SVC: Secure VANET-Assisted Remote Healthcare Monitoring System in Disaster Area

Xuefeng Liu[1, 3], Hanyu Quan[1], Yuqing Zhang[2], Qianqian Zhao[1], Ling Liu[1]
[1] School of Cyber Engineering, Xidian University, Xi'an, China
[e-mail: liuxf@mail.xidian.edu.cn, hyquan@stu.xidian.edu.cn,{liul, zhaoqq}@nipc.org.cn]
[2] National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences
Beijing, China
[e-mail: zhangyq@uacs.ac.cn]
[3] State Key Laboratory of Information Security, Chinese Academy of Science
Beijing, China
*Corresponding author: Hanyu Quan

Received July 18, 2015; revised December 9, 2015; accepted January 21, 2016; published March 31, 2016

Abstract

With the feature of convenience and low cost, remote healthcare monitoring (RHM) has been extensively used in modern disease management to improve the quality of life. Due to the privacy of health data, it is of great importance to implement RHM based on a secure and dependable network. However, the network connectivity of existing RHM systems is unreliable in disaster area because of the unforeseeable damage to the communication infrastructure. To design a secure RHM system in disaster area, this paper presents a Secure VANET-Assisted Remote Healthcare Monitoring System (SVC) by utilizing the unique "store-carry-forward" transmission mode of vehicular ad hoc network (VANET). To improve the network performance, the VANET in SVC is designed to be a two-level network consisting of two kinds of vehicles. Specially, an innovative two-level key management model by mixing certificate-based cryptography and ID-based cryptography is customized to manage the trust of vehicles. In addition, the strong privacy of the health information including context privacy is taken into account in our scheme by combining searchable public-key encryption and broadcast techniques. Finally, comprehensive security and performance analysis demonstrate the scheme is secure and efficient.

Keywords: RHM System, VANET, Security and Privacy, Disaster Area

This research was supported by China Postdoctoral Science Foundation funded project (Grant No. 2014M562377), and National Natural Science Foundation of China (Grant No. 61402352, No. 61272481, No. 61572460.)

http://dx.doi.org/10.3837/tiis.2016.03.016 **ISSN : 1976-7277**

1. Introduction

Remote healthcare monitoring (RHM), providing a convenient and low-cost way to monitor patients outside of conventional clinical settings, has been extensively used in post-acute care and chronic disease management. A study report from IMS Research indicates that in 2012 there was estimated to be 308,000 patients remotely monitored by healthcare providers, and the number will increase to 1.8 million worldwide by 2017 [1]. In a typical RHM system, a patient deploys body sensors in a wireless body sensor network at home to collect the health parameters such as blood pressure, heart rate, body temperature, and SpO2 etc, and sends these personal health information (PHI) to healthcare provider's end. Such a system enables disease progression track and early detection, and thus can evidently reduce readmission rate and decrease the healthcare spending on both patient personal cost and nation health expenditure. According to the American Heart Association, chronic heart failure alone costs the US economy more than $33.7 billion per year, of which $16 billion is attributed to readmission, while 42% of the readmission are preventable by adequate patient monitoring, instruction and education outside hospital [2].

As one of the most important components of RHM system, network is responsible for transmitting the PHI from patient's end to the healthcare provider's end (e.g., a health center). In recent years, there are many research works concerned with the practical RHM systems [3-10]. Most of the works use normal wireless communication technology such as 3G cellular networks with base stations, or WiFi access point connected with Internet to transmit the PHI. Unfortunately, all these networks rely on communication infrastructures which are vulnerable in natural disaster (e.g., Hurricane Katrina) or technical failure (e.g., the August 2003 electrical blackout in North America). The network connectivities are unpredictable due to the unforeseeable destructions to the infrastructures (e.g., cellular base stations, wireless access points, fiber and cable connections, power supplies) caused by the disaster. Therefore, an emergency infrastructure-free RHM system which can work normally in disaster area is highly desired.

