Nkenyereye *et al. EURASIP Journal on Wireless Communications and Networking* (2016) 2016:196
DOI 10.1186/s13638-016-0687-0

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

A secure billing protocol over attribute-based encryption in vehicular cloud computing

Lewis Nkenyereye, Youngho Park and Kyung Hyune Rhee*

Abstract

The integration of cloud computing into vehicular ad hoc networks (VANETs) has allowed the possibility of offering multiple services to the vehicle owners ranging from safety to entertainment services. The ubiquitousness of cloud computing involves a multitude of service providers; thus, an efficient and secure access control mechanism is required. However, rigorous security features need to be addressed for such commercial-based services to be fully adopted. In this paper, we present a secure billing protocol over attribute-based encryption in vehicular cloud computing. We achieve the identity privacy of the vehicles and their requested services through pseudonym techniques. Certificateless signature scheme is used to assure the authentication of legitimate vehicles which can enjoy the provided services. We use attribute-based encryption to guarantee access control based on the purchased services. We make use of hash chain technique to provide authorization through electronic voucher (credits) which a vehicle has to possess in order to purchase a service. Unlike existing protocols in VANETS, the proposed protocol is not built on expensive bilinear pairing operations. We provide the efficiency of the proposed protocol through performance analysis and simulation.

Keywords: Access control, Attribute-based encryption, Certificateless signature scheme, Vehicular cloud computing

1 Introduction

Combining cloud computing (CC) with vehicular ad hoc networks (VANETs) to form vehicular cloud computing (VCC) appeals the existing cloud service providers (CSPs) such as Amazon EC2, S3, Microsoft Azure to also extend their services to vehicle users. Taking advantage of the vehicle's on-board unit (OBU), the vehicle users would have additional computing resources to enjoy various services from safety to infotainment-related services. In conventional cloud computing, CSPs usually offer a pay-per-use billing system in their pricing model which means that a user will only be charged for exactly the amount of services provided. A vehicle user can acquire the services on the move using the OBU's visual and computational capabilities. As pointed out by Li et al., a key success of commercial applications over vehicular environment will inevitably be featured by entity authentication and billing while simultaneously embracing the vehicle mobility [1].

Basic security requirements in VCC have been addressed such as entity authentication, authorization, and privacy [2, 3]. Existing literature has more focused on access control mechanisms which allow a CPS to provide multiple services within a single package [4–6]. To enforce access control in different services, attribute-based encryption (ABE) has widely been adopted to offer a number of services embedded within a single package [4, 5]. Even though ABE ensures that a service is accessed by a legitimate user, bad-intentioned vehicle user might over use the services as long as the access structure permits it. Thus, secure billing feature is required in order the vehicle users to strictly access what they consent to pay for. Secure billing systems which provide evidence to the vehicle user when it comes to payment need to be considered for a full adoption of the commercial services in VCC.

*Correspondence: khrhee@pknu.ac.kr
Department of IT Convergence and Application Engineering, Pukyong National University, 45 Yongso-ro, Nam-gu, Busan, Republic of Korea

Springer Open

© 2016 The Author(s). **Open Access** This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

Among the relevant works with secure billing feature in VANETs, Yeh et al. proposed a local and proxy-based authentication and billing protocol in order to reduce the communication overhead. Their protocol proposed an incentive-aware multi-hop forwarding technique for vehicles in the VANETs [7]. The protocol did not consider secure access control which is indispensable for CSPs within the VCC architecture. In another work, Yeh et al. proposed a portable authentication/authorization/accounting (AAA) framework for purchasing services from the road entities (RSUs). They used signature-based and key policy attribute-based encryption (KP-ABE) in their billing mechanism to achieve localized fine-grained access control [4]. However, in their protocol, the system master secret key must be distributed to every vehicle temper proof device. Therefore, in case the temper proof device is compromised, the system security features are affected [8]. Moreover, these protocols are built based on expensive pairing operations which will hinder the whole system efficiency since the CSPs would also provide voluminous files such as mp3 files or movies.

In this paper, we present a secure billing protocol over attribute-based encryption in vehicular cloud computing. The identity privacy of the vehicles and their requested services is achieved through pseudonym techniques. We make use of certificateless signature scheme to assure the authentication of legitimate vehicles which can enjoy the provided services [9]. ABE is adopted to guarantee rigorous access control based on the provided access structure [10]. Hash chain technique is to used to guarantee the authorization property through electronic voucher which a vehicle has to possess before enjoying any giving service [11].

1.1 Motivation and contribution

The vehicles on the move need also to enjoy a variety of services provided by the CSPs as individuals do through the smart phones. Additionally, the vehicles on the move are predicted to easily and efficiently enjoy the CSP's services due to the technological features such as visual, computing, and networking in-built capabilities. However, the CSP owners have to make sure that the vehicle users pay for the provided services along with additional security properties which need to be met before the adoption of the commercial services in VCC. We describe our contributions as follows:

- We first present an application model for a secure billing protocol over attribute-based encryption in vehicular cloud computing which allows the vehicle users to enjoy a variety of service on the move. We define the security requirements to be met by the proposed protocol.
- We present a secure billing protocol over attribute-based encryption in vehicular cloud computing based on the techniques of attribute-based encryption, secret sharing scheme, certificateless signature scheme, and hash chain technique.
- We apply electronic voucher (credits) feature in the system to restrict the vehicles from over using the acquired access structure in order to enjoy the embedded services. Thus, a vehicle is not prompt to enjoy a given service in a limited time. The electronic coin boosts the confidence of the CSPs over non-repudiation of payment.
- We provide analysis of the proposed protocol in terms of security objectives. We further evaluate the performance of the proposed protocol through computational delay, transmission overhead, and simulation.

The remainder of the paper is organized as follows. We first present the related work and the preliminaries in Section 2 and Section 3, respectively. We present the system architecture of the proposed protocol in Section 4 and the design of our protocol in Section 5. We discuss the security analysis and performance of the proposed protocol in Section 6 and finally conclude in Section 7.

2 Related work

In this section, we present the related work which is subdivided into two sub-sections. We first present the evolution of vehicle communication architectures from the conventional VANET framework to vehicular cloud computing extensions along with related security mechanisms. Then, we present the existing work on billing schemes within the CC environment and VCC.

2.1 VANET architecture

VANET result as an extension of mobile ad hoc netwoks (MANETs) [12]. In VANETs, the main entities represent the vehicles, RSUs, and an over-viewer third party called Trusted Authority (TA) in charge of registration, certification, and revocation of all the entities within the VANET architecture [13]. Conventional VANETs avail two major communication means through the dedicated short-range communication (DSRC) as V2V and V2I communications [14]. A considerable number of applications were predicted to be achieved through the VANET architecture; however, the computational cost of the value-added applications in VANETs require huge computation capabilities which led to the mixture of VANETs and cloud computing [15].

