A Fine-Grained Privacy Preserving Protocol over Attribute Based Access Control for VANETs

Lewis Nkenyereye, Bayu Adhi Tama, Youngho Park, and Kyung Hyune Rhee*
IT Convergence and Application Engineering, Pukyong National University
599-1 Daeyeon 3-Dong Namgu, Busan 608-737, Republic of Korea
{nkenyele, bayuat, pyhoya, khrhee}@pknu.ac.kr

Abstract

Vehicle safety related applications which are drawing increasing attention in public have attracted extensive research both in academic and industry areas. However, it is assumed that one service is offered by one provider, thus forcing vehicle drivers to subscribe to several service providers within limited computation capabilities. In this paper, we present a fine-grained privacy preserving protocol over attribute access control for VANETs which allows a service provider to offer a range of safety related services to vehicle drivers. The vehicles which have appropriate service attributes are authorized to access the requested services. In order for a vehicle to access to the authorized services, we propose a fined-grained access control mechanism based on linear secret sharing scheme. We consider the concept of an ID-based signature, an attribute based encryption (ABE) and a linear secret sharing scheme (LSSS) as our building blocks.

Keywords: vehicular ad hoc networks (VANETs), ID-based signature, attribute based encryption, fined grained access control.

1 Introduction

Initially, vehicular ad hoc network (VANETs) is described as a set of mobile hosts equipped with wireless communication devices called on board unit (OBU) and road side units (RSUs) where both vehicle to vehicle communication (V2V) and vehicle to infrastructure (V2I) communication are possible [1]. The vehicles and RSUs can communicate using the dedicated short range communications (DSRC) standardized by the IEEE [2]. Road safety applications are predicted to offer a wide range of services such as Computing as Service (CompaaS), Storage as a Service (STaaS), Network as a Service (NaaS), Cooperation as a Service (CaaS), Entertainment as a Service (ENaaS), Information as Service (INaaS) and Traffic-Information as Service (TIaaS) [3].

TIaaS includes the Dynamic Route Information Panels (DRIPs) service which give information about congestion on certain road segments and, at the individual vehicle level, TIaaS also offers navigation systems which give information about the route to a particular destination. Some of the services can be offered by a service provider after examining their combination acceptability. For example, a driver can request for a congestion prediction service which is in TIaaS, then after checking the congestion duration, the driver would ask for an mp3 music download which is within ENaaS, thus a provider which could offer multiple services in VANETs would be needed. However, current assumptions for VANETs researches assume that every service requires a credential or a service is offered by one provider.

Yeh *et al*. [4] proposed an attribute based access control system to provide emergency services over VANETs. In this protocol, the identity of the vehicle is made by a set of attribute which requires attribute based encryption/decryption for authenticating a vehicle before accessing the emergency service.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 6, number: 2, pp. 98-112
*Corresponding author: Tel: +82-51-629-6247, Fax: +82-51-626-4887, Web: http://www.lisia21.net/

Furthermore, a trusted authority (TA) sends an emergency message which is also encrypted under the set of attribute, thus attribute based encryption is done twice during a single phase which requires excessive computational cost. In this paper, we propose a fine-grained privacy-preserving protocol based on attribute access control for VANETs that tackles the problems of [4]. We use anonymous certificates computed over vehicle pseudo identities to provide authentication of vehicle during the credential request phase. We make use of a linear secret sharing scheme, an attribute based access control,an attribute based encryption [5] and an ID-based signature [6] as our building blocks.

1.1 Related Work

VANETs which is a component of Intelligent Transportation System (ITS) is primary designed to offer several services to vehicle drivers for a better driving environment. Several researches have been done to address potential security and privacy issues in VANETs [7] [8] [9] [10] which are reported as the main hindrance of full adoption of VANETs. VANETs services such as navigation services which allow a driver to find the best route to his destination have received much attention for the last years. Chim *et al*. [11] proposed a VANET-based secure navigation protocol which takes advantages of anonymous credentials to provide secure navigation services to drivers. The protocol searches for a route with minimum traveling delay using the real-time information of the road condition. As pointed out by Cho *et al*. [12], the utilization of master secret in [11] necessitates an additional tamper proof for each vehicle. In [12], authors proposed an improved navigation protocol by removing the system master secret distribution and update procedure for anonymous credential gaining . However, these protocols assume that a vehicle acquire a service credential to access a navigation service, and any other service would require at least its proper credential or even a different service provider. Other researches addressed multi-services in VANETs [13] [14] [15], but their schemes are constructed based on the authentication, authorization and accounting (AAA) architecture which is different from the VANETs architecture. In this paper, we propose a protocol which offers road safety multiservice in VANETs using a single credential with fine-grained access control mechanism. In [4], the authors proposed an attribute based access control system over VANETs. Built on emergency service scenario, their scheme needs an excessive computational cost due to vehicle identity which is made over a set of attribute. In order to choose the legitimate vehicle, a trusted authority verifies if the set of attribute of a vehicle satisfies the access structure of an emergency message to be sent at later stage. To alleviate the computational cost of [4], we propose a fined-grained privacy preserving protocol over attribute based access control for VANETs which offers multiple road safety services in VANETs.