The emergence of vehicular ad hoc network (VANET) puts forward a potential solution for post-disaster communication through its “store-carry-forward” feature. In VANET, each vehicle is equipped with an OnBoard Unit (OBU) communication device capable of storing, which allows messages to be transmitted in the network by intermittent connections while the fixed Roadside Units (RSUs) deployed along the roadside is optional [9][11]. However, using VANET to design an RHM system for post-disaster PHIs transmission comes with a set of new challenges. The first challenge is how to create a practical VANET when the disaster happens. A trivial solution is that the health center sends the ambulances it possesses into the disaster area to compose a VANET. Due to the limited number of the official vehicles, i.e., the number of the network nodes, the performance of such a network will be inefficiency. In addition, security and privacy are also the primary challenges to an RHM system. A recent study shows that 75% Americans consider the privacy of health information important or very important [12]. They may refuse to submit the PHIs to an insecure VANET without privacy protection. Therefore, a comprehensive privacy preserving scheme for the RHM system is indispensable. There are some research works discussing the topic of security and privacy of the RHM system in recent years [7-10]. We will review these works in the section of Related Works and show that they are not suitable for an RHM system working in disaster area.

Based on the above analysis, in this paper, we propose a Secure VANET-assisted Remote HealthCare Monitoring System, named SVC, for post-disaster PHIs transmission in disaster area.The main contribution of this paper is twofold.

First, we present a novel two-level VANET to help transmit the PHIs in the RHM system. Specially, the first level nodes are official vehicles such as ambulances, and common vehicles are introduced into the VANET as the second level nodes. Such a structure increases the number of the VANET nodes so that to improve the network performance. In addition, a corresponding two-level key management model is proposed by mixing certificate-based cryptography and ID-based cryptography to manage the trust of the vehicles.

Second, under the two-level network model, we propose a secure PHIs transmission scheme, Speically, PHI is encrypted with a symmetric key that can only be decrypted by the corresponding doctor. Moreover, the context privacy of the PHI is protected by using searchable public-key encryption and broadcast techniques. Security analysis shows the security requirements including message autentication, identity privacy, content privacy, and context privacy are all achieved, while an extensive analysis of performance domenstrates the scheme is effective and efficient.

The rest of this paper is organized as follows. Section 2 introduces some preliminaries relevant to our work. Section 3 describes the system and threat model, and identifies the security requirements. The SVC system is presented in detail in Section 4, followed by the security analysis and the performance evaluation in Sectioin 5 and Section 6, respectively. We discuss the related works in Section 7, and conclude our work in Section 8.

2. Preliminaries

2.1 IBC and Bilinear Maps

ID-based cryptosystem (IBC) enables the public key of an entity to be its public ID (such as the name or the email address), which avoids the use of public key infrastructure (PKI) [13]. D.Boneh et al. proposed the first full functional ID-based encryption scheme based on bilinear maps [14]. Let G and G_T be two multiplicative cyclic groups of the same prime order q. Let $e: G \times G \to G_T$ denote a bilinear map constructed with the following properties:

1. Bilinear: for all $a,b \in Z_q^*$ and $g_1, g_2 \in G$, $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$.
2. Non-degenerate: there exists a point g_1 such that $e(g_1, g_1) \neq 1$.
3. Computable: there is an efficient algorithm to compute $e(g_1, g_2)$ for any $g_1, g_2 \in G$.

A bilinear map satisfying the three properties above is said to be an admissible bilinear map, and the Weil pairing on elliptic curves is an example of such a map.

2.2 Computational Assumptions

The security of SVC depends on the hardness of Computational Diffie-Hellman (CDH) problem and Bilinear Diffie-Hellmanm (BDH) problem.

Definition 1 (Computational Diffie-Hellman Assumption). For unknown $a,b \in Z_q^*$, given $g, g^a, g^b \in G$, it is infeasible to compute $g^{ab} \in G$.

Definition 2 (Bilinear Diffie-Hellman Assumption). For unknown $a,b,c \in Z_q^*$, given $g, g^a, g^b, g^c \in G$, it is infeasible to compute $e(g,g)^{abc} \in G_T$.

Note that the BDH problem in $\langle G, G_T, e \rangle$ is no harder than the CDH problem in G. In other

words, an algorithm for CDH in G is sufficient for solving BDH in $\langle G, G_T, e\rangle$ [15].

2.3 Batch Verification

Batch verification can verify all the signatures received in a time window with rather short time compared to verify each signature one after another. Let $\sigma_1,\cdots,\sigma_n$ denote n signatures of different messages. With batch verification, the n signatures can be combined into a "batch" form σ_{batch}, and one can verify it once instead of verifying σ_i $(1\le i\le n)$.

The first batch verification scheme was introduced by Fiat [16] in Crypto 1989, which is based on RSA. In this paper, BLS [17] and ChCh [18] signature techqines that support batch verification will be used to speed up the message authentication.

