Signal Processing 120 (2016) 682–690

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

An efficient message access quality model in vehicular communication networks

Xuejiao Liu [a], Zhenyu Shan [a,*], Luming Zhang [b], Wei Ye [a], Ruoyu Yan [c]

[a] Institute of Service Engineering, Hangzhou Normal University, Hangzhou, China
[b] School of Computing, National University of Singapore, Singapore
[c] College of Computer and Information Engineering, Henan University of Economics and Law, Zhengzhou, China

ARTICLE INFO

Article history:
Received 5 September 2014
Received in revised form
18 November 2014
Accepted 20 November 2014
Available online 28 November 2014

Keywords:
VANET security
Attribute-based encryption
Attribute-based signature
Message authentication

ABSTRACT

In vehicular ad hoc network (VANET), vehicles equipped with computing, sensing, and communication capabilities can exchange information within a geographical area to distribute emergency messages and achieve safety system. Then how to enforce fine grained control of these messages and ensure the receiving messages coming from the claimed source in such a highly dynamic environments remains a key challenge that affects the quality of service. In this paper, we propose a hierarchical access control with authentication scheme for transmitted messages with security assurance over VANET. By extending ciphertext-policy attribute-based encryption (CP-ABE) with a hierarchical structure of multiple authorities, the scheme not only achieves scalability due to its hierarchical structure, but also inherits fine-grained access control on the transmitted messages. Also by exploiting attribute-based signature (ABS), the scheme can authorize the vehicles that can most appropriately deal with the message efficiently. The results of efficiency analysis and comparison with the related works show that the proposed scheme is efficient and scalable in dealing with access control and message authentication for data dissemination in VANET.

1. Introduction

Vehicular ad hoc network (VANET) is regarded as a promising approach for future intelligent transportation system, which enables communication between vehicles to vehicles and vehicles to roadside units. Although various parallelized fusion [1] and domain decomposition [2] are applied in intelligent transport system to understand the transport data, in VANET network vehicles can exchange information (e.g., detour, traffic accident, congestion information, and life-critical emergence messages) and provide early warnings to nearby vehicles in order to reduce traffic jams near the affected areas, and the traditional methods are not suitable in vehicular communication network. VANET will greatly enhance driving safety and experience, improve roadway system efficiency. Further, widespread deployment of VANET is heavily based on a secure and reliable infrastructure for providing accurate traffic and road system data. However, providing security in a vehicular network is more difficult than in other networks such as WSN due to the high mobility and wide range of vehicles [3]. Nowadays, the security issues, such as confidentiality, authentication, non-repudiation, localization and verification of data [4], are still the most important problem to be solved that affect the quality of service (QoS) in vehicular network.

Vehicular ad hoc networks are usually operated among vehicles moving at high speeds, thus their communication

* Corresponding author.
E-mail address: shanzhenyu@zju.edu.cn (Z. Shan).

http://dx.doi.org/10.1016/j.sigpro.2014.11.012
0165-1684/

relations can be changed frequently. In such a highly dynamic environment, traditional security solutions face many challenges in VANET caused by the complex vehicular communications system, dynamic user groups, real-time constraints, etc. The privacy and confidentiality of the transmitted messages should be protected in VANET communications. Also the messages must be authenticated to prevent attackers from injecting, altering and replaying messages, as well as to prevent eavesdropping. Intuitively, it is extremely dangerous that if the messages are controlled by the attackers. This could easily cause confusions or unexpected situations especially in some emergency applications. In many cases, it is also desirable to provide a fine-grained access control mechanism to guarantee that messages transmitted to corresponding users.

Specially speaking, let us see the following scenario. In case of an emergency (e.g., a traffic accident, a fire or a bomb threat) in a certain area of a city, police headquarters will immediately transmit emergency messages. On one aspect, they intend to notice policemen to deal with the emergency at the time of accidents. On the other aspect, they want to broadcast an alert message to the vehicles which are in this district or will in this district, to avoid this emergency. Then, traffic jams or serious accidents can possibly be prevented if these emergency messages can be shared among vehicles. Also they want to define a policy that allow someone (e.g., police car) in selected locations near the scene of the accident to take over the control of traffic lights in order to facilitate rescue and carry out orderly vehicle evacuation.

In this paper, we propose a hierarchical access control scheme with authentication in VANET. We develop ciphertext-policy attribute-based encryption algorithm into a hierarchical access control scheme, which is a flexible hierarchical structure to organize all of the trust authorities in VANET. Each vehicle has its capabilities and access rights according to the attributes it owns. Then only the vehicles that have certain attributes satisfying the access policy can decrypt the broadcasted messages. Also, we apply attribute-based signature to authenticate and authorize the appropriate vehicles to handle the messages that satisfy specific policy. Our contributions can be addressed in the following aspects:

(1) We propose a hierarchical message access quality model in VANET network, by encrypting the transmitted messages in ciphertext-policy attribute based encryption with multiple authorities. The model is scalable and efficient in dynamic vehicular communication environment.
(2) Our scheme achieves fine-grained access control among various types of vehicles using well defined attributes. When a message broadcasted in VANET, only those vehicles that possess the selected attributes can access the messages.
(3) Our scheme enforces message authentication by integrating attribute-based signature, in order to ensure message integrity checking and maintain anonymity and privacy of the vehicles.

The rest of the paper is organized as follows: Section 2 details previous work in the aspects of VANET security. In Section 3 we present the related technologies used in our scheme. Section 4 presents system model and algorithm definition. We give the specific construction and performance evaluation in Section 5. Finally, we conclude the paper in Section 7.

2. Related work

Proving a secure communication plays a vital role in establishing a more reliable driving environment in vehicular network. There are several security threats in vehicular communication, such as forging messages and transmitting bogus warnings by the malicious attackers, dropping or modifying messages by man-in-the-middle attackers, and privacy violations. To protect vehicular communication against these various attacks, the use of cryptographic algorithm is inevitable. ElGamal signature scheme [5] is a way to create a secure communication in which each vehicle has a specific public and private key (k_{pu}, k_{pr}). However, this scheme is not suitable for broadcasting messages in dynamic vehicular environment.