1.2 Our Contribution

In this paper, we propose a fine-grained privacy preserving protocol over attribute based access control for VANETs which insures simultaneously the multiple compatible services with a single credential by a same service provider. We make the following contributions:

- We present an application model for a fine-grained privacy preserving protocol over attribute based access control for VANETs which allows vehicle drivers to access multiple road safety services within a single credential, then define the security requirements for our proposed protocol.
- We use an access structure which is based on attribute based access control coupled with linear secret sharing scheme to enforce fine-grained access control to better provide multiple services in VANETs for vehicle drivers.
- We construct a fine-grained privacy preserving protocol over attribute based access control for VANETs based on anonymous certificate for vehicle authorization. We make use of ID-based

signature but we exchange vehicle identities by their pseudonyms in order to provide privacy to vehicles. Our protocol makes use of attribute based encryptions for road safety services issuance.

- We provide the security analysis of the proposed protocol in terms of aforementioned security objectives. Additionally we evaluate the performance of our protocol through the simulations and confirm the efficiency of our protocol compared with [4].

The remainder of the paper is organized as follows. We first present the cryptographic primitives for constructing the proposed protocol in section 2. We present the system architecture in section 3 and the design of the proposed protocol in section 4. We discuss security and performance of the proposed protocol in section 5 and finally conclude in section 6.

2 Preliminaries

The preliminaries related to the proposed protocol include linear secret sharing scheme (LSSS), bilinear mapping, ID-based digital signature and attribute based encryption are presented in this section.

2.1 Linear Secret Sharing Scheme (LSSS)

An access control system represents a collection of components and methods that determine the correct admission to activities by legitimate users based upon preconfigured access permissions and privileges outlined in the access security policy [16]. The fundamental goal of any access control system is restricting a user to exactly what she/he should be able to do and protect information from unauthorized access. There is a wide variety of methods, models, technologies and administrative capabilities used to propose and design access control systems. Thus, each access control system has its own attributes, methods and functions, which derive from either a policy or a set of policies [17].

Secret-sharing schemes (SSS) are used to divide a secret among a number of parties. The information given to a party is called the share (of the secret) for that party. Every SSS realizes some access structure that defines the sets of parties who should be able to reconstruct the secret by using their shares.

Linear secret-sharing scheme (LSSS) is a type of SSS which realizes an access structure τ, a third party called the dealer holds a secret y and distributes the shares of y to parties such that y can be reconstructed by a linear combination of the shares of any authorized set. Further, an unauthorized set has no information about the secret y [18]. In attribute based encryption (ABE), ciphertexts are labeled with a set of descriptive attributes. Decryption keys are identified by a tree-access structure in which each interior node of the tree is a threshold gate and the leaves are associated with attributes. For example, we can represent a tree with *AND* and *OR* gates. A user will be able to decrypt a ciphertext with a given key if and only if there is an assignment of attributes from the ciphertexts to nodes of the tree such that the tree is satisfied [19].

Let τ be an access tree with root r. Denote by τ_x the subtree of τ rooted at the node x. Hence τ is the same as τ_r. If a set of attributes γ satisfies the access tree τ_x, we denote it as $\tau_x(\gamma) = 1$. We compute $\tau_x(\gamma)$ recursively as follows:

If x is a non-leaf node, evaluate $\tau_{x'}(\gamma)$ for all children x' of node x. $\tau_x(\gamma)$ returns 1 if and only if at least k_x children return 1. If x is a leaf node, $\tau_x(\gamma)$ returns 1 if and only if $att(x) \in \gamma$. We denote the parent of the node x in the tree by $parent(x)$. The function $att(x)$ is defined only if x is a leaf node and denotes the attribute associated with the leaf node x in the tree [5].

2.2 Bilinear Maps

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of some large prime order q. The bilinear map $\hat{e}$: $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ satisfies the following properties:

- Bilinear: $\hat{e}(aP, bQ) = \hat{e}(P,Q)^{ab}$, for all $P, Q \in \mathbb{G}_1$ and all $a, b \in \mathbb{Z}_q^*$.
- Non-degenerate: If P is a generator of $\mathbb{G}_1$ then $\hat{e}(P,P)$ is a generator of $\mathbb{G}_2$.
- Computable: There is an efficient algorithm to compute $\hat{e}(P,Q)$ for any $P, Q \in \mathbb{G}_1$.

2.3 Attribute Based Encryption

A key policy attribute based encryption (KP-ABE) consists of four algorithm: Setup, Encryption, Key-Generation and Decryption.

- **SetUp**: This is a randomized algorithm which is run by the authority and outputs the public key parameters PK and the master key MK. The public key parameters are published and the master key is kept secret.
- **Key-Generation**(τ, MK): It is a randomized algorithm which is run by the authority and takes an access structure τ and the master key MK as input. The algorithm outputs the decryption key D corresponding to the access structure τ.
- **Encryption**$(Params, M, \gamma)$: This algorithm outputs a cipher-text CM by taking the message M to be encrypted, the attributes set γ that the data user should satisfy, and the public key parameters PK as input.
- **Decryption**$(D, CM, Params)$:This algorithm is run by the receiver and takes the cipher-text CM encrypted under the attributes set γ , the decryption key D for access control structure τ with the public key parameters PK as input. This algorithm decrypts the cipher-text CM and outputs message M if and only if $\tau(\gamma) = 1$.

2.4 ID-based Signature

ID-based signature scheme consists of the following sub protocols:

- **Setup**: A Key-Generation Algorithm (KGA) runs the master-key generation algorithm $MKGen$ on input 1^k , where $k \in \mathbb{N}$ is a security parameter, to obtain a master public/secret key pair (mpk, msk).
- **idKeyGen**(msk, id):Given an identity id, it outputs ID-based signing key SK_{id} associated to id under the master secret key msk of a key generator.
- **idSig**(SK_{id}, m): Given a secret key SK_{id} and a message m, it computes a signature σ for the message m under the signing key SK_{id}.
- **idVrf**(m, id, σ): The algorithm verifies if a signature σ of a message m for an identity id is valid or not.