2.4 Searchable Public-Key Encryption

Public-key encryption with keyword search (PEKS), also named "searchable public-key encryption", was first introduced by D.Boneh et al. in Eurocrypt 2004 [20]. In that work, the PEKS scheme is developed for an email system that enables a server to retrieve messages containing certain keywords without learning any other information. Specially, consider an email server that stores a message encrypted for Alice by someone else in the form of $E_{A_{pub}}(M)\|PEKS(A_{pub},W_1)\|\cdots\|PEKS(A_{pub},W_n)$, where A_{pub} is Alice's public key, M is the plaintext, and W_i is the keyword. Given a trapdoor T_W computed by Alice, the server can test whether one of the keywords associated with the message is equal to the keyword W of Alice's choice, i.e., whether $W_i=W$ for $PEKS(A_{pub},W_i)$, $1\le i\le n$. If $W_i\ne W$, the server learns nothing more about W_i.

In SVC, we combine the PEKS scheme with broadcast techniqueto protect the context privacy which defined in next section.

3. System and Security Models

3.1 System Model

We consider the entire system works in disaster area where the communication infrastructure (e.g., cellular 3G/4G, Wi-Fi public access, and Internet, etc.) is unavailable. With the "store-carry-forward" feature, we design a special VANET in SVC to help transmitting the PHI from the patient's house to the health center. The system model is divided into three domains: the wireless body area network (WBAN), the vehicular ad-hoc network (VANET), and the health center, as shown in **Fig. 1**.

Health Center includes a PHI database (DB) and physicians (PHs). DB is responsible for receiving, storing, and forwarding the PHIs to the corresponding PHs. In SVC, DB is assumed to be honest-but-curious [21][22], in other words, it follows the protocol correctly but attempts to obtain as much secret information in the stored PHIs as possible. All entities in the health center are managed by a TA, which is a trusted server that takes charge of key management.

VANET in SVC consists of two types of vehicles: the leading vehicles (L-vehicles) and the assistant vehicles (A-vehicles). L-vehicles belong to the health center. When the disaster happens, they will be sent into the disaster area to set up the VANET for transmitting the PHIs. A-vehicles are common vehicles (e.g., personal cars) who volunteer to join the VANET to help transmit the PHIs.

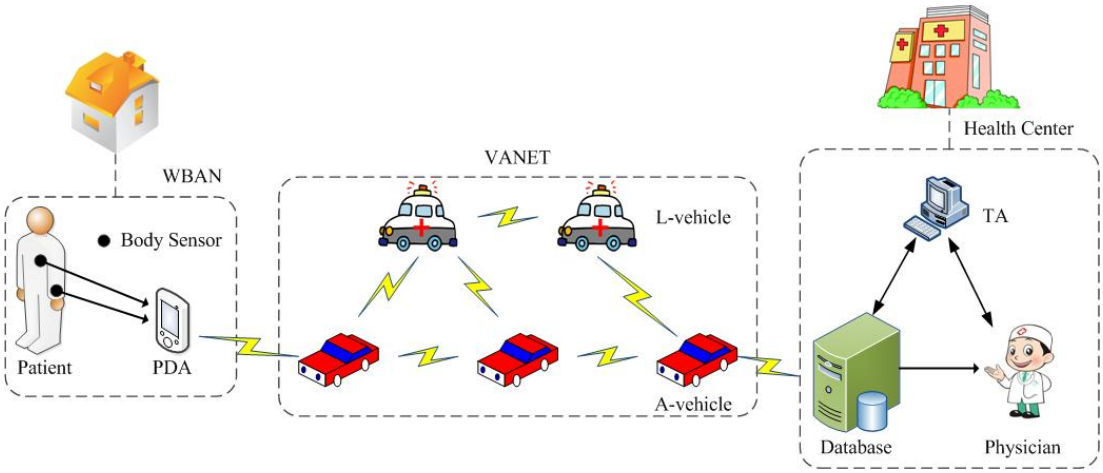


Fig. 1. The system model of SVC

To improve the motivation of the A-vehicles for participating in the VANET, some incentive protocols [33], [34] can be adopted in our VANET model, which is however out of the scope of this paper. Since the PHIs are of paramount importance and the VANET is a disaster network [11] whose duty is to transmit the PHIs, it is reasonable to assume that both L-vehicles and A-vehicles have no incentives to impede the system such as launching black hole attack [23]. They are also assumed to be honest-but-curious. In addition, they are allowed to collude with each other, even with the DB in the health center. Note that we consider the extreme situation in disaster area, i.e., there are no road-side units (RSUs) in the VANET and the only communication mode is vehicle-to-vehicle (V2V). This is the fundament of that SVC does not rely on the communications infrastructure.

