ABACS: An Attribute-Based Access Control System for Emergency Services over Vehicular Ad Hoc Networks

Lo-Yao Yeh, Yen-Cheng Chen, and Jiun-Long Huang

***Abstract*—In this paper, we propose an Attribute-Based Access Control System (ABACS) for emergency services with security assurance over Vehicular Ad Hoc Networks (VANETs). ABACS aims to improve the efficiency of rescues mobilized via emergency communications over VANETs. By adopting fuzzy identity-based encryption, ABACS can select the emergency vehicles that can most appropriately deal with an emergency and securely delegate the authority to control traffic facilities to the assigned emergency vehicles. Using novel cryptographic preliminaries, ABACS realizes confidentiality of messages, prevention of collusion attacks, and fine-grained access control. As compared to the current PKI scheme, the computational delay and transmission overhead can be reduced by exploiting the advantages afforded by message broadcasting, which is heavily used in ABACS. The performance evaluation demonstrates that ABACS is a suitable candidate for realizing emergency services via VANETs.**

***Index Terms*—Attribute-based encryption, access control, emergency management, VANETs**

I. Introduction

WITH THE advancements in wireless communications, it is anticipated that all vehicles will be equipped with a wireless communication device, called an On-Board Unit (OBU), and there will be a number of stationary communication units, called roadside units (RSUs). Both OBUs and RSUs can communicate with each other to enhance road safety. Such a network that is composed of RSUs and OBUs is called a *Vehicular Ad Hoc Network* (VANET). VANETs are regarded as an important development that may serve to improve road safety and satisfy emerging service demands. In addition, VANETs are expected to provide various entertainment-related services, including Internet connection, local information acquisition (e.g., maps and travel guide information), and electronic advertisements [1]. Recently, many communities, including academic, institutions, industries, and governments, have begun researching various aspects of VANETs. IEEE 802.11p, a revised version of 802.11 that is referred to as Wireless Access for the Vehicular Environment (WAVE), has been developed to support Intelligent Transportation System (ITS) applications. 802.11p can be used as the underlying communication protocol in the *Dedicated Short Range Communications* (DSRC) standard [2] for wireless communications between RSUs and vehicles in VANETs.

Communications in VANETs can be classified into roadside-to-vehicle communication (RVC) and intervehicle communication (IVC). DSRC recommends that each vehicle should periodically broadcast traffic-related messages, including position information, current time, vehicle direction, speed, and acceleration/deceleration status. Furthermore, a vehicle will immediately transmit emergency messages when it witnesses a traffic accident. Thus, traffic jams or serious accidents can possibly be prevented if these traffic and emergency messages can be shared among vehicles. Essentially, the traffic-related messages are one-hop broadcasts without message relay, whereas emergency messages are transmitted in a multi-hop fashion to efficiently disseminate information about the occurrence of an emergency event.

Although many possible advantages of VANETs are known, some problems need to be overcome before VANETs can be employed widely. Recently, many studies [1], [3], [4], [5], [6], [7], [8], [9], [10] have addressed potential security and privacy issues in VANETs. Without security assurance in VANETs, any adversary can easily jeopardize a transportation system utilizing VANETs by disseminating bogus messages. Furthermore, vehicles involved in VANET communications may require privacy protection such that they cannot be tracked from the transmitted messages. Indeed, many solutions [1], [3], [5], [11], [7], [12] have been proposed to ensure the security and privacy of VANETs. However, most of these solutions focus on designing efficient and secure message authentication schemes for traffic-related messages. Some papers [13], [14], [15] address secure dissemination of emergency messages in the MAC layer. Only a few studies [4] have considered the security issues of emergency messages.

In this paper, we discuss the secure utilization of VANETs to improve the rescue efficiency when an emergency event occurs. Because the introduction of VANETs is mainly driven by the need to enhance road safety, there is considerable demand for an effective communication process for dealing with a traffic emergency event. Instead of proposing an independent communication scheme for disseminating emergency messages, this paper considers the entire rescue process for an emergency event as an emergency service. A typical scenario of an emergency service is illustrated in Figure 1. In this

Manuscript received 5 January 2010; revised 7 May and 12 July 2010. This work was supported in part by the National Science Council of Taiwan, ROC, under contract NSC 98-2219-E-002-021.

L.-Y. Yeh and J.-L Huang are with the Department of Computer Science, National Chiao Tung University, Hsinchu 300, Taiwan, R.O.C. (e-mail: lyyeh@cs.nctu.edu.tw; jlhuang@cs.nctu.edu.tw).

Y.-C. Chen is with the Department of Information Management, National Chi Nan University, Puli, Nantou 545, Taiwan, R.O.C. (e-mail: ycchen@ncnu.edu.tw) corresponding author.

Digital Object Identifier 10.1109/JSAC.2011.110312.

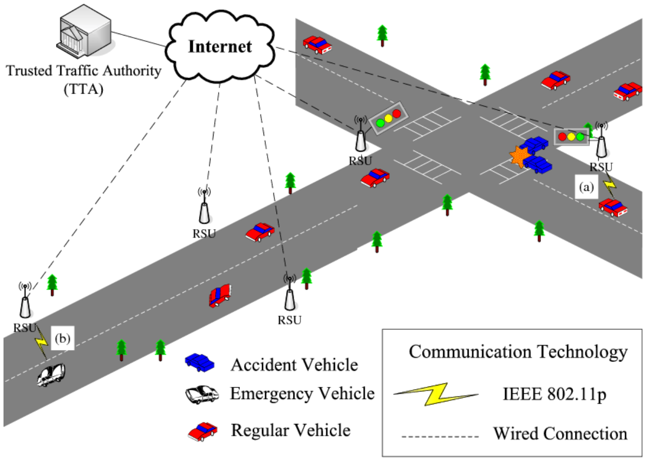


Fig. 1. Emergency Event Processes; (a) Vehicle detects the occurrence of an emergency event. (b) TTA assigns appropriate emergency vehicles to deal with the emergency event and delegates the right to control traffic signals.

emergency scenario, after an emergency event occurs at a road intersection, a witness vehicle immediately reports the emergency event to Trusted Traffic Authority (TTA) through an adjacent RSU. TTA is responsible for assigning the most appropriate emergency vehicles (EVs), such as police vehicles and ambulances, to deal with the emergency event. Moreover, TTA may delegate the authority of controlling traffic facilities, e.g., traffic signals in the neighborhood, to the assigned EVs for better rescue efficiency. During the emergency response, the communications between TTA and EVs should be well protected to ensure the security of message exchanges. The current IEEE Trial-Use standard [16] for VANET security adopts a traditional public-key-based signature scheme, ECDSA, for message authentications. The emergency service may involve many message encryptions and authentications, especially when TTA has to disseminate messages to many *EV*s with distinct public keys. As a result, the communications during the rescue process will be inefficient because several public-key-based encryptions are required for different EVs.

The *EV*s involved in an emergency service are usually those of certain types within a certain area, e.g., police vehicles in the neighborhood. Therefore, the abovementioned communications between TTA and *EV*s may be context-based. That is, TTA may broadcast a query message via the VANET to indicate the context of the emergency event, e.g., location, event type, or rescue requirements. Only EVs within the context will be notified to get involved in the emergency service. This paper will make use of the context-based characteristic to develop a secure and efficient communication system. We introduce an **A**ttribute-**B**ased **A**ccess **C**ontrol **S**ystem for emergency services, named ABACS, over VANETs. To efficiently broadcast rescue-related messages to all EVs, ABACS exploits a novel fuzzy identity-based encryption [17] to realize secure one-to-many broadcast communications. In ABACS, each emergency vehicle is associated with a set of attributes, e.g., *State, County, District, Department, EV_type,* and *ELP* (Electronic License Plate)[6], where the *ELP* is used as the identification attribute of a vehicle. TTA will include a list of attribute values in a broadcast message based on the context of an emergency event. On receiving the broadcast message sent by TTA, each EV looks up the attributes and determines whether it is one of the EVs that the message is destined to. Moreover, only the EVs specified by the attributes can successfully decrypt the message. Accordingly, the most appropriate EVs will be selected to get involved in the rescue process. Therefore, the proposed ABACS affords the following advantages.

1) Rescue efficiency: According to the context of an emergency event, ABACS can effectively find the most appropriate EVs to handle the emergency event. For better rescue efficiency, these EVs also gain the authority to control traffic facilities from ABACS.
2) Scalability: Irrespective of the number of EVs selected, only one message will be broadcast by TTA. Furthermore, due to the nature of broadcasting, the message delivery does not require dynamic routing support in the VANET. Thus, ABACS achieves scalability in terms of the number of EVs.
3) Fine-grained access control: Using well-defined attributes, ABACS can enforce fine-grained access control among various types of EVs. When TTA broadcasts a rescue-related message[1] along with certain attributes, only those EVs that possess the selected attributes can access the rescue-related message.
4) Security properties: Message confidentiality and entity authentication can be realized in ABACS. With fuzzy identity-based encryption, rescue-related messages are well protected. Moreover, each assigned EV is implicitly authenticated by the attributes.

To the best of our knowledge, this paper is the first study that addresses both the security and efficiency issues of emergency services in VANETs based on a provable cryptographic approach.

II. System Model and Cryptographic Preliminaries

A. System Model

A vehicular communication network for emergency services consists of two conceptual layers, as shown in Figure 1. The upper layer is composed of Trusted Traffic Authority (TTA) and RSUs. Connected with each RSU through a secure channel, e.g., the transport layer security (TLS) protocol, TTA is responsible for managing the overall traffic environment. Assume that, at critical intersections, RSUs are installed to serve as gateways to the lower layer. Some RSUs may be installed on traffic signal poles. The traffic signals can be controlled via these RSUs. The lower layer is composed of regular vehicles and emergency vehicles (EVs), such as police vehicles, fire engines, and ambulances. In general, if there are *EV*s standby in emergency report centers (ERCs), these EVs can be easily notified to join a rescue mission via the fixed wired/wireless networks in ERCs. On the other hand, there are other *EV*s on patrol. ABACS can be used to effectively find patrolling *EV*s in the neighborhood and assign a rescue mission to near *EV*s for accelerating the rescue efficiency.

[1] In this paper, the rescue-related messages include the Rescue Query Message (RQM), Rescue Response Message(RRM), and Mission Assign Messge(MAM) introduced in Section III.

