Adaptive Multimedia Data Forwarding for Privacy Preservation in Vehicular Ad-Hoc Networks

Yingjie Xia, *Member, IEEE*, Wenzhi Chen, *Member, IEEE*, Xuejiao Liu, Luming Zhang, *Member, IEEE*, Xuelong Li, *Fellow, IEEE*, and Yang Xiang, *Senior Member, IEEE*

***Abstract*— Vehicular ad-hoc networks (VANETs) have drawn much attention of researchers. The vehicles in VANETs frequently join and leave the networks, and therefore restructure the network dynamically and automatically. Forwarded messages in vehicular ad-hoc networks are primarily multimedia data, including structured data, plain text, sound, and video, which require access control with efficient privacy preservation. Ciphertext-policy attribute-based encryption (CP-ABE) is adopted to meet the requirements. However, solutions based on traditional CP-ABE suffer from challenges of the limited computational resources on-board units equipped in the vehicles, especially for the complex policies of encryption and decryption. In this paper, we propose a CP-ABE delegation scheme, which allows road side units (RSUs) to perform most of the computation, for the purpose of improving the decryption efficiency of the vehicles. By using decision tree to jointly optimize multiple factors, such as the distance from RSU, the communication and computational cost, the CP-ABE delegation scheme is adaptively activated based on the estimation of various vehicles decryption overhead. Experimental results thoroughly demonstrate that our scheme is effective and efficient for multimedia data forwarding in vehicular ad-hoc networks with privacy preservation.**

***Index Terms*— Attributed-based encryption, outsourcing decryption, multimedia message, vehicular ad-hoc networks, decision tree.**

I. Introduction

VEHICULAR ad-hoc networks utilize the capability of wireless communications protocols to confidently disseminate sensitive information among peers, restricted to a particular geographic area, as well as the advanced safety-assets, on road sensors and sophisticated driving-assistance features of top-generation vehicles. Such a complement are not only oriented to offer a more pleasant in-car experience for driver and passengers, but also are intended to introduce autonomous and efficient ways to prevent hazardous situations on roads. Such vehicular ad-hoc networks deployment should follow a primary task based on reliable message handling for sharing traffic conditions, weather variables, driving assistance, navigation support, entertainment content multicasting and even spurious notifications. Vehicular ad-hoc networks typically consist of on-board Units (OBUs) installed in the vehicles and road side units (RSUs) deployed at the roadside. That is to say, vehicular ad-hoc networks are constituted of two layers networks, the RSUs networks with fixed topology and vehicular flow networks (OBUs networks) with temporal topology. They support the cooperative communications of high speed between vehicles and RSUs. The widespread deployment of vehicular ad-hoc networks largely depends on a secure and reliable mechanism to provide effective data services in transportation systems. Many security issues have been raised in vehicular ad-hoc networks [1]. Among them, data integrity and confidentiality are the most essential.

The integration of social networks into vehicular ad-hoc networks provides some novel applications, mainly devoted to safety, and entertainment [2], [3]. As an instance, let us consider a driver receiving a warning message about an accident occurred on a near place. Under emergency circumstances (e.g., traffic accident, traffic congestion, natural disaster, fire), safety-related messages communication in vehicular ad-hoc networks could convey early warning messages to the vehicles. Multimedia messages, such as audio and video, are effective in vehicular communication since they are more descriptive, comprehensive, and user-friendly, compared with the plain text based services. Also, with the popularity of mobile devices, the multimedia messages like video and photo retargeting has became a useful technique [4], [5]. For instance, videos describing an accident can provide precise and live clues, which is helpful to make a timely and accurate decision. According to these prompt and precise information, vehicles can conveniently select appropriate routes toward driving safety and efficiency. On the other side, trusted people sharing the same trip, or neighborhood, can discuss about common interests (e.g., students going to school talk about lectures) [6], [7]. Therefore, in vehicular ad-hoc networks, it is valuable to provide tailored access services to guarantee that the right messages can be delivered to the right vehicles.

Manuscript received February 24, 2016; revised May 29, 2016, August 17, 2016, and October 31, 2016; accepted January 8, 2017. This work was supported in part by the National Natural Science Foundation of China under Grant 61502134, Grant 61472113, and Grant 61304188; in part by the Zhejiang Provincial Natural Science Foundation of China under Grant LZ13F020004 and Grant LR14F020003; and in part by the Zhejiang Provincial Science and Technology Innovation Program under Grant 2013TD03. The Associate Editor for this paper was J. Cao.

Y. Xia and W. Chen are with the College of Computer Sciences, Zhejiang University, Hangzhou, 310027 China (e-mail: xiayingjie@zju.edu.cn).

X. Liu is with the Institute of Service Engineering, Hangzhou Normal University, Hangzhou, 311121 China.

L. Zhang is with the School of Computing, National University of Singapore, 119077 Singapore.

X. Li is with the State Key Laboratory of Transient Optics and Photonics, Xi'an Institute of Optics and Precision Mechanics, Chinese Academy of Sciences, Xi'an, 710119 China.

Y. Xiang is with the School of Information Technology, Deakin University, Burwood, VIC, 3125 Australia.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TITS.2017.2653103

To ensure the security of message dissemination in vehicular communication, the conventional encryption mechanism might be unsuitable. This is because the traditional public key infrastructure requires to encrypt each message with the recipient vehicle's public key. That is to say, if the encrypted message is shared by multiple vehicles, the message would be encrypted many times into different versions of ciphertexts. This fails to meet the real-time requirement of message dissemination. In other words, symmetrical encryption methods require extra communication cost and security risks to exchange session keys between message senders and recipients. In summary, real-time access control of message dissemination with privacy preservation is a tough challenge for vehicular communication in the vehicular ad-hoc network.

A large number of works have been reported. Huang and Verma [8] introduced the ciphertext-policy attribute based encryption (CP-ABE) [9] in vehicular ad-hoc networks. Each vehicle has its capabilities and access rights according to its attributes. Afterward, only vehicles with attributes satisfying the access policy can decrypt the broadcast messages to preserve data privacy. Experiments in [10] validate that, for an ABE ciphertext containing 100 attributes, the decrypting on a mobile terminal device with a high computational power would take nearly 30 seconds, followed by a significant consumption of battery power. Generally speaking, OBUs have resource-limited processors to make vehicular ad-hoc networks cheaply available [11]. Solutions based on traditional CP-ABE are frustrated by the limited resources of OBUs for multimedia messages. Vehicular network requires advanced cryptography to balance the security requirements of algorithm and the computational cost of OBUs.

Moreover, as the vehicular ad-hoc networks combines the RSUs networks with fixed topology and vehicular flow networks with temporal topology, we can infer that a vehicle always moves between different RSUs, rather than under the same RSU. In other words, the information which each OBU has gotten is derived from different RSUs dynamically along with time. For example, since each RSUs coverage is limited and the decryption takes time, some OBUs begin to receive information when they are moving out of one RSUs coverage. In this situation, the OBU are likely to receive incomplete information which may reduce the user experience. Therefore, predicting when and which RSU involving disseminate the message in advance based on the vehicular ad-hoc networks two layers topology, will offer users better experience. It is essential to develop a complete encrypt/decrypt scheme for the vehicular ad-hoc networks. To tackle the highly dynamic topology in vehicular ad-hoc networks, previous work mostly focused on reliable dissemination of short plain text message using a minimal bandwidth. Multimedia data are not supported because of their size and heterogeneity. Thus, without proper dissemination controlling strategy they may cause severe network congestion. The situation becomes more serious when the security technique is employed. Generally, multimedia messages should be delivered to all the dedicated vehicles in vehicular ad-hoc networks both reliably and efficiently. For all the messages, RSUs broadcast them to the vehicles within the transmission range. We assume that the traffic-related multimedia messages are uniformly one hop broadcast. Based on the message attributes, e.g., data type, size, contents, we propose to adaptively determine whether to conduct direct encryption/decryption, delegated encryption/decryption, or improve the computational efficiency.

The contributions of this paper can be summarized as:

1) We propose a privacy-preserving message dissemination scheme with policy enforcement in vehicular ad-hoc networks, by encrypting messages using well-defined access policy generated from the features of traffic-related messages.
2) We present the construction of attribute-based encryption with delegating decryption algorithm. The computation largely depends on vehicle delegated to the nearest RSU without violating the privacy.
3) An adaptive message forwarding scheme is proposed for decryption. It guarantees that the right vehicles receive the right messages in the RSU transmission range.

This paper is organized as follows. Sec II overviews some related work. We then introduce the technique preliminaries including multi-layer social networks, ciphertext-policy attribute-based encryption and decision tree construction in Sec III. In Sec IV, we formulate our developed system and introduce the corresponding assumption. The detailed system construction is elaborated in Sec V. In Sec VI, we present the simulation evaluation of our proposed system. Sec VII concludes.