Verifying the authentication of users is also important in vehicular communication network, that is, determining whether someone or something is the one who or what it is claimed to be to receive the message or deal with the message. There are some studies on this aspect in vehicular network. Kim et al. [6] propose an auditable and privacy-preserving authentication in vehicular based on the MAC-chain method for privacy-preserving authentication. Several efforts [7–9] have been made to protect user privacy in the authentication process, but most of them use a policy that places full trust on the roadside units or the servers.

Access control is a challenging aspect in vehicular network in which an identification of the user is checked before gaining access to the resource. Huang et al. [10] are the first one to introduce ciphertext-policy attribute based encryption [11] in VANET in which vehicles are divided into several groups and two vehicles belonging to two different RSUs' communication ranges cannot communicate with each other directly. An improved scheme is proposed in [12], which addresses the abovementioned issues by employing the decentralized attribute based encryption scheme of Lewko et al. [13]. Gongjun et al. [14] proposed that various access control levels are predefined and each user belongs to a specific cluster based on its role in the network. Nevertheless, none of these schemes can provide mechanism for authenticating senders and authorizing receivers to handle the messages.

3. Building blocks

3.1. Bilinear maps

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two multiplicative cyclic groups of prime order p. Let g be a generator of $\mathbb{G}$ and e be a bilinear map, $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ with the following properties:

1. *Bilinearity*: for all $u, v \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p$, we have $e(u^a, v^b) = e(u, v)^{ab}$.

2. *Non-degeneracy*: $e(g,g) \neq 1$.

If the group operation in $\mathbb{G}$ and the bilinear map $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ are both efficiently computable, then we say $\mathbb{G}$ is a bilinear group.

3.2. Attribute-based encryption

ABE is a public key cryptography primitive for one-to-many communications. Ciphertext-policy attribute-based encryption (CP-ABE) provides a mechanism to specify an access policy over attributes in the encryption process. Then the user can decrypt the ciphertext if and only if the attributes associate with the user satisfy the access structure.

3.3. Attribute-based signature

To ensure user authentication, Attribute-based Signature (ABS) were introduced by Maji et al. [15] to provide authentication without disclosing the identity of the users. In ABS, users have a claim predicate associated with a message. The claim predicate helps us to identify the user as an authorized one, without revealing its identity. Other users can verify the user and the validity of the message stored.

ABE only can guarantee users to deal with data, when attributes satisfy the access policy, but do not provide any authentication mechanism to verify the users. ABS can be combined with ABE to achieve authenticated access control without disclosing the identification of the user.

4. Model and definitions

In this section, we present an overview of our system model and a formal definition of algorithms in our proposed solution.

4.1. System overview and assumptions

We consider VANET framework with multiple authorities organized in a hierarchical manner, as shown in Fig. 1. The system model consists of the following four parties: a global certificate authority (CA), the trust authorities (TAs), the fix roadside units (RSUs) at the road side and on board units (OBUs) equipped on mobile vehicles.

The CA is a global trusted certificate authority and responsible for managing trust authorities in the system. It sets up the system and generates the global secret key and the global public key.

Each TA is a registration and certification center for RSUs and OBUs, corresponds to road authority. There are many TAs which divide the city roads into several domains, which depend on different decomposition methods. Recently, many graph-based models are applied in intelligence systems and multimedia. They can be used as geometric image descriptors [16,17] to enhance image categorization. Besides, these methods can be used as image high-order potential descriptors of superpixels [18]. Further, graph-based descriptors can be used as general image aesthetic descriptors to improve image aesthetics ranking, photo retargeting and cropping [19].

RSUs connect with the TA by wired channel and OBUs by wireless channel through a secure channel, e.g., transport layer security (TLS) protocol. RSUs serve as the gateways to receive requests from users and deliver messages to corresponding OBUs. At critical intersections, some RSUs may be installed on traffic signal poles, and the traffic signals can be controlled via these RSUs. We assume RSU is *honest but curious*, which means that it is trusted to carry out computations delegated to them by the vehicles. It does not skip or distort computations, but may try to learn some additional information about the messages.

Vehicles with OBUs broadcast traffic related status information among vehicles in VANET network. We assume that the vehicles have a great number of different on-board devices, including GPS, wireless transceivers, and on-board radar devices. They also have tamper resistance devices to store critical data such as equipment identifier (EID) and cryptographic keys [20].

Attribute-based cryptography is used to greatly improve the efficiency of secure communication among multiple vehicles. The efficiency is due to the nature of using attributes that can confine data access based on various roles of vehicles.

In the system, attributes can be generally described as follows: (i) ownership of vehicles; (ii) type of events: accidents, a fire, a bomb threat, etc.; and (iii) property of events. Also, attributes can be further classified as dynamic and static attributes, depending on whether the attributes change frequently. There are many static attributes such as car types (e.g., police vehicles, fire engines, ambulances, general civilian vehicles, commercial vehicles) and affiliations. Attributes can also be dynamic according to on-road situations (e.g., location and time stamp). Each static attribute is associated with a unique private key that is derived from the global certificate authority (CA). The dynamic attributes and corresponding private keys can be derived from the local trusted authority (TA).

4.2. Main idea

Recall the emergency scenario as an example, when the vehicles involve an emergency jam, it needs to cooperate among the vehicles to promote the rapid dissipation of congestion and reschedule the traffic lights. Generally speaking, the data dissemination process compromises message creation phase, message broadcasting phase and mission execution phase.