According to DSRC, the communication range of an RSU is typically larger than that of vehicles. We assume that TTA and RSUs trust each other and cannot be compromised by adversaries[2]. Moreover, TTA takes charge of public parameter settings and private value configurations for each EV.

B. Requirements

This paper aims to develop a secure and efficient rescue process over VANETs. The functional requirements in terms of security and efficiency are presented as follows.

1) When receiving an emergency event report, TTA can secretly assign appropriate *EV*s to avert eavesdropping by malicious individuals or groups. Moreover, TTA can issue a traffic facility credential to the assigned EVs to control traffic facilities, such as traffic signals.
2) There are several kinds of emergency events whose rescues require *EV*s of different types. An efficient way to find desired *EV*s is essential to accelerate a rescue process.
3) It is possible that some *EV*s may be compromised by adversaries. The adversaries cannot benefit from the information held by the compromised *EV*s.
4) After an emergency event occurs, it is essential that a rescue mission could be enforced immediately and the rescue process be executed efficiently. An effective emergency service should make use of VANET communications to achieve better rescue efficiency.

C. Design objectives

To meet the above requirements, ABACS is proposed to achieve the following objectives.

1) Rescue-related message confidentiality. All rescue-related messages exchanged between TTA and *EV*s should be confidential without revealing any rescue-related information.
2) Fine-grained access control. Through fine-grained access control, only the desired *EV*s will be selected and authorized to join a rescue mission. Therefore, *EV*s can be recruited efficiently via VANETs.
3) Prevention of collusion attacks. If some EVs are compromised by an adversary, the adversary cannot combine parameters/attributes held by the compromised EVs to decrypt the rescue-related messages sent by TTA.
4) Rescue efficiency. TTA can communicate with *EV*s of certain types via a single encrypted rescue-related message sent over VANETs. The message can only be decrypted by specific *EV*s. As a result, the proposed scheme can efficiently find the most appropriate *EV*s and delegate the authority to control traffic facilities to them.

D. Cryptographic Preliminaries

1) Bilinear Pairing: Recently, bilinear pairing has been widely adopted to develop various security schemes [3], [5], [17], [18], [19] because of its smaller computational cost and transmission overhead, as compared to traditional cryptographic algorithms, such as RSA or ElGamal [3]. The proposed scheme adopts bilinear pairing in the underlying cryptosystem. We briefly introduce bilinear pairing as follows.

Definition 1: (Admissible Bilinear Map [20]): Let G and G_1 be two cyclic additive groups, and G_T be a cyclic multiplicative group of the same prime order q. Let P and P_1 be two generators of G and G_1, respectively. An admissible bilinear map is a map $\hat{e}$: $G \times G_1 \rightarrow G_T$ with the following properties.

1) Bilinearity: $\forall (R, Q) \in G \times G_1$, and $\forall a, b \in Z_q^*$; $\hat{e}(aR, bQ) = \hat{e}(R, bQ)^a = \hat{e}(aR, Q)^b = \hat{e}(R, Q)^{ab}$.
2) Non-degeneracy: $\hat{e}(P, P_1) \neq 1_{G_T}$.
3) Computability: There exists a polynomial algorithm to compute $\hat{e}(R, Q)$, for all $(R, Q) \in G \times G_1$.

Definition 2: (Bilinear Parameter Generator [20]): A bilinear parameter generator $\mathcal{G}$ is a probabilistic algorithm that takes a security parameter k as an input and outputs (q, P, P_1, G, G_1, G_T, $\hat{e}$) satisfying that q is a prime with $2^k < q < 2^{k+1}$, $|G|=|G_1|=|G_T|=q$, and $\hat{e}$: $G \times G_1 \rightarrow G_T$. There exists an isomorphism ψ: $G_1 \rightarrow G$ with $\psi(P_1) = P$. Therefore, the generator $\mathcal{G}(k)$ generates (q, P, G, G_T, $\hat{e}$) for simplicity, where $\hat{e}$: $G \times G \rightarrow G_T$.

The following underlying assumptions [17] exist with the respect to the security foundations of the proposed protocol.

1) **Elliptic Curve Decisional Bilinear Diffie-Hellman (ECBDH)**: *Suppose a challenger chooses a, b, c, d* $\in Z_q$ *at random. The Decisional ECBDH assumption is that no polynomial-time adversary is to be able to distinguish the tuple* ($A = aP$, $B = bP$, $C = cP$, $Z = e(P, P)^{abc}$) *from the tuple* ($A = aP$, $B = bP$, $C = cP$, $Z = e(P, P)^z$) *with more than a negligible advantage.*
2) **Elliptic Curve Decisional Modified Bilinear Diffie-Hellman (ECMBDH)**: *Suppose a challenger chooses a, b, c, d* $\in Z_q$ *at random. The Decisional ECMBDH assumption is that no polynomial-time adversary is to be able to distinguish the tuple* ($A = aP$, $B = bP$, $C = cP$, $Z = e(P, P)^{\frac{ab}{c}}$) *from the tuple* ($A = aP$, $B = bP$, $C = cP$, $Z = e(P, P)^z$) *with more than a negligible advantage.*

2) Secret Sharing Scheme: The concept of secret sharing was introduced by Shamir [21]. In a secret sharing scheme, a dealer distributes a secret s among a set of n players, $P = \{P_1, ..., P_n\}$. Each player P_i holds a piece s_i of the secret s. In order to recover the secret s, it is necessary to collect several or all pieces s_i of the secret s. A (t, n)-threshold secret sharing scheme is a particular case in which at least t pieces of s_i are required to retrieve the secret s. A typical secret sharing example is Shamir's threshold secret sharing scheme based on Lagrange polynomial interpolation [21], as described below.

Let Z_q be a finite field with $q > n$, and $s \in Z_q$ be the main secret to be shared. First, the dealer chooses a random polynomial $f(x)$ with degree $t - 1$ such that $f(0) = s$. The polynomial can be written as $f(x) = a_0 + a_1 x + ... + a_{t-1} x^{t-1}$ $= a_0 + \sum_{j=1}^{t-1} a_j x^j$ where $a_0 = s$ and $a_j \in_R Z_q$. Next, the dealer

[2] Some schemes [1], [11] can be applied to implicitly authenticate RSUs to prevent the bogus RSU attack.

TABLE I
NOTATIONS

Notation	Descriptions
EV	Emergency vehicle
RSU	Roadside unit
TTA	Trusted traffic authority
$\mathcal{UA}$	Universe attributes
$\mathcal{DA}$	Dummy attributes
$\widehat{ID}_{EV}$	Identity of an emergency vehicle
$\widehat{ID}_{M}$	Identity of message M
RQM	Rescue query message
RRM	Rescue response message
MAM	Mission assignment message
TFC	Traffic facility credential
G	Cyclic additive group
G_T	Cyclic multiplicative group
P	Generator of the cyclic group G
q	Order of the group G and G_T
$\hat{e}$	Bilinear map: $G \times G \to G_T$
d	Minimal number of overlapped attributes
$f(x)$	Polynomial with d-1 degrees
$\triangle_{i,S}$	Lagrange coefficient of a set S
t_i, y	Master keys of TTA, where i = 1,...,$\vert\mathcal{UA}\vert + d - 1$
z, v, r	Random numbers
σ	Credential signature
T_{expire}	Expired time for credential signature
h(.)	Collision-free one-way hash function such as SHA-1
||	Message concatenation operation

assigns a known value $\omega_i \in Z_q$ to each player P_i, and privately delivers the share $s_i = f(\omega_i)$ to P_i, for i = 1,...,n. As a result, a set of $\mathcal{L} \subset P$ with $|\mathcal{L}| \geq t$ is able to obtain the secret $s = f(0)$ by interpolating the set of shares s_i held by each $P_i \in \mathcal{L}$ as follows.

$$s = f(0) = \sum_{P_i \in \mathcal{L}} s_i \lambda_i^{\mathcal{L}} = \sum_{P_i \in \mathcal{L}} s_i(\prod_{P_j \in (\mathcal{L} \backslash P_i),} \frac{x-j}{i-j})$$

where parameters $\lambda_i^{\mathcal{L}}$ are called the Lagrange coefficients. It has been proven that it is impossible to retrieve the secret s with less than t players [21].

III. ATTRIBUTE-BASED ACCESS CONTROL SYSTEM (ABACS) FOR EMERGENCY SERVICES

In this section, we introduce the attribute-based access control system (ABACS) for emergency services in detail. Figure 2 illustrates the rescue process flow in the emergency scenario. A rescue process comprises an emergency event report phase, emergency vehicle recruiting phase, and rescue mission dispatch phase. In general, ABACS works as follows.

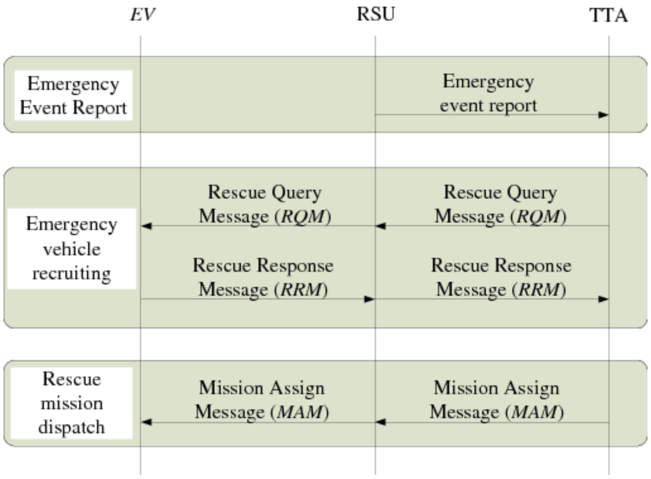

EV
RSU
TTA
Emergency Event Report
Emergency event report
Emergency vehicle recruiting
Rescue Query Message (RQM)
Rescue Query Message (RQM)
Rescue Response Message (RRM)
Rescue Response Message (RRM)
Rescue mission dispatch
Mission Assign Message (MAM)
Mission Assign Message (MAM)

Fig. 2. Rescue process flow for an emergency event

- Emergency event report phase: When an emergency event occurs, the witness vehicle sends an emergency event report message [4], which contains emergency event type and location, to an adjacent RSU. The RSU first confirms the validity of the emergency event report message.[3] If the emergency event report message is invalid, the RSU drops this message; otherwise, the RSU informs TTA of the emergency event.
- Emergency vehicle recruiting phase: After receiving the emergency event report from the RSU, TTA issues a rescue query message (RQM) to search the most appropriate EVs to deal with the emergency event. While obtaining an RQM, if an EV is available, the EV will send a rescue response message (RRM) back to TTA to confirm that it can tackle the emergency event.
- Rescue mission dispatch phase: Based on RRMs obtained from available EVs, TTA can determine which ones are most suitable for the rescue mission. Finally, TTA sends a mission assignment message (MAM), containing a traffic facility credential (TFC), to the assigned EVs. The TFC can be used to control the traffic facilities with the aid of RSUs for better rescue efficiency.

