}\right) ts_v Q_{id}\right) \hat{e}\left(P, s_{\mathrm{RSU}} Q_{id}\right)}{\hat{e}\left(P, ts_v Q_{id}\right)^{h(t\parallel r, R_{id})}} \\ &= \frac{\hat{e}\left(P, ts_v Q_{id}\right)^{h(t\parallel r, R_{id})} \hat{e}\left(P, s_{\mathrm{RSU}} Q_{id}\right)}{\hat{e}\left(P, ts_v Q_{id}\right)^{h(t\parallel r, R_{id})}} \\ &= \hat{e}\left(P, s_{\mathrm{RSU}} Q_{id}\right) = \hat{e}\left(s_{\mathrm{RSU}} P, Q_{id}\right) = \hat{e}\left(Q_{\mathrm{RSU}}, Q_{id}\right). \end{aligned} \tag{11}$$

If the delivered signature U passes the above verification, the validity of the requesting vehicle can be guaranteed. Thereafter, the authentication phase is completed.

4.3. Group Key Distribution Phase. After the authentication phase, the generated group key is distributed to the legitimate vehicle. It is worth emphasizing that the group key is assumed to be chosen by TA. Meanwhile, the key is delivered to RSUs in a secure way. In this way, when a certain vehicle travels from the effective range of one RSU to the next, the group key is always effective and can be continuously used.

We assume that the secret $\mathcal{K} \in \mathbb{Z}_{\mathcal{P}}^*$ is randomly chosen by TA and then delivered to RSU. In certain time point T, RSU computes

$$\begin{aligned} W &= \mathcal{K} T Q_v \\ F &= h\left(W \parallel v, s_u\right) \end{aligned} \tag{12}$$

and sends $\langle W, F, T\rangle$ to vehicle. Note that the RSU could generate the partial private key s_u using the known information. In this way, the secret $\mathcal{K}$ is combined with current time stamp T and previously acquired intermediate value v.

Similarly, the vehicle first compares the received value F with the stored one. If F is valid, vehicle derives the secret by computing

$$\begin{aligned} N &= T^{-1} s_v^{-1} W = T^{-1} s_v^{-1} \mathcal{K} T Q_v = T^{-1} T s_v^{-1} s_v \mathcal{K} P \\ &= \mathcal{K} P. \end{aligned} \tag{13}$$

At this point, the final group key gk can be acquired according to

$$gk = h\left(N\right) = h\left(\mathcal{K} P\right). \tag{14}$$

Therefore, the group key gk is successfully allocated to the legitimate vehicle. Note that gk will be used in the subsequent communication such as road message dissemination, reporting, and evaluation. The delivered packet format is as follows:

$$\left\langle type, E_{gk}\left(E_{R_{id}}\left(m\right) \parallel id \parallel TS\right), TS\right\rangle, \tag{15}$$

where the transmitted message m is symmetrically encrypted using both R_{id} and the group key gk. Similarly, the current

time stamp denoted as TS is adopted in the encryption. Note that $E_x(y)$ represents the symmetric encryption on y using secret key x. Additionally, type indicates the type of m. For security consideration, the communication between vehicle and RSU adopts the assigned group key gk for encryption.

5. Proposed Road Message Dissemination Scheme

In this section, we describe the corresponding road message dissemination scheme in detail. Meanwhile, the message evaluation and award mechanism are presented.

5.1. Road Message Reporting. We assume the scenario that a specific vehicle with identity id is within the effective range of a RSU. Note that the vehicle has successfully passed the authentication and acquired the group key gk. Subsequently, in a certain time point TS, the vehicle passes through a particular spot where road event occurs. For example, when the vehicle passes through the road accident scene, the driver could consider this accident as a road message and report it to the RSU. According to (15) in previous section, the RSU gets the packet involving the encrypted message and the detailed time point TS. The decryption process is as follows.

First, the decryption with group key gk is conducted in the RSU side according to

$$D_{gk}\left(E_{gk}\left(E_{R_{id}}(m) \parallel id \parallel TS\right)\right) = E_{R_{id}}(m) \parallel id \parallel TS. \quad (16)$$