Once an event happens, the witness vehicle sends an emergency report message [21], which contains emergency event type and location to an adjacent RSU. The RSU first confirms the validity of that message by the current standard ECDSA method [22] or other schemes [21]. If the message is invalid, RSU will drop the message; otherwise, RSU will inform top-level TA about the event. For some information like taxi information, the vehicles can create a message and broadcast itself without noticing RSU. Then TA enforces an access policy with authentication over attributes to specify who should know the message and determine which ones are most suitable for the rescue mission. So we use attribute-based signature on the message to show that only the vehicles who satisfy the signing

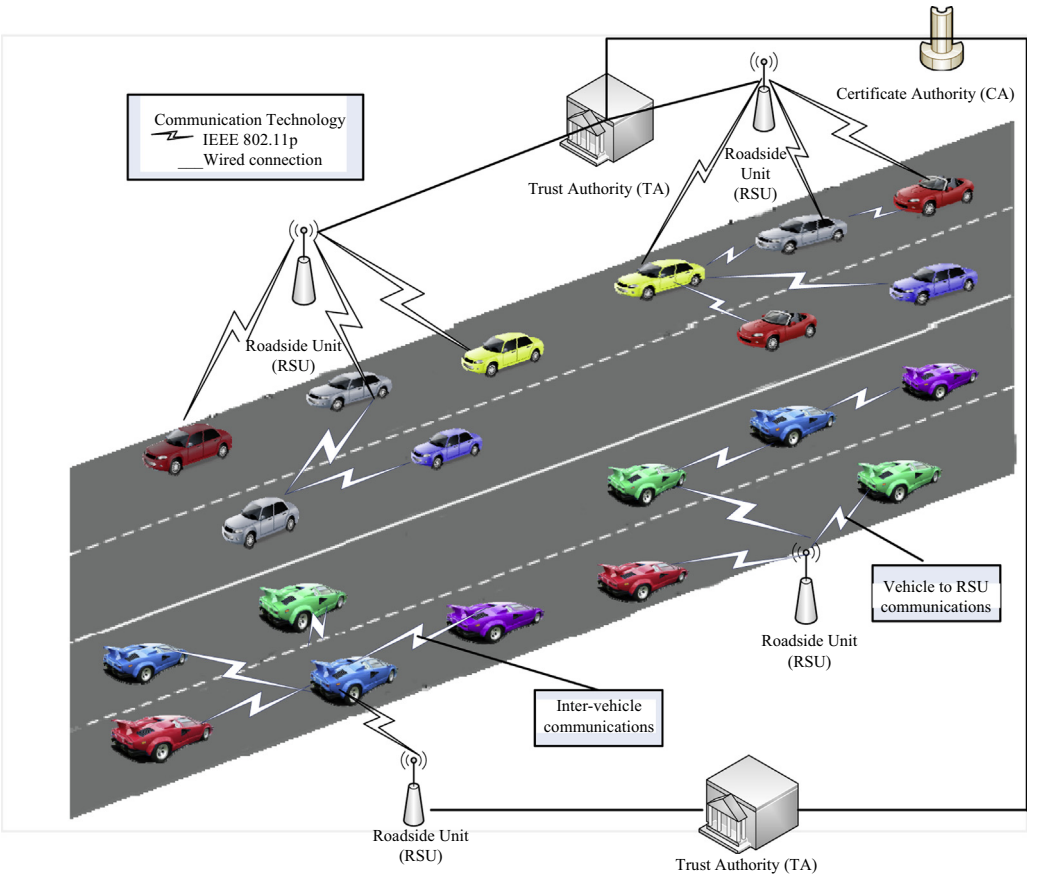

Fig. 1. System model.

structure can verify the signature and only the vehicles who satisfy the access policy can do some reschedule of the traffic facilities.

In this paper, we focus on the design of last two phases, as the message creation phase can adopt the existing schemes. To ensure security and privacy over broadcasted messages, an access control mechanism that takes into account the attribute values or the properties of the recipient vehicles is suitable. We present an efficient data access control model with authentication which provides the desired expressiveness of the access control policies.

In order to achieve flexible data access control to broadcasted data in vehicle network, we combine and exploit two latest cryptographic techniques, CP-ABE and ABS [23]. The data access control policy can be divided into two levels: message authentication and access control policy. The coarse-grained message authentication focuses on allowing desired users to access the data, and fine-grained access control policy provides traffic credential to corresponding vehicles.

In our system (Fig. 1), once a message is generated, the message sender encrypts it by CP-ABE with its access policies $\mathcal{T}_{enc}$ and then signs the encrypted file by ABS with the monotone boolean claim-predicate (access structure) $\mathcal{T}_{sig}$. Then the message sender broadcasts the encrypted message with its signature to the nearest district.

Let $\mathcal{T}_{enc}$ be a tree representing an access structure, we use the same structure as in [11]. Each non-leaf node of the tree represents a threshold gate, described by its children and a threshold value. Each leaf node x of the tree is described by an attribute and a threshold value $k_x=1$. Let $\mathcal{T}_{sig}$ be claim-predicates represented as monotone span program in ABS scheme [24,25,15]. If a set of attributes U satisfies the structure, we denote $\mathcal{T}_{enc}(U)=1$ and $\mathcal{T}_{sig}(U)=1$.

4.3. Algorithm definition

In this section, we give the definition of our privacy preserving access control scheme in vehicular communication network as follows. Table 1 presents the notions to be used in our scheme. The scheme consists of the following six algorithms:

Setup: In this operation, both of the certification authority and trust authorities should be set up. The CA takes the implicit security parameters as input and output two public and master key pairs (PK_e, MK_0) and (PK_s, MK_s). The TA takes the global public parameters PK_e for encryption and outputs the trust authorities' master key.

Key generation ($MK_0, MK_s, u, \mathcal{A}$): The private key generation algorithm takes as inputs the identity of vehicle u, the master key MK_0, MK_s and a set of attributes $\mathcal{A}$ that

Table 1
Notations used in our scheme.

Notation	Description
PK_e, PK_s	System public key for encryption and signature
MK_0, MK_s	Master key for encryption and signature
$SK_{u,e}, SK_{u,s}$	Encryption key and signing key for user u
$\mathcal{T}_{sig}, \mathcal{T}_{enc}$	Key structure for encryption and signature
MK_i	Master key of trust authorities for encryption
Y	Set of leaf nodes in $\mathcal{T}_{enc}$
σ	The data owner's signature on message

describe the user. It outputs the vehicle's encryption key $SK_{u,e}$ and signing key $SK_{u,s}$.