In ABACS, we focus on the design of the emergency vehicle recruiting phase and rescue mission dispatch phase, because the emergency event report phase can adopt the current standard ECDSA scheme or related works [4]. Note that the rescue-related messages, including RQM, RRM and MAM, should be well protected without leakage of information. For ease of reference, Table I lists the notations used throughout the following description of the proposed system.

A. System Initiation

There exist various emergency vehicles. In ABACS, each EV can be described by a set of attributes. Let d be the minimal number of attributes required for selecting *EV*s by TTA to select EVs. In the following parameter setup phase, TTA will associate a random d-1 degree polynomial $f(x)$ with each EV with the restriction that the value of point 0 in each polynomial is the same, as denoted by $f(0) = y$.

1) Parameter Setup: Initially, TTA sets up the public parameters as follows. Let G be a cyclic additive group generated by P, and G_T be a cyclic multiplicative group. G and G_T have the same prime order q such that $|G|$ = $|G_T|$ = q. A security parameter k determines the size of the groups. There exists an admissible bilinear map $\hat{e}$: $G \times G \to G_T$ that satisfies the following properties.

1) Bilinearity: $\forall V$, Q, $R \in G$, and $\forall a, b \in Z_q^*$, $\hat{e}(Q, V+R)$ = $\hat{e}(Q,V) \cdot \hat{e}(Q,R)$. In particular, $\hat{e}(aP, bP)$ = $\hat{e}(aP,P)^b$ = $\hat{e}(P,P)^{ab}$ = $\hat{e}(P,aP)^b$ = $\hat{e}(bP,aP)$.

[3] Emergency event report messages can be verified by the current standard ECDSA method [16] or other schemes [4].

2) Non-degenerate: If V, $R \in G$ then $\hat{e} : (V, R) \neq 1_{G_T}$.
3) Computability: There exists an efficient algorithm to compute $\hat{e}(V, R)$ for $\forall V, R \in G$.

The identity of each EV will be a subset of the universe attributes $\mathcal{UA}$. For instance, an EV can be identified by the following attributes {*State, County, District, Department, EV_type, ELP*} as identity $\widehat{ID}_{EV}$. In the list of attributes, *EV_type* is used to indicate the type of an *EV*, for instance, a police car or an ambulance. The *ELP* (Electronic License Plate)[6], i.e., car license number, can be independently used to uniquely identify an *EV*. When receiving a rescue-related message with identity $\widehat{ID}_M$, an EV can check whether $|\widehat{ID}_{EV} \bigcap \widehat{ID}_M| \geq d$. If yes, the EV can successfully decrypt the rescue-related message; otherwise, the rescue-related message is not meant for the *EV* and can be discarded.

According to the requirements of an emergency service, TTA first defines the universe attributes $\mathcal{UA}$. For simplicity, we assume 1,.., $|\mathcal{UA}|$-1 (mod q) are the indices used to represent all the possible universe attributes except for *ELP*. We use $|\mathcal{UA}|_{EV_i}$ to indicate the *ELP* attribute of each EV. Moreover, TTA also chooses d-1 dummy attributes $\mathcal{DA}$, which are used in mission assignments. Similarly, we assume ($|\mathcal{UA}|$ + 1),..., ($|\mathcal{UA}|$ + d - 1) as the indices required to represent all dummy attributes. Next, TTA chooses $t_1, ...t_{|\mathcal{UA}|-1}, t_{|\mathcal{UA}|_{EV_i}}, t_{|\mathcal{UA}|+1}, ..., t_{|\mathcal{UA}|+d-1}$ uniformly at random from Z_q, and selects y uniformly at random from Z_q. Finally, TTA publishes the following public parameters[4]:

$$T_1 = t_1 P,\ ...,\ T_{|\mathcal{UA}|-1} = t_{|\mathcal{UA}|-1} P,\ T_{|\mathcal{UA}|+1_1} = t_{|\mathcal{UA}|+1} P, ...,\ T_{|\mathcal{UA}|+d-1} = t_{|\mathcal{UA}|+d-1} P,\ Y = \hat{e}(P, P)^y.$$

The master key is:

$$t_1, ...t_{|\mathcal{UA}|-1}, t_{|\mathcal{UA}|_{EV_i}}, t_{|\mathcal{UA}|+1}, ..., t_{|\mathcal{UA}|+d-1}, y.$$

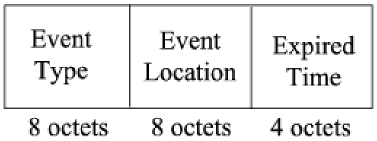
For ease of presentation, we define the Lagrange coefficient $\triangle_{i,S}$ for $i \in Z_q$ and a set S of attributes in Z_q:

$$\triangle_{i,S}(x) = \prod_{j \in S \setminus i} \frac{x - j}{i - j} \tag{1}$$

2) Key Generation: TTA is responsible for generating the private key values for each EV. First, it determines the proper attributes for describing an EV as its identity $\widehat{ID}_{EV} \subseteq \mathcal{UA}$, and randomly chooses a polynomial $f(i)$ with $d-1$ degree such that $f(0) = y$. Moreover, each EV also defines d - 1 dummy attributes $\mathcal{DA}$. The private key values for the *EV* are $(D_i)_{i \in \widehat{ID}_{EV} \cup \mathcal{DA}}$, where $D_i = \frac{f(i)}{t_i} P$ for each $i \in \widehat{ID}_{EV} \cup \mathcal{DA}$. These private key values are preloaded to the *EV* in the manufacture phase or via a secure channel outside the VANETs.

B. Emergency Vehicle Recruiting Phase

When receiving an emergency event report forwarded by any RSU, TTA will generate a rescue query message (RQM) and then broadcast it over the VANETs. RQM broadcasting is used to find appropriate EVs. If any EV is able to join the rescue mission, the EV will reply with a rescue response message (*RRM*). Both RQM and RRM should be transmitted securely. The proposed encryption scheme for RQM and RRM is described as follows.



Event Type	Event Location	Expired Time
8 octets	8 octets	4 octets

Fig. 3. Rescue Query Message Format

1) Rescue Query Message (RQM)
   a) RQM Generation: TTA generates an RQM to query available EVs. The RQM includes the emergency event type, location, and expired time as illustrated in Figure 3.
   b) RQM Identity Selection: Before sending the RQM, TTA determines the identity $\widehat{ID}_{RQM}$ of the RQM based on the context of the emergency event. $\widehat{ID}_{RQM}$ is composed of a set of attribute values that describe the EVs required to join the rescue mission. For instance, TTA may require EVs of certain types within a specific district or administrated by a certain department.
   c) RQM Encryption: After generating $RQM \in G_T$ and selecting the proper identity $\widehat{ID}_{RQM}$, TTA chooses a random value $z \in Z_q^*$ that makes ABACS a probabilistic encryption scheme. Then, the encrypted *RQM* is published as
      $E = (\widehat{ID}_{RQM}, E' = RQM \cdot Y^z, \{E_i = zT_i\}_{i \in \widehat{ID}_{RQM}})$
      E is then broadcast over the VANETs.
   d) RQM Decryption: When an *EV* receives an encrypted RQM, it determines whether the RQM can be decrypted by checking $|\widehat{ID}_{EV} \bigcap \widehat{ID}_{RQM}| \geq d$. If not, the encrypted message is discarded. If yes, the EV extracts theRQM by computing
      $$E' / \prod_{i \in S} (\hat{e}(D_i, E_i))^{\triangle_{i,S}(0)} = RQM$$
      where the attribute set S = $(\widehat{ID}_{EV} \bigcap \widehat{ID}_{RQM})$. The decryption can be verified as follows.

$$\begin{aligned} & E' / \prod_{i \in S} (\hat{e}(D_i, E_i))^{\triangle_{i,S}(0)} \\ =& RQM \cdot \hat{e}(P, P)^{zy} / \prod_{i \in S} (\hat{e}(\frac{f(i)}{t_i} P, z t_i P))^{\triangle_{i,S}(0)} \\ =& RQM \cdot \hat{e}(P, P)^{zy} / \prod_{i \in S} (\hat{e}(P, P)^{z f(i)})^{\triangle_{i,S}(0)} \\ =& RQM \cdot \hat{e}(P, P)^{zy} / (\hat{e}(P, P)^{z(\sum_{i \in S} f(i) \cdot \prod_{j \in S \setminus i} \frac{x-j}{i-j})}) \\ =& RQM \cdot \hat{e}(P, P)^{zy} / (\hat{e}(P, P)^{z(y)}) \\ =& RQM \end{aligned}$$

2) Rescue Response Message (RRM)
   a) RRM Generation: The fields of an RRM are vehicle identity, vehicle type, vehicle location, vehicle

[4] Note that the parameter $T_{|\mathcal{UA}|_{EV_i}}$ is only used for the *ELP* of an individual EV. It is not necessary to make the parameter public. However, the parameter could be queried from TTA while it is required in some cases.

Vehicle ELP	Vehicle Location	Vehicle Direction	Vehicle Velocity
4 octets	8 octets	4 octets	4 octets

Fig. 4. Rescue Response Message Format

Traffic Facility Credential			Credential Signature
Assigned Vehicle ELPs	Expired Time	(Optional)	
16 octets	4 octets	(16 octets)	20 octets

Fig. 5. Mission Assignment Message Format

direction, and vehicle velocity, as illustrated in Figure 4.

b) RRM Encryption: To ensure the confidentiality, the EV chooses a random number $v \in Z_q^*$ and encrypts the RRM based on Elliptic Curve ElGamal encryption as follows.

$$C = (C^{''} = RRM + vT_1, V = vP)$$

C is then sent to TTA by a unicast over the VANETs.

c) RRM Decryption: While obtaining the ciphertext C, TTA extracts RRM by computing

$$\begin{aligned}&C^{''} - t_1V\\ =&RRM + vT_1 - t_1V\\ =&RRM + v \cdot t_1P - t_1 \cdot vP\\ =&RRM\end{aligned}$$

C. Rescue Mission Dispatch Phase

After receiving RRMs in a predefined short time period, TTA will dispatch the most appropriate EVs to deal with the emergency event. TTA generates a mission assignment message (MAM) for the assigned EVs. For better rescue efficiency, the MAM contains a traffic facility credential (TFC) that is used to delegate the authority to control traffic facilities. Using the TFC, the assigned EVs can control traffic signals or other facilities around the area where an emergency event has occurred.