Vehicular cloud was introduced by Olariu et al. for the first time [16]. An extension of their work suggested an autonomous vehicular cloud (AVC) architecture as a special case of VANET cloud [17]. Hussain et al. defined three

types of architectures which originated from the combination of VANETs and cloud computing [18]. *VANETs using cloud* is defined as vehicles equipped with smart devices and communicating with the cloud the same way as our mobile phones connect to different servers located in the cloud. *Vehicular cloud* refers to the full utilization of vehicle devices as computers to form mobile servers. In this architecture, one could use the vehicle OBU's to make his/her personal cloud. *Hybrid vehicle cloud* is a combination of the above architectures also referred as VCC. The feasibility of VCC was adopted by several researchers [19, 20], though security issues within the cloud computing are still an attractive on-going research whereby different secure protocols have been proposed [21]. In this work, we construct our protocol based on *VANETs using cloud* architecture.

2.2 Secure billing schemes

A billing transaction refers to the saving of the the movement logs in order to verify the billing operations. Billing transactions are part of electronic payment schemes. Time-based billing and content-based billing are the main billing approaches in cloud computing and depend on the type of required services. However, several CSPs seem to embrace content-based billing rather than time-based billing [22]. A considerable number of electronic payment schemes have been suggested in the literature. Among them are micro-payment-based schemes such as MiniPay and Netpay [23]. These e-payment systems allow the users of cloud-based applications to securely and efficiently perform payments. These schemes are built using one-way hash functions that generate chains of hash values. The cloud users will first release several hashes with the hash chain in order to perform billing transactions. On the basis of the micro-payment-based scheme, Pay-as-you-Browse [24] and XPay [22] fused the micro-payment concept into cloud-hosted services. Though those schemes have less billing latency, they do not support additional security features required for billing transactions in cloud-based services.

Within the vehicular environment, secure billing feature is core prerequisite for a full adoption of commercial-based services by the CSPs in VCC. Several billing mechanisms have been proposed for VANET applications [4, 7, 25, 26]. In [7], Yeh et al. proposed a local and proxy-based authentication and billing scheme to reduce the communication overhead. The protocol proposed an incentive-aware multi-hop forwarding for the vehicles within the VANET architecture. They adopted batch verification technique in their scheme to fulfill the security requirements and signature-based communications. However, the protocol does not satisfy access control property, thus cannot allow multiple services in a single package. In [4], Yeh et al. proposed a portable AAA framework which allow the vehicle users to enjoy CSP's services from the RSUs. They used signature-based and KP-ABE in the billing protocol to attain localized fine-grained access control and also employed E-coin to provide service authorization. However, the proposed protocol is built based on expensive pairing operations which might not be efficient due to voluminous sizes of various files.

3 Preliminaries

In this section, we present the basic properties of lightweight attribute-based encryption (lABE) based on Elliptic Curve Integrated Encryption Scheme (ECIES) and certificateless signature scheme which form the basic cryptographic primitives of the proposed protocol.

3.1 Lightweight ABE scheme

The lABE scheme of [10] based on elliptic curve cryptography consists of Setup, Encryption, Key-Generation, and Decryption algorithms.

3.1.1 lABE.Setup

Suppose that the attribute space of the system is defined as the universe of attributes $U = \{1, 2, \ldots, n\}$. Let G be an additive group with a prime order q and $P \in G$, where G consists of points on an elliptic curve and P is a generator of G. lABE.Setup() algorithm generates lABE parameters as follows:

1. Choose a random $s \in Z_q^*$ as the attribute master secret key and computes the corresponding public key $PK = s \cdot P$.
2. For each attribute $i \in U$, choose an attribute secret $t_i \in Z_q^*$ and compute the attribute public key $P_i = t_i \cdot P$.
3. Set $amk = \{s, t_1, \ldots, t_{|U|}\}$ and $labe.params = \{PK, P_1, \ldots, P_{|U|}\}$
4. Returns $\langle amk, labe.params \rangle$

3.1.2 lABE.Encrypt

Given a message m, an attribute set ω, and *labe.params*, lABE.Encrypt(m, ω, *labe.params*) outputs the cipertext CM as follows:

1. Choose $k \in Z_q^*$ and compute the key $K = k \cdot PK$.
2. Compute $C = Enc_K(m)$.
3. For each $i \in \omega$, compute $W_i = k \cdot P_i$, respectively.
4. Return the cipertext $CM = \langle \omega, C, \{W_i \mid i \in \omega\} \rangle$

3.1.3 lABE.KeyGen

For the given master secret amk and the access tree Γ, lABE.KeyGen(amk, Γ) algorithm generates secret shares of the decryption key for the encrypted message under the attribute set ω.

1. For the access tree Γ, assign index to each node other than root.
2. For each node, a polynomial $q_{node}(x)$ over Z_q^* is defined in top-down manner where each polynomial is of degree $d_{node} - 1$ and d_{node} is the threshold value of the node.
   - for the root, set $q_{root}(0) = s$.
   - for other nodes including leafs, set $q_{node}(0) = q_{parent}(index(node))$ where $index(node)$ is the index value of the node.
3. Let n be the number of leaves in Γ, for each leaf node $leaf_l$ $(1 \le l \le n)$, a secret share of the decryption key is computed as $D_{leaf_l} = q_{leaf_l}(0) \cdot t_i^{-1}$ where i is the attribute associated to $leaf_l$ and t_i is the random number for i chosen in lABE.Setup.
4. Return $D = \{D_{leaf_l} \mid leaf_l \in \Gamma\}$

3.1.4 lABE.Decrypt

The decryption algorithm lABE.Decrypt(CM, D, $labe.params$) decrypts the cipertext CM, if and only if the attributes set ω satisfies the access tree Γ, by using NodeKey(CM, D, $node$) for a node in the access tree recursively. In the lABE scheme [10], secret sharing based on Lagrange interpolation [Shamir] is used to reconstruct the decryption key.

1. For each leaf node to which an attribute i is associated, NodeKey(CM, D, $leaf_l$) is defined as follows:
   - if the associated attribute i to $leaf_l$ is not included in ω, then NodeKey(CM, D, $leaf_l$) = $\perp$.
   - otherwise,

$$\begin{aligned}\text{NodeKey}(CM, D, leaf_l) &= D_{leaf_l} \cdot W_i \\ &= q_{leaf_l}(0) \cdot t_i^{-1} \cdot k \cdot P_i \\ &= q_{leaf_l}(0) \cdot t_i^{-1} \cdot k \cdot t_i \cdot P \\ &= q_{leaf_l}(0) \cdot k \cdot P\end{aligned}$$

2. For a non-leaf node u, it calls NodeKey(CM, D, z) for all children z of the node u.
   - Let ω_u be an arbitrary d_u sized set of children nodes such that NodeKey(CM, D, z) $\neq \perp$. If no such set exist NodeKey(CM, D, u) returns $\perp$.
   - Otherwise, let $\Delta_{index(z),\omega'_u} = \prod_{j \in \omega'_u, j \neq index(z)} \frac{x-j}{i-j}$ be the Lagrange coefficient where $\omega'_u = \{index(z) \mid z \in \omega_u\}$,

$$\begin{aligned}\text{NodeKey}(CM, D, u) &= \sum_{z \in \omega_u} \Delta_{index(z),\omega'_u}(0) \\ &\quad \times \text{NodeKey}(CM, D, z) \\ &= \sum_{z \in \omega_u} \Delta_{index(z),\omega'_u}(0) \cdot q_z(0) \cdot k \cdot P \\ &= \sum_{z \in \omega_u} \Delta_{index(z),\omega'_u}(0) \\ &\quad \times q_{parent}(index(z)) \cdot k \cdot P \\ &= \sum_{z \in \omega_u} \Delta_{index(z),\omega'_u}(0) \\ &\quad \times q_u(index(z)) \cdot k \cdot P \\ &= q_u(0) \cdot k \cdot P\end{aligned}$$

3. Calculate the decryption key K = NodeKey(CM, D, $root$) = $q_{root}(0) \cdot k \cdot P = s \cdot k \cdot P$.
4. Return the decrypted message $m = Dec_K(C)$.