3 System Architecture

3.1 Architecture

In this section we describe the communication entities within our protocol which are made of the trusted authority (TA), central transportation authority (CTA), road side units (RSU) and vehicles which communicate through the on board unit (OBU) as shown in figure 1.

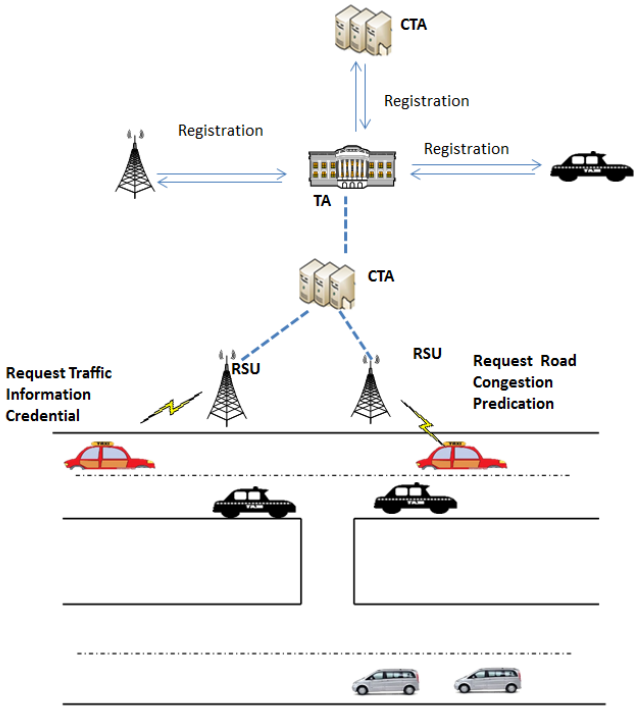

Figure 1: System Architecture.

- Trusted Authority (TA): It is in charge of the registration of all entities (CTA, RSU and vehicle) inside our system and issues cryptographic materials during the system initialization.

- Central Transportation Authority(CTA): CTA is in charge of offering credential for road safety services such as traffic information service package which contains different services like dynamic route information, GPS map or congestion prediction. Then latter on , CTA offers services according to the credential.

- Vehicles: Vehicles are equipped by OBU and communicate with CTA through RSUs in order to receive different road safety services.

The proposed approach is made by the following sub protocols:

- System Setup: TA generates its public/ private key based on digital signature techniques. CTA submits the universe of attribute *UA* to TA which generates attribute public parameters and attribute master key.TA generates the certificates for vehicles and CTA based on their pseudo identities.

- Credential Issuance: Each vehicle v_i first generates a signing key based on the pseudo identity provided by TA. v_i submits a request to CTA which later generates a credential that contains a set of attributes γ and an access tree τ. $\{\gamma, \tau\}$ will later determine the range of services which v_i can access. Based on $\{\gamma, \tau\}$, v_i generates a decryption key.

- Traffic Information Issuance : A vehicle sends a request to CTA for one or many road safety services such as traffic information service package which contains congestion prediction service, and Dynamic Route Information Panel service. CTA verifies the credential and generates a message according to the attributes within the credential key note. Before recovering the message, v_i decrypt the nodes which make the access tree τ in order to reach the node r (for example) corresponding to a given service, then v_i can recover the message.

3.2 System Objectives

The followings are security requirements for the proposed protocol:

- Identity privacy preserving: The real identity of a v_i should be kept anonymous from other vehicles as well as from CTA

- Authentication and Authorization: Only legitimate vehicle should be able to request and receive road safety services within our protocol. The messages exchanged between vehicles to CTA through RSU should be authenticated in order to avoid impersonation and forgery attacks.

- Fine-grained access control: Through fine-grained access control, CTA is able to provide a range of services according to the credentials offered to vehicles.

- Traceability: Although a vehicle's real identity should be hidden from other vehicles and malicious users, TA should be able to reveal the real identity of a vehicle in case of disputes.

4 Proposed Protocol

In this section, we design a fine-grained privacy-preserving protocol based on attribute access control for VANETs based ID-based signature and attribute based encryption. Table 1 shows the notations used in describing the proposed protocol.

4.1 System Setup

In order to initialize the system, TA performs the following:

- TA choose bilinear map groups $(\mathbb{G}_1, \mathbb{G}_2)$ of the same order q and a random generator $P \in \mathbb{G}_1$.

- TA assigns itself an identity ID_{TA} and set its signing key SK_{TA} such that $ID_{TA} = P^{SK_{TA}}$.

- TA picks a random $b \in \mathbb{Z}_q^*$ as an ID- based signature generation secret and set $P_{TA} = bP$ as a public parameter.

- For CTA_j, TA computes its pseudo identity as $PID_{CTA} = H_1(uP||ID_{CTA})$ where ID_{CTA} is the real identity of CTA_j and $u \in \mathbb{Z}_q^*$ is a random value.

- TA generates a certificate for CTA_j as $Cert_{CTA} = \{PID_{CTA}, Sig_{TA}(PID_{CTA})\}$ where $Sig_{TA} = H_1(PID_{CTA}.SK_{TA})$ is the signature of TA on PID_{CTA}.