1) Mission Assignment Message (MAM)

a) MAM Generation: An MAM contains the traffic facility credential (TFC) and the credential signature (σ), as illustrated in Figure 5. Note that the TFC contains the *ELP*s[5] of the delegated EVs and T_{expire} for enabling the selected EVs to control traffic facilities before the time specified by T_{expire}. Note that if secure communications between the selected EVs are required, the optional field can be used for assigning a session key. To guarantee the validity of TFC , TTA also creates a credential signature σ as follows.

$$\sigma = h(TFC||T_{expire}) \cdot yP$$

a) MAM Identity Selection: TTA may assign multiple EVs to cooperatively tackle a serious emergency event. Therefore, TTA takes advantage of dummy attributes $\mathcal{DA}$ to ensure that only the assigned EVs can decrypt the encrypted MAM. TTA selects all the *d*-1 dummy attributes $\mathcal{DA}$ as well as the *ELP* attributes of the assigned EVs as the identity $\widehat{ID}_{MAM}$. Therefore, an assigned EV can decrypt the encrypted MAM based on its own ELP attribute as well as the *d*-1 dummy attributes.

b) MAM Encryption: In a manner similar to RQM encryption, TTA randomly selects $r \in Z_q^*$ and generates the ciphertext $\overline{E}$ as follows.

$\overline{E} = (\widehat{ID}_{MAM}, \overline{E}' = MAM \cdot Y^r, \{E_i = rT_i\}_{i\in\widehat{ID}_{MAM}})$

To avoid redundant transmissions, TTA only sends $\overline{E}$ by multicasting to those RSUs where the assigned EVs are converging.

c) MAM Decryption: While obtaining the ciphertext $\overline{E}$, each EV examines whether $|(\widehat{ID}_{EV} \cup \mathcal{DA}) \bigcap \widehat{ID}_{MAM}| \geq d$. If not, the EV drops the MAM; otherwise, the EV realizes that it has been assigned to go on the rescue mission, and then obtains the TFC and σ[6] from *MAM* by calculating

$$\begin{aligned}&E'/\prod_{i\in S}(\hat{e}(D_i, E_i))^{\triangle_{i,S}(0)}\\ =&MAM\end{aligned}$$

where the attribute set $S = (\widehat{ID}_{EV} \cup \mathcal{DA}) \bigcap \widehat{ID}_{MAM}$. The verification of MAM decryption is shown as follows.

$$\begin{aligned}&E'/\prod_{i\in S}(\hat{e}(D_i, E_i))^{\triangle_{i,S}(0)}\\ =&MAM \cdot \hat{e}(P,P)^{ry}/\prod_{i\in S}(\hat{e}(\frac{f(i)}{t_i}P, rt_iP)^{\triangle_{i,S}(0)}\\ =&MAM \cdot \hat{e}(P,P)^{ry}/\prod_{i\in S}(\hat{e}(P,P)^{rf(i)})^{\triangle_{i,S}(0)}\\ =&MAM \cdot \hat{e}(P,P)^{ry}/(\hat{e}(P,P)^{r(\sum_{i\in S} f(i)\cdot \prod_{j\in S\setminus i}\frac{x-j}{i-j})})\\ =&MAM \cdot \hat{e}(P,P)^{ry}/(\hat{e}(P,P)^{r(y)})\\ =&MAM\end{aligned}$$

2) Traffic Facility Credential Verification

As a rescue mission proceeds, an assigned EV may send TFC and credential signature σ to ask RSUs to control traffic facilities. When an RSU receives the TFC and credential signature σ, the RSU believes the TFC is valid if

[5] In general, we assume that four EVs are assigned to handle an emergency event. In addition, the field of the assigned vehicle ELPs is extensible.

[6] The credential signature σ can be used to ensure the integrity of TFC and to implicitly confirm that the MAM is sent by TTA.

$\hat{e}(\sigma, P) = Y^{h(TFC||T_{expire})}$, as verified below.

$$\begin{aligned}&\hat{e}(\sigma, P)\\ =&\hat{e}(h(TFC||T_{expire})yP, P)\\ =&\hat{e}(P, P)^{h(TFC||T_{expire})y}\\ =&Y^{h(TFC||T_{expire})}\end{aligned}$$

If the verification is valid, the EV gains the authority to control the traffic signals/facilities governed by the RSU. After the EV applies the authority to control the traffic signal/facilities, the RSU will send a control acknowledgement to TTA to confirm that the EV has accepted the mission.

D. Discussion

1) Computational Delay: To further investigate the rescue efficiency, we first evaluate the computational delay of ABACS. In a manner similar to previous analyses [4], [5], [12], we mainly focus on the cost of point multiplication in elliptic curve and pairing computations, which require the most computation time. Let T_{mul} denote the time required to perform one point multiplication in an elliptic curve, and T_{pair} be the time required to execute a pairing operation. We adopt the experiment in [22] in which the processing time (in milliseconds) was observed for a super-singular curve of embedding degree k = 6 over $\mathbb{F}_{3^{97}}$ and executed it on an Athlon XP 2 GHz machine. The following results were obtained: T_{mul} = 0.78 ms and T_{pair} = 2.82 ms. Based on the computational delay of cryptographic operations, we can calculate the total computational delay of a complete round, denoted as T_{V_total}, in ABACS for an EV as follows.

$$\begin{aligned}T_{V\_total} &= (dT_{pair} + 1T_{mul}) + (2T_{mul}) + (dT_{mul} + 1T_{mul})\\ &= 2dT_{pair} + 4T_{mul}\\ &= 2d \times 2.82 + 4 \times 0.78\ ms\end{aligned}$$

That is, the decryption of RQM or MAM requires $d\ T_{pair}$ for the product of sum and $1T_{mul}$ for point multiplication with Lagrange coefficient $\triangle_{i,S}$. The encryption of RRM requires 2 T_{mul} based on Elliptic Curve ElGamal cryptography.

2) Receiving Ratio Analysis : In the rescue mission dispatch phase of ABACS, TTA delivers an MAM to the assigned EVs. To minimize bandwidth consumptions, TTA only delivers the MAM by means of multicasting to the RSUs whose signal coverage includes the assigned EVs. That is, the MAM is sent back to the same RSUs where the previous *RRM*s came from. However, *EV*s may move away from the RSUs during the emergency vehicle recruiting phase. Therefore, TTA has to generate the MAM within a stringent time limit. Moreover, to find the most appropriate EVs to deal with the emergency event, TTA needs to wait for a short time period ξ in order to receive more RRMs from different EVs. Therefore, we analyze the relationship between the vehicle movement speed v and the short waiting period ξ. The following assumptions are made to simulate a practical scenario:

- The average speed of emergency vehicles (denoted as v) ranges from 20 m/s ~ 50 m/s (or 72 km/hr ~ 180 km/hr). The valid coverage range of an RSU (denoted as C_{RSU}) is 300 m [7], [12].
- The number of attributes required for selecting an EV is 4 (d = 4) and 10 (d = 10). Therefore, the total computation delay T_{V_total} is (2 × 4) × 2.82 + 4 × 0.78 = 25.68 ms and (2 × 10) × 2.82 + 4 × 0.78 = 59.52 ms, respectively.

To evaluate the receiving ratio of an EV, we first estimate the required coverage range (denoted by C_{req}) over which an RSU successfully transmits the MAM to the assigned EV. The minimal required coverage range of an RSU is

$$C_{req} = v \times T_{V\_total}$$

Then, we further discuss the receiving ratio, denoted as R_{ratio}, by considering the coverage range C_{RSU} of an RSU and the short waiting period ξ. The following formula can be used to estimate the receiving ratio R_{ratio}.

$$R_{ratio} = \frac{C_{RSU}}{C_{req} \times \xi} = \frac{C_{RSU}}{v \times T_{V\_totoal} \times \xi}$$

where $C_{RSU} \geq C_{req}$. Finally, R_{ratio} can be measured as

$$R_{ratio} = \begin{cases} 1 & ,\text{if } \frac{C_{RSU}}{T_{V\_total}} \cdot \frac{1}{v \times \xi} \geq 1; \\ \frac{C_{RSU}}{T_{V\_total}} \cdot \frac{1}{v \times \xi} & ,\text{otherwise.} \end{cases}$$

Figure 6, with d = 4 and T_{V_total} = 25.68 ms, shows the receiving ratio with respect to velocity v, $20 \leq v \leq 50$, and waiting period ξ, $0 \leq \xi \leq 300$. It is observed that an EV can successfully receive the MAM when $20 \leq v \leq 39$ and $1 \leq \xi \leq 233$. Therefore, the proposed ABACS works well in most cases when d = 4. In the case of d = 10 and T_{V_total} = 59.52 ms, the receiving ratio is shown in Figure 7. The receiving ratio is 100% only when $1 \leq \xi \leq 100$. The analysis indicates that the receiving ratio decreases due to the greater computational delay that is caused by the use of a larger d. To cope with this problem, in the next subsection, a predictive transmission method is proposed to increase the receiving ratio.

3) Predictive Transmission: In this subsection, we propose a predictive transmission method to increase the receiving ratio for delivering MAMs. The following assumptions are required for the predictive transmission.

- TTA has the location information of each RSU, denoted as L_{RSU}.
- The transmission ranges of neighboring RSUs are partly overlapped.