3.2 Certificateless signature scheme

The certificateless signature (CLS) scheme of [9] consists of the following algorithms.

- CLS.Setup() algorithm generates a master key and public system parameters as follows:
  - Choose an additive group G with a prime order q and a generator $P \in G$ defined on an elliptic curve.
  - Select master secret key $s \in Z_q^*$ and computes the master public key $P_{pub} = s \cdot P$.
  - Choose two cryptographic hash functions $H_1 : \{0,1\}^* \times G^2 \to Z_q^*$ and $H_2 : \{0,1\}^* \times G^3 \to Z_q^*$.
  - Set public system parameters $cls.params = \{G, q, P, P_{pub}, H_1, H_2\}$.
  - Return $\langle s, cls.params \rangle$
- CLS.SetSecret(id) outputs a secret value for the given identity id as follows:
  - Select randomly $x_{id} \in Z_q^*$ as a secret value and compute $P_{id} = x_{id} \cdot P$.
  - Return $S_1 = \langle x_{id}, P_{id} \rangle$
- CLS.PartialKey(x, id, P_{id}) generates a partial private and public key for the id as follows:
  - Choose a random $r_{id} \in Z_q^*$ and compute $R_{id} = r_{id} \cdot P$.
  - Compute $s_{id} = r_{id} + s \cdot H_1(id, R_{id}, P_{id}) \pmod q$.
  - Return $S_2 = \langle s_{id}, R_{id} \rangle$ as the partial private key.
- CLS.SetKey(S_1, S_2) sets $sk_{id} = \langle x_{id}, s_{id} \rangle$ and $pk_{id} = \langle P_{id}, R_{id} \rangle$ as the private key and public key for the entity of id, respectively.

- CLS.Sign(m, sk_{id}) generates the signature for a message m as follows:
  - Choose a random $l \in Z_q^*$ such that gcd($l+h$, q) = 1, where $h = H_2(m, R, P_{id}, R_{id})$ and $R = l \cdot P$.
  - Compute $r = (l+h)^{-1}(x_{id} + s_{id})$ (mod q).
  - Return the signature $\sigma = \langle r, R \rangle$.
- CLS.Verify(m, id, pk_{id}, σ) verifies the signature σ for the message m under the id as follows:
  - Compute $h_1 = H_1(id, R_{id}, P_{id})$ and $h_2 = H_2(m, R, id, P_{id}, R_{id})$.
  - Check if $r \cdot (R + h_2 \cdot P) \stackrel{?}{=} P_{id} + R_{id} + (h_1 \cdot P_{pub})$.

4 Proposed protocol

In this section, we first present the system architecture of the proposed protocol. Secondly, we present the security requirements of the proposed protocol, and lastly, we outline the main phases of the proposed protocol.

4.1 Architecture

We describe the communication entities within our protocol which are made of Trusted Authority (TA), Service Providers (SPs), Road Side Cloud (RSC), and vehicles which communicate through the OBU as shown in Fig. 1:

- TA: It is in charge of the registration of all entities (RSC, SPs, and vehicles) inside our system and issues cryptographic materials during the system initialization.
- RSC: RSCs are databases located along the roads and accessible by the vehicles. The RSCs store the service files (SFs) provided by the SPs. In that case, the vehicles can acquire the files through the RSCs. The vehicles get the electronic voucher from SPs through the RSCs. Due to the advancements of technology, we assume that RSCs are connected to an electricity power generator with enough computational capability.
- SPs: It is a server located in the cloud belonging to a cloud-based commercial service providers (CSPs). SPs offer a range of services, and one service package can incorporate several services such as mp3 audio, a map, or a short video clip. SPs send their service files to RSCs so that the vehicles can easily download them. However, in order to convince the vehicles of the services they need to be charged for, TA provides an electronic voucher with a given value which a vehicle has to satisfy in order to get the services. Moreover, the electronic voucher logs are sent to TA in non-rushing hours for accountability and non-repudiation of payment.
- Vehicles: Vehicles are equipped with OBUs which allow them to communicate with RSCs in order to require files from the SPs.

4.2 Security objectives

Our protocol should satisfy the following security requirements:

- Authentication and authorization: Each vehicle should be authenticated before it can receive a service file from SPs through the RSCs. Additionally, only

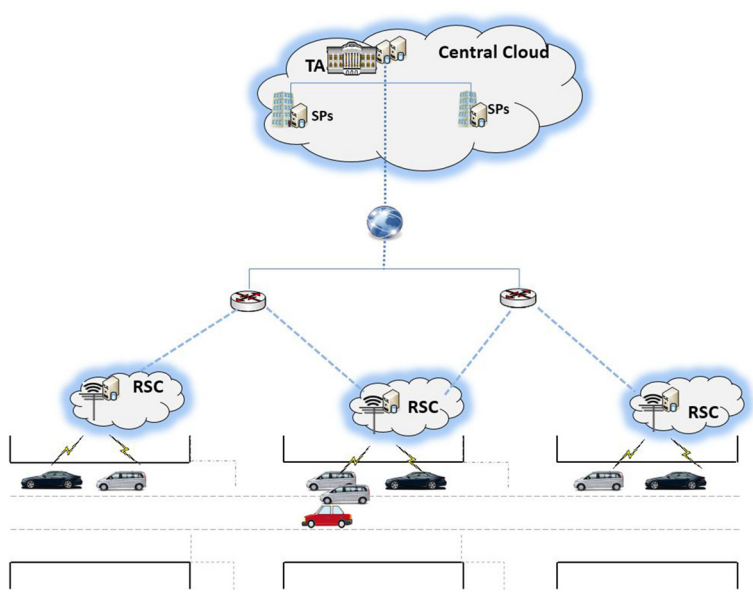

Fig. 1 System architecture

legitimate subscribers should get access to use SP's services.

- Identity privacy preservation: The real identity of a vehicle should be kept secret from other vehicles, RSC, and SPs.
- Fine-grained access control: Through fine-grained access control based on ABE, a vehicle should strictly be able to open a service corresponding to its access structure.
- Double-spending resistance: A vehicle should not over use its purchased electronic voucher to open additional files.
- Non-repudiation of payment: A vehicle should not deny the electronic voucher which it has used to open a given file. This would help in case of disputes over billing issues.
- Traceability: TA should be able to reveal the real identity of SPs and vehicles.