II. Related Work

Basically, a vehicular ad-hoc networks(VANET) is comprised of two fundamental parts i.e., (i) a vehicular ad-hoc network(VANET) that represents the physical layer, and (ii) a social network framework running on top of such a physical vehicular network [12]. A VANET is an ad-hoc network that changes over time, while a social network consists of users, social ties or relationships among users, and common interests. When designing message dissemination protocols, several factors need to be considered as main issues related to vehicular ad-hoc network, such as the lack of integration of several technologies together with sensors, of which the security and privacy aspects still remain one of the most significant issues [1], [13]–[16].

A. The Security Issues in VANET

In the area of security and privacy of vehicular ad-hoc networks, a number of research works have been done on anonymous authentication, conditional privacy preservation, and key management, and etc to ensure security and privacy.

A large body of schemes make use of pseudonyms [17]–[19] or anonymous credentials [20]. With the anonymous schemes, a huge set of anonymous keys are preloaded in the vehicle, and each vehicle randomly takes one of the keys in the set to sign a message. And the authority simply keeps all the anonymous certificates of all the vehicles in order to maintain

[1]The mobile device in our implementation is a 412MHz iPhone with 128MB RAM.

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

the traceability. Once a malicious message is detected, it will leads to tremendous complex work for the authority to find the real identity vehicle related to the message in a large database. Instead of relying on a huge storage space at the vehicle as most of the previously anonymous-based schemes did, another approach is to deploy signature-based technique to achieve anonymous authentication, such as group signature, ring signature and identity-based signature. Sun *et al.* proposed a group signature and identity-based signature scheme to meet the unique requirements of vehicular communication networks [21]. In their scheme, group signature is used to secure the communication between OBUs and OBUs, while identity-based cryptography is used to authenticate the message sent by RSUs. The designated confirmer signatures are presented to confirm or deny an alleged undeniable signature [22].

In vehicular networks anonymous message authentication is a double-edge sword. A well-behaved vehicle needs necessary privacy protection mechanism, while a maliciously-behaved vehicle may abuse the privacy to damage the regular driving environment. Therefore, the anonymous message authentication in vehicular networks should be conditional [23], such that a trusted authority can track a targeted vehicle and collect the messages it has disseminated when necessary, even though it can not be traced by the public. To address the condition privacy preserving problems for secure vehicular communications, Lu *et al.* presented an efficient conditional privacy preservation (ECPP) protocol by the generation of on-the-fly short-time anonymous key generation between OBUs and RSUs [23], which can provide anonymous authentication and privacy tracking while minimizing the required storage for short-time anonymous keys.

Key management plays an important role to help authenticate messages, identify valid vehicles, and remove malevolent vehicles for VANET security. In order to build key management mechanisms that allow senders to establish and update keys for security-sensitive operations, Studer *et al.* propose a key management scheme based on temporary anonymous certified keys (TACKs) [11], which can prevent eavesdroppers from linking a vehicle's different keys and provide timely revocation of misbehaving participants.

Thus, ensuring secure and flexible access control is still challenging in message dissemination in vehicular ad-hoc networks.

B. Data Dissemination in VANET

Establishing trust among drivers is still a challenge, and security and privacy aspects need to be deeply investigated in VANETs. Vehicular communications can be considered as the "the first social network for automobiles", since each driver can share data with other neighbors. In order to provide more advanced and innovative applications, some researchers exploit mobility aspects, and basics of traditional social networks to create novel approaches of data dissemination in vehicular ad-hoc network.

In order to establish the trust of message exchange in vehicle communication, De Oliveira *et al.* propose the use of certificates to exchange cryptographic material in daily relationships, like meeting with friends [24]. In this way, users in the network establish a trust degree, and reputation can become a reward for users with good behavior in forwarding of traffic information. Lu et al. propose a novel Social-based PRivacy-preserving packet forwardING (SPRING) protocol for vehicular networks [25]. SPRING exploits the concept of deploying RSUs at high social intersections, so that RSUs can assist cars in packet forwarding, by temporarily storing packets via V2I communications, whenever next-hop forwarders are not available for retransmissions. This approach also provides a conditional privacy preservation, and resists most attacks existing in vehicular networks. Another work is [26], where a privacy-preserving data dissemination approach for mobile social networks is presented.

With regards to securely dissemination of data in VANET, these schemes take advantage of certificate or social relationship to establish trust among the vehicles. For the certification mechanism, the cars should share keys through direct contacts between two acquaintances that warrant their identity, which is inconvenient and insecure as key sharing so frequently may sometimes leak some information. We also note that it is difficult for these techniques to achieve fine-grained access control in the process of data dissemination.

C. Access Control Scheme in VANET

Establishing access control by means of well-known public key infrastructure (PKI) certificates is an effective method. The use of certificates can provide one-to-one message confidentiality between vehicles. However, it can not enforce fine-grained access control for many receivers in dynamic vehicular communication networks. In addition, multimedia messages needs to be considered, since they can convey more intuitive information for broadcasting to the nearby vehicles, such as warning clues to the vehicles about an emergency situation.

Yeh *et al.* adopted a fuzzy identity-based encryption, based on which an attribute-based access control system (ABACS) is designed for emergency services, including sending alert messages and selecting rescue vehicles in the vehicular ad-hoc networks [27]. Compared with the existing PKI scheme, extensive studies have been conducted to calculate the computational delay. Besides, the transmission overhead can be reduced by an attribute-based encryption. But these schemes cannot support complex policy definition with predicates. Huang and Verma introduced the ciphertext-policy attribute based encryption [9] in the vehicular ad-hoc networks, aiming to construct an attribute-based security policy enforcement (ASPE) [8], [28]. They assumed that RSUs are free from the requirement that the key management in each group is achieved by the RSU within their scope. Sushmita *et al.* [29] presented an improved access controlling scheme in the presence of compromised RSU, by adopting the decentralized attribute based encryption method. However, most of the existing ABE schemes require a large number of exponentiations during decryption. Along with the complexity of access policy, the computational complexity of decryption increases linearly, which is a bottleneck limiting its application.

To alleviate the computational burden, some work have been proposed to improve the decryption efficiency of

CP-ABE [10], [30]–[32]. Green *et al.* [10] introduced an outsourced decryption of ABE cipheretext and further proposed a transformation key (TK) to the proxy by key blinding. Zhou and Huang [31] presented a privacy preserving cipher policy attribute-based encryption (PP-CP-ABE) scheme to protect user data and outsourced the encryption/decryption computation to the cloud. However, these methods impose a heavy computational and communication burden during data encryption/decryption delegation. More specifically, the set of outsourcing keys are generated and issued by the data owner [30]. TK is transferred from user to proxy each time when the user intend to decrypt [10]. These schemes may not perform satisfactorily on the vehicular ad-hoc networks, which bring extra computation and communication for OBU in the vehicle.

In addition, it is important to maintain reliable messages reception, high messages reachability and low end-to-end communication delays. Aiming at these, we focus on improving the efficiency of message decryption using CP-ABE and propose an adaptive forwarding scheme for message decryption, by encoding multiple factors including message data type, message size, vehicles location.

III. Technique Preliminaries

In this section, we introduce the background of basic techniques in our scheme.

A. Multi-Layer Vehicular Network

It is important to take multi-layer features into account to try to improve our understanding of vehicular ad-hoc networks. Multi-layer networks include multiple subsystems and layers of connectivity, in which a set of entities interact with each other in complicated patterns that can encompass multiple types of relationships, change in time and include other types of complications [33]. In this paper, we present a general two-layered network to describe the typical vehicular ad-hoc networks which is consist of RSUs with fixed topology and OBUs with temporal topology. Such a vehicular ad-hoc networks is more realistic and possesses some properties of social networks, such as a heavy-tailed degree distribution, the small-world property, containing nodes that play central roles and/or have modular structures. The vehicular ad-hoc networks brings new challenges in cooperating topology dynamics with secrity and integrity of communicating data.

B. Attribute-Based Encryption

As introduced by Waters *et al.* [9], [34], ciphertext-policy attribute-based encryption(CP-ABE) is a promising cryptographic tool for access control on encrypted data. It allows data owner to encrypt data by defining an access policy over attributes, thereby only users associated with attributes satisfying the policy can decrypt the data. In the literature, a variety of variants of ABE schemes [35]–[40] in different settings have been proposed, including non-monotonic access structures, user accountability, attribute revocation, security proof and etc.

In our implementation, ABE and its variant delegated ABE are adopted to protect the privacy of disseminated messages.