Next, RSU checks the time stamp TS with the derived one in order to ensure that the received message is timely and effective. Additionally, id of the vehicle is derived. According to the aforementioned design, the RSU acquires the relevant secret R_{id} in its storage so that the transmitted road message m can be acquired according to

$$m = D_{R_{id}}\left(E_{R_{id}}(m)\right). \quad (17)$$

At this point, the RSU is aware of the identity information of the reporting vehicle. Hence, according to id, RSU requests TA for the vehicle priority parameter, which is considered as the initial element in the message management process. In practical scenario with multiple vehicles existing in one RSU's effective range, it is possible that more than one vehicles report the same road message to TA. For example, two vehicles V_1 and V_2 may successively pass through a certain accident scene. Hence, both of them report this event to RSU. In this case, the RSU stores this road message m in its storage and assigns the broadcast priority $\mathrm{br}(m)$ for m, which can be calculated using the priority of the two reporting vehicles as follows:

$$\mathrm{br}(m) = \frac{1}{2}\left[\mathrm{pr}(id_1) + \mathrm{pr}(id_2)\right], \quad (18)$$

where the identifiers of V_1 and V_2 are denoted as id_1 and id_2, respectively. Meanwhile, the priorities of the two vehicles are $\mathrm{pr}(id_1)$ and $\mathrm{pr}(id_2)$. The calculated $\mathrm{br}(m)$ here represents the broadcast priority right after the two vehicles report the message. Moreover, among all the vehicles, it is assumed that only V_1 and V_2 report m to RSU such that $\mathrm{br}(m)$ is achieved as the average value of all the reporting vehicles' priority.

In a nutshell, we assume that the vehicle set $V = \{V_i \mid i \in [1, n],\ n \in \mathbb{N}^*\}$ denotes the n legitimate vehicles that have already passed the authentication process conducted by the effective RSU. Among these n vehicles, the vehicle subset $RP_m = \{V_j \mid j \in [1, g],\ g \in \mathbb{N}^* \wedge g \leq n\}$ consists of all the g vehicles that report road message m. Note that the identity of V_j is denoted as id_j. Hence, the broadcast priority is $\mathrm{pr}(id_j)$ and $RP_m \subseteq V$ holds. It is assumed that the g vehicles report message following the sequence of $V_1, \ldots, V_g$. Moreover, the road event $Event_m^{loc}$ is denoted as follows:

$$Event_m^{loc} = \{loc, type, cont\}, \quad (19)$$

which indicates that $Event_m^{loc}$ happened in location loc and the detailed information is showed in $cont$. Moreover, the event type is defined as $type$. In this way, the road message m contains the essential elements of $Event_m^{loc}$.

In our assumption, after $Event_m^{loc}$ occurred, within certain time interval g vehicles will report the event to the RSU. Hence, after RSU receives the road report from V_1 for the first time, the broadcast priority is computed as $\mathrm{br}(m) = \mathrm{pr}(id_1)$. Similarly, the broadcast priority after RSU receives the road report for k ($1 \leq k \leq g$) times, and $\mathrm{br}(m)$ can be computed as

$$\mathrm{br}(m) = \frac{1}{k}\sum_{i=1}^{k}\mathrm{pr}(id_i), \quad (20)$$

which is defined as the average vehicle priorities of all the reporting vehicles. Hence after Δt, the broadcast priority for m is

$$\mathrm{br}(m) = \frac{1}{g}\sum_{i=1}^{g}\mathrm{pr}(id_i). \quad (21)$$

Practically, one RSU handles multiple different road messages simultaneously. Therefore, each message will be assigned a broadcast priority and then stored in the storage. In our design, the creditability and accuracy of the road message are highly related to the reporter's previous records. And the vehicle priority is able to reflect this property properly. Consequently, RSU sorts all these messages so that the reliable messages will be broadcast first.

5.2. Road Message Dissemination. As illustrated in the above section, the RSU manages all the road information within its effective range. Periodically, RSU broadcasts the messages in certain sequence. Note that all the road messages are encrypted using the distributed group key gk. Hence, only the registered vehicles can get access to this service. The aforementioned broadcast priority $\mathrm{br}(m)$ is roughly decided by reliability of the reporting vehicles. In this way, a predefined parameter $\mathscr{W}$ is set as the minimum requirement for message dissemination. That is to say, the messages m will be broadcast only if $\mathrm{br}(m) \geq \mathscr{W}$. Otherwise it will be considered as unreliable information and then temporarily disabled from the broadcast list. In this case, in future, if other vehicles

report the same message, $\mathrm{br}(m)$ will be compared with $\mathscr{W}$ again. After a predefined time interval, if $\mathrm{br}(m) < \mathscr{W}$, RSU permanently deletes the message in its storage. Following the above procedure, vehicles could acquire road messages in an accurate way. Thus the driving security can be improved with this service.