The proposed protocol consists of the following sub-protocols:

- System Setup: TA sets up its master secret key and its corresponding public key. Each vehicle provides its real identity, and TA generates the corresponding pseudo identity from which a partial private key is computed. SPs and RSCs also provide their real identities, and TA computes their partial private keys. Each SP generates the service files along with their access structures. SPs send securely the attribute master key of each file to TA. SPs also send the service files to RSC along with the corresponding secret keys which will be used for E-voucher generation through hash chain technique.
- E-voucher Generation: Periodically, a vehicle registers for SP's services. During the registration, the vehicle specifies the service files it wishes to acquire. Then, TA generates an electronic voucher (EV) which contains the secret shares corresponding to the access structure which the vehicle registered for. E-voucher will work as a transaction evidence for the purchased services.
- Service Purchase: RSCs periodically advertise the SP's services. v_i can request of any service among the advertised services. Depending on the E-voucher balance, RSC$_j$ first computes a new value of EV based on the requested services and sends the services to v_i along with the secret shares corresponding to the access structure of the requested service.

5 Proposed description

In this section, we design a secure billing protocol over attribute-based encryption in vehicular cloud computing. Table 1 shows the notations used in describing the proposed protocol.

Table 1 Notations and descriptions

Notation	Description
$\mathbb{G}$	Elliptic curve group with the same order q
$P \in \mathbb{G}$	A generator of $\mathbb{G}_1$
sk_{id}, pk_{id}	private, public key pair of an entity X
t_i	SP's master secret for each attribute i
amk	SP's attribute master key
T_i	Public key for each attribute $i \in U$
$alias_{v_i}$	v_i's pseudonym
U	Universe of attribute
Γ	Access tree
ω	Attribute set
D	Set of secret share $D_{leaf_i} in \Gamma$
SF_j	Service file
AT_j	Access tree corresponding to SF_j
$Enc_k(.)$	Symmetric encryption under key k

5.1 System setup

In setup phase, TA generates global system parameters and any other entities register to the TA as follows:

1. TA chooses an elliptic curve group $\mathbb{G}$ of order q and a generator $P \in \mathbb{G}$.
2. To generate master secret sk_{TA} and public key pk_{TA}, TA runs CLS.Setup() and sets $\langle sk_{TA}, cls.params \rangle \leftarrow$ CLS.Setup(), then publishes $cls.params$.
3. For registering each vehicle v_i, TA assigns a pseudonym $alias_{v_i}$ to each v_i.
4. Each RSC_j and SP_k registers to the TA and generate CLS private keys as follows:
   - RSC_j and SP_k generate $S_{1,RSC_j} \leftarrow$ CLS.SetSecret(RSC_j) and $S_{1,SP_k} \leftarrow$ CLS.SetSecret(SP_k), and requests partial private key to the TA, respectively.
   - TA issues $S_{2,RSC_j} \leftarrow$ CLS.PartialKey(sk_{TA}, RSC_j, P_{RSC_j}) and $S_{2,SP_k} \leftarrow$ CLS.PartiaKey(sk_{TA}, SP_k, P_{SP_k}) to each entity securely.
   - RSC_j and SP_k set $\langle sk_{RSC_j}, pk_{RSC_j} \rangle \leftarrow$ CLS.SetKey(S_{1,RSC_j}, S_{2,RSC_j}) and $\langle sk_{SP_k}, pk_{SP_k} \rangle \leftarrow$ CLS.SetKey(S_{1,SP_k}, S_{2,SP_k}), respectively.
5. Similarly, each v_i generates $S_{1,v_i} \leftarrow$ CLS.SetSecret($alias_i$), TA issues $S_{2,v_i} \leftarrow$ CLS.PartKeyExtract(sk_{TA}, $alias_i$, P_{v_i}), then v_i sets $\langle sk_{v_i}, pk_{v_i} \rangle \leftarrow$ CLS.SetKey(S_{1,v_i}, S_{2,v_i}).

In addition, each service provider SP prepares service files served under a given access structure as follows:

1. SP decides the universe of attributes $U = \{1, \ldots, N\}$, generates ABE parameters as $\langle amk, labe.params \rangle \leftarrow$

lABE.Setup(), and publishes *labe.params* to the system.
2. Let l be the number of service files. SP decides access tree AT_j and prepares encrypted service file SF_j $(1 \le j \le l)$ under a given attribute set ω_j as $SF_j \leftarrow$ lABE.Encrypt($file_j$, ω_j, *labe.params*).
3. SP picks a secret key α to be shared with TA and RSCs and provides $\langle amk, \alpha, \{SF_j \mid 1 \le j \le l\}, \{AT_j \mid 1 \le j \le l\}\rangle$ to RSCs and α to the TA securely.

5.2 E-voucher generation

Periodically, the vehicles request an electronic voucher (EV) which permits to enjoy the services offered by any SPs through the RSCs. To acquire an EV from TA, v_i performs the following:

1. v_i composes an electronic voucher request message $EVR = \{alias_i, K, ts\}$ where ts is the time stamp and K is a secret key to be used later.
2. v_i sends $C_1 = Enc_{PK_{TA}}\{EVR, pk_{v_i}, \delta_i\}$ to the TA, where δ is the signature for the EVR set as δ_i = CLS.Sign(EVR, sk_{v_i}).
3. Upon receiving the message C_1, TA first decrypts C_1 using its private key, then verifies the signature as CLS.Verify(EVR, $alias_i$, pk_{v_i}, δ). If it holds, TA generates E-voucher (EV) as follows:
   - Let d be the maximum credits for v_i to purchase service files. Compute $hk_d = hash^d(\alpha)$ where $hash^d()$ represents the d-th hash chain, i.e., $hk_d = hash(hash^{d-1}(\alpha)) = hash(hash(\ldots(hash(\alpha))\ldots))$.
   - Generate $EV = \langle alias_i, exp, d, MAC_{hk_d}(alias_i|exp|d)\rangle$ where exp is the expiration date.
4. TA sends $C_1 = Enc_K(EV)$ to v_i. Then, v_i can recover EV by decrypting the C_1 under the shared secret key K.

5.3 Service purchase

A vehicle after getting the EV can enjoy file services from any chosen RSC_j. RSC_j advertises periodically the services along with their denomination value $\hat{d}$.

1. From service file lists advertised, v_i chooses a list for SF'_j and composes a service request message $mf = \{SF'_j, EV, alias_i, pk_{v_i}, K', ts\}$ where K' is a secret key to be shared with RSC_j, and sets $\delta_j \leftarrow$ CLS.Sign(mf, sk_{v_i}). v_i sends $C_2 = Enc_{PK_{RSC_j}}(mf, \delta_i)$ to RSC_j.
2. RSC_j decrypts the C_2 and verifies the signature δ_i as CLS.Verify(mf, $alias_i$, pk_{v_i}, δ_i). If it holds and the balance $d \ge \hat{d}$,
   - Compute $hk' = hash^d(\alpha)$ and check if $MAC_{hk'}(alias_i|exp|d) \stackrel{?}{=} MAC_{hk_d}(alias_i|exp|d)$.
   - Generate a new E-voucher $EV = \langle alias_i, exp, d', MAC_{hk_{d'}}(alias_i|exp|d')\rangle$ where $d' = d - \hat{d}$ and $hk_{d'} = hash^{d'}(\alpha)$.
   - Set $\bar{D} \leftarrow$ lABE.KeyGen(amk, AT_j).
   - Generate $C_3 = Enc_{K'}(EV|\bar{D})$.
3. RSC_j provides $\langle SF_j, C_3\rangle$ to v_i.
4. v_i decrypts C_3 to recover EV and $\bar{D}$, and runs lABE.Decrypt(SF_j, $\bar{D}$, *labe.params*) to get the original file of SF_j.