Encrypt$(PK_e, m, \mathcal{T}_{enc})$: The encryption algorithm is a randomized algorithm that takes as input the public parameter PK_e, a message m, and an access structure $\mathcal{T}_{enc}$. It outputs a ciphertext CT such that only a user who possesses a set of attributes that satisfies the access structure will be able to decrypt the message.

Sign$(PK_s, SK_{u,s}, CT, \mathcal{T}_{sig})$: The sign algorithm is a randomized algorithm that takes as input the public parameter PK_s and signing key $SK_{u,s}$, a ciphertext CT, and a structure $\mathcal{T}_{sig}$. It outputs a signature σ such that only a user who possesses a set of attributes that satisfies the structure $\mathcal{T}_{sig}$ will be able to verify the signature.

Decrypt$(SK_{u,e}, CT)$: The decryption algorithm takes as input a ciphertext CT which contains an access structure $\mathcal{T}_{enc}$ and encryption key $SK_{u,e}$ for user u. It outputs a message m such that only the attributes associate with the encryption key $SK_{u,e}$ satisfy the access structure $\mathcal{T}_{enc}$ associated with the ciphertext CT.

Verify$(PK_s, CT, \mathcal{T}_{sig}, \sigma)$: The verify algorithm takes as input public key for signature PK_s and the owner's signature on ciphertext CT. It returns true such that only the attributes associated with the signature σ satisfy the structure $\mathcal{T}_{sig}$ associated with the ciphertext CT.

5. Construction

We design our privacy preserving authenticated access control scheme for securing data in vehicular communication. This scheme achieves flexible, policy-based access control by extending CP-ABE and combining ABS. In the following section we mainly give the scheme description in detail. We conduct extensive studies to demonstrate that our framework can provide security protection in VANET. Furthermore, we also give a detailed comparison of our scheme with several latest existing schemes.

5.1. Scheme description

5.1.1. System initialization

There are two steps during the system initialization phase: the `CASetup` and the top level `TASetup`. The certificate authority runs the Setup algorithm to create system public parameters and master key:

`ABE.CASetup`(d): Here d is the numbers of the trust authorities. The algorithm chooses a bilinear group G_0 of prime order p with generator g:

$$\begin{aligned} MK_i = (&\mathbb{A}, D_i = g^{(\alpha + r^{\{aa\}})/\beta_i}, \\ &\text{for } 1 \le i \le m, 1 \le j \le n_i : D_{i,j} = g^{r_i^{\{aa\}}} \\ &\cdot H(a_{i,j})^{r_{i,j}^{\{aa\}}}, D'_{i,j} = g^{r_{i,j}^{\{aa\}}}) \end{aligned} \quad (1)$$

Next it will choose two random exponents $\alpha, \beta_i \in Z_p$, $\forall i \in \{1, 2 \ldots d\}$. Here we give an example of 2, and it can be extended to any numbers d. The public key is published as follows:

$$\begin{aligned} &PK_e = (G_0, g, h_1 = g^{\beta_1}, f_1 = g^{1/\beta_1}, \\ &h_2 = g^{\beta_2}, f_2 = g^{1/\beta_2}, e(g,g)^{\alpha}) \end{aligned}$$

and the master key is $MK_0 = (\beta_1, \beta_2, g^{\alpha})$.

`ABS.CASetup`(d): The algorithm chooses suitable cyclic groups G and H of prime order p, equipped with a bilinear pairing $e: G \times H \to G_T$. It also chooses a collision-resistant hash function $\mathcal{H}: \{0,1\}^* \to \mathbb{Z}_p^*$. Then it chooses random generators: $g \leftarrow G$; $h_0, \ldots h_{tmax} \leftarrow H$. The public key is $PK_s = (G, H, \mathcal{H}, g, h_0, \ldots h_{tmax})$.

Trust authority grant: A trust authority is associated with a unique ID TA and a recursive attribute set $\mathbb{A} = \{A_0, A_1, \ldots, A_m\}$, where $A_i = \{a_{i,1}, a_{i,2}, \ldots, a_{i,n_i}\}$ with $a_{i,j}$ being the jth attribute in A_i and n_i being the number of attributes in A_i. When a new authorized trust authority wants to join the system, the certificate authority calls `ABE.TASetup` to generate the master key for TA_i. After getting the master key, TA_i can authorize the next level attribute authorities or users in its domain.

`ABE.TASetup`$(PK_e, MK_0, \mathbb{A})$: The trust authority setup algorithm will choose a random number $r^{\{ta\}} \in \mathbb{Z}_p$ for the trust authority ta, and choose m random numbers $r_i^{\{ta\}} \in \mathbb{Z}_p$, one for each set $A_i \in \mathbb{A}$. And then it selects a random number $r_{i,j}^{\{ta\}} \in \mathbb{Z}_p$ for each attribute $a_{i,j}, 1 \le i \le m$, $1 \le j \le n_i$. It computes the master key MK_i for $TA_i, \forall i \in \{1, 2\}$ as shown in Eq. (1).

`ABS.TASetup`: The algorithm chooses random $a_0, a, b, c \leftarrow \mathbb{Z}_p^*$ and set: $C = g^c; A_0 = h_0^{a_0}; A_j = h_j^a$ and $B_j = h_j^b$ $(\forall j \in [t_{max}])$. The master key of the trust authority is (a_0, a, b), and the public key of the trust authority is $(A_0, \ldots A_{t_{max}}, B_1, \ldots B_{t_{max}}, C)$:.

$$\begin{aligned} SK_{u,e} \text{ or } MK_{i+1} = (&\mathcal{A}, \tilde{D} = D_i f_i^{\tilde{r}^{\{aa\}}}, \\ &\text{for} a_{i,j} \in \mathcal{A} : \tilde{D}_{i,j} = D_{i,j} \cdot g^{\tilde{r}_i^{\{aa\}}} \\ &\cdot H(a_{i,j})^{\tilde{r}_{i,j}^{\{aa\}}}, \tilde{D}'_{i,j} = D'_{i,j} g^{\tilde{r}_{i,j}^{\{aa\}}}) \end{aligned} \quad (2)$$