5.3. Evaluation and Priority Management. For practical consideration, an appropriate evaluation mechanism towards the road messages is necessary. In this subsection, we describe the proposed evaluation and priority management scheme. The value of the stored road message is decided by not only the reputation of the reporter but also the message itself. In order to achieve this, we assume that the vehicles have the capability of evaluating the received road messages. Following the above assumptions, the vehicle subset $RV_m = \{V_l \mid l \in [1, f],\ f \in \mathbb{N}^*\}$ denotes f vehicles who receive the road message m within time interval Δt_{RC}. After $V_l \in RV_m$ approaches the location loc where the road event $Event_m^{loc}$ happened, V_l could evaluate whether the received road information is correct, which helps improve the road report accuracy. The format of the evaluation message is as follows:

$$\left\langle type, E_{gk}\left(E_{s_u}\left(ifNO \parallel assess\right) \parallel id \parallel TS_{ev}\right), TS_{ev}\right\rangle, \quad (22)$$

where the message type denoted as $type$ here indicates that it is an evaluation message. $ifNO$ denotes the assigned information number for message m. In addition, TS_{ev} is the current time stamp. Note that this evaluation will be sent back to RSU. According to

$$\begin{aligned} &D_{gk}\left(E_{gk}\left(E_{s_u}\left(ifNO \parallel assess\right) \parallel id \parallel TS_{ev}\right)\right) \\ &\quad = E_{s_u}\left(ifNO \parallel assess\right) \parallel id \parallel TS_{ev}, \end{aligned} \quad (23)$$

RSU checks the time stamp TS_{ev} with the derived one in order to ensure that the message is timely and effective. Additionally, id of the vehicle is derived. RSU acquires the relevant secret s_u in its storage so that the transmitted evaluation on message m can be acquired according to

$$D_{s_u}\left(E_{s_u}\left(ifNO \parallel assess\right)\right) = ifNO \parallel assess. \quad (24)$$

In this way, the evaluation can be combined to m according to $ifNO$. As a result, for road message m, the RSU could receive h_m evaluation messages where $h_m \le f$. For practical consideration, the $assess$ can be analyzed using different state parameters such as $sp \in \{-2, -1, 0, 1, 2\}$, where $sp = 2$ means that $assess$ is totally accurate and helpful, while $sp = -2$ means that $assess$ is of no help and thus is considered as the fake message. The h_m state parameters are $\{sp_u \mid u \in [1, h_m],\ u \in \mathbb{N}^*\}$. During every certain period Δt_{RD}, RSU analyzes all the received evaluation messages and updates the broadcast priority following the steps below:

(i) Screening: firstly, RSU checks whether

$$Rate_m^{\Delta t_{RD}}\left[sp_u > 0\right] \ge \mathscr{V} \quad (25)$$

holds, where $Rate_m^{\Delta t_{RD}}[sp_u > 0]$ denotes the proportion of the received $assess$ whose $sp_u > 0$ among all the h_m evaluation on m. Furthermore, $\mathscr{V}$ is the predefined system parameter according to different practical scenarios. In this case, if most of the users give negative assessments, m is considered as invalid information and must be discarded from the storage immediately.

(ii) Updating: secondly, the updating on broadcast priority is conducted as

$$\begin{aligned} \mathrm{br}'(m) &= \mathrm{br}(m) + \frac{\sum_{u=1}^{h_m}\left[\mathrm{pr}\left(id_u\right) \times sp_u\right]}{h_m} \\ &= \frac{\sum_{i=1}^{g}\mathrm{pr}\left(id_i\right)}{g} + \frac{\sum_{u=1}^{h_m}\left[\mathrm{pr}\left(id_u\right) \times sp_u\right]}{h_m}, \end{aligned} \quad (26)$$

where $[\mathrm{pr}(id_u)]_{u\in[1,h_m]}$ denotes the priority of h_m vehicles.

At this point, the updating process for Δt_{RD} is completed. Similarly, after n time periods $n\Delta t_{RD}$, the broadcast priority for m is

$$\begin{aligned} \mathrm{br}^{n\Delta t_{RD}}(m) = &\frac{\sum_{i=1}^{g}\mathrm{pr}\left(id_i\right)}{g} \\ &+ \sum_{i=1}^{n}\left(\frac{\sum_{u=1}^{h_m^i}\left[\mathrm{pr}\left(id_u^i\right) \times sp_u^i\right]}{h_m^i}\right), \end{aligned} \quad (27)$$

where h_m^i, $\mathrm{pr}(id_u^i)$, and sp_u^i are the parameters in ith time periods $i\Delta t_{RD}$. Note that the above process should be conducted for each stored road message in RSU. Hence, the broadcast sequence is updated. In future, after $x\Delta t_{RD}$, m will be deleted if $br^{x\Delta t_{RD}}(m) < \mathscr{N}$, where $\mathscr{N}$ is the preset system parameter.