6 Performance

In this section, we evaluate the performance of the proposed protocol based on the security analysis, the computation delay, the transmission cost, the communication overhead, and simulation.

6.1 Security

According to the aforementioned security objectives, we analyze and discuss the security of the proposed protocol.

- Authentication: The authentication of each v_i requesting a service file is guaranteed by the certificateless signature scheme on message $\mathrm{EVR} = \{\mathrm{alias}_i, K, \mathrm{ts}\}$ with $C_1 = \mathrm{Enc}_{PK_{\mathrm{TA}}}\{\mathrm{EVR}, pk_{v_i}, \delta_i\}$. No adversary can forge a valid signature due to the hardness of DL problem. Otherwise, the verifier could check the validity of the message EVR by running CLS.Verify(m, id, pk_{id}, σ) to check if $r \cdot (R + h_2 \cdot P) \stackrel{?}{=} P_{id} + R_{id} + (h_1 \cdot P_{\mathrm{pub}})$. Thus, the proposed protocol provides message authentication.
- Authorization: Any vehicle has to be acquire a electronic voucher before it can use SP's service. v_i sends $C_1 = \mathrm{Enc}_{PK_{\mathrm{TA}}}\{EVR, pk_{v_i}, \delta_i\}$ to the TA to request electronic voucher. After a successful verification, TA sends $C_1 = \mathrm{Enc}_K(\mathrm{EV})$ where $\mathrm{EV} = \langle \mathrm{alias}_i, \mathrm{exp}, d, \mathrm{MAC}_{hk_d}(\mathrm{alias}_i|\mathrm{exp}|d)\rangle$ as v_i's EV which allows the v_i to access SP's services.
- Identity privacy preservation: An attacker cannot obtain a real identity of a vehicle throughout our proposed protocol. During the registration phase of the vehicle by TA, each vehicle v_i is given a pseudo-identity alias_{v_i}. Even though the attacker captures the EVR request message $\mathrm{EVR} = \{\mathrm{alias}_i, K, \mathrm{ts}\}$, the only plain identity of v_i available is its pseudo-identity alias_{v_i}. In the remaining protocol's operations, the only available information of v_i is its pseudo-identity alias_{v_i}. We conclude that the proposed protocol guarantees identity privacy preservation.
- Fine-grained access control: In our protocol, the service file $C_3 = \mathrm{Enc}_{K'}(\mathrm{EV}|\bar{D})$ which is sent to v_i is

first encrypted under a shared symmetric key K'. Moreover, unless a vehicle possesses the required secret shares $D_{\text{leaf}_l} = q_{\text{leaf}_l}(0) \cdot t_i^{-1}$ from AT_j, the vehicle cannot reconstruct the root node R to be able to get the secret $q_{\text{root}}(0) \cdot k \cdot P = s \cdot k \cdot P$. During the decryption phase based on the root or child node, unless v_i possesses the required secret shares, the decryption process output $\perp$. Thus, even the vehicles which share a number of attributes cannot collude together to recover the secret which allow the decryption of the service file.

- Double-spending resistance: A vehicle cannot over use its access structure to enjoy beyond what its electronic voucher can allow. Before RSC_j sends a service file to v_i, a new value of E-voucher $EV = \langle \text{alias}_i, \exp, d', \text{MAC}_{hk_{d'}}(\text{alias}_i \| \exp \| d') \rangle$ where $d' = d - \hat{d}$ and $hk_{d'} = \text{hash}^{d'}(\alpha)$ is generated. Thus, we confirm that the proposed protocol is resistant to double spending of E-voucher.
- Non-repudiation for payment: A vehicle cannot deny of using the services because a log message is attached to ensure that the vehicle transactions are saved. Moreover, though the RSC does not control the electronic spending of v_i, it keeps records of the number of turns E-voucher has been regenerated.
- Traceability: Even though it is hard for an attacker to know the real identity of a vehicle, TA has the capability of revealing the vehicle's real identity in case of disputes. TA makes a search to find which real identity corresponds to any given or reported alias_{v_i}. We conclude that the proposed protocol satisfies the traceability property.

6.2 Computational delay

In this section, we evaluate the performance of our protocol in terms of computational delay. Note that we ignore the time complexity involved in setup because it is assumed to be done offline and occasionally. We mainly consider the operations that dominate the speed of signature generation and signature verification such as one point multiplication, one pairing operation over an elliptic curve, asymmetric encryption, asymmetric decryption, symmetric encryption, signature generation, and signature verification. We neglect all other small operations such as additions. We consider the implementation parameters in [27, 28] with embedding degree 6, with $\{\mathbb{G}, q\}$ represented by 161 and 160 bits, respectively. The implementation was executed on a *3.5-GHz, core i-5, 16GB RAM* desktop computer. The obtained results are shown in Table 2.

As described in Section 3.2, v_i sends a request for SP's file by computing $h = H_2(m, R, P_{id}, R_{id})$, $R = l \cdot P$, and $r = (l + h)^{-1}(x_{id} + s_{id}) \pmod q$ which equals to $2T_{\text{mul}}$.

Table 2 Measurement of cryptographic operations

Notation	Operations	Time (ms)
T_{pair}	Bilinear pairing	2.82
T_{mul}	Point scalar multiplication	0.78
$T_{\text{as-enc}}$	Asymmetric encryption	1.17
$T_{\text{as-dec}}$	Asymmetric decryption	0.61
$T_{s-\text{enc}}$	Symmetric encryption	0.51
$T_{s-\text{dec}}$	Symmetric decryption	0.55
T_h	Execution time of a general hash function	0.0001

RCS_j computes $W_i = k \cdot P_i$ and $q_{\text{leaf}_l}(0) \cdot t_i^{-1}$, which equals to $(I + 1)T_{\text{mul}}$ where I is the number of attributes for the requested files. During the service purchase phase in Section 5.3, to recover the main secret based on the secret shares, v_i computes $q_{\text{leaf}_l}(0) \cdot k \cdot P$ which equals to dT_{mul} where d is the number of nodes in the access structure. The E-voucher verification and regeneration is similar for both v_i and RSC_j which equals to T_h. If we set the number of attributes ($I = 5$) and the number of leaf node ($d = 5$), then the computational cost equals to 9.36 ms for the proposed protocol and 40.2 ms for PBS [4]. The overall computational cost is illustrated in Table 3.