The scenario of the predictive transmission is shown in Figure 8. In the emergency scenario, an EV has received an RQM via RSU1, and TTA performs predictive transmission for the neighboring RSU, i.e., RSU2, based on the probability that the EV enters the area covered by RSU2. Assume C_{RSU} is the transmission range of an RSU, *Dir* is the direction of the EV, and ℓ is the distance between EV and RSU2. Moreover, we assume that the locations of EVs are randomly distributed according to a uniform distribution, which has been widely assumed in previous literatures [7], [23], [24]. According to

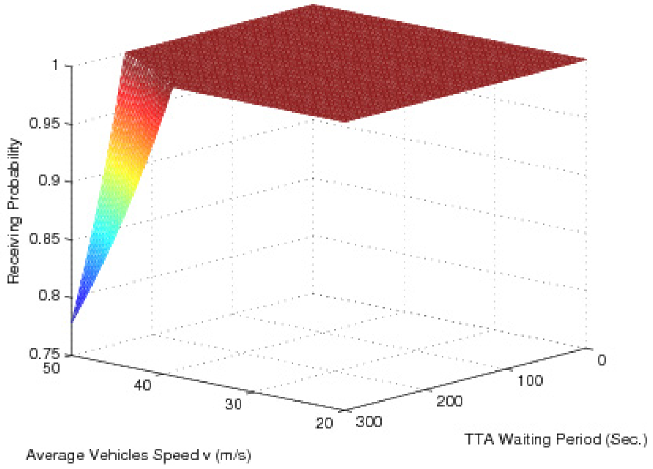


Fig. 6. Receiving ratio of an emergency vehicle ($d = 4$, T_{V_total} = 25.68 ms)

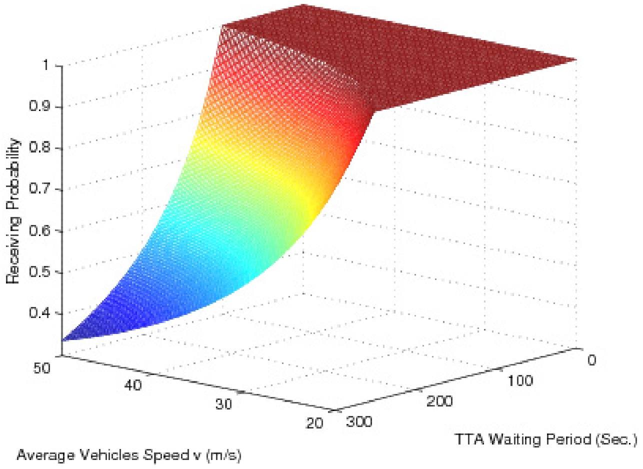


Fig. 7. Receiving ratio of an emergency vehicle ($d = 10$, T_{V_total} = 59.52 ms)

[7], the probability density function of the distance between the EV and reference RSU2 is measured as

$$f(\ell) = \frac{1}{v\cdot(\xi + T_{C\_TTA})}, \quad 0 \le \ell \le v\cdot(\xi + T_{C\_TTA}) \tag{2}$$

where v is the velocity of the EV, ξ is the short waiting period, and T_{C_TTA} represents the delay caused by TTA in assigning the appropriate EV and generating the corresponding MAM. Based on the analysis of previous studies [7], [25], the velocity of an EV is assumed to follow a truncated Gaussian distribution with parameter ($\overline{v}$, σ^2). Therefore, the probability (denoted as P_{enter}) that the EV enters the transmission range of RSU2 in the $(\xi + T_{C\_TTA})$ time interval can be measured as

$$P_{enter} = P(\ell - C_{RSU} < v\cdot(\xi + T_{C\_TTA})|v)$$

which can be expressed as follows.

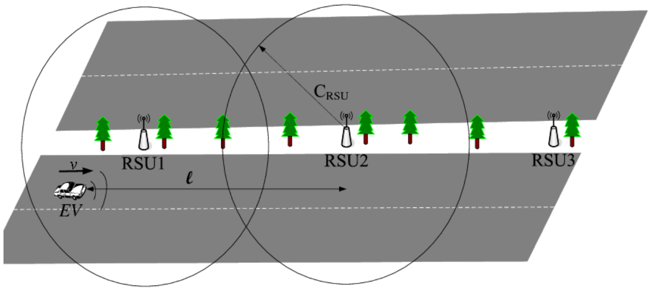


Fig. 8. Predictive transmission scenario

$$\begin{cases} \text{if } Dir \text{ is } opposite, \quad P_{enter} = 0 \\ \text{if } Dir \text{ is } toward, \quad P_{enter}= \\ \iint P(\ell < v\cdot(\xi + T_{C\_TTA}) + C_{RSU}|v) f(\ell)\; d\ell dv, \\ = \frac{1}{\sigma\sqrt{2\pi}(v\cdot(\xi+T_{C\_TTA}))}\int_{vL}^{vH}(v\cdot(\xi+T_{C\_TTA})+C_{RSU}) \\ \cdot exp(\frac{-1}{2}(\frac{v-\overline{v}}{\sigma})^2)\; dv \end{cases} \tag{3}$$

As a result, TTA can predict the entering probability P_{enter} to determine whether neighboring RSUs can help to deliver the MAM to the EVs.

IV. Security analysis

The security of the proposed ABACS is analyzed as follows.

1) Rescue-related message confidentiality: Based on Elliptic Curve Decisional Bilinear Diffie-Hellman (ECBDH) and Modified Bilinear Diffie-Hellman (ECMBDH) assumptions [17], the confidentiality of the rescue-related message is guaranteed. The security of the adopted fuzzy identity-based encryption has been proven in [17]. In [17], a fuzzy selective-ID model is used to show that the probability of the overall advantage of an adversary is only $\frac{1}{2}\epsilon$ for each bit. That is, an adversary cannot gain a advantage greater than guessing a bit without any information.
2) Fine-grained access control: In ABACS, each emergency vehicle (EV) possesses a set of attributes as its identity. Through the set of attributes, TTA can decide which types of EVs are able to decrypt the rescue-related messages to achieve fine-grained access control.[7] Because each EV holds a unique *ELP* and corresponding private key values, TTA can customize an identity for a multicast message intended to the desired EVs. Not only the computational delay but also the transmission overhead can be reduced by ABACS.
3) Prevention of collusion attacks: To prevent collusion attacks, ABACS randomly chooses different polynomials for distinct EVs. Therefore, each EV will keep different private key values generated with different polynomials. As a result, even if some EVs are compromised, an attacker cannot combine their private key values to derive the master private key values [17].

[7] To provide further fine-grained access control, the key-policy attribute-based encryption (KP-ABE) [26] can be adopted.

4) Rescue efficiency and security: One of the advantages of ABACS is the efficient communications between TTA and EVs, which are achieved by attributed-based multicast. Moreover, the assigned EVs can rapidly join a rescue mission with the aid of the received *TFC* for controlling traffic signals and facilities. As compared to the current VANET security standard [16], ABACS can secretly and efficiently deliver the rescue-related messages to EVs without requiring additional key-establishment phases [1].

V. Performance Evaluation

In this section, we evaluate the performance of ABACS in terms of computational delay and transmission overhead. To the best of our knowledge, there is no similar security scheme for emergency services. Therefore, we compared ABACS with the ECDSA scheme, which is adopted by the current IEEE1609.2 standard [16] as a security scheme for VANETs.

A. Computational Delay

As described in Section III-D1, the total computational delay (denoted as T_{V_total}) for an EV in ABACS is $2d \times T_{pair}$ + 4 $\times$ T_{mul} ms. Here, we focus on the computational delay for TTA, because TTA is designed to handle all rescue-related messages sent from a number of EVs. Table II shows the computational delay of the dominant cryptographic operations, including point multiplication T_{mul} and bilinear pairing T_{pair}, for TTA in ABACS and ECDSA schemes in communications with a single *EV* or multiple *EV*s. Since ECDSA does not provide message confidentiality, we assume that the Elliptic Curve ElGamal encryption is adopted in ECDSA. Thus, it costs 2 T_{mul} for an encryption operation and 1 T_{mul} for a decryption operation. According to [5], [27], the time required to perform ECDSA signature and certificate verification is 4 T_{mul}, and the time required to sign an ECDSA message is 1 T_{mul}. Therefore, an encryption in ECDSA costs 3 T_{mul} (EC ElGamal encryption + ECDSA signing) and a decryption in ECDSA costs 5 T_{mul} (ECDSA verification + EC ElGamal decryption). An RQM encryption in ABACS requires 1 T_{mul} for $\bar{E}$ and i T_{mul} for E_i, where i is the total number of selected attributes ($i \geq d$). For ease of evaluation, we set i = d + 2 in the following performance evaluation. A decryption in ABACS requires 1 T_{mul} for EC ElGamal decryption. The computational delay for an MAM encryption is $(a+d-1)T_{mul}$, in which aT_{mul} is for the ELPs attributes of the assigned EVs and $(d-1)T_{mul}$ is for the dummy attributes.

Referring to [22], the computational delay for T_{mul} and T_{pair} is 0.78 ms and 2.82 ms, respectively. Figure 9 (a) shows the relationship between the computational delay and the number of queried emergency vehicles (n), if the number of assigned EVs involved in a rescue is 5 (a = 5). It is observed that ABACS can greatly reduce the computational delays for different values of d. Moreover, Figure 9 (b) shows the ratio of the computational delay of ABACS to that of ECDSA. In a general rescue mission with only a few assigned *EV*s, ABACS is more than 80% faster than ECDSA when the number of queried EVs is greater than 40. Moreover, we investigate the computational delay for an disaster event requiring different numbers of assigned *EV*s. As shown in Figure 10 (a), when 100 EVs are queried, i.e., *n* = 100, ABACS achieves smaller computational delays than ECDSA for different numbers of assigned *EV*s. In fact, ABACS generates only an MAM for all the assigned EVs, whereas ECDSA has to produce distinct MAMs to individual *EV*s. This also explains why the computational delays in ABACS moderately increases by at most 163.8 ms (d = 4) and 173.16 ms (d = 10), as the number of assigned *EV*s increases. On the other hand, the computational delay in ECDSA also increases as more *EV*s are assigned; however, all are greater than 626.34 ms due to the computations in RQM and RRM. The computational delay ratios, illustrated in 10 (b), show that the computational delay of ABACS is only at most only 19% and 20.1% of that of ECDSA when d = 4 and d = 10, respectively.