Table 1: Notations and Descriptions

Notation	Description
$\mathbb{G}_1, \mathbb{G}_2$	bilinear map groups with the same order q
$P \in \mathbb{G}_1$	a generator of $\mathbb{G}_1$
b	master secret for ID-based signature
P_{TA}, ID_{TA}	TA's public keys
SK_{TA}	TA's signing key
ID_{v_i}, CTA_j	real identities of v_i and CTA
PID_{v_i}, PID_{CTA}	pseudo identity of v_i and CTA_j
$Cert_{v_i}, Cert_{CTA}$	anonymous certificates of v_i and CTA_j
U	Universe of attribute
γ	set of attributes
τ	Access tree
$Enc_k(.)$	symmetric encryption under key k
$Cred_{v_i}$	Road services credential of a vehicle v_i
d	Minimal number of overlapped attribute v_i

- For v_i, TA computes its pseudo identity as $PID_{v_i} = H_1(Pa||ID_{v_i})$ where ID_{v_i} is the real identity of v_i and $a \in \mathbb{Z}_q^*$ a random.
- TA generates a certificate for v_i as $Cert_{v_i} = \{PID_{v_i}, Sig_{TA}(PID_{v_i})\}$ where $Sig_{TA} = H_1(PID_{v_i}.SK_{TA})$ is the signature of TA on PID_{v_i}
- TA generates Lagrange coefficient $\Delta_{i,S}$ for $i \in \mathbb{Z}_q^*$ and a set S of elements in $\mathbb{Z}_q$: $\Delta_{i,S}(x) = \Pi_{j \in S, j \neq i} \frac{x-j}{i-j}$ and each attribute is associated with a unique element in $\mathbb{Z}_q^*$.
- From the universe of attribute $U = \{1, 2, ..N\}$ submitted to TA from CTA_j, TA choose a random number $t_i \in \mathbb{Z}_q^*$ for each attribute $i \in U$.
- TA publishes public parameters $params = \{T_1 = P^{t_1}, ..., T_{|U|} = P^{t_{|U|}}, Y = \hat{e}(P,P)^y, P_{TA}, ID_{TA}, H_1, H_2\}$ where $y \in \mathbb{Z}_q^*$ is a random and $H_1 : \{0,1\}^* \rightarrow \in \mathbb{Z}_q^*$, $H_2 : \{0,1\}^* \rightarrow \in \mathbb{Z}_q^*$ are two hash functions.
- TA generates an attribute-based master key $MK = \{t_1, ...t_{|U|}, y\}$.
- TA stores $(VID_i, Cert_{v_i})$ and provides v_i with $(PID_{v_i}, b, Cert_{v_i})$ securely.
- TA stores $(CTA_j, Cert_{CTA})$ and provides CTA_j with $(PID_{CTA}, Cert_{CTA}, MK)$ securely.

4.2 Credential generation

Before a vehicle get any road safety service, it has to acquire for a credential from CTA_j and v_i first generates its signing key according to ID-based signature [6] as follows:

- Picks $r \in \mathbb{Z}_q^*$ and compute $R = rP$
- Computes $c_1 = H_1(P_{TA}, PID_{v_i}, R)$ where PID_{v_i} is the pseudo identity generated by TA
- Computes $c_2 = r - c_1 \cdot b(modq)$
- Recomputes $c_1 = H_1(P_{TA}, PID_{v_i}, c_1 P_{TA} + c_2 P)$

- Generates $SK_{v_i} = \{c_1, c_2, PID_{v_i}, P_{TA}\}$

v_i compose a credential request message $crm = \{CR, PID_{v_i}, Stype, k\}$ representing respectively the credential keyword, the pseudo identity, the service type and k is a session key used for a symmetric encryption scheme such as AES, then generates a signature on the message as follows.
v_i computes $W = wP$ where $w \in Z_q^*$, then computes $n = H_2(P_{TA}, PID_{v_i}, crm, W, c_1)$ and $\mu = w - n \cdot c_2(modq)$ and return $\sigma_{v_i} =< c_1, W, \mu >$ and sends $< \sigma_{v_i}, crm, PID_{v_i}, Cert_{v_i} >$ to CTA_j via RSU. CTA_jperforms the following before it issues the credential:

- CTA_j performs the verification of TA's signature on $Cert_{v_i}$
- CTA_j verifies TA's signature on $Cert_{v_i}$ by checking the equality $\hat{e}(Sig_{TA}(PID_{v_i}), P) = \hat{e}(H_1(PID_{v_i})), ID_{TA})$ holds

If it holds, CTA_j performs the following to verify v_i signature:

- CTA_j computes $n = H_2(P_{TA}, PID_{v_i}, m, W, c_1)$ and verifies if $c_1 = H_1(P_{TA}, PID_{v_i}, c_1 P_{TA} + n^{-1}(W - \mu P))$ and rejects the response if the equality does not satisfy.