WBAN is a wireless network which is composed of some body sensors and a gateway (e.g., a smartphone). Body sensors monitor the patient's health status such as heart rate, blood pressure, and body temperature, and report these information (i.e., the PHI) to the gateway. Then the gateway transmits the PHI to an L-vehicle or an A-vehicle near the house in a privacy-preserving mode. When a patient registers with TA in the health center, she/he will get some devices suitable for her/him, which can be used to deploy a WBAN at home. As there have been many researches concerning the secure communications in WBAN [24][25], we suppose that the gateway can get the PHI securely.

3.2 Security Requirement

In SVC, we aim to solve the following security and privacy problems.

3.2.1 Message Authentication

Message authentication is one of the most important requirements in SVC. The VANET should only transmit the legitimate PHI packets because of its limited computing and storing power, and only these PHI packets are accepted by DB.

3.2.2 Content Privacy

This requirement means that the PHI's content can only be read by the corresponding physician. In other words, no adversary (including any mid-entity in the transmission process) can reveal the PHI by eavesdropping and analyzing the PHI packet transmitted over the VANET and the health center.

3.2.3 Identity Privacy

The PHI packet should not be linked with the patient's real identity. That is, from a PHI packet transmitted in SVC, no entity can infer who is ill except the TA. On the other hand, the A-vehicle may prefer to serve as a volunteer anonymously. In this paper, we use pseudonym technique to preserve identity privacy while the side information (SI) attacks [26] are outside the scope of our work.

3.2.4 Context Privacy

Context privacy was first defined by P. Kamat et al. in sensor network [27]. It concerns protecting the context associated with message transmission. In SVC, specially, context privacy means the unlinkability between the source and the destination of a PHI packet. Context privacy is important and meaningful in healthcare system. For instance, if an adversary notices that a PHI packet is sent to a heart disease physician, she/he can deduce that the source of the PHI packet may suffer from heart disease. Interested readers can refer to [7] for a comprehensive probability analysis of context privacy.

In addition, since the VANET in SVC is a special and temporary network, we don't consider the location privacy of the vehicles in the VANET.

3.3 Threat Model

In this paper, we use the Dolev-Yao threat model [28] that considers both inside and outside attacks. Specially, inside attack can be individually or collusively launched by the mid-entity such as L-vehicles, A-vehicles, and DB. Besides, we should also achieve the security requirements against an external global adversary. We assume the adversary does not compromise any L-vehicle and A-vehicle and the DB, but it has the ability to monitor all the traffic in SVC. Therefore, an external global adversary can log the whole path the PHI packet passed by and attempt to reveal the private content. Besides the eavesdropping, the adversary can also inject bogus packet or modify legitimate packet to disrupt the system performance, moreover, it can collude with the inside entities (i.e., L-vehicles, A-vehicles, and DB). In addition, we do not consider the revocation in this work, which is of independent interest and one can refer to [41] for detailed descriptions.

4. The Proposed System: SVC

In this section ,we present the SVC system. Before delving into the technical protocol, we first give an overview of the system

4.1 Overview of SVC

SVC is a post-disaster healthcare system for remote healthcare monitoring in disaster area. For starting the system seamlessly as soon as the disaster happens, TA sets up the system before the disaster. When the disaster happens, L-vehicles will move into the disaster area to compose the VANET with A-vehicles. The VANET has a two-level key management model, as shown in **Fig. 2**. TA is the certificate-based key manager of all L-vehicles while each L-vehicle is a ID-based key manager of a group of A-vehicles. Under this key management model, an A-vehicle can register with any L-vehicle in the disaster area instead of registering with TA in the health center.

The PHI packets transmission in SVC is composed of 4 processes: 1) From WBAN gateway

to L-vehicle or A-vehicle. 2) Over the VANET by V2V communications. 3) From L-vehicle or A-vehicle to DB. 4) From DB to PHs by broadcast. In the 1st process, the PHI is transmitted in a privacy-preserving mode in which the destination of the PHI packet is hidden by the PEKS scheme, i.e., encrypting the PH's identity as the keyword under her/his public key. Combined with the broadcast in the 4th process, only the PH herself/himself can identify that the PHI packet is sent to her/him (only she/he can test whether the keyword is her/his identity). In addition, we use symmetric encryption to protect content privacy and identity-based signature for message authentication. In the 3rd process, we make the DB verify the A-vehicles (and the L-vehicles) in a batch manner to improve the system efficiency.