B. Transmission Overhead

In this section, we compare the transmission overhead of the two schemes. The transmission overhead mostly arises from the communications between TTA and the RSUs. The following evaluation focuses on the transmission overhead introduced by the signature, certificate, and encryption/decryption parameters, while the message itself is not considered. According to [16], the format of a signed message contains a 56-byte ECDSA signature and a 125-byte certificate. In ABACS, the transmitted parameters of RQM include 4*i bytes[8] for the identity and 20*i bytes for the decryption parameters, where i is the total number of selected attributes ($i \geq d$). As in Section V-A, we set i = d + 2 in the following performance evaluation. As for RRM, the parameters consist of 4 bytes for the identity, and 20 bytes for the decryption parameters. With regard to MAM, the parameters consist of 4 * (a + d - 1) for the identity, 20 bytes for the encrypted credentials, and 20 * (a + d - 1) for the decryption parameters. According to DSRC [2], the bandwidth of a wireless data channel in VANETs is 10 MHz, corresponding to a channel data rate within the range of 3-27 Mb/s [28]. A typical data rate of 6 Mb/s is usually assumed for VANETs. Under the assumption of d = 10 and i = 12, the length of RQM will be 4*12 + 20 + 20*12 = 308 bytes. According to [5], there can be 180 vehicles within the communication range of an RSU. In a extreme case that all 180 vehicles are *EV*s, the demanded throughput for RQM is at most 0.42 Mb/s ($\frac{180\times1\times308\times8}{1024\times1024}$ Mb/s). Similarly, the throughput for RRM and MAM is 0.05 Mb/s and 0.45 Mb/s, respectively. Therefore, the maximal demanded throughput of ABACS is much smaller than 6 Mb/s.

Suppose that N_{TRSU} is the total number of RSUs and N_{ARSU} is the number of RSUs where the assigned EVs are visiting. Because the RQM is disseminated by broadcasting over N_{TRSU} RSUs, the transmission overhead of the RQM delivery can be estimated by $(4i$ + $20i)N_{TRSU}$. The transmission overhead of MAM is (24a + 24d - 4)N_{ARSU}, because the MAM is only multicast to N_{ARSU} RSUs. Table III summarizes the transmission overhead in ABACS and ECDSA schemes. From Figure 11 (a), it can be seen that the transmission overhead of ECDSA is significantly higher than that of ABACS for d = 4 and d = 10. Because of the use

[8] We assume each attribute is of 4 bytes.

TABLE II
COMPARISONS OF COMPUTATIONAL DELAY FOR TTA (MS)

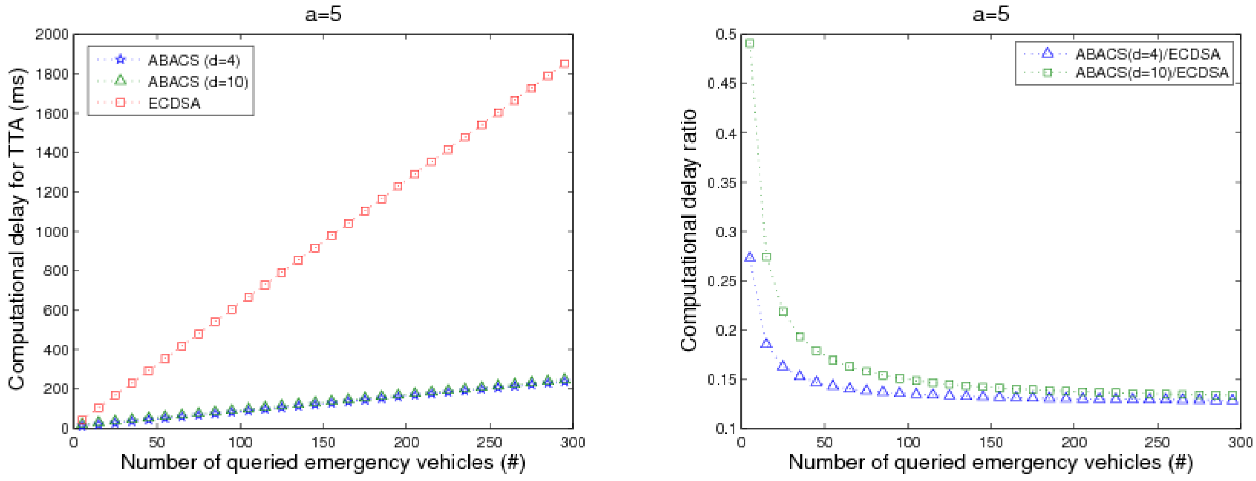
	Communication with a single emergency vehicle		Communication with n emergency vehicles	
	ABACS	ECDSA	ABACS	ECDSA
RQM Encryption	$(1 + i)T_{mul}$	$3T_{mul}$	$(1 + i)T_{mul}$	$3nT_{mul}$
RRM Decryption	$1T_{mul}$	$5T_{mul}$	nT_{mul}	$5nT_{mul}$
MAM Encryption	$(a + d - 1)T_{mul}$	$3T_{mul}$	$(a + d - 1)T_{mul}$	$3aT_{mul}$
Total	$(a + d + i + 1)T_{mul}$	$11T_{mul}$	$(a + d + i + n)T_{mul}$	$(3a + 8n)T_{mul}$

i: Total number of selected attributes ($i \geq d$), d: Minimal number of overlapped attributes; a: Number of the assigned EVs.

TABLE III
COMPARISONS OF TRANSMISSION OVERHEAD (BYTES)

	Communication with a single emergency vehicle		Communication with n emergency vehicles	
	ABACS	ECDSA	ABACS	ECDSA
RQM	$4i + 20i$	181	$(4i + 20i)N_{TRSU}$	$181n \times N_{TRSU}$
RRM	4 + 20	181	$(4 + 20)n$	$181n$
MAM	$4(a + d - 1) + 20 + 20(a + d - 1)$	181	$(24a + 24d - 4)N_{ARSU}$	$181a \times N_{ARSU}$
Total	$24(a + d + i\ ) + 20$	543	$(4i + 20i)N_{TRSU} + (24a + 24d - 4)N_{ARSU} + 24n$	$181(n \times N_{TRSU} + a \times N_{ARSU} + n\ )$

N_{TRSU} : Total number of RSUs; N_{ARSU} : Number of RSUs where the assigned EVs are visiting.



(a) Computation delay vs. number of queried emergency vehicles

(b) Computational delay ratio vs. number of queried emergency vehicles

Fig. 9. Computation delay evaluation in regular emergency events

of broadcasting and multicasting, the transmission overhead incurred by ABACS moderately increases as the number of queried EVs increases. Figure 11 (b) shows the ratio of the transmission overhead of ABACS to that of ECDSA is shown. It can be seen that the more the number of EVs are queried, the lower is the transmission overhead ratio that can be achieved. More precisely, when the number of queried EVs is greater than 61, the transmission overhead of ABACS for d = 4 and d = 10 is only 1.4% and 2.6% that of ECDSA, respectively.

C. Simulation

In addition to the theoretical analysis of computational delay in Section V-A, we further evaluate the average processing delay and message loss ratio via a simulation on ns-2 [29]. In the simulation, we consider an area of 1×1 km^2 in urban areas. The simulation parameters are given in Table IV. We also adopt the TraNS [30] tool in the simulation for a better mobility model for vehicles. It is assumed that the maximum vehicle speed is 70 km/h. Predictive transmission is also implemented in the simulation. The Medium Access Control (MAC) protocol follows the IEEE 802.11a standard, which is the basis of DSRC [27], [30].

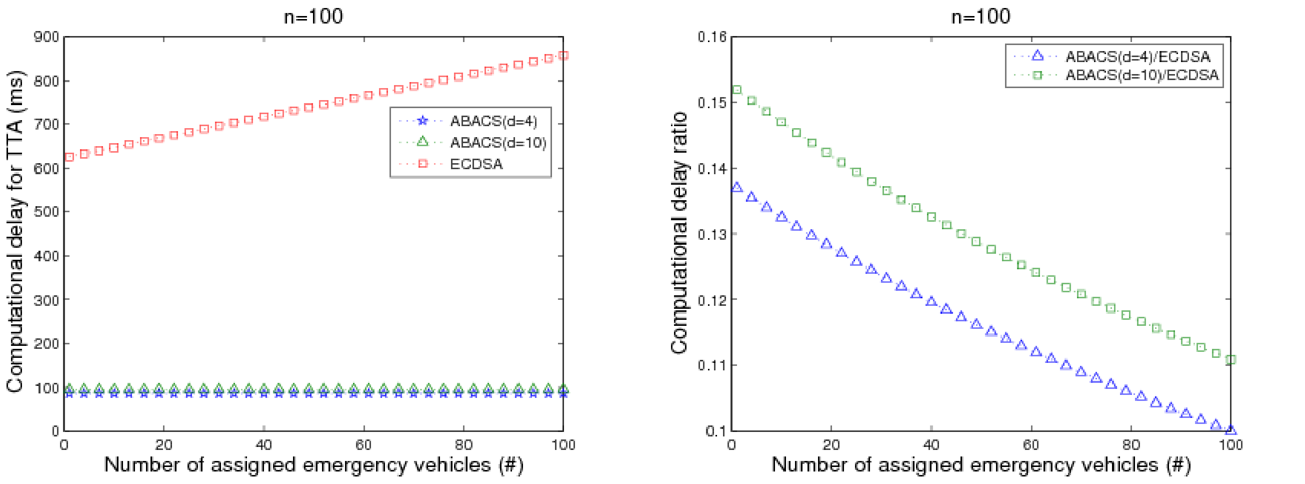
TABLE IV
SIMULATION PARAMETERS

City simulation area	1000m × 1000m
RSU Communication range	400 m
Simulation time	100 s
Wireless Protocol	802.11a
Wireless channel bandwidth	6 Mbs
Wired channel bandwidth	100 Mbs
Packet size for ECDSA message	181 bytes
Packet size for RQM message (d = 4 or 10)	164 or 308 bytes
Packet size for RRM message (d = 4 or 10)	40 bytes
Packet size for MAM message (d = 4 or 10)	184 or 328 bytes