6.3 Number of transmission RSCs

Taking into consideration the computational delay on v_i and RSC_j, we investigated the number of transmission RSCs that are needed to send a file (based on the size) which will influence the predictive handoff protocols to be adopted [29]. We consider the following settings to simulate a practical scenario [30]:

- The average velocity of a vehicle (denoted v) ranges from 10 to 40 m/s (36–144 km/hr).
- The valid coverage range of an RSC (denoted C_{RSU}) is 300 to 600 m.
- The data rate α of a service channel can be up to 54 Mbps,
- The vehicle density (denoted de) of an RSC on two-lane two-way streets varies from 50 to 150 vehicles.
- The service files size (denoted s) is assumed to weight from 0.5 to 20 Mbytes. The files may contain maps, mp3, mp4, or videos.

Table 3 Computational cost [4] of and proposed protocol

Scheme phase	PBS: [4]	Proposed
Access control on v_i	$(d+2)T_{\text{pair}} + 3T_{\text{mul}}$	$(1+d)T_{\text{mul}}$
Access control on RSC_j	$(1+l)T_{\text{mul}}$	$(1+l)T_{\text{mul}}$
Billing on v_i	$T_{\text{pair}} + 3T_{\text{mul}}$	T_h
Billing on RSC_j	$T_{\text{pair}} + 7T_{\text{mul}}$	$3T_h$

(d number of leaf node, l set of attribute)

Let η be the probability that each vehicle issues a service request, and let X be a random variable representing the number of requesting vehicles among a total of de vehicles. As a result, X follows a binomial distribution $\mathbb{B}(de, \eta)$, and we have:

$$P\{X = x\} = \binom{de}{x} \eta^x (1-\eta)^{de-x}, x = 0, 1, 2, \ldots, de$$

and an expectation value of

$$E(X) = \sum_{x=o}^{de} \binom{de}{x} \eta^x (1-\eta)^{de-x} = de \cdot \eta$$

The RSC verifying the service requests will estimate how many RSCs are needed (denoted N_{RSC}) to transmit the requested file. We measure how much time (denoted T_{Req}) is required for a service file as $T_{\text{Req}} = \frac{s \times 1024 \times 1024 \times 8 \times E(X)}{\alpha \times 54 \times 1024 \times 1024} = \frac{s \times de \times \eta \times 8}{\alpha \times 54}$.

We then compute $N_{\text{RSC}} = \frac{(T_{v_i} + T_{\text{RSC}}) \times v \times T_{\text{Req}}}{C_{RSC}}$ where T_{v_i} and T_{RSC} represent the computational overhead of v_i and RSC_j, respectively, as shown in Table 3.

We further compare our protocol with existing scheme [4] which considers privacy, access control, and billing features. As noted in [4], PBS protocol requires 10 RSCs to complete forwarding a service of 20 Mbytes. However, in the same circumstances, the proposed protocol requires only 2 RSCs as shown in Figs. 2 and 3, respectively.

6.4 Communication overhead

In this section, we analyze the communication overhead of the proposed scheme. The sizes of the elements are $64 \times 2 = 128$ bytes for pairing based operations and $20 \times 2 = 40$ bytes for ECC-based elements [31]. The sizes of the general hash function's output and time stamp are 20 and 4 bytes, respectively. Compared to [4], the proposed protocol offers lower communication overhead since PBS [4] is build based on expensive pairing operations. The total message size is 70 bytes for the proposed protocol in which we consider that the access structure Γ contains 5 nodes (I = 5).

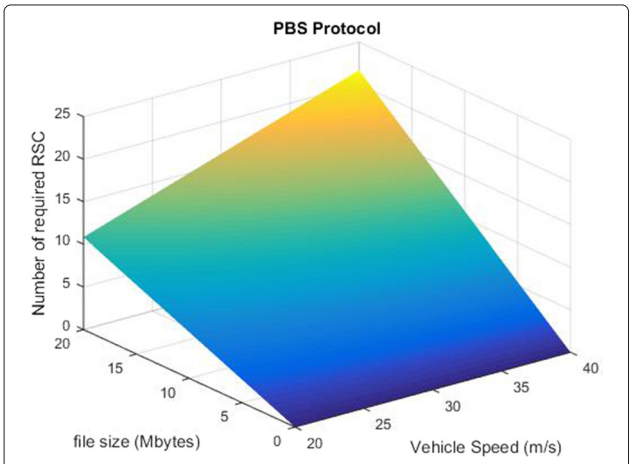

Fig. 2 Required number of RSCs for PBS [4]

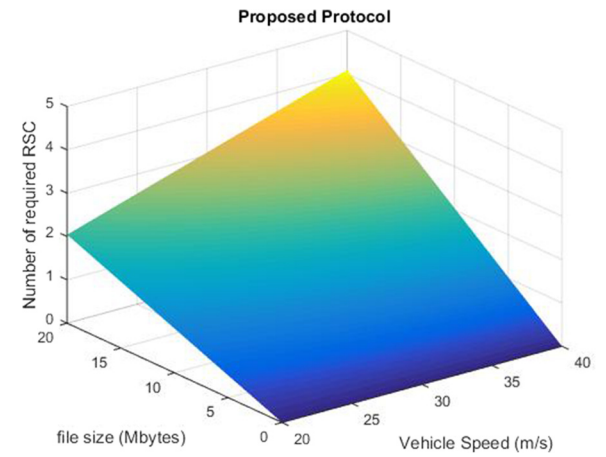

Fig. 3 Required number of RSCs for proposed protocol

6.5 Simulation

Additionally, we evaluate the performance of the proposed protocol through simulation. We used VANET-SIM simulator for vehicle mobility coupled with ns-3 simulator for network simulation [32]. We further set our scenario based on the IEEE 802.11p VANET platform range which is 2.56 Mbps in highly populated street such as highways that use DSRC, to a maximum transmission range of 6 Mbps. We consider a city scenario with a map downloaded from OpenStreepMap database [33] with a random speed for the vehicles ranging from 10 to 40 m/s (36–144 km/hr). The details of the simulation are shown in Table 4. The average overall delay (denoted Av_D) is defined as:

$$Av_D = \frac{1}{N_{\text{Req}V}} \sum_{i=1}^{N_{\text{Req}V}} \frac{1}{N_{\text{RSC}}} \sum_{j=1}^{N_{\text{RSC}}} \left(T_{v_i}^{\text{Send}} - T_{v_i}^{\text{Rec}v} \right)$$

where $N_{\text{Req}V}$ is the number of vehicles requesting for SP's services and N_{RSC} is the number of roadside clouds. $T_{v_i}^{\text{Send}}$ is the time at which v_i sends a request to RSC_j and $T_{v_i}^{\text{Rec}v}$ is the time at which v_i receives a response from RSC_j. The average loss ratio denoted as Av_{Loss} is defined as follows:

$$Av_{\text{Loss}} = \frac{1}{N_{\text{Req}V}} \sum_{i=1}^{N_{\text{Req}V}} \frac{1}{N_{\text{RSC}}} \sum_{j=1}^{N_{\text{RSC}}} \left(\frac{NS_{v_i}^{\text{Rec}v} + NR_{RSC_j}^{\text{Rec}v}}{NR_{v_i}^{\text{Send}} + NS_{\text{RSC}_j}^{\text{Send}}} \right)$$

where $NS_{v_i}^{\text{Rec}v}$ is the number of service files received by v_i from RSC_j, and $NR_{\text{RSC}_j}^{\text{Rec}v}$ is the number of requests received by RSC_j. $NR_{v_i}^{\text{Send}}$ is the number of requests sent by v_i to

Table 4 Simulation settings

Tools/parameter	Value/specification
Mobility generation tool	VANETSIM 2.02
Network simulation tool	ns-3
Trans range	6 MBps
Number -of -vehicle	100
Simulation time	200 min
Wireless protocol	802.11a
Departure interval	200 min
RSU radius	600 m
Mobility model	shortest path
Message size for [4]	109 bytes
Message size for proposed	70 bytes

RSC_j and $NS^{\mathrm{Send}}_{\mathrm{RSC}_j}$ is the number of service files sent by RSC_j to v_i.