We present the technical protocol of SVC in the following, which includes system setup, patients registration, A-vehicles registration, and PHI packets transmission.

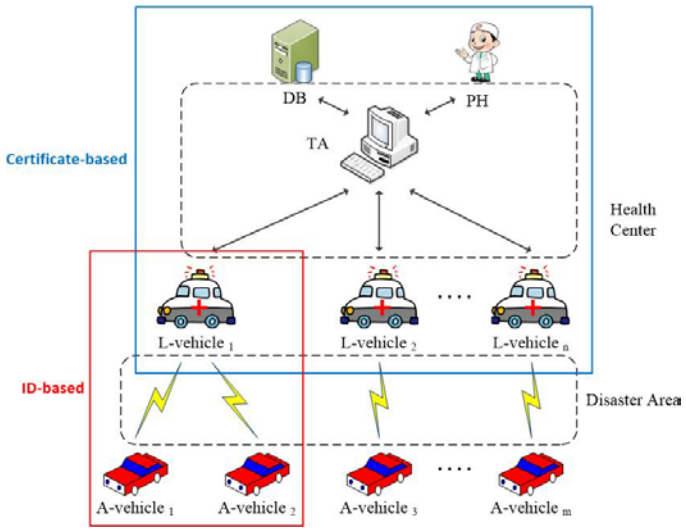


Fig. 2. The two-level key management model in SVC

4.2 System Setup

To set up the SVC system, TA first generates the system parameter as follows:

1. Given a security parameter k, TA generates a 4-tuple (q, G, G_T, e), in which G and G_T are two multiplicative cyclic groups of the same prime order q, respectively, and $e: G \times G \to G_T$ is an admissible bilinear map.
2. Pick a random $s \in Z_q^*$ as the master-key. Choose a generator $g \in G$, and compute the system public key $P_{pub} = g^s$.
3. Choose three hash function H_1, H_2 and H_3, where $H_1: \{0,1\}^* \to G$, $H_2: G_T \to Z_q^*$, and $H_3: \{0,1\}^* \times G \to Z_q^*$, and a secure symmetric encryption algorithm $Enc(\,)$ such as AES [29].
4. Publish the system parameter $param = (q, G, G_T, e, g, P_{pub}, H_1, H_2, H_3, Enc())$, and keep the master-key s in secret.

Suppose ε is an entity in the health center ($\mathcal{E}$ can be the DB, the L-vehicle, or the PH) with the public and private key pair $PK_\varepsilon = g^x, SK_\varepsilon = x, x \in Z_q^*$. To certify the validity of the public key, TA will issue a public-key certificate to $\mathcal{E}$ using the BLS scheme [17] as follows:

$$cert_{\varepsilon} = H_1(ID_{\varepsilon} || PK_{\varepsilon})^{s} \quad (1)$$

where ID_{ε} is ε's identity. Thus $cert_{\varepsilon}$ provides a binding between ε's identity and the public key [30].

4.3 Patients Registration

When the patient registers with TA, TA chooses a random $PID_{PA} \in G$ as her/his pseudonym and computes the private key $SK_{PA} = H_1(PID_{PA})^{s}$ for her/him. Note that the private key is based on the identity PID_{PA} (i.e., IBC), the public key is $PK_{PA} = H_1(PID_{PA})$, and no public-key certificate is needed. Then, the patient selects a PH and gets some suitable sensors based on her/his requirement. Finally, TA sends $(PID_{PA}, SK_{PA}, PK_{PH})$ to the patient through a secure channel, where PK_{PH} is the PH's public key. With the body sensors, the patient can deploy a WBAN at home to monitor her/his health condition and collect the PHI. We point out that in fact TA will choose a set of N pseudonyms $PID_{PAi}|_{i=1}^{N}$ and compute the corresponding $SK_{PAi}|_{i=1}^{N}$ for the patient so that she/he can update the pseudonym to protect the identity privacy [31].