The verification works because of the following holds:

$$
\begin{aligned}
& H_1(P_{TA}, PID_{v_i}, c_1 P_{TA} + n^{-1}(W - \mu P)) \\
&= H_1(P_{TA}, PID_{v_i}, c_1 P_{TA} + n^{-1}(wP - (w - nc_2)P)) \\
&= H_1(P_{TA}, PID_{v_i}, c_1 P_{TA} + n^{-1}(wP - (wP - nc_2P))) \\
&= H_1(P_{TA}, PID_{v_i}, c_1 P_{TA} + n^{-1}(wP - wP + nc_2P)) \\
&= H_1(P_{TA}, PID_{v_i}, c_1 P_{TA} + n^{-1}(nc_2P)) \\
&= H_1(P_{TA}, PID_{v_i}, c_1 P_{TA} + c_2P) \\
&= c_1
\end{aligned}
$$

For each service, CTA_j provided a set of meaningful attributes for access control. Different services may have the same attribute subsets. Moreover, each vehicle is given an access structure implemented by an access tree τ, as shown in Fig. 2. Interior access tree nodes are threshold gates. Leaf access tree nodes are associated with attributes, thus we can enforce fine-grained access control using this linear secret sharing scheme [7]. For instance CTA_j offers tree type of main services which are Entertainment as a Service (ENaaS), Network as Service (INaaS) and Traffic-Information as Service (TIaaS). Within TIaaS, it offers congestion prediction and Dynamic Route Information Panels and for each service corresponds to a given node r or r_1.
After a successful verification of the request message sent by v_i, CTA_j performs the following to generate a credential:

- Compose a credential message $CRE_v = \{CreKN, \gamma, \tau, ts, MK\}$ representing respectively the credential key note, the set of attribute, the access tree of the attributes, the time stamp and the master secret in order for v_i to generate the decryption key according the v_i access tree τ.
- CTA_j encrypts $C = Enc_k\{CRE_v\}$ where k is a symmetric sent during credential request and send $< C, Cert_{CTA} >$ to CTA_j
- v_i verifies the TA's signature on $Cert_{CTA}$ and decrypts the message using the symmetric key and recover the credential CRE_v.

v_i retrieves the access tree τ and the set set of attribute γ which corresponds to the type of service which v_i requested. Note that the decryption key generation algorithm outputs a key that enables v_i to decrypt a message encrypted under a set of attributes γ if and only if $\tau(\gamma) = 1$, then v_i generate its decryption key as follows:

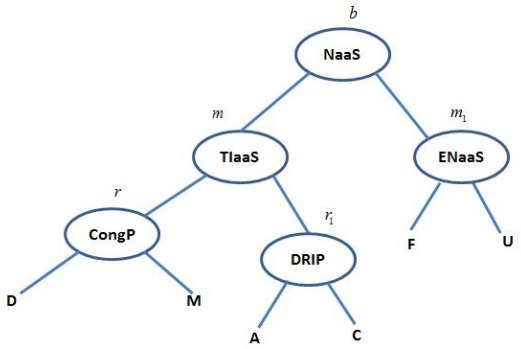

Figure 2: Access Structure Example.

- Choose a polynomial q_x for each node x (including the leaves) in the tree τ within the credential CRE_v. The polynomials are chosen in a top-down manner till to the node which corresponds to a service, for instance r corresponds to congestion prediction service.

- v_i set the degree d_x of the polynomial q_x to be one less than the threshold k_x of that node, that is $d_x = k_x - 1$

- v_i set for the root node r $q_r(0) = y$. For any other node x, set $q_x(0) = q_{parent(x)}(index(x))$ to completely define q_x

- After a successful description of all the polynomial for each leaf node x, v_i generates $D_x = P^{\frac{q_x(0)}{t_i}}$ where $i = att(x)$. The decryption key is the set of all the secret value as $D_{vi} = \{D_x, ..., D_n\}_{x \in \tau}$

4.3 Road Safety Service Request

- When v_i needs one or two type of road safety services such as congestion prediction service , it composes a road service request message $M = \{CreKN, ts, Stype, k_1\}$ representing respectively the credential key note, the time stamp, the service type and k_1 is a session key used for a symmetric encryption scheme such as AES.

- v_i generates sends $< \sigma_{v_i}, M^{'}, PID_{v_i}, Cert_{v_i} >$ to CTA_j representing respectively the signature, the encrypted message $M^{'} = Enc_k(M)$, the pseudo identity and the certificate.

- First CTA_j makes the verification as described in section 3.2, then checks if the credential key note $CreKN$ corresponds to the pseudo identity of the vehicle and lastly checks if $CreKN$ suites the type of services requested.

- In case the requested service is a congestion prediction service for example, CTA_j composes a congestion prediction message $mpre = \{prfile, ts\}$ where $prfile$ and ts representing respectively the congestion prediction file and the time stamp.

CTA_j encrypts $mpre$ under the set of attribute γ as follows:

- Choose $s \in \mathbb{Z}_q^*$ and publishes the cipher text as $E = (E^{'} = mpreY^s, \{E_i = T_i^s\}_{i \in \gamma})$

- CTA_j sends $C^{'} = Enc_{k_1}\{E, Cert_{CTA}\}$ to v_i through RSU

Upon receiving the message, v_i performs the following:

- Verifies TA's signature on $Cert_{CTA}$
- Decrypts the message under the symmetric shared key k_1

For each node z which are the children of node x such as node (D,M) being the children of node r in figure 2; let S_x be an arbitrary k_x-sized set of child nodes z such that F_z is not an empty set $(F_z \neq \perp)$.

- v_i computes $F_x = \prod_{z \in S_x} F_z^{\Delta_{i,S_x^{'}}(0)}$ where $i = index(z)$ and $S_x^{'} = \{index(z) : z \in S_x\}$
  $= \prod_{z \in S_x} (\hat{e}(P,P)^{s.q_z(0)})^{\Delta_{i,S_x^{'}}(0)}$
  $= \prod_{z \in S_x} (\hat{e}(P,P)^{s.q_{parent(z)^{index(z)}}})^{\Delta_{i,S_x^{'}}(0)}$
  $= \prod_{z \in S_x} \hat{e}(P,P)^{s.q_x(i).\Delta_{i,S_x^{'}(0)}}$
  $= \hat{e}(P,P)^{s.q_x(0)}$

If the node to be decrypted is a childless node such as r_1 representing DRIP service in our scenario, v_i computes $\hat{e}(D_x, E_i)$

- $\hat{e}(D_x, E_i)$
  $= \hat{e}(P^{\frac{q_x(0)}{t_i}}, P^{s.t_i})$
  $= \hat{e}(P,P)^{s.q_x(0)}$ if $i \in \gamma$
  $= \hat{e}(P,P)^{ys} = Y^s$ if the cipher text satisfy the tree,thus $mrec$ is recovered because $E^{'} = mpreY^s$

5 Analysis

Our secure privacy preserving protocol over attribute based access control for VANETs is analyzed in terms of security and computation cost.