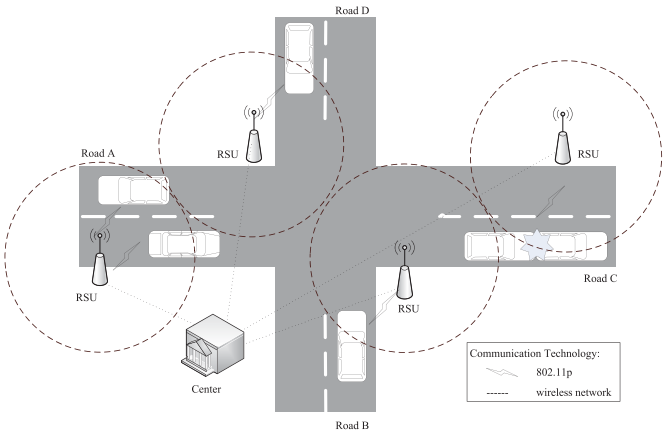


Fig. 1. System Model.

C. Decision Tree

Decision tree is a non-parametric supervised learning model popularly used for classification and regression [41]. The objective is to predict the target variable by learning simple decision rules inferred from the data features. It is effective in approximating discrete-valued functions, robust to noisy data, and capable of learning disjunctive expressions. The C4.5 tree is one of the well-known decision tree in the literature.

In our implementation, we use the C4.5 tree to determine the message encryption, by adopting the ABE or delegated ABE based on the features of traffic-related messages.

IV. System Model and Problem Formulation

A. System Model and Assumption

In vehicular ad-hoc networks, as shown in Fig.1, there are three main components, trusted center (TC), roadside units (RSUs) along the road, and on-board units (OBUs) equipped on the running vehicles. Vehicles can communicate with each other with the nearest RSUs using dedicated short range communication (DSRC). The communication is based on the IEEE 802.11p [42]. It works in 5.9 GHz band with a bandwidth of 75 MHz and a range of 500 meters.

The RSUs are installed across the roads to provide infrastructure support for communication points to and from a WAN, e.g., Internet.

The TC is comprised of multiple modules, including trusted authentication, message encryption, message dispatch, and etc. The trusted authentication module controls the registration of both immobile RSUs and mobile OBUs, managing system attributes, generating and distributing security keys for the vehicles. The TC verifies message and then estimates the transmission range of the message, i.e., broadcasting messages to vehicles in the affected roads. After this, the TC encrypts the messages with the corresponding attributes of vehicles.

RSUs function as the communication relays for vehicle to infrastructure (V2I) communication, which sends the messages into the road network in a broadcast way. Each RSU maintains its local learning knowledge base and makes adaptive decision in sending the ciphertext messages to the vehicles. It decides whether to conduct most of the decryption for vehicles, by

encoding multiple factors, e.g., the ciphertext size and the distance between vehicles and RSUs.

We identify each running vehicle with OBUs by a set of attributes related to the vehicle. Particularly, we divide the attributes into two types, persistent attributes and dynamic attributes. Persistent attribute values remain constant, e.g., vehicle type, color, brand, and etc. Comparatively, dynamic attribute values change frequently, such as road, direction, location of the vehicle, and etc. We assume that each vehicle is equipped with devices like tamper resistance to store private keys, as introduced in [28].

Our method is also based on the assumption that TC is a fully trusted organization and RSUs are honest-but-curious infrastructures. More specifically, the RSUs carry out the computations delegated by the vehicle and infer the privacy information additionally. But they fail to recover the encrypted data.

B. Problem Formulation

To efficiently disseminate messages to select vehicles in vehicular ad-hoc networks, we formulate the above problem focusing on the requirements of security and performance.

An attacker may acquire the policy encrypted messages by injecting, altering, or replaying after the message is released. At the same time, the attacker may collude with other vehicles to access an encrypted message. Based on these, we identify the security requirements described as follows.

1) Privacy preserving is a major security requirements in the vehicular ad-hoc networks [43]. The vehicles without security keys satisfying the access policy of the messages must be prevented from accessing in the Vehicular ad-hoc networks.
2) Policy Enforcement. Messages should be constrained by the access policy in ciphertexts and be delivered selectively to the vehicles, without disclosing any content of the policy and the message. Due to the inseparable relationship between an OBU equipped in the vehicle and its user, social-based relationship and mobility aspects of vehicles have been exploited in vehicular ad-hoc network.

Since the message contents are multimedia, it is necessary to achieve efficient encryption/decryption computation at the vehicle. The necessary cryptographic operations by OBUs should be designed in lightweight according to the message types, as they hold resource-limited processors. In addition, the new model should not introduce significant communication overhead.

V. The Proposed Scheme

In this section, we present the CP-ABE based adaptive multimedia data forwarding scheme for privacy preservation in vehicular ad-hoc networks.

A. Vehicle Attestation and Registration

`Setup`(λ, U): In the system setup, we employ security parameter λ and attribute set U as the input. Also, the public key and master secret key are the output. The algorithm first chooses a group $\mathbb{G}$ with prime order p and a generator g from that group. Then, it chooses a large number of group elements $h_1, \ldots, h_U \in \mathbb{G}$ associated with each attribute of the attribute set U. Besides, the system chooses two exponents in $\mathbb{Z}_p$ randomly, i.e., $\alpha_1 \in \mathbb{Z}_p$, $\alpha_2 \in \mathbb{Z}_p$, and let $\alpha = (\alpha_1 + \alpha_2) \bmod p$. Finally, the public key PK is denoted as

$$g, e(g,g)^{\alpha}, g^{a}, h_1, \ldots, h_U.$$

The master secret key is represented as $\mathrm{MK} = \alpha_1, \alpha_2, \alpha$.

Algorithm 1 OBU Attestation and Registration

1: **for** each vehicle v moves across RSU **do**
2: Vehicle $(LN_v)_{PK_{RSU}} \rightarrow$ RSU
3: RSU gets LN_v by SK_{RSU}
4: **if** $LN_v \in$ DMV **then**
5: persistent attributes: $\{type, color, year, \ldots\}_{LN_v}$
6: dynamic attributes:$\{road, loc, dir, \ldots\}_{LN_v}$
7: **end if**
8: RSU transfers these attributes to center along with the LN_v
9: Center runs `Key Generate`(MK,S)$\rightarrow$AK, SK
10: Then center AK $\rightarrow$ RSU, SK $\rightarrow$ vehicle
11: **end for**

When vehicles move across RSUs, they have to register at a nearby RSU. Before this, the vehicles obtain their OBU modules attested by the RSU to verify that it is a valid device. After attestation, the RSU records the vehicles' attributes values. OBUs in vehicles will then transfer information such as the position, time, direction, speed, and etc.

As shown in Algorithm 1, to receive a vehicle's request, the local RSU first performs attestation of the OBU in the vehicle. The target is to authenticate the vehicle by verifying whether a valid and uncorrupted software is installed in the OBU. Then, the RSU retrieves and registers the vehicle's attributes with the center, including persistent and dynamic attributes values. The RSU can obtain all its static attributes (e.g., vehicle type) from the Department of Motor Vehicles (DMV) for vehicle information. It further employs the location proof methodologies for location-related attributes [44]. The dynamic attributes include road name, vehicle location, direction. From the dynamic attributes of all vehicles, the traffic flow characteristics of overall traffic flow can be understood and analyzed [45]. Thereafter, the RSU transfers these vehicle registration information to the center. The center executes `Key Generate`(MK,S) algorithm and generates three keys. The first is concealed in what we called an "attribute key" AK and is fed into the RSU. The second is stored in SK which maintains by the OBU privately. The last is a full secret key (FK) related to the vehicles' attributes.

`Key Generate`(MK,S): In the key generation step, the algorithm takes the master secret key and attributes related to a user as the input. The algorithm randomly chooses a $t \in \mathbb{Z}_p$. It then generates the private key as three parts, one is AK, which is "attribute key" for the proxy; the second is SK, which is private "security key" for the vehicles; and the last is FK, which is "full key" for the vehicles.

$$\mathrm{AK} : (K_1 = g^{\alpha_1} g^{at}, L = g^{t}, \forall x \in S : K_x = h_x^{t})$$

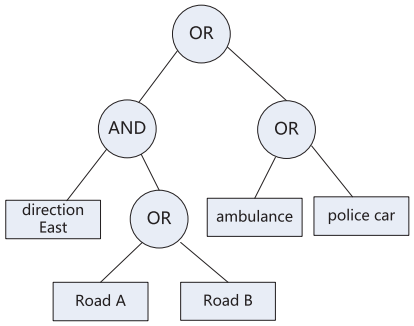


Fig. 2. Access policy.

$$\text{SK}: (K_2 = g^{\alpha_2} g^{at})$$
$$\text{FK}: (K_3 = g^{\alpha} g^{at}, L = g^{t}, \forall x \in S: K_x = h_x^t)$$

B. Message Verification and Encryption

When a message is reported for a particular event, e.g., a traffic accident or a fire, the trusted center immediately launches the emergency plan. First, it verifies the status of the emergency. Then, an alert message will be generated toward the related vehicles. Also, a rescue message will be released toward the nearest rescue cars. For example, to alert the coming vehicles to take an alternative route, these messages should be disseminated not only based on the vehicles' functions, e.g., police cars, ambulances, but also according to their movements, such as the location and direction. These applications require a selective message delivering mechanism to perform access control on the disseminated messages.