5.1.2. Key generation

When a new user or a new subordinate trust authority, denoted as TA_{i+1}, wants to join the system, the top-level trust authority denoted as TA_i will first verify whether the new entity is valid. If true, TA_i assigns an attribute set $\mathcal{A} \subset \mathbb{A}$. The master key of TA_i is of the form $MK_i = (\mathbb{A}, D,$ for$1 \le i \le m, 1 \le j \le n_i : D_{i,j}, D'_{i,j})$. The algorithm randomly chooses $\tilde{r}^{\{ta\}} \in \mathbb{Z}_p$ for each user u or trust authority, a random number $\tilde{r}_i^{\{ta\}} \in \mathbb{Z}_p$ for each set $A_i \in \mathcal{A}$, and a random number $\tilde{r}_{i,j}^{\{ta\}} \in \mathbb{Z}_p$ for each $a_{i,j} \in \mathcal{A}$. Then it computes the encryption key for the user or the trust authority as shown in Eq. (2).

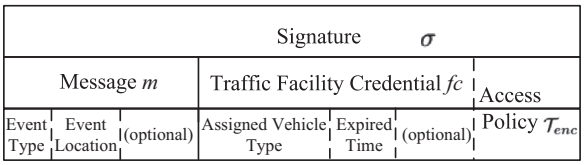

Fig. 2. Message format.

The secret key $SK_{u,e}$ or MK_{i+1} is a secret key of the attribute set. Since the algorithm re-randomizes the key, the key is equivalent to the one received directly from the certificate authority.

`ABS.Key`: The algorithm takes the master key and attribute set as input, then choose random generator $K^{base} \leftarrow G$, then set $K_0 = K_{base}^{1/a_0}; K_i = K_{base}^{1/(a+bi)} (\forall i \in \mathcal{A})$, the signing key is then $SK_{u,e} = (K_{base}, K_0, \{K_i | i \in \mathcal{A}\})$.

5.1.3. Message broadcasting

As shown in Fig. 2, when receiving an emergency event report forwarded by any RSU, TA will generate a message m including event type and event location, also generate a facility credential fc including assigned vehicle type and expired time, then encrypt the credential with access policy $\mathcal{T}_{enc}$ for who could deal with the emergency, finally sign the whole message with policy $\mathcal{T}_{sig}$ in the form of σ, for providing authorization to the recipient vehicle, and finally broadcast it over VANET.

The traffic facility credential fc is encrypted with access policy $\mathcal{T}_{enc}$ in the following encrypt algorithm:

`Encrypt`$(PK_e, fc, \mathcal{T}_{enc})$: The algorithm first chooses a polynomial q_x for each node x (including the leaves) in the tree $\mathcal{T}_{enc}$. These polynomials are chosen in the following way in a topdown manner, starting from the root node R. For each node x in the tree, set the degree d_x of the polynomial q_x to be one less than the threshold value k_x of that node, that is, $d_x = k_x - 1$.

Starting with the root node R, the algorithm chooses a random $s \in \mathbb{Z}_p$ and set $q_R(0) = s$. Then, it chooses d_R other points of the polynomial q_R randomly to define it completely. For any other node x, it sets $q_x(0) = q_{\text{parent}(x)}(\text{index}(x))$ and chooses d_x other points randomly to completely define q_x. The function parent (x) denotes the parent of the node x in the tree. The access tree $\mathcal{T}_{enc}$ also defines an ordering between the children of every node, that is, the children of a node are numbered from 1 to num. The function index (x) returns such a number associated with the node x. Where the index values are uniquely assigned to nodes in the access structure for a given key in an arbitrary manner. 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.

Let Y be the set of leaf nodes in $\mathcal{T}_{enc}$. Then it computes encryption as

$$CT = (\mathcal{T}_{enc}, \tilde{C} = fc.e(g,g)^{\alpha s}, C_i = h_i^s,$$
$$\forall y \in Y: C_y = g^{q_y(0)}, C'_y = H(att(y))^{q_y(0)})$$

For better rescue efficiency, the whole message contains a traffic facility credential that is used to delegate the authority to control traffic facilities. The algorithm takes advantage of $\mathcal{T}_{enc}$ to ensure that only the attributes satisfying the $\mathcal{T}_{enc}$ can decrypt the encrypt message. Using the fc, the assigned vehicle can control traffic signals or other facilities around the area where an emergency has occurred.

Finally, the whole message mm is signed in signing algorithm as shown in Algorithm 1. The signature hides the attributes used to satisfy the predicate and any identifying information about the message sender.

Algorithm 1. `Sign`$(PK_s, SK_{u,s}, mm, \mathcal{T}_{sig})$.

1: Convert $\mathcal{T}_{sig}$ to its corresponding monotone span program $M \in (\mathbb{Z}_p)^{l \times t}$, with row labeling $u: [l] \to \mathbb{A}$.
2: Compute the vector $\vec{v}$ that corresponds to the satisfying assignment.
3: Compute $\mu = \mathcal{H}(mm || \mathcal{T}_{sig})$.
4: Pick random $r_0 \leftarrow \mathbb{Z}_p^*$ and $r_1, \ldots, r_l \leftarrow \mathbb{Z}_p$
5: Compute $Y = K_{base}^{r_0}; S_i = (K_{u(i)}^{v_i})^{r_0} \cdot (Cg^u)^{r_i} (\forall i \in [l])$;
$W = K_0^{r_0}; P_j = \prod_{i=1}^{l} (A_j B_j^{u(i)})^{M_{ij} \cdot r_i} (\forall j \in [t])$.
6: The signature is $\sigma = (Y, W, S_1, \ldots, S_l, P_1, \ldots P_t)$.

5.1.4. Rescue mission execution

After receiving the signed message in a predefined short time period, the message recipient vehicle first verifies the signature by running `Verify`$(PK_s, \sigma, mm, \mathcal{T}_{sig})$ algorithm to verify the signature attached in the data, to ensure the receiving messages coming from the claimed source. Also only the recipients' attributes satisfy the policy in the signature can the recipients verify the signature.