5.1 Security

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

- Authentication : During the credential request phase, a vehicle attaches its certificate $Cert_{v_i} = \{PID_{v_i}, Sig_{TA}(PID_{v_i})\}$ which is generated based on the pseudo identity of v_i $PID_{v_i} = H_1(Pa||ID_{v_i})$. PID_{v_i} does not reveal the real identity of v_i, making it hard to launch an impersonation attack.
- Authorization : Before a vehicle request of one or several range of services, it has to have a credential $CRE_v = \{CreKN, \gamma, \tau, ts\}$ provided by CTA_j. The credential is sent encrypted under a symmetric key $C = Enc_k\{CRE_v\}$. Moreover, the credential request message is signed with an ID-based signature which CTA_j verifies.
- Identity Privacy Preservation: v_i uses its pseudo identity $PID_{v_i} = H_1(Pa||ID_{v_i})$ during the protocol, even the certificate of v_i is generated based on PID_{v_i}. So neither a malicious user or CTA_j can reveal the real identity of v_i.

- Fine-grained access control: In our protocol, an access tree τ is attached within the credential $CRE_v = \{CreKN, \gamma, \tau, ts, MK\}$ which is exchanged after being encrypted under a symmetric key in order for the vehicle to decrypt the nodes within the tree. During the request of the road services, note that, only the credential keynote *CreKN* corresponding to the credential within the message $M = \{CreKN, ts, Stype, k_1\}$ is sent to CTA_j, thus even though a malicious user eavesdrops the request, he can not decrypt the service sent by CTA_j. No user which does not satisfy the access tree τ can decrypt the message.

- Traceability: Even though it is hard for an attacker and CTA_j to know the real identity of a vehicle, TA should have the capability of revealing vehicle's real identity in case of disputes. The pseudo identity is based on v_i real identity as $PID_{CTA} = H_1(Pu||ID_{CTA})$.

5.2 Performance

In this section, we evaluate the performance of our protocol in terms of computational delay and compared it to ABACS [4]. We start by analyzing the time complexity of our protocol. Note that we ignore the time complexity involved in setup because it is assumed to be done offline and occasionally. The measurement of cryptographic operations are shown in table 2. Let T_{mul} and T_{pair}denote the time required to perform one point multiplication and one pairing operation over an elliptic curve respectively. Also let T_{as-enc}, T_{as-dec},T_{sig}, T_{ver} be the time required to perform asymmetric encryption, asymmetric decryption, symmetric encryption, signature generation and signature verification respectively. These operations dominate the speed of signature generation and signature verification and we neglect all others operations such as addition, scalar value manipulation, and one-way hash function [20]. We consider the experiment in [21] [4] in which the processing time (in milliseconds) was observed for a supersingular curve of embedding degree $k = 6$ and executed it on an Athlon XP 2 GHz machine. Based on the computational delay of cryptographic operations, we then calculate the total computational delay of a complete round, denoted as $T_{t-round}$ for our protocol as follows:
According to section 4.2, it takes $\{T_{sig} + T_{ver} + T\,pair + T_{as-enc} + T_{as-dec}\}$ for credential issuance phase. From section 4.3, it takes$\{T_{sig} + T_{ver} + 2dT_{pair} + 2T_{mul}\}$ for road service package issuance.We estimated the computational costs of the proposed protocol based on two main sub-phases: credential issuance phase and service issuance phase. Note the number of attribute taken in our access structure is $d = 4$. Table 3 shows the results as compared with ABACS [4].

Table 2: Measurement of cryptographic operations

Notation	Operations	time (ms)
T_{pair}	bilinear pairing	2.82
T_{mul}	point scalar multiplication	0.78
T_{as-enc}	asymmetric encryption	1.17
$T_{as-decc}$	asymmetric decryption	0.61
T_{sig}	signature generation	1.56
T_{ver}	signature generation	3.12

The difference between the two protocols is that in [4], an attribute based encryption/decryption is performed during the credential issuance phase (recruitment phase) based to v_i identity. However, in our protocol, a vehicle is authenticated based on its anonymous certificate for credential issuance phase and credential for service issuance phase. The computational cost depends on value d which is the minimal number of overlapped attribute, thus attribute based encryption should be performed as less as possible.

Table 3: Computational cost of ABACS and proposed protocol

Phase	*ABACS*[19]	Proposed
$Credential-Issuance$	$dT_{pair}+2T_{mul}$	$T_{sig}+T_{ver}+T_{pair}+T_{as-enc}+T_{as-dec}$
$Service-Issuance$	$dT_{pair}+2T_{mul}$	$dT_{pair}+T_{mul}$
Total cost (ms)	25.68	21.26

We further compare our protocol with existing scheme [12] which offers one credential per road safety service and [4] in terms of privacy and security as described in table 4. We only took the computational cost for credential issuance and service issuance. The comparison shows that attribute based access control which can allow multiple services for one credential would so much decrease the computational capabilities of service provider. Note the number of attribute taken in our access structure is d=4 which offer 4 services at maximum.