The average processing delay (denoted as *avgD*) is defined as

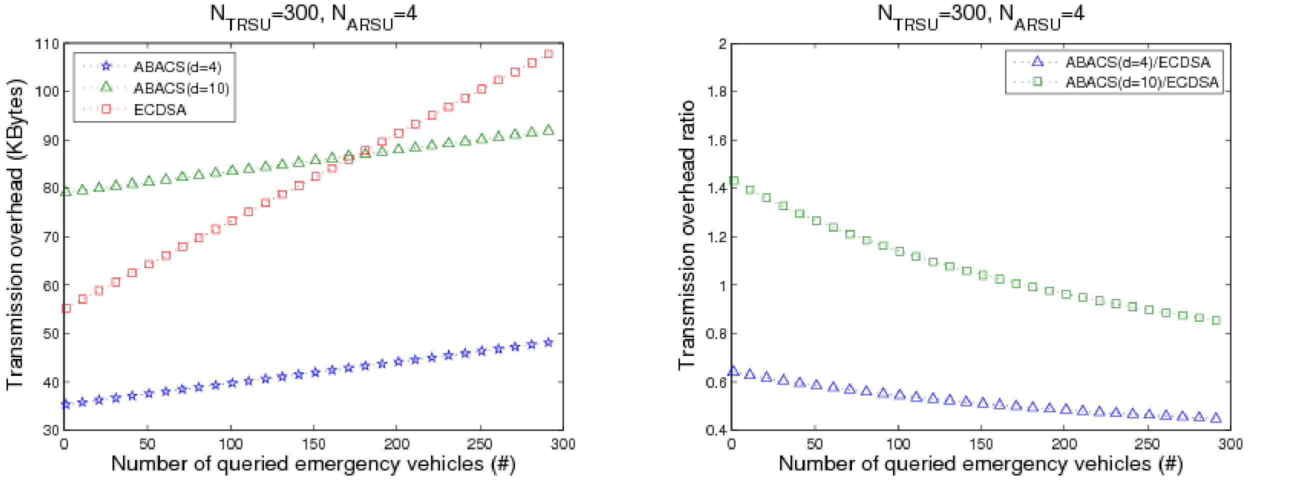
$$avgD = \frac{1}{N_r}\sum_{i=1}^{N_r}\frac{1}{N_{EV}}\sum_{j=1}^{N_{EV}}(T_{Recv}^{i,MAM,j} - T_{Send}^{i,RQM,j}),$$

where N_r is the number of emergency event reports, and N_{EV} is the number of *EV*s. $T_{Send}^{i,RQM,j}$ is the time when the application layer of TTA sends the rescue query message



(a) Computational delay vs. number of assigned emergency vehicles (b) Computational delay ratio vs. number of assigned emergency vehicles

Fig. 10. Computational delay evaluation in disaster events



(a) Transmission overhead vs. number of queried emergency vehicles (b) Transmission overhead ratio vs. number of queried emergency vehicles

Fig. 11. Transmission overhead evaluation

(RQM) of the i-th emergency event report to the j-th *EV*. $T^{i,MAM,j}_{Recv}$ is the time when the application layer of the $j-$th *EV* receives the mission assignment message (MAM) of the i-th emergency event report sent from TTA.

Figure 12 shows the average processing delay versus the number of queried *EV*s in regular emergency events. Note that the short waiting period (ξ) is not included in the average processing delay. As in Section V-A, we assume the number of assigned *EV*s is 5 (a = 5). The simulation result shows that the average processing delay of ABACS (d = 4) is close to that of ABACS (d = 10), and ECDSA consumes more processing delay than the others. It is also seen that the more *EV*s are queried, the more advantages of ABACS can be achieved. This result is basically the same as the analysis shown in Figure 9(a). The simulation result for disaster emergency events is shown in Figure 13. In general, there are only slight variations of processing delay in ABACS with respect to the number of assigned *EV*s. However, the processing delay of ECDSA increases as more EVs are involved. This result also corresponds with the analysis shown in Figure 10(a).

The average loss ratio, denoted as *avgLR*, is defined as

$$avgLR = \frac{1}{N_r}\sum_{i=1}^{N_r}\frac{1}{N_{EV}}\sum_{j=1}^{N_{EV}}\left(\frac{M^{i,RQM,j}_{Recv}+M^{j,RRM,i}_{Recv}+M^{i,MAM,j}_{Recv}}{M^{i,RQM,j}_{Send}+M^{j,RRM,i}_{Send}+M^{i,MAM,j}_{Send}}\right),$$

where N_r is the number of emergency event reports. $M^{i,RQM,j}_{Send}$ is the number of RQMs sent to the j-th *EV* for the i-th emergency event report[9], $M^{j,RRM,i}_{Send}$ is the number of RRMs sent by the j-th *EV* for the i-th emergency event report, and $M^{i,MAM,j}_{Send}$ is the number of MAMs sent to the j-th *EV* for the i-th emergency event report. $M^{i,RQM,j}_{Recv}$ represents the number of RQMs received by the j-th *EV* for the i-th emergency event report, $M^{j,RRM,i}_{Recv}$ represents the number of RRMs received by TTA for the i-th emergency event report, and $M^{i,MAM,j}_{Recv}$ represents the number of MAMs received by the j-th *EV* for the i-th emergency event report.

Figure 14 shows the relationship between the average loss ratio and the number of queried *EV*s in regular emergency events. The loss ratio of ECDSA is up to about 40% when the number of queried *EV*s is more than 50, while ABACS

[9] Note that messages sent via broadcasting should be counted multiple times as many as the number of receivers.

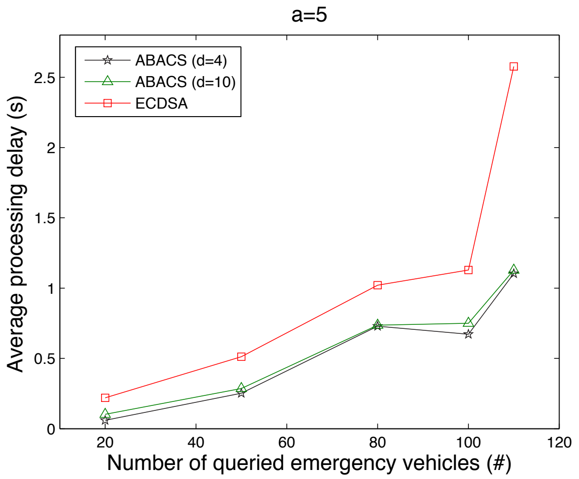


Fig. 12. Average processing delay in a regular emergency event

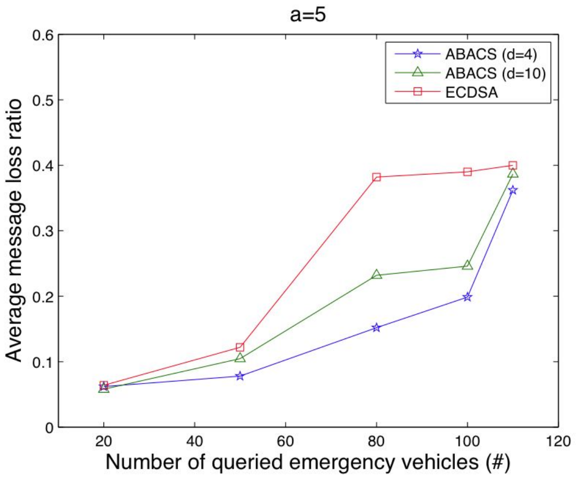


Fig. 14. Average message loss ratio in regular emergency events

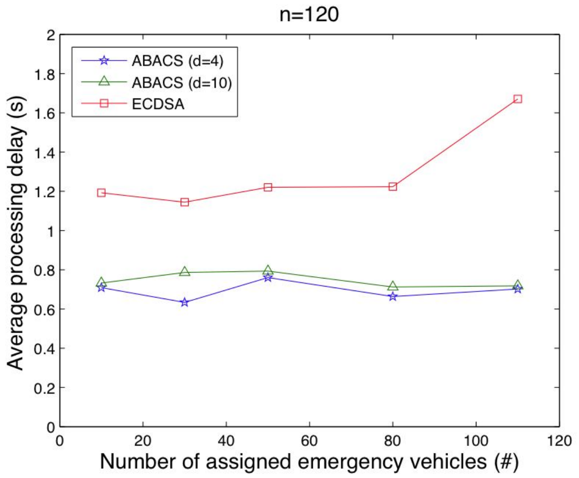


Fig. 13. Average processing delay in disaster events

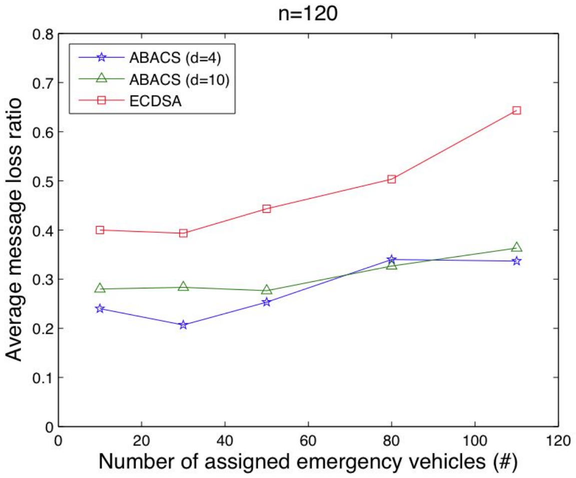


Fig. 15. Average message loss ratio in disaster events

attains the same loss ratio when the number of queried *EV*s is more than 100. Furthermore, we also investigate the loss ratio in disaster events, shown in Figure 15. It can be seen that the loss ratio of ECDSA rapidly increases as the number of assigned *EV*s grows. The reason is that in ECDSA there needs a dedicated MAM message for each assigned EV. Each *MAM* message is encrypted using the public key of the EV, and is sent separately over the VANET. On the other hand, the loss ratio of ABACS only gradually rises no more than 40% as the number of assigned *EV*s increases, because in ABACS only one encrypted MAM message is required. It can be observed that the average loss ratio of the two ABACS-based schemes is only slightly affected by the number of assigned EVs. Some studies [13], [14] in the MAC layer can be used to further improve the packet loss problem.