We investigate the effect of the number of vehicles on the average delay. As described in [4], we consider 100 vehicles with a probability of launching a SP's service request equals to 0.5 ($\eta = 0.5$). The number of attributes of each access structure AT_j is set to 5 ($I = 5$). The average delay based on the vehicle's density is around 0.39 for 100 vehicles for PBS [4] whereas it is 0.21 for the proposed protocol as depicted in Fig. 4. This occurs due to the time which v_i has to wait before it receives an SP's service which depends on the verification and regeneration of E-voucher as shown in Table 3. In Fig. 5, the proposed protocol performs better when we investigate the average delay based on the speed of vehicles. For a normal speed ranging from 10 to 35 m/s, the average delay is 0.35 for the PBS [4] and 0.11 for the proposed protocol.

When we study the impact of vehicle's density on the average loss ratio, the proposed protocol performs better with 0.18 for 100 vehicles compared to PBS [4] with 0.25 for the same settings as shown in Fig. 6. We further investigate the impact of vehicle's moving speed on the average loss ratio. As shown in Fig. 7, the loss ratio is 0.19 for vehicles moving from 10 to 30 m/s in PBS protocol [4] whereas it is 0.09 for the proposed protocol in the same conditions.

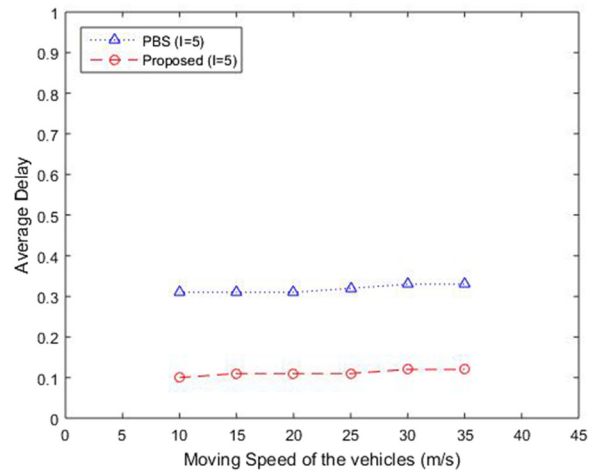

Fig. 5 Impact of vehicle speed on average delay

7 Conclusions

In this paper, we proposed a secure billing protocol over attribute-based encryption in vehicular cloud computing. We used pseudonym techniques to achieve the identity privacy of the vehicles and their requested services. Certificateless signature scheme is applied to assure the authentication of legitimate vehicles which can enjoy the provided services. We adopted ABE to guarantee rigorous access control based on the purchased access structure.

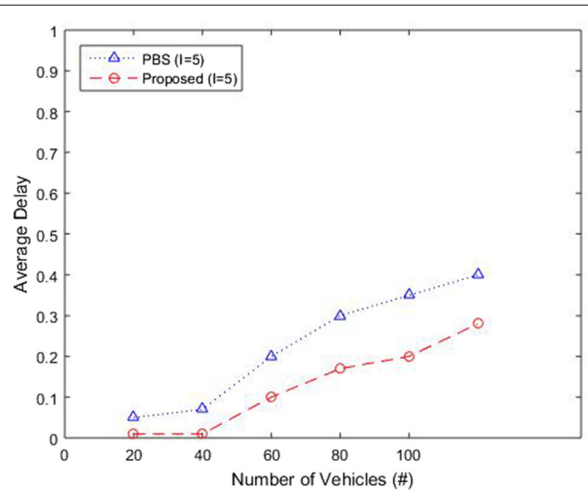

Fig. 4 Impact of vehicle density on average delay

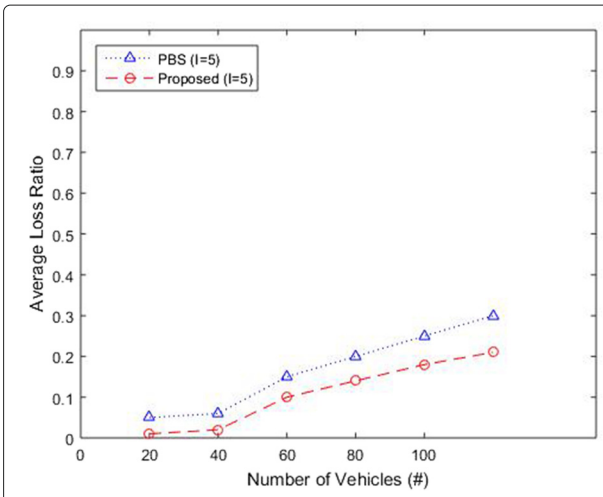

Fig. 6 Impact of vehicle density on average loss ratio

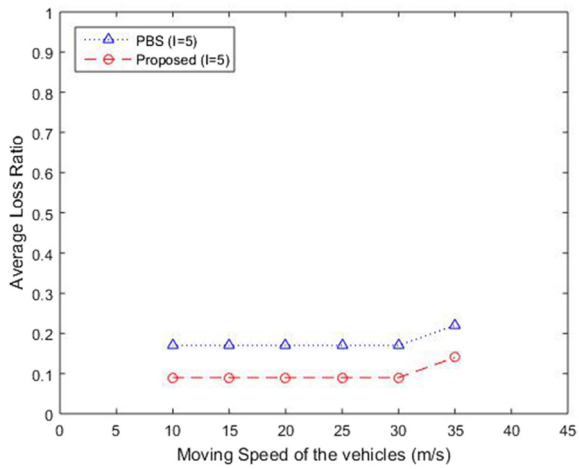

Fig. 7 Impact of vehicle speed on average loss ratio

We used hash chain technique to provide authorization property through electronic voucher which a vehicle has to possess before enjoying any giving service. Security analysis and experimental results based on transmission overhead, average delay, and average loss ratio are provided. Compared to relevant existing work under the same scenario, the proposed protocol achieves efficient billing features with less computational overhead for vehicular cloud computing.

In the future, we will continue to investigate on revocation technique based on the updating of the access structure rather than the vehicle's identity-based revocation.

Acknowledgements
This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (No. NRF-2014R1A2A1A11052981).