5.4. Vehicle Priority Management. As illustrated above, the vehicle priority on vehicle id is $\mathrm{pr}(id)$, which is a significant user property in both the broadcast priority computing and updating processes. As a matter of fact, the reporting vehicle plays a crucial role in the message dissemination scheme. Hence, appropriate rewarding strategy is essential to motivate drivers' enthusiasm on road situation reporting. The incentives will be given according to the vehicle priority. To achieve this, $\mathrm{pr}(id)$ will be updated according to the value of his reporting road message.

We assume that road message m is reported by several vehicles in $B = \{vp_i \mid 1 \le i \le n,\ i \in \mathbb{N}^*\}$. After a sufficient time period, for example, twenty-four hours, one road message m has been evaluated by multiple vehicles. According to (25) in the previous section, m is valid if

$$Rate_m^{\Delta t_{RD}}\left[sp_u > 0\right] \ge \mathscr{V} \quad (28)$$

holds. In this way, $\mathrm{pr}(vp_i)$ of all $vp_i \in B$ are updated as

$$\mathrm{pr}\left(vp_i\right) = \mathrm{pr}\left(vp_i\right) + 1. \quad (29)$$

In contrast, if m is evaluated to be invalid and discarded by RSU, $\mathrm{pr}(vp_i)$ of all $vp_i \in B$ are updated as

$$\mathrm{pr}\left(vp_i\right) = \mathrm{pr}\left(vp_i\right) - 1. \tag{30}$$

Note that the driver could change it into incentives such as coupons of cooperative stores or scorecard in the road service area.

6. Security Analysis

In this section, we analyze the security properties of the proposed authentication scheme. The security theorems as well as the corresponding proofs are given below.

6.1. Unforgeability against Chosen Message Attack. We analyze the unforgeability against chosen message attack in the proposed protocol.

Theorem 1. *The proposed certificateless authentication scheme is existentially unforgeable against adaptive chosen message attack under the assumption of random oracle model if and only if the CDHP is hard.*

Proof. The security of unforgeability is formally defined through game $\mathscr{G}_1$. Let $\mathscr{A}_1$ be a probabilistic polynomial time adversary. $\mathscr{C}_1$ denotes the challenger; h and H denote the random oracles. In order to solve CDHP problem, it is assumed that $\mathscr{C}_1$ is able to simulate all the related oracles. In $\mathscr{G}_1$, $\mathscr{A}_1$ can conduct the following corresponding queries to $\mathscr{C}_1$.

h Query. We assume that the adversary $\mathscr{A}_1$ itself does not have the ability to directly compute the hash function $h(\cdot)$. Hence, the response to *h Query* is simulated by maintaining a list $List_h$ initialized to be empty. That is to say, when the oracle is queried with the input values $\langle t, r, R_{id}\rangle$, if the query $\langle t, r, R_{id}\rangle$ already exists in $List_h$, $\mathscr{C}_1$ outputs $v = h(t \parallel r, R_{id})$ to $\mathscr{A}_1$. Otherwise, $\mathscr{C}_1$ chooses a random number $v \in \mathbb{Z}^*$ and forwards it to $\mathscr{A}_1$. After that, $\langle t, r, R_{id}, v\rangle$ will be subsequently added to $List_h$.

Extract Query. The adversary $\mathscr{A}_1$ is able to query the partial private key of any given key set $\langle Q_v, id\rangle$. According to id, $\mathscr{C}_1$ outputs the partial private key s_u to $\mathscr{A}_1$.

H Query. $\mathscr{A}_1$ can query the random oracle H at any time. The response to *H Query* is simulated by maintaining a list $List_H$. Note that $List_H$ is initialized to be empty. When the oracle H is queried with input values $\langle id, Q_{\mathrm{RSU}}\rangle$, if the query $\langle id, Q_{\mathrm{RSU}}\rangle$ already exists in $List_H$, $\mathscr{C}_1$ outputs $Q_{id} = H(id, Q_{\mathrm{RSU}})$ to $\mathscr{A}_1$. Otherwise, $\mathscr{C}_1$ chooses a random number $Q_{id} \in \mathbb{Z}^*$ and forwards it to $\mathscr{A}_1$. After that, $\langle id, Q_{\mathrm{RSU}}, Q_{id}\rangle$ will be subsequently added to $List_H$.

Authenticating Query. $\mathscr{C}_1$ simulates the authenticating oracle by responding to the authenticating query as follows:

(i) $\mathscr{C}_1$ randomly chooses $U \in \mathbb{G}_1$ as the certificate and $v \in \mathbb{Z}^*$ as the intermediate parameter.

(ii) $\mathscr{C}_1$ computes $r = \widehat{e}(P, U)/\widehat{e}(Q_1, Q_{id})^v$. If $\langle t, r, R_{id}, v\rangle$ already exists in $List_h$, $\mathscr{C}_1$ chooses other values and tries again.