Algorithm 2. `Verify`$(PK_s, \sigma(Y, W, S_1, \ldots, S_l, P_1, \ldots P_t) mm, \mathcal{T}_{sig}>)$.

1: Convert $\mathcal{T}_{sig}$ to its corresponding monotone span program $M \in (\mathbb{Z}_p)^{l \times t}$, with row labeling $u: [l] \to \mathbb{A}$.
2: Compute $\mu = \mathcal{H}(mm || \mathcal{T}_{sig})$.
3: if $Y = 1$, then reject;
4: Otherwise for $j \in [t]$, check the following constraints:
$e(W, A_0) \stackrel{?}{=} e(Y, h_0)$
$\prod_{i=1}^{l} e(S_i, (A_j B_j^{u(i)})^{M_{ij}}) \stackrel{?}{=} \begin{cases} e(Y, h_1) e(Cg^u, P_1), j = 1 \\ e(Cg^u, P_j), j > 1 \end{cases}$ 5:
Return *accept* if all the above checks succeed, and *reject* otherwise.

If the vehicle has the attributes to gain the authority to control the traffic signals/facilities governed by the RSU, it then can run `Decrypt`$(SK_{u,e}, CT)$ algorithm to decrypt the traffic facilities fc.

`Decrypt`$(SK_{u,e}, CT)$: We specify the decryption procedure as a recursive algorithm. We first define a recursive algorithm `DecryptNode`$(CT, SK_{u,e}, x)$ that takes as input a ciphertext CT, a private key, which is associated with a set of attributes $\mathcal{A}$ and a node x from $\mathcal{T}_{enc}$.

If the node x is a leaf node then we let $i = att(x)$ and define as follows: If $i \in \mathcal{A}$, then

$$\text{DecryptNode}(CT, SK_{u,e}, x) = \frac{e(D_{i,j}, C_x)}{e(D'_{i,j}, C'_x)} = e(g,g)^{rq_x(0)}.$$

If $i \notin \mathcal{A}$, we define $\text{DecryptNode}(CT, SK_{u,e}, x) = \perp$.

We now consider the recursive case when x is a non-leaf node. The algorithm DecryptNode then proceeds as follows: For all nodes z that are children of x, it runs

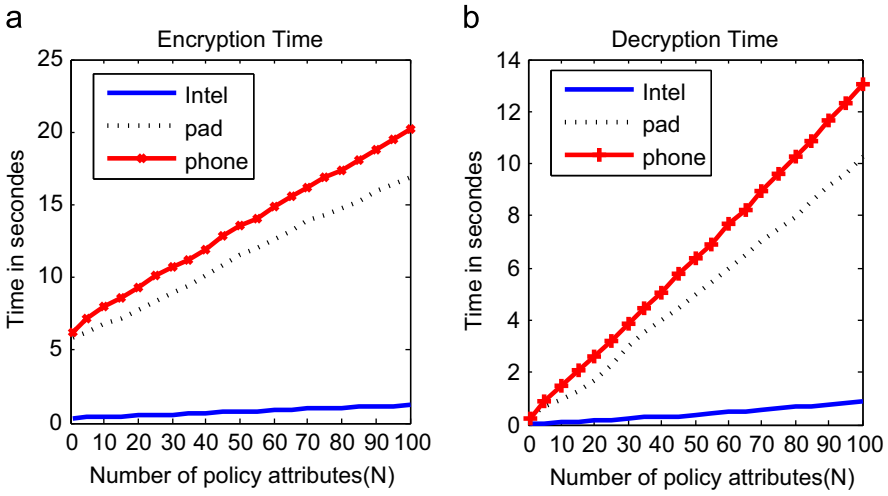

Fig. 3. Performance of CP-ABE algorithm.

$\texttt{DecryptNode}(\mathrm{CT}, \mathrm{SK}_{u,e}, z)$ and stores the output as F_z. Let $\mathcal{A}_x$ be an arbitrary k_x-sized set of child nodes z such that $F_z \neq \perp$. If no such set exists then the node was not satisfied and the function returns $\perp$. Otherwise, we compute

$$F_x = \prod_{z \in \mathcal{A}_x} F_z^{\Delta_{i,\mathcal{A}'_x}(0)}, \quad \text{where } \mathcal{A}'_x = \{index(z): z \in \mathcal{A}_x\}$$

$$= \prod_{z \in \mathcal{A}_x} (e(g,g)^{r \cdot q_z(0)})^{\Delta_{i,\mathcal{A}'_x}(0)}$$

$$= \prod_{z \in \mathcal{A}_x} (e(g,g)^{r \cdot q_{parent(z)}(index(z))})^{\Delta_{i,\mathcal{A}'_x}(0)}$$

$$= \prod_{z \in \mathcal{A}_x} e(g,g)^{r \cdot q_x(i) \cdot \Delta_{i,\mathcal{A}'_x}(0)}$$

$$= e(g,g)^{r \cdot q_x(0)} \quad \text{(using polynomial interpolation)}$$

and return the result.

Now that we have defined our function DecryptNode, we can define the decryption algorithm. The algorithm begins by simply calling the function on the root node R of the tree $\mathcal{T}_{enc}$. If the tree is satisfied by $\mathcal{T}_{enc}$ we set $\mathrm{A} = \texttt{DecryptNode}(\mathrm{CT}, \mathrm{SK}_{u,e}, r) = e(g,g)^{r q_R(0)} = e(g,g)^{rs}$. The algorithm now decrypts:

$$\tilde{C} / (e(D_i, C_i)/A) = \tilde{C} / (e(h_i^s, g^{(\alpha + r)/\beta_i})/e(g,g)^{rs}) = fc.$$

Then, the vehicle can get the traffic facility credential fc to control the traffic signals/facilities with the help of nearest RSU.

6. Implementation

In this section, we demonstrate the performance analysis based on practical implementation and give the complexity analysis in terms of the computational overhead that put on each operation. Also, we give a detailed comparison of our scheme with several latest existing works.