To achieve data privacy and effective access control, we employ an advanced encryption standard (AES) to encrypt the multimedia transmitted messages. Afterward, we combine an improved ciphertext-policy attribute-based encryption (CP-ABE) to encrypt the message key with an access policy. Fig. 2 shows a cryptography-binding access policy for message dissemination as described in Fig. 1.

Making a policy means specifying multiple attributes and logical predicates, to ensure data access by authorized vehicles. In our scheme, the trusted center defines the access policy, which typically involves the constraints on the attribute values of the potential recipient vehicles.

`Encrypt`(PK, $(M, \rho), m$): In the encryption step, the algorithm will generate a message m, a public key PK, and an access structure $\mathbb{A}$ to encrypt the message as input, and further output the corresponding ciphertext. In our implementation, the algorithm takes a linear secret sharing scheme (LSSS) to specify the access matrix (M, ρ). M is an $l \times n$ matrix, and ρ denotes the function mapping the rows of M to the attributes.

The algorithm first specifies a vector $\upsilon = (s, y_2, \ldots, y_n)^T \in \mathbb{Z}_p^n$. Each component $s \in \mathbb{Z}_p$ is randomly chosen as the secret to be shared. The other values are adopted to share the encryption exponent s. For $i = 1$ to l, it calculates $\lambda_i = M_i \upsilon$, where M_i is the vector associated with the ith row of M. Also, it will select several random exponents $r_1, \ldots, r_l \in \mathbb{Z}_p$ in the encryption calculation. The ciphertext CT is generated as: $C = me(g,g)^{\alpha s}, C' = g^s, (C_1 = g^{a\lambda_1} h_{\rho(1)}^{-r_1}, D_1 = g^{r_1}), \ldots, C_l = g^{a\lambda_l} h_{\rho(l)}^{-r_l}, D_l = g^{r_l})$

Due to the severity of emergency, the trusted center estimates the time required to solve it, and further decides the transmission range to broadcast the message. Afterward, the center disseminates the messages to the corresponding RSUs in the range with internet, and RSUs broadcast the messages via DSRC. Obviously, only vehicles with attributes satisfying the policy $\mathbb{A}$ can decrypt the message.

C. Message Dissemination and Forward

To receive ciphertexts from the trusted center, the RSUs forward the encrypted messages to vehicles in its transmission range. The OBUs in the vehicles decrypt the ciphertexts in order to take effective measurement promptly. To reduce the computational cost for the OBU, we propose an improved CP-ABE algorithm which assigns most of the decryption computation to the RSUs. It first performs transform decryption for the vehicles by its attribute keys. Afterward, it transfers the partially-decrypted ciphertexts to the vehicles. Based on this, the vehicles conduct pairing computation of CP-ABE decryption only once, regardless of the policy complexity.

RSUs transform ciphertexts for the vehicles one by one. Thus, vehicle density is an important factor in the efficiency of message dissemination. Some vehicles may leave the current RSU and enter another. Therefore, these vehicles may not get the messages timely. The decryption delay of the received ciphertexts is an important problem in vehicular ad-hoc networks. Under such circumstance, we assume that the RSUs conduct an adaptive ciphtertext forwarding. Thereby, the ciphertexts can be transferred to all the vehicles in its transmission range.

To accurately determine messages encryption/decryption, an adaptive decision making method is proposed based on the vehicle-related and message-related factors. It guarantees that the messages can be delivered to vehicles before it is out of the communication scope. Also, it takes the location of all vehicles within the range of RSU communication into account. It further estimates the residence time of the vehicle within the coverage of the RSU.

For delegating decryption, it considers the RSU delegation decryption time t_{dele}, the transmission time of partially decrypted ciphertext t_{par_tran}, and the decryption time at the vehicle t_{fina}. The total time taken by message decryption is calculated as:

$$T_{dede} = t_{dele} + t_{par\_tran} + t_{fina}$$

Regarding to the non-delegation decryption, it includes the decryption time at the vehicle t_{dec} as well as the transmission time of the entire decrypted ciphertext t_{tran}.

$$T_{nonde} = t_{tran} + t_{dec}$$

Data mining technique automatically detect the relevant patterns or information from the raw data, using the data mining algorithms. In Data mining algorithms, decision trees are the best and commonly used approach for representing the data and classification [46]. Using these decision trees, data can be represented as a most visualizing form. The factors

Algorithm 2 Adaptive Ciphertext Forwarding Scheme

for each ciphertext CT in the RSU **do**
  $t_{out} \leftarrow$ distance $\div$ speed;
  $t_{tran} \leftarrow$ size $\div$ communication speed;
  $t_{dele\_dec} \leftarrow t_{dele} + t_{par\_tran} + t_{fina}$;
  $t_{non\_dec} \leftarrow t_{dec} + t_{tran}$
  if $t_{dele\_dec} < t_{out} \times 0.8$ **then**
    delegate decryption and transfer the partial decrypted ciphertext to the vehicle.
  end if
  transfer the whole ciphertext to the vehicles.
end for

associated with decrypting the messages are encoded into a decision tree, which is popularly adopted to classify data for dimensional cubes.

The pipeline of the algorithm is described in Algorithm 2. For each ciphertext message, the RSU computes the average distance between the vehicles and RSU for most vehicles, and next estimates the time the vehicles will depart. By integrating all the factors, it compares the entire time of both delegating and non-delegate decryption and gives the prediction result.

D. Message Decryption

The `Transform Ciphertext` algorithm can be formulated as follows.

`Transform Ciphertext`(CT,AK): This algorithm takes a ciphertext CT for access structure (M, ρ) and an attribute key AK for a set of attributes S as input. We denote S as a set of attributes satisfying the access structure (M, ρ), which means an authorized user. We denote $I \subset \{1, 2, \ldots, l\}$ as $I = \{i, \rho(i) \in S\}$ and define $\{w_i \in \mathbb{Z}_p\}_{i \in I}$ as a set of constants. According to the access structure of M, only if $\sum_{i \in I} w_i \lambda_i = s$, then $\{\lambda_i\}$ can be considered as the valid shares of secret s.

1) In terms of the following equation, the proxy checks whether users can decrypt the ciphertext.

$$\sum_{i \in I} M_i w_i = (1, 0, ..0)$$

2) The proxy transforms the ciphertext CT into CT′.

$$\begin{aligned} \mathrm{CT}' &= e(C', K_1)/(\prod_{i \in I}(e(C_i, L)e(D_i, K_{\rho(i)}))^{w_i})^2 \\ &= e(g^s, g^{\alpha_1} g^{at})/(e(g, g)^{ats})^2 \\ &= e(g, g)^{\alpha_1 s}/e(g, g)^{ats} \end{aligned}$$

The proxy finally send CT′ to users.

Since the attribute keys of registered vehicles are preserved in the RSU, its test will performs rapidly to decide whether the attributes in vehicle's AK matches access policy in ciphertexts. If the test returns false, then the RSU will not deliver the messages to the vehicles. Otherwise, the RSU will perform the `Transform Ciphertext`(CT,AK) algorithm, which takes in a ciphertext CT and an AK corresponding to the vehicle's attributes S. The algorithm transforms the ciphertext into CT′. Finally, the RSU sends CT′ to the responding vehicles. It is worth emphasizing that the vehicle consumes little decryption computation through its own secret key.

By delegating decryption using the RSU, the vehicle only conduct the final decryption step. That means the decryption only requires pairing computation once. Therefore, the scheme not only guarantees data security, but also achieve a rapid decryption at the user side.

`The Final Decrypt`(CT′,SK): The algorithm takes the transformed ciphertext CT′ and user's private key SK as input, and then outputs the plaintext m.

$$\begin{aligned} e(\mathrm{SK}, C')\mathrm{CT}' &= e(g^{\alpha_2} g^{at}, g^s)e(g, g)^{\alpha_1 s}/e(g, g)^{ats} \\ &= e(g, g)^{\alpha_2 s} e(g, g)^{ats} e(g, g)^{\alpha_1 s}/e(g, g)^{ats} \\ &= e(g, g)^{\alpha s} \end{aligned}$$

The plaintext m is obtained by $m = C/e(g, g)^{\alpha s}$.