(iii) $\mathscr{C}_1$ adds the above $\langle t, r, R_{id}, v\rangle$ to $List_h$.

(iv) $\mathscr{C}_1$ outputs $\langle id, t, v, U\rangle$ as the certificate.

According to the *Forking Lemma* [43], $\mathscr{A}_1$ produces two valid certificates $\langle id, t, v, U\rangle$ and $\langle id, t, v', U'\rangle$ $(v \neq v')$. In this case,

$$\begin{aligned} U &= tvs_v Q_{id} + s_u \\ U' &= tv' s_v Q_{id} + s_u, \end{aligned} \tag{31}$$

hold. Hence we can get

$$s_v Q_{id} = \frac{\left(v - v'\right)^{-1}\left(U - U'\right)}{t}. \tag{32}$$

In this way, we show that the CDHP problem can be solved. In other words, the attacker needs to solve the CDHP problem in order to forge the certificate. However, this contradicts the hardness of the CDHP problem [44, 45]. In conclusion, an attacker cannot forge the certificate in the authentication process [46, 47]. □

6.2. Resistance to Replay Attack. The replay attack is achieved by reusing the previous generated message to pass the current authentication process. The security property against replay attack is discussed in this section.

Theorem 2. *During the certificateless authentication process, replay attack can be prevented. That is, the previous messages of the past authentication sessions cannot pass the current authentication process in RSU side.*

Proof. We discuss the resistance to replay attack through game $\mathscr{G}_2$. Similarly, let $\mathscr{A}_2$ be a probabilistic polynomial time adversary. It is assumed that, in time point $\mathscr{T}_1$, $\mathscr{A}_2$ has access to all the published system parameters as well as the transmitted messages from $\mathscr{T}_0$ to $\mathscr{T}_1$ $(\mathscr{T}_0 < \mathscr{T}_1)$. Randomly, $\mathscr{A}_2$ chooses the message $\langle id, \mathscr{T}_r, v^{\mathscr{T}_r}, U^{\mathscr{T}_r}\rangle$ at time $\mathscr{T}_r \in [\mathscr{T}_0, \mathscr{T}_1]$. At $\mathscr{T}_1$, $\mathscr{A}_2$ sends $\langle id, \mathscr{T}_1, v^{\mathscr{T}_r}, U^{\mathscr{T}_r}\rangle$ as the replaying message. Note that $U^{\mathscr{T}_r} = \mathscr{T}_r v^{\mathscr{T}_r} s_v Q_{id} + s_u$. In this way, $r \neq \widehat{e}(Q_{\mathrm{RSU}}, Q_{id})$. Hence, the previous message cannot pass the current authentication. □

6.3. Forward Security. In this section, we analyze the forward security property of the proposed protocol.

Theorem 3. *The proposed authentication scheme provides forward security against adversary. That is, the adversary cannot pass the authentication with the acquired vehicle secret key from the compromised RSU.*

Proof. We assume that the RSU has already been compromised by brute-force attack and all the stored key information is leaked to the adversary $\mathscr{A}_3$. The secret key set $\{s_u^i \mid i \in [1, n]\}$ denotes the private keys of all the n vehicles. In this case, $\mathscr{A}_3$ is able to use the derived partial private key s_u for

Table 1: Comparison of storage overhead.

Protocol	ICPA [10]	DAKM [4]	ABAP [8]	SAAP [32]	Our protocol
Storage (Vehicle)	2112 bits	2712 bits	3432 bits	2904 bits	2520 bits
Storage (RSU)	$1440n + 1056$ bits	$1676n + 1144$ bits	$1936n + 1048$ bits	$2008n + 2392$ bits	$1592n + 768$ bits

certificate generation. However, the private key contains both s_u and s_v, while s_v is chosen by the vehicle itself. Due to the hardness of the aforementioned DLP problem, the probability that $U = tvs_vQ_{id} + s_u$ can be correctly computed is illustrated as $1/2^{\varpi}$, where ϖ is the size of s_v. In general, the certificateless authentication property guarantees the forward security of the proposed scheme. □

6.4. Session Key Establishment. In the system model of this paper, it is necessary to generate a shared session key between the RSU and vehicle so as to guarantee the data confidentiality and transmission security, which is analyzed as follows.

Theorem 4. *In the proposed protocol, the shared session key is established after successfully authentication between RSU and vehicle.*

Proof. According to the protocol design, $\mathcal{K}$, along with the current time stamp and the previously acquired intermediate value v, is transmitted to the vehicle. In the vehicle side, the below derivation of $\mathcal{K}$ is conducted as $N = T^{-1}s_v^{-1}W = \mathcal{K}P$, where s_v is stored in vehicle already. Note that the security assurance of the message transmission is based on the hardness of DLP problem. The final group key is generated and adopted to the following message transmission. □

6.5. Mutual Authentication. In this section, we analyze the mutual authentication property in the proposed authentication protocol.