6.1. Performance analysis

In order to evaluate the performance of our scheme, we use libfenc library [26], which uses key encapsulation mechanism, and adopt a 224-bit MNT elliptic curve from the Stanford Pairing-Based Crypto library [27] to implement our scheme in software. Our experiments are done on three dedicated hardware platforms: a 3.20 GHz Intel Core CPU with 4 GB of RAM running 32-bit Linux Kernel version 3.2.0, a 1.3 GHz ARM-based OPPO R829T with 960.54 MB of RAM running Android OS, and a 1.3 GHz ARM-based Nexus ME370T with 1 GB of RAM running Android OS.

In a CP-ABE scheme, the ciphertext size and the encryption/decryption time depend on the complexity of access policy in the ciphertext, and they increase linearly with the growing number of attributes in the access policy. To illustrate this, we randomly choose 100 attributes, and each attribute is defined as A_i. Then we build the most complex policies as the form (A_1 AND A_2 AND…AND A_n) of which the values of N increase from 1 to 100 in policy. Also we construct a corresponding standard decryption key that contains exact N attributes. This approach ensures that all the attributes are involved in the encryption and decryption phases.

Fig. 3 demonstrates the encryption and decryption time with the increase of access policy attributes. We give the most complex policies in the experiments, whereas the number of attributes may be just no more than ten in VANET network. As shown in the figure, we can see that our scheme is comparatively efficient with a certain number of attributes in various devices, even in mobile devices with limited resources. We believe that ABE is crucial for achieving data privacy in the internet of thing, in contexts such as Smart Homes [28] and Smart Cities [29] due to its advantages over traditional public key encryption.

6.2. Computational complexity analysis

The computational complexities which are included in the main steps are summarized in Table 2.

Table 2
Computational complexity.

Operation	Complexity
System setup	$O(2N)$
Create the message	$O(2\|Y\|+lt)$
Read the message	$O(2\|Y\|)$
Get the credential	$O(2lt)$

Table 3
Comparison of our scheme with existing schemes.

Schemes	Access policy expressiveness	Type of authorities	Anonymous authentication
[10]	Restricted	One CA	No
[12]	Complex	One CA, multi-RSUs	No
Ours	Flexible	One CA, multi-hierarchical RSUs	Yes

System setup: When the system is set up, the certificate authority selects a bilinear group and some random numbers. When PK and MK for encryption and signature are generated, there will be several exponentiation operations. So the computational complexity of system setup is $O(1)$. For trust authority or new user granting, the computation of MK_i consists of two exponentiations for each attribute in the operation, and the computational complexity is $O(2N)$, where N is the number of the attributes in the set of new user or trust authority.

Create a message: In this operation, the message sender vehicle needs to encrypt the facility credential using CP-ABE and sign the whole message with ABS. Encrypting the facility credential with a tree access structure $\mathcal{T}_{enc}$ consists of two exponentiations per leaf node in $\mathcal{T}_{enc}$. The computational cost of `ABS.sign` grows linearly with the size of access structure's matrix $\{l \times t\}$, which is the monotone span program that converted from its corresponding access structure, so the computational complexity is $O(2|Y|+lt)$, where Y denotes the leaf nodes of $\mathcal{T}_{enc}$.

Read the message: In this operation, the computational overhead generated by one operation of `ABS.verify`.

Get the credential: In this operation, the message recipient first runs Decrypt algorithm. The Decrypt algorithm consists of two pairing operations for every leaf node used to satisfy the tree, one pairing and one exponentiation for each node on the path from the leaf node to the root. So the computational complexity varies depending on the access tree and key structure.

6.3. Discussion

Recall that our privacy preserving access control scheme is extended from CP-ABE [11] with a hierarchical structure using a delegation algorithm and ABS [15] with multi-authorities. We prove the security of our scheme directly based on the security of CP-ABE and ABS. Thus, our scheme is expected to have the same security property as them, which has been proven to be secure under the generic bilinear group model [11] and the random oracle model [15].

In the following, we analyze security properties of our proposed scheme, whose focus is to provide fine-grained access control, full delegation of RSUs and to efficiently share confidential data among vehicles. Our proposed scheme achieves both security and scalability. Our hierarchical attribute-based access control scheme inherits not only scalability due to its hierarchical structure, but also flexibility access control in supporting message authentication. We compare our scheme with existing schemes in Table 3 and show that our scheme is flexible and scalable.

Fine-grainedness of access control: In our proposed scheme, the message sender vehicle is able to define and enforce expressive and flexible access structure for the selected vehicles. Whereas the paper in [10] handles only one type of access policy, which is a very restrictive assumption. Specifically, our scheme also exploits attribute-based signature for supporting anonymous authentication on the message.

Full delegation of RSUs: There is no coordination among different RSUs in [10]. Although it can communicate with one another across domains of different RSUs in [12], the RSUs are not scalable. In our scheme, multiple RSUs are delegated from the CA and structured in a hierarchical manner.

Data confidentiality: Our data is encrypted using ciphertext-policy attribute based encryption, security of the proposed scheme is merely relied on the security of hierarchical CP-ABE. Actually, the standard CP-ABE is provably secure under generic group heuristic [11].

7. Conclusion

Recently, security and privacy issues in VANET network have attracted considerable attention. In this paper, we introduce a hierarchical attribute-based access control for realizing scalable and fine-grained access control in transmitted messages over VANET. The scheme not only provides fine-grained access control but also authenticates vehicles who could have the privilege to control traffic lights/signals. The comparison between existing latest works shows that this scheme achieves a good performance on the efficiency of access control in VANET network.

Our future work will be on the investigation of more application scenarios for message broadcasting in different VANET configurations.

Acknowledgment

This research is supported in part by the following funds: National Natural Science Foundation of China (Grant no. 61472113 and 61304188), Zhejiang Provincial Natural Science Foundation of China (Grant no. LZ13F020004 and LR14F020003), Zhejiang Provincial Science and Technology Innovation Program (Grant no. 2013TD03), and Joint Funds of the National Natural Science Foundation of China (Grant no. U1404605).