Table 4: Comparison in terms of privacy and security

Phase	[4]	[19]	Proposed
Privacy during Credential-Issuance	*Yes*	*No*	*Yes*
Privacy during Service-Issuance	*Yes*	*Yes*	*Yes*
Multiservice/ single credential	*No*	*Yes*	*Yes*
Estimated cost credential/Service (ms)	28.52	25.68	21.26

Additionally, we analyze the relationship between the vehicle movement speed v and the short waiting period ξ. The following assumptions are made to simulate a practical scenario as described in [4]:

- The average speed of v_i (denoted as v) ranges from 10 m/s- 50 m/s (or 72 km/hr - 180 km/hr).The valid coverage range of an RSU (denoted as C_{RSU}) is 300 m [22].
- The number of attributes required for selecting an v_i is 4 (d = 4). Therefore, the total computation delay of our protocol is $T_{sig}+T_{ver}+T_{as-enc}+T_{as-dec}+T_{pair}+dT_{pair}+T_{mul}$= 21.26 ms for d= 4. The total computational cost is 25.68 ms for [4].

To evaluate the receiving ratio of v_i, we estimate the required coverage range (denoted by C_{RSU}) over which an RSU successfully transmits the message *mpre* to v_i . The minimal required coverage range of an RSU is calculated as:
$C_{rg} = v \times T_{t-round}$
We further estimate the receiving ratio, denoted as R_{rat}, by considering the coverage range C_{RSU} of an RSU and the short waiting period ξ. The following formula can be applied to calculate the receiving ratio [4]:
$R_{rat} = \frac{C_{RSU}}{C_{rg}\times\xi} = \frac{C_{RSU}}{v\times T_{t-round}\times\xi}$ where $C_{RSU} \geq R_{rg}$.

$$R_{rat} = \begin{cases} 1 & \text{if } \frac{C_{RSU}}{T_{t-round}} \cdot \frac{1}{v\times\xi} \geq 1; \\ \frac{C_{RSU}}{T_{t-round}} \cdot \frac{1}{v\times\xi} & \text{otherwise.} \end{cases}$$

In figure 3, with d = 4 and $T_{r-round}$= 21.26 ms, we show the receiving ratio with respect to velocity v, $40 \leq v \leq 50$, and the waiting time ξ, $0 \leq \xi \leq 300$. It is observed that v_i can successfully receive a

message *mpre* better than that of [4]. In the proposed protocol, within the same speed range, the ratio decreases to 0.002, however for [4], it decreases to 0.001.

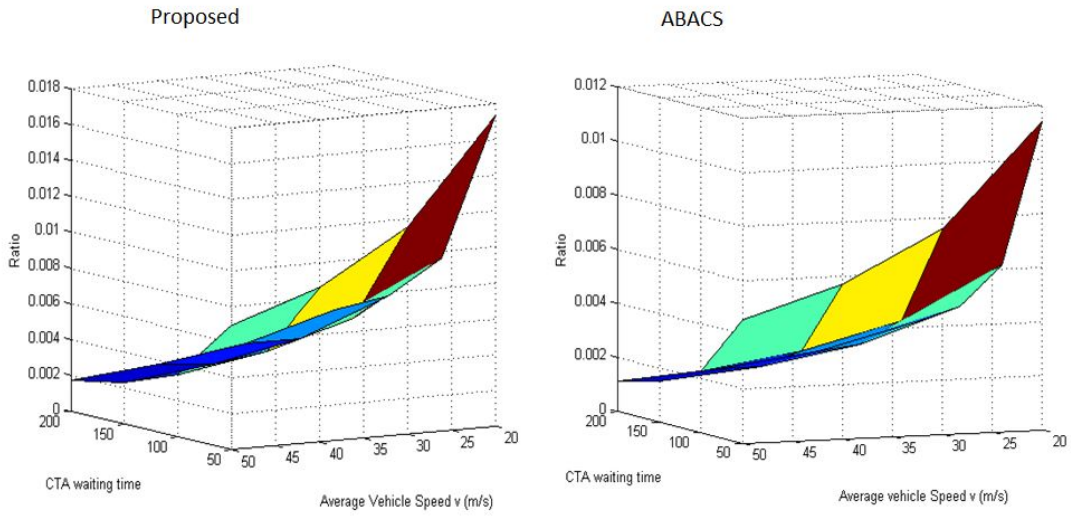

Figure 3: Comparison of receiving ratio between our protocol and [4] for $d = 4$

6 Conclusion

In this paper, we have proposed a fine-grained privacy-preserving protocol over attribute based access control for VANETs which could be useful in providing multi services without requiring a supplementary credential in VANETs. Compared to [4] which identifies a user based on the attributes, the proposed protocol relies on anonymous credential , thus requiring less computational cost.Our protocol is based on the concept of ID-based signature, attribute based encryption over linear secret sharing scheme. The analysis of the protocol confirms the fulfillment of the security objectives and the efficiency of the proposed protocol.

Acknowledgments

This work was supported by a Research Grant of Pukyong National University (2014 Year).

References

[1] B. Sharma and A. K. Singh, "A token based protocol for mutual exclusion in mobile ad hoc networks," *Journal of Information Processing Systems*, vol. 10, no. 1, pp. 36–54, 2014.