4.4 Vehicles Registration

As discussed before, at the moment the disaster happens, the L-vehicles move into the disaster area which help information transmition and take the charge of key managmant for A-vehicles. ..Under the two-level key management model shown in **Fig. 2**, the A-vehicle does not have to go to the health center for registration, instead it can register with any L-vehicle it encounters in the disaster area in the following way. First, the L-vehicle chooses a random $ID_{AV} \in G$ as the A-vehicle's identity. Then, it computes the private key $SK_{AV} = H_1(ID_{AV})^{x}$, and sends $(ID_{AV}, SK_{AV}, ID_{LV}, PK_{LV}, Cert_{LV})$ to the A-vehicle through a secure channel (there have been many researches concerning the secure channel in VANET, such as [32]), where x is the L-vehicle's private key. To protect the identity privacy, the L-vehicle will also choose $ID_{AVi}|_{i=1}^{N}$ and compute the corresponding $SK_{AVi}|_{i=1}^{N}$ for the A-vehicle. For the system consistency, we make each L-vehicle register with itself so that it can work on the behavior of an A-vehicle in PHI packets transmission.

4.5 PHI Transformation

4.5.1 From WBAN to A-vehicle

After obtainingthe PHI M, a WBAN gateway sends M to an A-vehicle nearby in a privacy-preserving mode. This communication process is executed by the following steps:

1. The A-vehicle broadcasts the beacon message within its range. Specially, it chooses a random number $\gamma \in Z_q^*$, signs the current timestamp T_{beacon} as (X, Y), where

$$X = H_1(ID_{AV})^{\gamma}, Y = SK_{AV}^{\gamma+\eta} \quad (2)$$

$$\eta = H_3(T_{beacon}, X) \quad (3)$$

Then the A-vehicle broadcasts $ID_{AV}||ID_{LV}||PK_{LV}||Cert_{LV}||T_{beacon}||X||Y$ as the beacon message, the subscript LV represents the L-vehicle with whom the A-vehicle registered.

2. Upon receiving the beacon message at time T'_{beacon}, the gateway first checks whether $T'_{beacon} - T_{beacon} \le \Delta T$, where ΔT is the expected time for transmission delay. If it doesn't hold, the gateway thinks it is a replay attack and abandons it. Then the gateway checks whether

$$e(P_{pub}, H_1(ID_{LV}||PK_{LV}))=e(g, cert_{LV}) \quad (4)$$

$$e(g,Y)=e(PK_{LV}, XH_1(ID_{AV})^{\eta}) \quad (5)$$

if both Equations 4 and 5 hold, the beacon message is accepted. The correctness and security can refer to [17] and [18], respectively.

3. The WBAN gateway makes the PHI packet as shown in **Table 1** and sends it to the A-vehicle. *Data* is the privacy-preserving PHI data computed by **Algorithm 1**, in which lines 1 to 3 use $Enc(\,)$ with a session key k to encrypt the PHI M, and lines 4 to 5 use the PEKS scheme to encrypt the target PH's identity ID_{PH} as the keyword. T_{PHI} is the current timestamp. σ_{PA} is the signature in the form of (U,V), where

$$U = H_1(PID_{PA})^r, V = SK_{PA}^{r+h} \quad (6)$$

$$h = H_3(PID_{PA}||Data||T_{PHI}, U) \quad (7)$$

$r \in Z_q^*$ is a random number chosen by the gateway. In this step, for deceasing the time overhead, *Data* can be pre-computed, i.e., the gateway can compute *Data* before the A-vehicle coming.

Table 1. Message Format for PHI packet

PID	Privacy-Preserving PHI Data	Timestamp	Signature
PID_{PA}	*Data*	T_{PHI}	σ_{PA}

Algorithm 1. Compute Privacy-Preserving PHI Data

Input:
The PHI M
The system parameter *param*
The destination PH's public key PK_{PH}

Output:
The privacy-preserving PHI *Data*

1. Choose a random number $y' \in Z_q^*$
2. Compute $k = PK_{PH}^{y'}$
3. Compute $C = Enc_k(M)$
4. Choose a random number $r \in Z_q^*$
5. Compute $PEKS(PK_{PH}, ID_{PH}) = [g^r, H_2(t)] = [A, B]$, where $t = e(H_1(ID_{PH}), PK_{PH}^r)$
6. **return** $Data = g^{y'}||C||A||B$

4. When the A-vehicle receives the PHI packet, it first checks the timestamp T_{PHI}, then it checks whether

$$e(g,V)=e(P_{pub},UH_1(PID_{PA})^h) \tag{8}$$

the equation (8) holds. If so, the A-vehicle accepts the PHI packet and keeps *Data* until it is transferred to another A-vehicle or to the DB in health center. Note that from here when we say the PHI packet, we mean *Data* only.