Theorem 5. *The proposed protocol can provide mutual authentication between RSU and vehicle if the DLP problem is intractable.*

Proof. During the authentication process, the RSU-to-vehicle security is preserved by the aforementioned certificate $\langle id, t, v, U\rangle$, which has been discussed in the proof of Theorem 1. On the other hand, the vehicle-to-RSU security is based on the hardness of DLP problem. Specifically, $F = h(W \parallel v, s_u)$ is contained in the delivered $\langle W, F, T\rangle$ and will be verified by the RSU with the known key information. Therefore, we could conclude that the proposed authentication scheme provides mutual authentication property. □

7. Performance Analysis

In this section, we present the performance analysis towards the proposed protocol. Our analysis on the performance mainly emphasizes the storage overhead, the computation cost, and the communication cost, which are the dominant factors in the proposed protocol.

7.1. Storage Overhead. In the proposed protocol, storage overhead is a crucial parameter for VANETs, especially for vehicles. Due to the inherent resource restriction, it is impractical for the vehicle to store massive key messages and communication data in its own memory. Moreover, the RSU is designed to handle both the key distribution and road message management simultaneously. As a result, the storage overhead in both the vehicle and RSU sides should be considered.

As for the vehicle in the proposed protocol, some essential key information is previously stored during the registration including $\langle id, R_{id}, Q_v, s_v, s_u\rangle$. The published public key of RSU, namely, Q_{RSU}, as well as the intermediate value $\langle Q_{id}, C\rangle$, is also stored in vehicle. Moreover, the transmitted message $\langle r, v, U\rangle$, and the necessary group key distribution value are stored, respectively, in the group key distribution phase. According to [48], we assume that the length of elements in $\mathbb{G}_{\mathcal{H}}$ and $\mathbb{G}_1$ is 256 bits. The lengths of relevant vehicle secret keys such as s_v, s_u, and gk are 160 bits. Moreover, it is assumed than the lengths of the adopted time stamps and the identity of vehicle id are 32 bits and 24 bits each. In this way, the storage overhead for each vehicle is $24 + 256 \times 5 + 160 \times 7 + 32 \times 3 = 2520$ bits. Similarly, we assume that the number of vehicles in the RSU range is n. Consequently, the storage overhead in RSU side includes key information of RSU itself and secret messages of all the n vehicles. In this way, the storage overhead for the RSU is $256+160\times3+32+n(24+256\times4+160\times3+32\times2) = 1592n+768$ bits. The comparison with the state-of-the-art VANETs authentication protocols ICPA [10], DAKM [4], ABAP [8], and SAAP [32] is illustrated in Table 1.

7.2. Computation Cost. In this section, we analyze the computation cost of the proposed protocol. The computation cost is defined as the time consumption for the group key distribution process. The comparison result with ICPA, DAKM, ABAP, and SAAP is given in Table 2. We denote modulo operation as mod, exponential operation as Ex, and bilinear pairing as $\hat{e}$. Enc and Dec refer to encryption and decryption. Additionally, H, M, D, and A represent one-way hash function, multiplication operation, division operation, and addition operation, respectively. Finally, the point multiplication operation is dented as p.

7.3. Communication Cost. The communication cost refers to the time consumption for message transmission. In this subsection, we consider the required communication passes for RSU to successfully authenticate vehicles. The comparison result on communication cost is given in Table 3.

8. Conclusion

Emphasizing the secure authentication and road message dissemination in VANETs, a secure certificateless authentication and road message dissemination protocol is proposed in this paper. In our design, certificateless cryptographic technique

Table 2: Comparison of computation cost.

Protocol	ICPA [10]	DAKM [4]	ABAP [8]	SAAP [32]	Our protocol
Computation cost (vehicle)	$3p + 3H + 2A + 2M + 2\text{mod}$	$1Dec + \text{mod} + 1Enc$	$1Dec + 4p + 2H + 2A + D$	$10p + 5H + 4A + M$	$4p + 3H + \widehat{e} + A + 3M$
Computation cost (RSU)	$3nM + (2n + 2)p + 2A$	$3Enc + 2nM + nD + (n-1)A$	$2nH + 2np + 2nM + 3n\widehat{e} + nA$	$4nH + (8n + 1)p + nM + 3nA$	$2nH + 2np + 2nM + 2n\widehat{e} + nEx$

Table 3: Comparison of communication cost.