[2] J. Jeong, S. Guo, Y. Gu, T. He, and D. H. Du, "Trajectory-based data forwarding for light-traffic vehicular ad hoc networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 5, pp. 743–757, 2011.

[3] R. Hussain, "Cooperation-aware VANET clouds: Providing secure cloud services to vehicular ad hoc networks," *Journal of Information Processing Systems*, vol. 10, no. 1, pp. 103–118, 2014.

[4] L.-Y. Yeh, Y.-C. Chen, and J.-L. Huang, "ABACS: An attribute-based access control system for emergency services over vehicular ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 630–643, 2011.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. of the 13th ACM conference on Computer and Communications Security (ACM CCS'06), Alexandria Virginia, USA*. ACM, October-November 2006, pp. 89–98.

[6] R. W. Zhu, G. Yang, and D. S. Wong, "An efficient identity-based key exchange protocol with KGS forward secrecy for low-power devices," *Theoretical Computer Science*, vol. 378, no. 2, pp. 198–207, 2007.

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

[8] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1557–1568, 2007.

[9] M. D. Dikaiakos, A. Florides, T. Nadeem, and L. Iftode, "Location-aware services over vehicular ad-hoc networks using car-to-car communication," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1590–1602, 2007.

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

[11] T. W. Chim, S. Yiu, L. C. Hui, and V. O. Li, "Vspn: Vanet-based secure and privacy-preserving navigation," *IEEE Transactions on Computers*, vol. 63, no. 2, pp. 510–524, 2014.

[12] W. Cho, Y. Park, C. Sur, and K. H. Rhee, "An improved privacy-preserving navigation protocol in vanets," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 4, no. 4, pp. 80–92, 2013.

[13] E. Coronado and S. Cherkaoui, "Provisioning of on-demand services in vehicular networks," in *Proc. of the IEEE 2009 Global Telecommunications Conference (GLOBECOM'09), Honolulu. Hawaii, USA*. IEEE, November-December 2009, pp. 1–6.

[14] C.-T. Li, M.-S. Hwang, and Y.-P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Computer Communications*, vol. 31, no. 12, pp. 2803–2814, 2008.

[15] H. Zhu, R. Lu, X. Shen, and X. Lin, "Security in service-oriented vehicular networks," *IEEE Wireless Communications*, vol. 16, no. 4, pp. 16–22, 2009.

[16] H. A. J. Narayanan and M. Giine, "Ensuring access control in cloud provisioned healthcare systems," in *Proc. of the 2011 IEEE Consumer Communications and Networking Conference (CCNC'11), Las Vegas, Nevada, USA*. IEEE, January 2011, pp. 247–251.

[17] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 7, pp. 1735–1744, 2014.

[18] M. Karchmer and A. Wigderson, "On span programs." in *Proc. of the the 8th Annual Structure in Complexity Theory Conference, San Diego, California, USA*. IEEE, May 1993, pp. 102–111.

[19] D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical identity based encryption with constant size ciphertext," in *Proc. of the 24th annual international conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT'05), Aarhus, Denmark, LNCS*. Springer Berlin Heidelberg, May 2005, vol. 3494, pp. 440–456.

[20] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. of the 27th Conference on Computer Communications (INFOCOM'08), Phoenix, Arizona, USA*. IEEE, April 2008.

[21] P. S. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *Proc. of the 11th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'05), Chennai, India, LNCS*. Springer Berlin Heidelberg, 2005, vol. 3788, pp. 515–532.

[22] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: Timed efficient and secure vehicular communications with privacy preserving," *IEEE Transactions on Wireless Communications*, vol. 7, no. 12, pp. 4987–4998, 2008.

Author Biography

Lewis Nkenyereye received his bachelor degree in Computer Science from Light University of Burundi , master degree in Information Technology from Uganda Christian University of Uganda in 2009 and 2012, respectively. Since September 2013, he is with the Lab of Information Security and Internet Applications, Department of IT Convergence and Application Engineering, Pukyong National University as a Ph.D. candidate. His research interests are related with cryptography and vehicular cloud security.

Bayu Adhi Tama received his bachelor degree in Electrical Engineering from Sriwijaya University, master degree in Information Technology from University of Indonesia in 2004 and 2008, respectively. Since March 2015, he is with the Lab of Information Security and Internet Applications, Department of IT Convergence and Application Engineering, Pukyong National University (PKNU) as a Ph.D. candidate. His research interest are related to data mining application and security in vehicular ad hoc network.

Youngho Park received his M.S. and Ph.D. degrees in Department of Computer Science and Information Security from Pukyong National University, Republic of Korea in 2002 and 2006, respectively. He is currently a postdoctoral researcher in Department of IT Convergence and Application Engineering, Pukyong National University. His research interests are related with information security, applied cryptography and network security; secure ad hoc network, authentication, key management, and identity-based cryptosystem.

Kyung Hyune Rhee received his M.S. and Ph.D. degrees from Korea Advanced Institute of Science and Technology (KAIST), Republic of Korea in 1985 and 1992, respectively. He worked as a senior researcher in Electronic and Telecommunications Research Institute (ETRI), Republic of Korea from 1985 to 1993. He also worked as a visiting scholar in the University of Adelaide, the University of Tokyo, and the University of California, Irvine. He has served as a Chairman of Division of Information and Communication Technology, Colombo Plan Staff College for Technician Education in Manila, the Philippines. He is currently a professor in the Department of IT Convergence and Application Engineering, Pukyong National University, Republic of Korea. His research interests center on key management and its applications, mobile communication security and security evaluation of cryptographic algorithms.