For the non-delegation decryption algorithm, the vehicle performs the whole decryption, which is linearly increasing with the number of attributes in the access policy. `Decrypt`(CT′,FK): The algorithm input is the ciphertext CT and user's full secret key FK, and the output is the plaintext m.

$$\begin{aligned} e(\mathrm{FK}, CT)\mathrm{CT} &= e(g^{\alpha_2} g^{at}, g^s)e(g, g)^{\alpha_1 s}/e(g, g)^{ats} \\ &= e(g, g)^{\alpha_2 s} e(g, g)^{ats} e(g, g)^{\alpha_1 s}/e(g, g)^{ats} \\ &= e(g, g)^{\alpha s} \end{aligned}$$

Finally, the plaintext m is calculated as $m = C/e(g, g)^{\alpha s}$.

VI. Simulation Evaluation

Having the insights into the various factors affecting the performance of our adaptive data forwarding scheme in VANET, we conduct experiments using real maps extracted from the Hangzhou database in this section. We perform a set of experiments using a smaller section of the map, and conduct several experiments to verify the efficiency of our proposed scheme.

A. Simulation Environment

As shown in Fig. 3, we adopt several major road segments in the west of Hangzhou, which is a typical region in Hangzhou. There are some fixed infrastructure devices like RSUs that vehicles communicate with them, which is marked with a point. The RSUs are mostly located at the crossroads and assembled in a cost-efficient manner to improve the coverage. There is at least one RSU covering the two roads at the crossroads because the V2I communication is more important in the intersection. In the backbone, there is a center and we deploy it in Aliyun cloud server. The data integrity in cloud can be achieved by the remote data integrity verification protocol [47]. The positions and their destinations of the vehicles equipped with active OBUs are uniformly random. Each vehicle follows the shortest path to its destination. We adopt the practical data from the real road segment. The number of road lanes is considered in consistent with the real roads. The number of vehicles and their density in the simulation are collected by bayonets which are deployed on the real road segments. Typically, we may assume that the

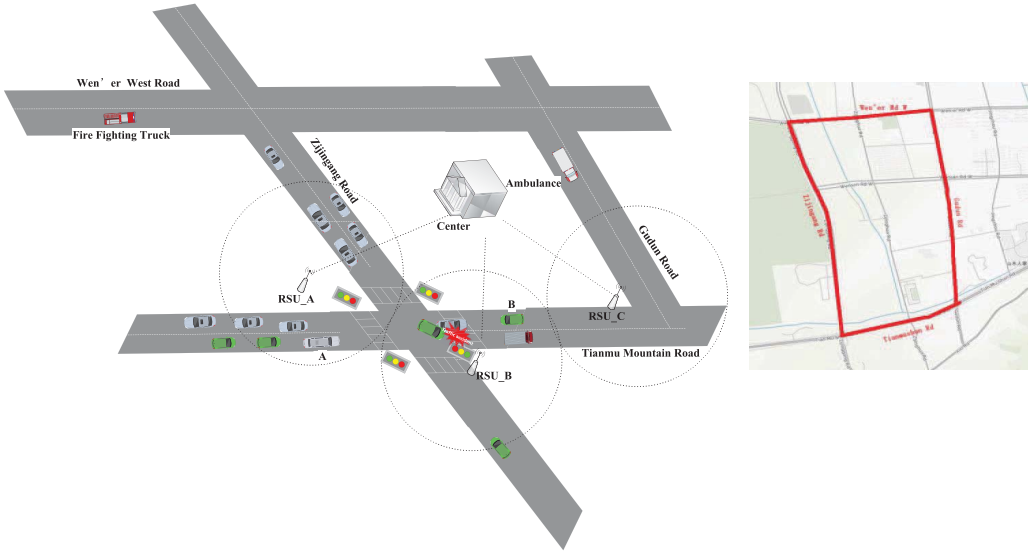


Fig. 3. Road segments in Hangzhou.

TABLE I
SIMULATION CONFIGURATIONS

System Parameter	Value
Vehicle Speed	60 km/h
DSRC Communication Range	0-500 m
Data Transmission Speed via DSRC	250 kb/s
RSU Coverage	10-50 vehicles
RSU Setting	2.5GHz, 4 core CPU
OBU Setting	1536MHz, 768 MB RAM

RSU has abundant computational resources (e.g., with several GB of RAM and a GHz processor). In contrast, the OBU equipped in the vehicle has limited processing power (e.g., a 400MHz processor [11]).

The parameter settings in the simulation are listed in Table I.

In order to capture the real-world scenarios, we simulate the behavior of vehicles following the data collected by bayonets, with average vehicle speed set to road speed limit 60km/h. We set the range of DSRC communication to 500m, and the bandwidth of DSRC channel to 250kb/s [48]. Without loss of generality, we assume that the average length of a vehicle is 5m. Besides, according to the vehicle density estimated from data collected by bayonets, we set that one RSU could cover 50 vehicles at most and simulate the RSU as a platform of 2.5GHz Intel 4 core CPU. And we have done several experiments on a 1536MHz ARM-based HTC G18 with 768 MB RAM as the vehicle's OBU. In general, we can conclude that the detailed information about the simulation settings is collected from practical scenarios, therefore definitely close to real conditions.

B. Simulation Results

We evaluate our scheme in terms of processing delay (including those imposed by cryptographic operations in our scheme). We define the processing time as the period from when one vehicle sends out its messages to when another vehicle finishes decrypting the information provided by all RSUs and vehicles along the returned path. Here the processing time includes the communication overhead, computation overhead, transform decryption time and final decryption time.

In this simulation, we can see that there is a traffic accident. The car A's driver takes a video about the accident, and then he posts the video to let other drivers avoid the accident. He defines an access policy "(Tianmu Mountain Road and East) or (Zijingang Road and SouthEast) or ambulance or policy car" on that messages. That is, the cars that will arrive at the scene of the accident in a short time and the special cars that should deal with the accident, these cars which satisfied with the policy will receive the video. When the emergency is happened, any approaching driver can be notified in time and then choose other way. However, for traditional message broadcasting method, it may take a while for the driver to figure out that whether it is true, which results in wasting time. When the traffic density becomes larger, a vehicle can not decrypt the messages sent by its neighbors in a timely manner, which results in time delay. The interesting observation can be also confirmed. RSUs are responsible for decrypting the part of the messages sent from vehicles and for notifying the results back to vehicles.

C. Communication Overhead

We use the libfenc library [49] that employs the key encapsulation mechanism. We also adopt the elliptic curve from the Pairing-Based Crypto library of Stanford [50] to implement the two ABE schemes (with both delegating and non-delegating decryptions). In the traditional CP-ABE scheme, both the decryption time and ciphertext size depend on the complexity of the access policy attached in the ciphertext. They increase linearly with the number of attributes in that policy. To demonstrate this, we choose 100 most complex policies from (A_1 AND A_2 AND...AND A_n), where A_i is an attribute and the values of N increase from 1 to 100. This approach guarantees that all the ciphertext components are

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

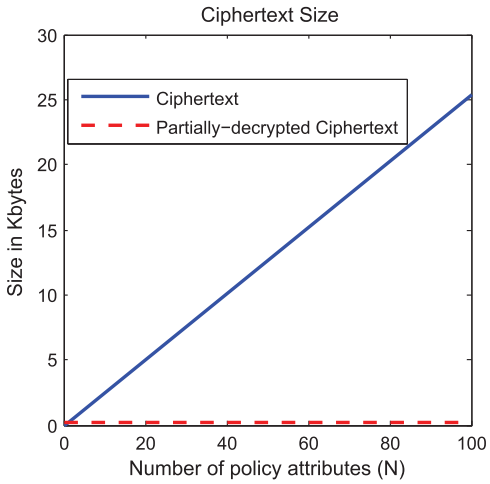


Fig. 4. The size of ciphertext and secret key in the vehicle.

involved in the decryption phrase. In each case, we construct a standard decryption key containing N attributes. In the vehicular ad-hoc networks, the number of attributes do not increase to 100 rapidly, but it will increases by the complex policy.

In practice, ABE is a pubic key encryption mechanism unsuitable for encrypting data directly. In our experiment, the message is encrypted separately using a symmetric encryption scheme AES (Advanced Encryption Standard) under a symmetric key k. The ABE ciphertext is the encryption of the symmetric key k. In our adaptive forwarding schemes, both the delegating and non-delegating decryption conduct the symmetric encryption and decryption of data. Here, we neglect the influence of symmetric encryption k.