4.5.2 Over the VANET

When an A-vehicle thinks it cannot carry the PHI packets any more, it will try to forward them to next-hop node of the VANET. We stress that in SVC it is assume that both L-vehicle (whose duty is to transmit the PHI packets) and A-vehicle (who volunteers to join the VANET) will not drop the PHI packets. In other word, they either carry the PHI packets or forward them to another node of the VANET. When the A-vehicle detects a nearby node willing to relay the PHI packets, it forwards them to the node. This communication process is similar to that of beacon message broadcast. In addition, some efficient incentive and routing mechanisms [33] [34] can be adopted in the VANET to improve the transmission efficiency, but they are beyond the scope of this paper.

4.5.3 From A-vehicle to DB

Suppose an A-vehicle with a PHI packet *Data* (in fact, an A-vehicle may carry more than one PHI packet) reaches the health center, it sends *Data* to DB in the form of $(ID_{AV}||ID_{LV}||PK_{LV}||cert_{LV}||Data||T||X'||Y')$, where T is the current timestamp, (X',Y') is the signature of $Data||T$ that is computed as Equation 2. After checking $cert_{LV}$ and verifying (X',Y') using the way of Equations 4 and 5, respectively, DB accepts (or rejects) *Data* by checking the timestamp.

In fact, it is possible that many A-vehicles reach the health center at the same time. In this case, however, it is inefficient to authenticate all the A-vehicles one by one using the above method. To address this problem, we use batch verification to improve the authentication efficiency. Suppose DB receives $(ID_{AV_i}||ID_{LV_i}||PK_{LV_i}||Cert_{LV_i}||Data_i||T_i||X_i'||Y_i')|_{i=1}^n$ from n different A-vehicles in a time window, it then batch checks the n public-key certificates $cert_{LV_i}|_{i=1}^n$ and batch verify the n signatures $(X_i',Y_i')|_{i=1}^n$ by testing whether

$$e(P_{pub},H_{batch})=e(g,cert_{batch}) \tag{9}$$

$$e(g,Y'_{batch})=\prod_{i=1}^{n} e(PK_{LV_i},X_i'H_1(ID_{AV_i})^{n!}) \tag{10}$$

where $cert_{batch}=\prod_{i=1}^{n} cert_{LV_i}$, $Y'_{batch}=\prod_{i=1}^{n} Y'_{batch}$, and $H_{batch}=\prod_{i=1}^{n} H_1(ID_{LV_i}||PK_{LV_i})$. If both Equations 9 and 10 hold, all the $Data_i$ are accepted. They follow since

$$\begin{aligned} e(P_{pub}, H_{batch}) &= e(g^s, \prod_{i=1}^{n} H_1(ID_{LV_i} || PK_{LV_i})) \\ &= e(g, \prod_{i=1}^{n} H_1(ID_{LV_i} || PK_{LV_i})^s) \\ &= e(g, \prod_{i=1}^{n} cert_{LV_i}) \\ &= e(g, cert_{batch}) \end{aligned} \tag{11}$$

$$\begin{aligned} e(g, Y'_{batch}) &= e(g, \prod_{i=1}^{n} Y_i') \\ &= e(g, \prod_{i=1}^{n} SK_{AV_i}^{\gamma_i' + \eta_i'}) \\ &= e(g, \prod_{i=1}^{n} H_1(ID_{AV_i})^{x_i(\gamma_i' + \eta_i')}) \\ &= e(g^{x_i}, \prod_{i=1}^{n} H_1(ID_{AV_i})^{\gamma_i'} H_1(ID_{AV_i})^{\eta_i'}) \\ &= \prod_{i=1}^{n} e(PK_{LV_i}, X_i' H_1(ID_{AV_i})^{\eta_i'}) \end{aligned} \tag{12}$$

where x_i is the L-vehicle's private key SK_{LV_i} and γ_i' is the random number chosen by the A-vehicle. If Equations 9 or 10 does not hold, it means there is at least one bogus packet in the n packets. In this case, DB can identify the bogus packet(s) efficiently using the techniques in [35] or [41]. We will compare the performance between the batch verification and the individual verification comprehensively in Section 6.