Competing interests
The authors declare that they have no competing interests.

Received: 1 April 2016 Accepted: 9 August 2016
Published online: 24 August 2016

References

1. C-T Li, M-S Hwang, Y-P Chu, A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. Comput. Commun. **31**(12), 2803–2814 (2008)
2. M Whaiduzzaman, M Sookhak, A Gani, R Buyya, A survey on vehicular cloud computing. J. Netw. Comput. Appl. **40**, 325–344 (2014)
3. G Yan, D Wen, S Olariu, MC Weigle, Security challenges in vehicular cloud computing. Intell. Transportation Syst. IEEE Trans. **14**(1), 284–294 (2013)
4. L-Y Yeh, J-L Huang, Pbs: a portable billing scheme with fine-grained access control for service-oriented vehicular networks. Mobile Comput. IEEE Trans. **13**(11), 2606–2619 (2014)
5. L-Y Yeh, Y-C Chen, J-L Huang, Abacs: an attribute-based access control system for emergency services over vehicular ad hoc networks. Selected Areas Commun. IEEE J. **29**(3), 630–643 (2011)
6. L Nkenyereye, BA Tama, Y Park, KH Rhee, A fine-grained privacy preserving protocol over attribute based access control for vanets. J. Wireless Mobile Netw. Ubiquitous Comput. Dependable Appl. **6**(2), 98–112 (2015)
7. L-Y Yeh, Y-C Lin, A proxy-based authentication and billing scheme with incentive-aware multihop forwarding for vehicular networks. Intell. Transportation Syst. IEEE Trans. **15**(4), 1607–1621 (2014)
8. W Cho, Y Park, C Sur, KH Rhee, An improved privacy-preserving navigation protocol in vanets. J. Wireless Mobile Netw. Ubiquitous Comput. Dependable Appl. **4**(4), 80–92 (2013)
9. D He, J Chen, R Zhang, An efficient and provably-secure certificateless signature scheme without bilinear pairings. Int. J. Commun. Syst. **25**(11), 1432–1442 (2012)
10. X Yao, Z Chen, Y Tian, A lightweight attribute-based encryption scheme for the internet of things. Future Gen. Comput. Syst. **49**, 104–112 (2015)
11. Y Liu, L Hu, H Liu, Using an efficient hash chain and delaying function to improve an e-lottery scheme. Int. J. Comput. Math. **84**(7), 967–970 (2007)
12. M Altayeb, I Mahgoub, A survey of vehicular ad hoc networks routing protocols. Int. J. Innov. Appl. Stud. **3**(3), 829–846 (2013)
13. SA Mohammad, A Rasheed, A Qayyum, in *Communication Technologies for Vehicles*. VANET architectures and protocol stacks: a survey (Springer, 2011), pp. 95–105. http://link.springer.com/chapter/10.1007%2F978-3-642-19786-4_9
14. JB Kenney, Dedicated short-range communications (dsrc) standards in the united states. Proc. IEEE. **99**(7), 1162–1182 (2011)
15. R Yu, Y Zhang, S Gjessing, W Xia, K Yang, Toward cloud-based vehicular networks with efficient resource management. Netw. IEEE. **27**(5), 48–55 (2013)
16. S Olariu, I Khalil, M Abuelela, Taking VANET to the clouds. Int. J. Pervasive Comput. Commun. **7**(1), 7–21 (2011)
17. M Eltoweissy, S Olariu, M Younis, in *Ad Hoc Networks*. Towards autonomous vehicular clouds (Springer, 2010), pp. 1–16. http://link.springer.com/chapter/10.1007/978-3-642-17994-5_1
18. R Hussain, Cooperation-aware vanet clouds: providing secure cloud services to vehicular ad hoc networks. J. Inform. Process. Syst. **10**(1), 103–118 (2014)
19. E Lee, E-K Lee, M Gerla, SY Oh, Vehicular cloud networking: architecture and design principles. Commun. Mag. IEEE. **52**(2), 148–155 (2014)
20. S Olariu, T Hristov, G Yan, in *Mobile ad hoc networking: cutting edge directions. 2nd ed.* The next paradigm shift: from vehicular networks to vehicular clouds (John Wiley & Sons, Inc., Hoboken, NJ, USA, 2013)
21. JK Lee, YS Jeong, JH Park, s-itsf: a service based intelligent transportation system framework for smart accident management. Human-centric Comput. Inform. Sci. **5**(1), 1–9 (2015)
22. Y Chen, R Sion, B Carbunar, in *Proceedings of the 8th ACM Workshop on Privacy in the Electronic Society*. Xpay: practical anonymous payments for tor routing and other networked services (ACM, 2009), pp. 41–50. http://dl.acm.org/citation.cfm?id=1655195
23. A Herzberg, H Yochai, Minipay: charging per click on the web. Comput. Netw. ISDN Syst. **29**(8), 939–951 (1997)
24. GO Karame, A Francillon, S Čapkun, in *Proceedings of the 20th International Conference on World Wide Web*. Pay as you browse: microcomputations as micropayments in web-based services (ACM, 2011), pp. 307–316. http://dl.acm.org/citation.cfm?id=1963451
25. H Zhu, X Lin, R Lu, P-H Ho, X Shen, Slab: A secure localized authentication and billing scheme for wireless mesh networks. Wireless Commun. IEEE Trans. **7**(10), 3858–3868 (2008)
26. H-Y Lee, Y-B Lin, et al., Credit pre-reservation mechanism for umts prepaid service. IEEE Trans. Wireless Commun. **9**(6), 1867–1873 (2010)
27. R Lu, X Lin, H Zhu, P-H Ho, X Shen, A novel anonymous mutual authentication protocol with provable link-layer location privacy. Vehic. Technol. IEEE Trans. **58**(3), 1454–1466 (2009)
28. A Miyaji, M Nakabayashi, S Takano, New explicit conditions of elliptic curve traces for fr-reduction. IEICE Trans. Fundamentals Electron. Commun. Comput. Sci. **84**(5), 1234–1243 (2001)
29. L Zhang, N Seta, H Miyajima, H Hayashi, in *Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*. Fast authentication based on heuristic movement prediction for seamless handover in wireless access environment (IEEE, 2007), pp. 2889–2893. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4224780&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4224780
30. Y Qian, K Lu, N Moayeri, in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*. A secure vanet mac protocol for dsrc applications (IEEE, 2008), pp. 1–5. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4698151&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4698151

31. D He, S Zeadally, B Xu, X Huang, An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. Inform. Forensics Secur. IEEE Trans. **10**(12), 2681–2691 (2015)
32. A Festag, P Papadimitratos, T Tielert, Design and performance of secure geocast for vehicular communication. Vehic. Technol. IEEE Trans. **59**(5), 2456–2471 (2010)
33. M Haklay, P Weber, Openstreetmap: user-generated street maps. Pervasive Comput. IEEE. **7**(4), 12–18 (2008)

Submit your manuscript to a SpringerOpen journal and benefit from:

- ► Convenient online submission
- ► Rigorous peer review
- ► Immediate publication on acceptance
- ► Open access: articles freely available online
- ► High visibility within the field
- ► Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com