In our ABE decryption delegation scheme, we outsource the partial decryption computation by generating an attribute key AK and applying the Transform Ciphertext algorithm to the ABE ciphertext accordingly. As shown in Fig. 4, an encryption under a ciphertext policy with 100 attributes generates a ciphertext of nearly 25.4KB. In our implementation, however, each partially-decrypted ciphertext has a constant size of 176 bytes. Each security key for the vehicle has 168 bytes, regardless of the complexity of the corresponding ciphertext policy. This reveals that, compared with the ABE, less time is required to transfer ciphertext from RSU to a vehicle.

Obviously, compared with the non-delegating decryption scheme, the transmitted ciphertexts in the proposed delegating decryption scheme are short and constant, which saves the network bandwidth and reduce the communication overhead remarkably.

D. Computation Overhead

The computational complexities included in the main steps are summarized in Table II. In the table, $|S|$ means the numbers of attributes in S, p denotes the computation cost of pairing.

There is no computationally intensive task involved during the key issuing and message encryption stage for the center. In the decryption phrase, the bulk of decryption operation is now handled by the RSU. It can be concluded that our scheme

TABLE II
COMPUTATION COMPLEXITY

Operation	Complexity
Setup	$O(1)$
Encrypt	$O(l \times n)$
Key Generate	O($\|S\|$)+O(1)
Transform Ciphertext (RSU)	$O((2+l)p)$
Decrypt Ciphertext (Vehicle)	$O(1)$

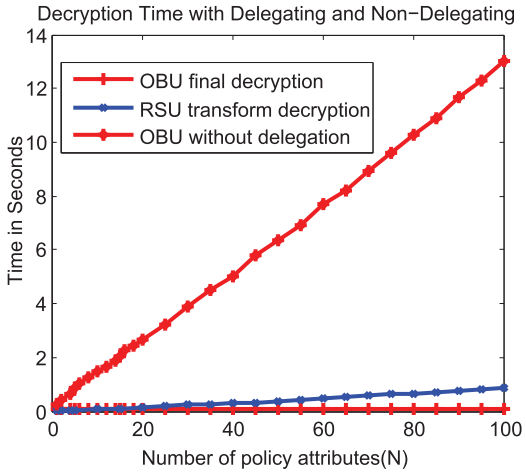


Fig. 5. The decryption time of OBU with non-delegating and delegating.

substantially reduces the decryption time required for vehicle to recover the plaintext by outsourcing.

Our solution for the decryption computation at the vehicle is extremely efficient than the traditional CP-ABE decryption scheme. In the way, the vehicle can relieve the computation workload by delegating most of the computation to the RSU. This solution, nonetheless, is at the expense of additional RSU decryption computation overhead. This issue on the overhead will be tackled in the next subsection. Fig. 5 presents the measured decryption times of OBU in the vehicles with non-delegating and delegating, as a function of policy attribute N. We repeat the experiment multiple times for each ciphertext policy. Then, we take the average values as shown in Fig. 5.

Without delegating, it takes nearly 1.47 seconds on the RSU platform to decrypt the ciphertext under a ciphertext policy with 100 attributes. Besides, the decryption time reduces dramatically on the OBU, and it requires 9.6 seconds under a policy with 100 attributes. By delegating the decryption of CP-ABE ciphertext using our ABE delegating scheme, the final decryption requires only 93 milliseconds on the OBU platform, regardless of the complexity of the policy. Noticeably, the time required in the transformed decryption of RSU is 130 milliseconds under a policy with 100 attributes.

In order to illustrate the decryption efficiency of our proposed delegation decryption scheme, we have done the experiments on three dedicated hardware platforms: a 3.20GHz Intel processor with 4GB RAM running 32-bit Linux Kernel version 3.2.0 (denoted by Intel), a 1.3GHz ARM-based OPPO R829T with 960.54 MB RAM running Android OS (denoted by phone), and a 1.3GHz ARM-based Nexus ME370T with

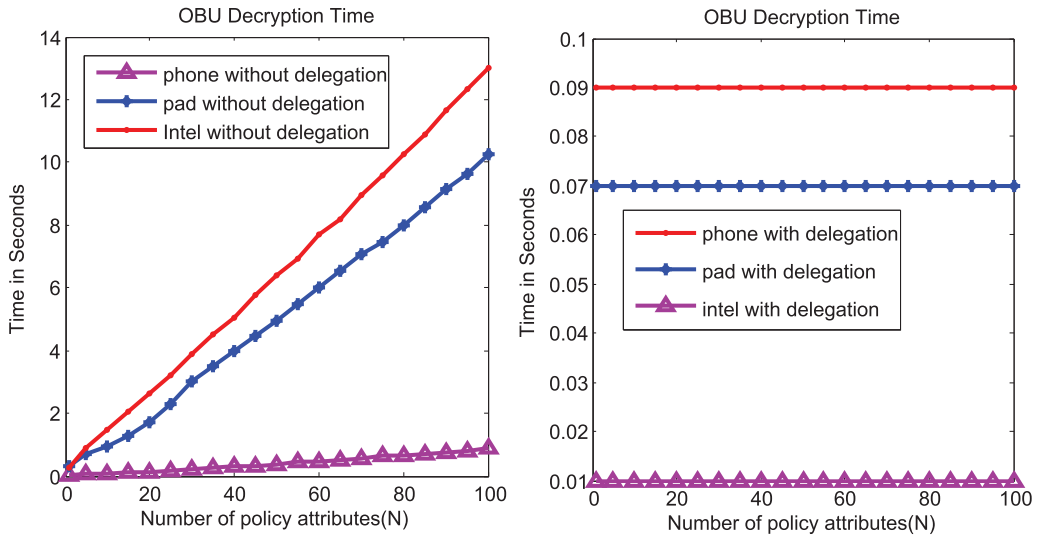


Fig. 6. OBU decryption time in different platforms.

1GB RAM running Android OS (denoted by pad). As it needs only one paring for OBU module in our scheme, the OBU decryption time in different platforms is shown in Fig. 6, and it is constant with the increase number of the attributes.

Compared with the existing access control scheme in data dissemination in VANET, we illustrate the difference of these works in Table III. As shown in the table, we can see that these schemes all propose an improved attribute based encryption in VANET, and take different security assumption of RSU. Our scheme makes the decryption cost at the vehicle const, regardless of the increasing number of attributes by delegating most of the decryption computation to RSU.

As expected as it, delegating the decryption dramatically decrease the computation time required for devices with limited computation resource to decrypt the ciphertext.

Compared with the existing ASPE scheme in [8], we give a comparison of decryption time with the size of packet payload in Fig. 7. It can be observed that, with the increasing size of packets, the decryption time in ASPE is increasing along with the packet size, while the time is constant in our scheme. As is shown in Fig. 7, for a packet size of 2300 bytes, the decryption time for ASPE scheme it is 0.052s, whereas in our scheme the time is only 0.01s at the vehicle. It is because we outsource the most complex decryption calculation to the RSU and and leave only one pairing to the vehicle. Although ASPE scheme optimized traditional ABE scheme to do the decryption. Our scheme outperforms their schemes. Thus, it can be proved that our scheme can enormously reduce decryption time at the vehicle.

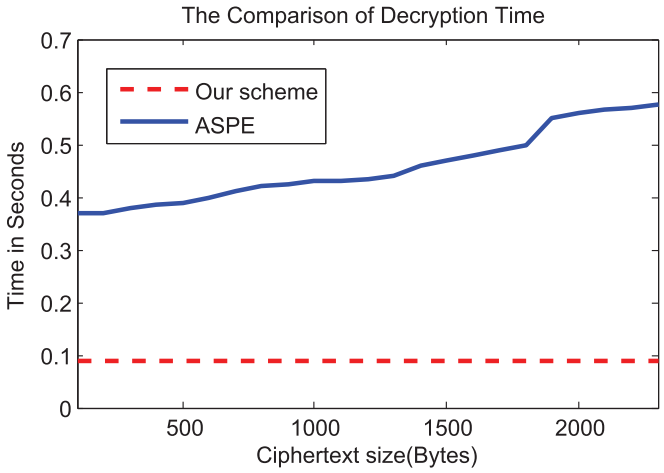


Fig. 7. The comparison of decryption time with the increase of packet size.

E. Transform Decryption Time

In our ABE delegating scheme, we delegate the most complex decryption calculation to RSUs. Fig. 8 displays the average transformed decryption time with multiple vehicles in the form of different numbers of vehicles at one time. As shown in the Fig. 8, the average transform decryption time of RSU is linearly increasing with the number of vehicles in the density. The more the number of vehicle is, the more transform decryption time it will cost. In the coverage range of DSRC system, the RSU will take at most 4s transform decryption time in the case of 50 vehicles. We found that the performance in dense VANETs degrades significantly when transform decryption decisions are limited to RSU, whereas in sparse VANETs, performance improves when vehicles also participate in decryption. And the time could be accelerated with high performance RSU devices.