Protocol	ICPA [10]	DAKM [4]	ABAP [8]	SAAP [32]	Our protocol
Computation rounds	$4n + 2$	$4n + 1$	$4n + 1$	$4n + 4$	$4n$

is employed for authentication and key distribution. Subsequently, an appropriate road message dissemination mechanism is designed. The security analysis and performance evaluation are given accordingly. The proposed protocol is suitable for practical VANET scenarios and is capable of providing timely road information services, which improves both the user safety and the driving experience.

Notations

TA, RSU:	Trustworthy authority, road-side units
$\mathbb{G}_{\mathscr{K}}$:	Cyclic additive group
$Q_{\mathscr{K}}$:	Generator of $\mathbb{G}_{\mathscr{K}}$
id:	Unique identifier of vehicle
h:	Secure hash function, $h : \{0,1\}^* \times \mathbb{G}_{\mathscr{K}} \to \mathbb{Z}^*_{\mathscr{P}}$
R_{id}:	Secret key for vehicle
s_{RSU}:	RSU private key
P:	Generator of cyclic additive group $\mathbb{G}_1$
Q_{RSU}:	RSU public key
s_v:	Vehicle partial private key
Q_v:	Vehicle partial public key
H:	Secure hash function, $H : \{0,1\}^* \times \mathbb{G}_1 \to \mathbb{G}_1$
s_u:	Vehicle partial private key
Q_{id}:	Intermediate authenticating value
$\mathscr{K}$:	Secret key generated by TA
gk:	Group key
$E_x(y)$, $D_x(y)$:	Symmetric encryption and decryption on y with x
m:	The disseminated message
$\text{br}(m)$:	Broadcast priority of m
$\text{pr}(id)$:	Vehicle priority
$Event_m^{loc}$:	Road event
g:	Number of reporting vehicles
$\mathscr{W}, \mathscr{V}, \mathscr{N}$:	Predefined system parameters.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the National Research Foundation of Korea (NRF) grants funded by the Korean government (MSIP) (nos. NRF-2016R1A2B4012638 and NRF-2017R1D1A3B03034005) and by the MIST (Ministry of Science & ICT), Korea, under the National Program for Excellence in SW, supervised by the IITP (Institute for Information & Communication Technology Promotion) (2017-0-00137).

References

[1] X. Peng, "A novel authentication protocol for vehicle network," in *Proceedings of the 2016 3rd International Conference on Systems and Informatics, ICSAI 2016*, pp. 664–668, Shanghai, China, November 2016.

[2] S. Guo, D. Zeng, and Y. Xiang, "Chameleon hashing for secure and privacy-preserving vehicular communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 11, pp. 2794–2803, 2014.

[3] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication," *Journal of Communications and Networks*, vol. 11, no. 6, pp. 574–588, 2009.

[4] P. Vijayakumar, M. Azees, A. Kannan, and L. J. Deborah, "Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015–1028, 2015.

[5] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 9, pp. 1227–1239, 2010.

[6] J.-L. Huang, L.-Y. Yeh, and H.-Y. Chien, "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 1, pp. 248–262, 2011.

[7] F.-K. Tseng, Y.-H. Liu, J.-S. Hwu, and R.-J. Chen, "A secure reed-solomon code incentive scheme for commercial Ad dissemination over VANETs," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 9, pp. 4598–4608, 2011.

[8] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 8, pp. 2193–2204, 2016.

[9] K.-A. Shim, "CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1874–1883, 2012.

[10] D. He, S. Zeadally, B. Xu, and X. Huang, "An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme

for Vehicular Ad Hoc Networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[11] J. Shen, H. Tan, Y. Zhang, X. Sun, and Y. Xiang, "A new lightweight RFID grouping authentication protocol for multiple tags in mobile environment," *Multimedia Tools and Applications*, vol. 76, no. 21, pp. 22761–22783, 2017.

[12] X. Sun, X. Lin, and P.-H. Ho, "Secure vehicular communications based on group signature and ID-based signature scheme," in *Proceedings of the 2007 IEEE International Conference on Communications, ICC'07*, pp. 1539–1545, Glasgow, UK, June 2007.

[13] K. Ansari, C. Wang, L. Wang, and Y. Feng, "Vehicle-to-vehicle real-time relative positioning using 5.9–GHZ DSRC media," in *Proceedings of the IEEE 78th Vehicular Technology Conference (VTC Fall' 13)*, pp. 1–7, September 2013.

[14] X. Cheng, L. Yang, and X. Shen, "D2D for intelligent transportation systems: A feasibility study," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 4, pp. 1784–1793, 2015.

[15] 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, Phoenix, AZ, USA, April 2008.

[16] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, "2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 2, pp. 896–911, 2016.