VI. Related work

In the past decade, several security related schemes [4], [5], [6], [7], [12], [27], [31], [32] have been proposed for VANETs. The main security issues addressed in these schemes includes message authentications, entity authentication, and privacy preservation. Some previous studies adopted the Public Key Infrastructure (PKI) as a solution to deal with abovementioned security issues. In [6], Raya *et al.* first proposed a security scheme to ensure message authentication and resolve privacy issues. In their approach, each vehicle has to pre-load many anonymous public/private key pairs that are then used to sign traffic-related messages. For better privacy protection, each vehicle will frequently change its public/private key pair. This approach incurs considerable overhead to maintain many key pairs. To realize better efficiency, a timed efficient and secure vehicular communications (TSVC) [7] scheme was proposed. Based on the TESLA scheme [33], the computational cost and transmission overhead can be significantly reduced by exploiting the advantage afforded by the hash-based message authentication code (MAC). In [5], a batch verification method is proposed to further improve the efficiency. Since each RSU has to verify hundreds of messages, batch verification can be used to accelerate the verification process. To realize better scalability, Lu *et al.* [12] proposed an Efficient Conditional Privacy Preservation (ECPP) protocol in which RSUs are responsible for issuing a temporary anonymous certificate without the aid of Trusted Authority (TA). Thus, anonymous certificates can be issued in a distributed manner. Recently, Wasef *et al.* [27] proposed an Efficient Distributed Certificate Service Scheme (DCS) for Vehicular Networks. Vehicles can update their certificates in a timely fashion. Therefore, CA will not become a bottleneck when many certificate update requests arrive. Moreover, a robust signature scheme using binary authentication tree (BAT) [32] was proposed for Vehicle-to-Infrastructure communications in VANETs. Using BAT, the bogus signatures in a batch signature verification scheme can be detected. To withstand internal attackers, Daza *et al.* [31] proposed a priori measure to ensure the validity of vehicle-generated announcements. Privacy issues, including anonymity and unlinkability, were also taken into consideration. They proposed protocols for dense and sparse VANETs respectively. In [11], the authors adopted group signatures to reduce the burden of the trust authority. RSUs take the responsibility to generate an on-the-fly group signature. For V2V communications, each vehicle can sign a message by a group signature with privacy. To check whether an anonymous sender was revoked, each vehicle can locally examine the revocation list without the aid of the remote centralized authority.

All of the above security schemes for VANETs focused on enhancing the efficiency, scalability, and security of message verification performed by RSUs or vehicles. To the best of our knowledge, no security scheme has been designed for improving the efficiency of the rescue mission after an emergency event is reported. With Regard to emergency management, only Zhu *et al.* [4] discussed how to improve the efficiency of emergency message authentication. In contrast to the abovementioned security schemes, we propose an attribute-based emergency service system to improve the overall rescue efficiency. ABACS realizes better efficiency by selecting the most appropriate emergency vehicles via multicasting and securely delegating the authority to control traffic facilities to the assigned emergency vehicles.

VII. Conclusions

Recently, emergency management in intelligent transportation systems (ITSs) has attracted considerable attention. Current security schemes over VANETs will thus become candidates for use in future ITSs. Most of these approaches focus on the security and privacy of message verification. In this paper, we have analyzed the steps involved in a rescue process after an emergency event is reported, and addressed the security and performance issues involved in initiating the rescue process over VANETs. By considering the rescue process as an emergency service, we have proposed an <u>A</u>ttribute-<u>B</u>ased <u>A</u>ccess <u>C</u>ontrol <u>S</u>ystem (ABACS) for emergency services over VANETs. The attributed-based secure multicast scheme adopted in ABACS can efficiently find and select emergency vehicles over VANETs. Our analysis shows that both security and better efficiency can be realized using ABACS. In ABACS, we have defined several messages for use in an emergency service. With regard to an emergency service in the real world, it is noted that different definitions of data fields in these messages may be required. Nevertheless, our theoretical approach can be regarded as the very first attempt to define a secure framework for providing emergency services over VANETs. Our future work will be on the investigation of more emergency scenarios, e.g., rescues for mass disasters, optimal mission assignment for multiple emergency events, and emergency services for different VANET configurations.

References

[1] C. Zhang, X. Lin, R. Lu, P. H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. Vol 57, No. 6, pp. 3357–3368, 2008.

[2] O. A. http://grouper.ieee.org/groups/scc32/dsrc/index.html, *Dedicated Short Range Communications (DSRC).*

[3] X. Lin, X. Sun, P. H. Ho, and X. Shen, "Gsis: a secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, No. 6, pp. 3442–3456, 2007.

[4] H. Zhu, X. Lin, R. Lu, P. H. Ho, and X. Shen, "Aema: An aggregated emergency message authentication scheme for enhancing the security of vehicular ad hoc networks," in *Proc. ICC*, pp. 1436–1440, 2008.

[5] C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. IEEE INFOCOM*, pp. 816–824, 2008.

[6] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, pp. 39–68, 2007.

[7] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "Tsvc: timed efficient and secure vehicular communications with privacy preserving," *IEEE Trans. Wireless Commun.*, vol. Vol. 7, No. 12, pp. 4987–4998, 2008.

[8] "Vehicle safety communications project," tech. rep., U.S. Department of Transportation, National Highway Traffic Safety Administration, 2006.

[9] M. Dikaiakos, A. Florides, T. Nadeem, and L. Iftode, "Location-aware services over vehicular ad-hoc networks using car-to-car communication," *IEEE J. Sel. Areas Commun.*, vol. 25, No. 8, pp. 1590–1602, 2007.

[10] M. Raya, I. A. P. Papadimitratos, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE J. Sel. Areas Commun.*, vol. 25, No.8, pp. 1557–1568, 2007.

[11] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communication," *to appear in IEEE Trans. Veh. Technol.*, 2010.

[12] 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 INFOCOM*, pp. 1229–1237, 2008.

[13] Y. Bi, H. Zhao, and X. Shen;, "A directional broadcast protocol for emergency message exchange in inter-vehicle communications," in *IEEE International Conference on Communication (ICC)*, 2009.

[14] J. Peng and L. Cheng, "A distributed mac scheme for emergency message dissemination in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 56, No. 6, pp. 3300–3308, 2007.

[15] E. V. de Velde and C. Blondia;, "Adaptive react protocol for emergency applications in vehicular networks," in *IEEE Conference on Local Computer Networks (LCN)*, 2007.

[16] *IEEE Trial-Use Standard for Wireless Access in Vehicular Environment-Security Services for Applications and Management Messges*. IEEE std. 1609.2-2006, Jul. 2006.

[17] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Eurocrypt* (LNCS, ed.), vol. 3494, pp. 457–473, Springer-Verlag, 2005.

[18] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Proc. Asiacrypt*, vol. 2248, pp. 514–532, 2001.

[19] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Proc. Eurocrypt*, vol. 2656, LNCS, Springer-Verlag, 2003.

[20] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proc. Advance in Cryptology-Crypto*, vol. 2139 of *LNCS*, pp. 213–229, Springer-Verlag, 2001.

[21] A. Shamir, "How to share a secret," *Communication of ACM*, vol. 22, No. 11, pp. 612–613, 1979.

[22] P. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *Proc. Asiacrypt*, pp. 515–532, 2005.

[23] J. Zhao, Y. Zhang, and G. Cao, "Data pouring and buffering on the road: a new data dissemination paradigm for vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 56, No. 6, pp. 3266–3277, 2007.

[24] M. Nekovee, "Modeling the spred of worm epidemics in vehicular ad hoc networks," in *Proc. Veh. Tech. Conf.*, 2006.

[25] J. E. Khoury and A. Hobeika, “Incorporating uncertainty into the estimation of the passing sight distance requirements,” *Computer-Aided Civil and Infrastructure Engineering*, vol. 22, no. 5, pp. 347–357, 2007.

[26] S. Yu, K. Ren, and W. Lou, “Fdac: Toward fine-grained distributed data access control in wireless sensor networks,” in *Proc. IEEE INFOCOM*, pp. 816–824, 2009.

[27] A. Wasef, Y. Jiang, and X. Shen, “Dcs: An efficient distributed certificate services scheme for vehicular networks,” *IEEE Trans. Veh. Technol.*, to appear.

[28] J. Yin, T. ElBatt, G. Yeung, B. Ryu, S. Habermas, H. Krishnan, and T. Talty, “Performance evaluation of safety application over dsrc vehicular ad hoc networks,” in *ACM Int. Workshop Vehicular Ad hoc Network*, pp. 1–9, 2004.

[29] O. A. http://nsnam.isi.edu/nsnam/index.php, *The Network Simulator-ns-2*.

[30] M. Piorkowski, M. Raya, A. L. Lugo, P. Papadimitratos, M. Grossglauser, and J.-P. Hubaux, “Trans: Realistic joint traffic and network simulator for vanets,” *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 12, Issue 1, 2008.

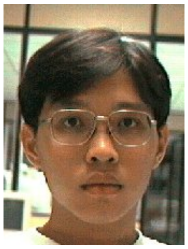
[31] V. Daza, J. Domingo-Ferrer, F. Sebe, and A. Viejo, “Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks,” *IEEE Trans. Veh. Technol.*, vol. 58, no. 4, pp. 1876–1886, 2009.

[32] Y. Jiang, M. Shi, X. Shen, and C. Lin, “Bat: a robust signature scheme for vehicular networks using binary authentication tree,” *IEEE Trans. Wireless Commun.*, vol. 8, no. 4, pp. 1974–1983, 2009.

[33] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, “The tesla broadcast authentication protocol,” *RSA Crypto.*, vol. Vol.5, No. 2, pp. 2–13, 2002.

Lo-Yao Yeh received the B.S. degree in Information Management from Da Yeh University, Taiwan, in 2003. He got the M.S. degree in department of Information Management from National Chi Nan University in 2005. Now, he is Ph.D candidate in the department of Computer Science in National Chiao Tung University. He was a visiting scholar in UC Berkeley. His current research interests include network security and overlay networks security, sensor networks.

Yen-Cheng Chen received the Ph.D. degree in computer science from the National Tsing Hua University, Taiwan, in 1992. He was an associative researcher of the ChungHwa Telecom Labs. from 1992 to 1998. From 1998 to 2001, he was an assistant professor of the Department of Information Management, Ming Chuan University, Taiwan. Currently, he is an assoicate professor of the Department of Information Management, National Chi Nan University, Taiwan. His current research interests are network management, wireless networks, and security.



Jiun-Long Huang received the BS and MS degrees from the Department of Computer Science and Information Engineering at National Chiao Tung University in 1997 and 1999, respectively, and the PhD degree from the Department of Electrical Engineering at National Taiwan University in 2003. Currently, he is an assistant professor in the Department of Computer Science at National Chiao Tung University. His research interests include: mobile computing, mobile data management, wireless networks, and Internet technology.