Also in our algorithm, we add a matching operation before the RSU's transforming of ciphertext, which is used to check whether the user can decrypt the ciphertext. It accelerates the decryption calculation remarkably. Since if the attributes of the vehicles are not satisfied with the access policy attached in the ciphertext, then the RSU would give a quick response to the vehicle, and would not transform the corresponding ciphertext.

TABLE III
COMPARISON WITH EXISTING WORKS

Schemes	ABE-related scheme	Security model of RSU	Decryption cost at the vehicle
ABACS [27]	attribute based access control system	trusted	increase with the number of attributes
ASPE [8]	attribute based security policy enforcement	not compromised	increase with the number of attributes
DABE [29]	decentralized attribute based encryption	resilient to compromised of RSUs	increase with the number of attributes
Ours	attribute based encryption with delegating decryption	semi-trusted	constant

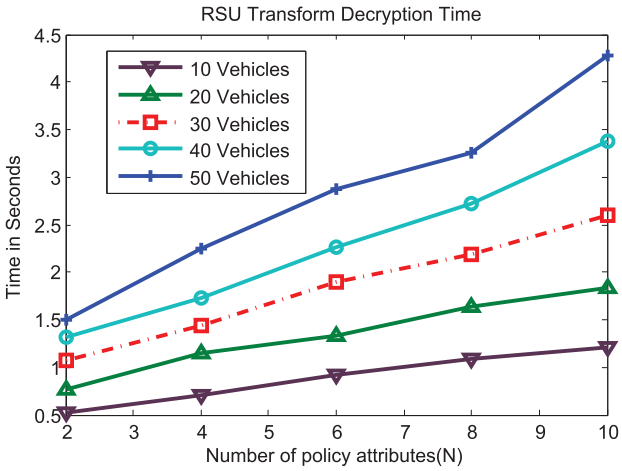


Fig. 8. RSU transformed decryption time.

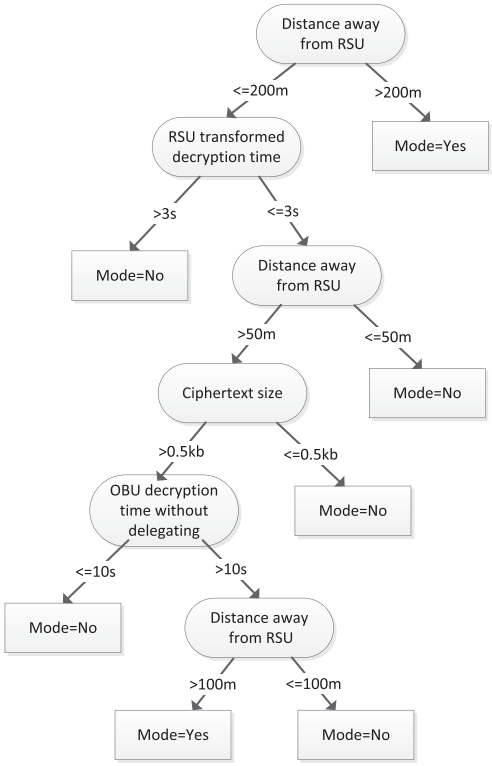


Fig. 9. Decision Tree.

F. Adaptive Data Forwarding

In our implementation, we simulate several messages dissemination in different circumstances to compute the decryption time with delegating and non-delegating. Then we can make better conclusion whether to perform decryption with delegation or without delegation. We apply a decision tree-based algorithm 2 on the experimental data, the decision tree is shown in Fig. 9.

The decision tree algorithm considers the main factors including the vehicles' location from RSU, the RSU transformation time, the ciphertext size, and the number of attributes in the access policy in the decision making. The label "Mode=Yes" means that the vehicles need delegate partial decryption to the RSU, while "Mode=No" means that the vehicles should perform message decryption independently. From the decision tree, we can see that the distance from the RSU is an important factor that influences the decision result, since it makes an impact on the communication overhead.

In the encrypted message dissemination, we choose to use different multimedia data, different number of attributes ranging from 2 to 10, different number of vehicles in the same RSU ranging from 10 to 50, different distance away from the RSU ranging from 100 to 500. And we perform the decryption with delegation or without delegation at the OBU. The lesser decryption time, the better decryption scheme it is. Then, we use our decision tree to predict the results. Based on the predicted results and real results, we can calculate the values of True Positive (TP), False Positive (FP), True Negative (TN), False Negative (FN). According to these values [51], we evaluate the 6 selected classifiers of the decision tree by computing the following four metrics: $Accuracy$, $Precision$, $Recall$ and $F-measure$.

$Accuracy$ is the percentage of correctly classified modules, defined as

$$Accuracy = (TN + TP)/(TP + FP + FN + TN)$$

$Precision$ is the number of classified fault-prone modules that actually are fault-prone modules, defined as

$$Precision = TP/(TP + FP)$$

$Recall$ is the percentage of fault-prone modules that are correctly classified, defined as

$$Recall = TP/(TP + FN)$$

$F-measure$ is the harmonic mean of precision and recall, which has been widely used in information retrieval, defined as

$$F - measure = (2 * Precision * Recall)/(Precision + Recall)$$

Compared with the decision tree, we use two other classical classification methods, support vector machine and k-nearest-neighbor, to process the same real world data in the road segments, and get the results as shown in Table IV.

By using the decision tree, the percentage of accuracy is 0.85, the percentage of precision is 0.78, the percentage of

TABLE IV
PERFORMANCE OF DIFFERENT CLASSIFICATION METHODS

Algorithm	Accuracy	Precision	Recall	F-measure
Decision Tree	0.85	0.78	1	0.87
Support Vector Machine	0.76	0.68	1	0.81
K-Nearest-Neighbor	0.714	0.64	1	0.78

recall is 1, and the percentage of F-measure is 0.87. From these results, we clearly see that the implemented decision tree can achieve high accuracy and precision for predictions.

VII. CONCLUSIONS

This paper presents an adaptive multimedia data forwarding scheme for privacy preservation in vehicular ad-hoc networks. In this scheme, the RSU dynamically decide whether delegating or non-delegating decryption of messages before forwarding them to the vehicles. A decision tree is constructed where the nodes represent the distance measurements, exact number of vehicles, data types, ciphertext size, and etc. The performance of delegated decryption and traditional non-delegated decryption of the CP-ABE scheme is analyzed under different access policies. Comprehensive simulation results demonstrate that our adaptive data forwarding scheme can provide an efficient and secure solution for transmitting multimedia messages.