[17] X. Li and L. Wang, "A rapid certification protocol from bilinear pairings for vehicular ad hoc networks," in *Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012*, pp. 890–895, Liverpool, UK, June 2012.

[18] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 616–629, 2011.

[19] H. Tan, D. Choi, P. Kim, S. Pan, and I. Chung, "Comments on "Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks"," *IEEE Transactions on Intelligent Transportation Systems*, no. 99, pp. 1–3, 2017.

[20] T. W. Chim, S. M. Yiu, L. C. Hui, and V. . Li, "VSPN: VANET-based secure and privacy-preserving navigation," *Institute of Electrical and Electronics Engineers. Transactions on Computers*, vol. 63, no. 2, pp. 510–524, 2014.

[21] B. Liu, D. Jia, J. Wang, K. Lu, and L. Wu, "Cloud-assisted safety message dissemination in VANET-cellular heterogeneous wireless network," *IEEE Systems Journal*, vol. 11, no. 1, pp. 128–139, 2017.

[22] M.-C. Chuang and M. C. Chen, "DEEP: density-aware emergency message extension protocol for VANETs," *IEEE Transactions on Wireless Communications*, vol. 12, no. 10, pp. 4983–4993, 2013.

[23] M. Milojevic and V. Rakocevic, "Location aware data aggregation for efficient message dissemination in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 12, pp. 5575–5583, 2015.

[24] J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, "Anonymous and Traceable Group Data Sharing in Cloud Computing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 912–925, 2018.

[25] J. Song, C. He, L. Zhang, S. Tang, and H. Zhang, "Toward an RSU-unavailable lightweight certificateless key agreement scheme for VANETs," *China Communications*, vol. 11, no. 9, pp. 93–103, 2014.

[26] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp. 1606–1617, 2010.

[27] D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 3, pp. 736–746, 2011.

[28] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 1, pp. 127–139, 2012.

[29] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.

[30] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," *RSA CryptoBytes*, vol. 5, 2005.

[31] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1711–1720, 2016.

[32] H. Xiong, "Cost-effective scalable and anonymous certificateless remote authentication protocol," *IEEE Transactions on Information Forensics & Security*, vol. 9, no. 12, pp. 2327–2339, 2014.

[33] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of the Advances in Cryptology*, pp. 47–53, 1984.

[34] 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 I, pp. 3442–3456, 2007.

[35] C.-C. Lee and Y.-M. Lai, "Toward a secure batch verification with group testing for VANET," *Wireless Networks*, vol. 19, no. 6, pp. 1441–1449, 2013.

[36] J. K. Liu, T. H. Yuen, M. H. Au, and W. Susilo, "Improvements on an authentication scheme for vehicular sensor networks," *Expert Systems with Applications*, vol. 41, no. 5, pp. 2559–2564, 2014.

[37] Y. Zhang, L. Yang, and S. Wang, "An efficient identity-based signature scheme for vehicular communications," in *Proceedings of the 11th International Conference on Computational Intelligence and Security, CIS 2015*, pp. 326–330, Shenzhen, China, December 2015.

[38] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Proceedings of the Advances in Cryptology-ASIACRYPT2003*, pp. 452–473, 2003.

[39] H. Xiong, Z. Chen, and F. Li, "Provably secure and efficient certificateless authenticated tripartite key agreement protocol," *Mathematical and Computer Modelling*, vol. 55, no. 3-4, pp. 1213–1221, 2012.

[40] H. Xiong and Z. Qin, "Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 7, pp. 1442–1455, 2015.

[41] J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, "Privacy-Preserving and Lightweight Key Agreement Protocol for V2G

in the Social Internet of Things," *IEEE Internet of Things Journal*, pp. 1-1, 2017.

[42] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *Journal of Computer and System Sciences*, vol. 18, no. 2, pp. 143–154, 1979.

[43] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, no. 3, pp. 361–396, 2000.

[44] D. Wang, D. He, P. Wang, and C.-H. Chu, "Anonymous Two-Factor Authentication in Distributed Systems: Certain Goals Are Beyond Attainment," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 4, pp. 428–442, 2015.

[45] C. Wang, G. Xu, and J. Sun, "An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks," *Sensors*, vol. 17, no. 12, article no. 2946, 2017.

[46] D. Wang and P. Wang, "Two Birds with One Stone: Two-Factor Authentication with Security Beyond Conventional Bound," *IEEE Transactions on Dependable and Secure Computing*, no. 99, pp. 1–14, 2016.

[47] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipfs law in passwords," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2776–2791, 2017.

[48] D. He, S. Zeadally, N. Kumar, and J. H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, no. 99, pp. 1–12, 2016.