References

[1] Y. Xia, X. Li, Z. Shan, Parallelized fusion on multisensor transportation data: a case study in cyberITS, Int. J. Intell. Syst. 28 (6) (2013) 540–564.

[2] Y. Xia, Y. Liu, Z. Ye, W. Wu, M. Zhu, Quadtree-based domain decomposition for parallel map-matching on gps data, in: Proceedings of the 15th International Conference on Intelligent Transportation Systems (ITSC), Anchorage, AK, IEEE, 2012, pp. 808–813.

[3] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, T. Weil, Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions, IEEE Commun. Surv. Tutor. 13 (4) (2011) 584–616.

[4] M. Whaiduzzaman, M. Sookhak, A. Gani, R. Buyya, A survey on vehicular cloud computing, J. Netw. Comput. Appl. 40 (2014) 325–344.

[5] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, in: Advances in Cryptology, Springer, Berlin Heidelberg, 1985, pp. 10–18.

[6] S.H. Kim, B.H. Kim, Y.K. Kim, D.H. Lee, Auditable and privacy-preserving authentication in vehicular networks, in: Proceedings of the Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM), Valencia, IEEE, 2008, pp. 19–24.

[7] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, A. Lioy, Efficient and robust pseudonymous authentication in vanet, in: Proceedings of the Fourth ACM international workshop on Vehicular ad hoc networks, ACM, New York, 2007, pp. 19–28.

[8] X. Sun, X. Lin, P.-H. Ho, Secure vehicular communications based on group signature and id-based signature scheme, in: Proceedings of IEEE International Conference on Communications (ICC), Glasgow, IEEE, 2007, pp. 1539–1545.

[9] Y. Xi, K.-W. Sha, W.-S. Shi, L. Schwiebert, T. Zhang, Probabilistic adaptive anonymous authentication in vehicular networks, J. Comput. Sci. Technol. 23 (6) (2008) 916–928.

[10] D. Huang, M. Verma, ASPE: attribute-based secure policy enforcement in vehicular ad hoc networks, Ad Hoc Netw. 7 (8) (2009) 1526–1535.

[11] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based encryption, in: IEEE Symposium on Security and Privacy, 2007, pp. 321–334.

[12] S. Ruj, A. Nayak, I. Stojmenovic, Improved access control mechanism in vehicular ad hoc networks, in: Ad-hoc, Mobile, and Wireless Networks, Paderborn, Germany, Springer, 2011, pp. 191–205.

[13] A. Lewko, B. Waters, Decentralizing attribute-based encryption, in: Advances in Cryptology (EUROCRYPT), Tallinn, Estonia, Springer, 2011, pp. 568–588.

[14] G. Yan, D.B. Rawat, B.B. Bista, Towards secure vehicular clouds, in: Proceedings of the Sixth International Conference on Complex, Intelligent and Software Intensive Systems (CISIS), Palermo, IEEE, 2012, pp. 370–375.

[15] H. Maji, M. Prabhakaran, M. Rosulek, Attribute-based signatures, in: Proceedings of the 11th International Conference on Topics in Cryptology, 2011, pp. 376–392.

[16] L. Zhang, Y. Han, Y. Yang, M. Song, S. Yan, Q. Tian, Discovering discriminative graphlets for aerial image categories recognition, IEEE Trans. Image Process. 22 (12) (2013) 5071–5084.

[17] L. Zhang, M. Song, X. Liu, J. Bu, C. Chen, Fast multi-view segment graph kernel for object classification, Signal Process. 93 (6) (2013) 1597–1607.

[18] L. Zhang, Y. Gao, K. Xia, Yingjieand Lu, J. Shen, R. Ji, Representative discovery of structure cues for weakly-supervised image segmentation, IEEE Trans. Multimedia 16 (2) (2014) 470–479.

[19] L. Zhang, M. Song, Q. Zhao, X. Liu, J. Bu, C. Chen, Probabilistic graphlet transfer for photo cropping, IEEE Trans. Image Process. 22 (2) (2013) 802–815.

[20] D. Huang, X. Hong, M. Gerla, Situation-aware trust architecture for vehicular networks, IEEE Commun. Mag. 48 (11) (2010) 128–135.

[21] H. Zhu, X. Lin, R. Lu, P.-H. Ho, X. Shen, AEMA: an aggregated emergency message authentication scheme for enhancing the security of vehicular ad hoc networks, in: Proceedings of IEEE International Conference on Communications (ICC), Beijing, IEEE, 2008, pp. 1436–1440.

[22] I.T.S. Committee, et al., IEEE Trial-Use Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages, IEEE Vehicular Technology Society Standard.

[23] X. Liu, Y. Xia, S. Jiang, F. Xia, Hierarchical attribute-based access control with authentication to outsourced data in cloud computing, in: Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Melbourne, Australia, IEEE, 2013, pp. 477–484.

[24] F. Zhao, T. Nishide, K. Sakurai, Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems, Information Security Practice and Experience, 2011, pp. 83–97.

[25] S. Ruj, M. Stojmenovic, A. Nayak, Privacy preserving access control with authentication for securing data in clouds, in: Proceedings of the 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), 2012, pp. 556–563.

[26] A.A.M. Green, M. Rushanan, libfenc: The Functional Encryption Library, ⟨http://code.google.com/p/libfenc/⟩.

[27] B. Lynn, Stanford Pairings-Based Crypto Library, ⟨http://crypto.stanford.edu/pbc/⟩.

[28] J. Zhang, Q. Li, E.M. Schooler, iHEMS: an information-centric approach to secure home energy management, in: Proceedings of IEEE Third International Conference on Smart Grid Communications (SmartGridComm), Tainan City, TanWan, IEEE, 2012, pp. 217–222.

[29] M. Ion, J. Zhang, E.M. Schooler, Toward content-centric privacy in ICN: attribute-based encryption and routing, in: Proceedings of the ACM SIGCOMM Conference, Hong Kong, ACM, 2013, pp. 513–514.