REFERENCES

[1] R. Di Pietro, S. Guarino, N. V. Verde, and J. Domingo-Ferrer, "Security in wireless ad-hoc networks—A survey," *Comput. Commun.*, vol. 51, pp. 1–20, Sep. 2014.
[2] K. M. Alam, M. Saini, and A. El Saddik, "*tNote*: A social network of vehicles under Internet of Things," in *Internet Vehicles—Technologies Services*. Berlin, Germany: Springer, 2014, pp. 227–236.
[3] S. Smaldone, L. Han, P. Shankar, and L. Iftode, "RoadSpeak: Enabling voice chat on roadways using vehicular social networks," in *Proc. 1st Workshop Social Netw. Syst.*, Apr. 2008, pp. 43–48.
[4] W. Wang, Y. Yan, L. Zhang, R. Hong, and N. Sebe, "Collaborative sparse coding for multiview action recognition," *IEEE MultiMedia*, vol. 23, no. 4, pp. 80–87, Oct./Dec. 2016.
[5] L. Zhang, X. Li, L. Nie, Y. Yan, and R. Zimmermann, "Semantic photo retargeting under noisy image labels," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 12, no. 3, Jun. 2016, Art. no. 37.
[6] Z. Li, C. Wang, S. Yang, C. Jiang, and X. Li, "LASS: Local-activity and social-similarity based data forwarding in mobile social networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 1, pp. 174–184, Jan. 2015.
[7] V. Smailovic and V. Podobnik, "Bfriend: Context-aware ad-hoc social networking for mobile users," in *Proc. 35th Int. Conv. MIPRO*, May 2012, pp. 612–617.
[8] D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks," *Ad Hoc Netw.*, vol. 7, no. 8, pp. 1526–1535, Nov. 2009.
[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2007, pp. 321–334.
[10] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," in *Proc. 20th Usenix Conf. Secur.*, 2011, p. 34.
[11] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," in *Proc. 6th Annu. IEEE Conf. Sensor, Mesh Ad Hoc Commun. Netw.*, Jun. 2009, pp. 1–9.
[12] A. M. Vegni and V. Loscrí, "A survey on vehicular social networks," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2397–2419, 4th Quart., 2015.
[13] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.
[14] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Veh. Commun.*, vol. 1, no. 2, pp. 53–66, Apr. 2014.
[15] S. Gillani, F. Shahzad, A. Qayyum, and R. Mehmood, "A survey on security in vehicular ad hoc networks," in *Communication Technologies for Vehicles*. Berlin, Germany: Springer, 2013, pp. 59–74.
[16] X. Liu, Y. Xia, W. Chen, Y. Xiang, M. M. Hassan, and A. Alelaiwi, "SEMD: Secure and efficient message dissemination with policy enforcement in VANET," *J. Comput. Syst. Sci.*, vol. 82, no. 8, pp. 1316–1328, Dec. 2016.
[17] X. Liu, Z. Fang, and L. Shi, "Securing vehicular ad hoc networks," in *Proc. 2nd Int. Conf. Pervasive Comput. Appl. (ICPCA)*, Jul. 2007, pp. 424–429.
[18] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proc. 4th ACM Int. Workshop Veh. Ad Hoc Netw.*, Sep. 2007, pp. 19–28.
[19] D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 3, pp. 736–746, Sep. 2011.
[20] A. I. González-Tablas, A. Alcaide, J. M. De Fuentes, and J. Montero, "Privacy-preserving and accountable on-the-road prosecution of invalid vehicular mandatory authorizations," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2693–2709, Nov. 2013.
[21] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 9, pp. 1227–1239, Sep. 2010.
[22] Y. Xia, X. Liu, F. Xia, and G. Wang, "A reduction of security notions in designated confirmer signatures," *Theor. Comput. Sci.*, vol. 618, pp. 1–20, Mar. 2016.
[23] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE 27th Conf. Comput. Commun. (INFOCOM)*, Apr. 2008, pp. 1229–1237.
[24] T. R. de Oliveira, S. de Oliveira, D. F. Macedo, and J. M. Nogueira, "Social networks for certification in vehicular disruption tolerant networks," in *Proc. IEEE 10th Int. Conf. Wireless Mobile Comput. Netw. Commun. (WiMob)*, Oct. 2014, pp. 479–486.
[25] R. Lu, X. Lin, and X. Shen, "SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.
[26] P. Zhong and R. Lu, "PAD: Privacy-preserving data dissemination in mobile social networks," in *Proc. IEEE Int. Conf. Commun. Syst. (ICCS)*, Nov. 2014, pp. 243–247.
[27] 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 J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 630–643, Mar. 2011.
[28] X. Hong, D. Huang, M. Gerla, and Z. Cao, "SAT: Situation-aware trust architecture for vehicular networks," in *Proc. 3rd Int. Workshop Mobility Evol. Internet Archit.*, Aug. 2008, pp. 31–36.
[29] S. Ruj, A. Nayak, and I. Stojmenovic, "Improved access control mechanism in vehicular ad hoc networks," in *Ad-Hoc, Mobile, and Wireless Networks*. Berlin, Germany: Springer, 2011, pp. 191–205.
[30] J. Li, C. Jia, J. Li, and X. Chen, "Outsourcing encryption of attribute-based encryption with mapreduce," in *Information and Communications Security*. Berlin, Germany: Springer, 2012, pp. 191–201.
[31] Z. Zhou and D. Huang, "Efficient and secure data storage operations for mobile cloud computing," in *Proc. 8th Int. Conf. Netw. Service Manage.*, Oct. 2012, pp. 37–45.
[32] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in *Public Key Cryptography*. Berlin, Germany: Springer, 2013, pp. 162–179.
[33] S. Boccaletti *et al.*, "The structure and dynamics of multilayer networks," *Phys. Rep.*, vol. 544, no. 1, pp. 1–122, Nov. 2014.
[34] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Adv. Cryptol.-Eurocrypto*, 2005, pp. 457–473.
[35] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, 2007, pp. 456–465.
[36] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Proc. Adv. Cryptol.-Eurocrypto*, 2010, pp. 62–91.
[37] J. Li, K. Ren, B. Zhu, and Z. Wan, "Privacy-aware attribute-based encryption with user accountability," in *Information Security*. Berlin, Germany: Springer, 2009, pp. 347–362.
[38] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, 2007, pp. 195–203.

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

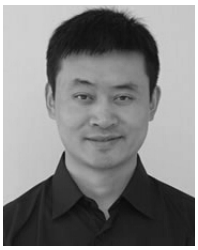
[39] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in *Proc. Adv. Cryptol.*, 2012, pp. 199–217.
[40] B. Waters, "Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions," in *Proc. Adv. Cryptol.*, 2009, pp. 619–636.
[41] R. C. Barros, M. P. Basgalupp, A. C. P. L. F. de Carvalho, and A. A. Freitas, "A survey of evolutionary algorithms for decision-tree induction," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 42, no. 3, pp. 291–312, May 2012.
[42] DSRC. *Dedicated Short Range Communications*, accessed on Oct. 24, 2015. [Online]. Available: http://www.leearmstrong.com/dsrc/dsrchomeset.htm
[43] I. A. Sumra, H. B. Hasbullah, and J.-L. B. AbManan, "Attacks on security goals (confidentiality, integrity, availability) in VANET: A survey," in *Vehicular Ad-Hoc Networks for Smart Cities*. Berlin, Germany: Springer, 2015, pp. 51–61.
[44] S. Saroiu and A. Wolman, "Enabling new mobile applications with location proofs," in *Proc. 10th Workshop Mobile Comput. Syst. Appl.*, Feb. 2009, Art. no. 3.
[45] Y. Xia, J. Chen, and C. Wang, "Formalizing computational intensity of big traffic data understanding and analysis for parallel computing," *Neurocomputing*, vol. 169, pp. 158–168, Dec. 2015.
[46] L. Rokach and O. Maimon, "Decision trees," in *Data Mining and Knowledge Discovery Handbook*. Berlin, Germany: Springer, 2005, pp. 165–192.
[47] Y. Xia, F. Xia, X. Liu, X. Sun, Y. Liu, and Y. Ge, "An improved privacy preserving construction for data integrity verification in cloud storage," *KSII Trans. Internet Inf. Syst.*, vol. 8, no. 10, pp. 3607–3623, 2014.
[48] P. Belanovic, D. Valerio, A. Paier, T. Zemen, F. Ricciato, and C. F. Mecklenbrauker, "On wireless links for vehicle-to-infrastructure communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 1, pp. 269–282, Jan. 2010.
[49] *Libfenc: The Functional Encryption Library*, accessed on Oct. 20, 2015. [Online]. Available: http://code.google.com/p/libfenc/
[50] B. Lynn. *Stanford Pairings-Based Crypto Library*, accessed on Oct. 20, 2015. [Online]. Available: http://crypto.stanford.edu/pbc/
[51] Y. Peng, G. Kou, G. Wang, H. Wang, and F. I. Ko, "Empirical evaluation of classifiers for software risk management," *Int. J. Inf. Technol. Decision Making*, vol. 8, no. 4, pp. 749–767, 2009.

Yingjie Xia (M'–) received the Ph.D. degree from the College of Computer Science, Zhejiang University, in 2009. He was a Research Scientist with the National Center for Supercomputing Applications, University of Illinois at Urbana–Champaign, USA. He is currently an Associate Professor with Zhejiang University, Hangzhou, China. His research interests cover information security and connected vehicles.

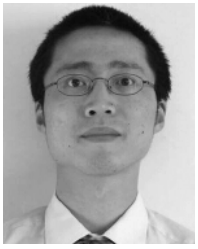
Wenzhi Chen (M'–) received the B.S., M.S., and Ph.D. degrees in computer science and technology from Zhejiang University, Hangzhou, China. He is a Professor with the School of Computer Science and Technology, Zhejiang University. His areas of research include computer architecture, system software, embedded system, and network security. He is a member of the ACM.

Xuejiao Liu received the B.S., M.S., and Ph.D. degrees in computer science from Central China Normal University, China. Her research interests cover information security and security for connected vehicles.

Luming Zhang (M'–) received the Ph.D. degree in computer science from Zhejiang University, China. His research interests include visual perception analysis, image enhancement, and pattern recognition.



Xuelong Li (M'02–SM'07–F'12) is a Full Professor with the State Key Laboratory of Transient Optics and Photonics, Center for OPTical Imagery Analysis and Learning, Xi'an Institute of Optics and Precision Mechanics, Chinese Academy of Sciences, Xi'an, China.



Yang Xiang (SM'–) received the Ph.D. degree in computer science from Deakin University, Australia. He is currently a Full Professor with the School of Information Technology, Deakin University. He is the Director of the Network Security and Computing Lab. He is currently leading his team developing active defense systems against large-scale distributed network attacks. He is the Chief Investigator of several projects in network and system security, Funded by the Australian Research Council. He has authored over 170 research papers in many international journals and conferences. His research interests include network and system security, distributed systems, and networking.