4.5.3 From DB to PH

In this process, the DB broadcasts the PHI packets to all the PHs in the health center. Suppose the DB broadcasts m PHI packets $Data_1, \cdots, Data_m$ each time, the communication process is executed by the following steps:

1. DB broadcasts $Data_1 || \cdots || Data_m || T_{broadcast} || \sigma_{DB}$, where σ_{DB} is the BLS signature of $Data_i|_{i=1}^{m}$ and the current timestamp $T_{broadcast}$.
2. When the PH with identity ID_{PH} receives the PHI packets, she/he first checks the timestamp $T_{broadcast}$ and the signature σ_{DB}. Then the PH performs **Algorithm 2** to recover the PHIs sent to her/him. Line 5 tests whether $Data_i$ includes the keyword ID_{PH}. The correctness can refer to [20] and the security will be discussed in the next section.

Algorithm 2. Recover the PHIs

Input:
The PHI packets $Data_1, \cdots, Data_m$
The system parameter $param$
The PH's private key SK_{PH}
Output:
The recovered PHIs set $\mathcal{M}$

1. Compute $T_{ID_{PH}} = H_1(ID_{PH})^{SK_{PH}}$ as the trapdoor of ID_{PH}
2. Set $\mathcal{M} = \{\varnothing\}$
3. **for** $i = 1$ to m **do**
4. Convert $Data_i$ to $g^{y_i} || C_i || A_i || B_i$, where $[A_i, B_i]$ is the searchable encryption of a certain PH's identity
5. Check whether $H_2(e(T_{ID_{PH}}, A_i)) = B_i$
6. **if** it does hold **then**

7. Compute $k' = g^{y_i' SK_{PH}} = g^{yy_i'}$
8. Recover $M_i = Dec_{k'}(C_i)$ and add M_i into $\mathcal{M}$
9. **end if**
10. **end for**
11. **return** $\mathcal{M}$

5. Security Analysis

In this section, we analyze how the security and privacy requirements are achieved in SVC system.

5.1 Message Authentication

Message authentication is performed in every communication process in SVC by using secure signature. Take the beacon message $ID_{AV}||ID_{LV}||PK_{LV}||cert_{LV}||T_{beacon}||X||Y$ in the first process for example, the WBAN gateway first checks $cert_{LV}$ after receiving the beacon message. IF and only if Equation 4 holds, the gateway believes the L-vehicle with whom the A-vehicle claimed that it registered is legitimate. Then the gateway verifies the signature (X,Y) using the L-vehicle's public key, if and only if Equation 5 holds, the beacon message is accepted (i.e., the beacon message come from an legitimate A-vehicle and doesn't be tampered). This is because both the adopted signature schemes [17] and [18] have been proven to be secure under chosen message attacks under the Computational Diffie-Hellman (CDH) assumption. In addition, each message in our scheme is marked by a timestamp to resist replay attacks.

5.2 Content Privacy

It is ensured by symmetric encryption. As discussed in **Algorithm 1**, the PHI M is encrypted to $C = Enc_k(M)$, where $k = g^{yy'}$ is the session key computed by multiplying a secret random number y' and the target PH's public key g^y. When the PH receives the PHI packet $Data$ which includes $g^{y'}||C$, she/he can compute the session key using her/his private key y. However, the adversary neither know the secret random number y' nor the private key y. Even the adversary eavesdrops $g^{y'}$ and knows the PH's public key g^y (in fact, we will demonstrate that SVC ensures the adversary does not know which PH the PHI packet is sent to, thus the adversary does not know g^y), she/he cannot compute $g^{yy'}$ in expected time under the Computational Diffie-Hellman (CDH) assumption. Therefore, with secure symmetric encryption $Enc()$ (e.g, AES), the Content Privacy can be protected in SVC.

5.3 Identity Privacy

Each patient in SVC uses N pseudonyms $PID_{PA_i}|_{i=1}^{N}$ instead of her/his real identity to protect identity privacy. The pseudonyms are chosen by TA randomly, which are independent of the real identities and indistinguishable from each other. The patient updates her/his pseudonym in different PHI packets and the adversary cannot link the pseudonym to her/his real identity. The A-vehicle identity privacy is protected in the same way except that the pseudonyms $ID_{AV}|_{i=1}^{N}$ are chosen by the L-vehicle.

5.4 Context Privacy

As discussed in Section 3, context privacy requires that no adversary can link the source and the destination of the PHI packet. Here, we consider a strong attacker who can collude with the insiders. In SVC, the destination ID_{PH} is hidden in $PEKS(PK_{PH}, ID_{PH})$ using the PEKS scheme in [20]. Before demonstrating how it achieves context privacy, we first discuss the security of the PEKS scheme. We have to ensure that $PEKS(PK_{PH}, ID_{PH})$ does not reveal any information about the recipient. In other words, $PEKS(PK_{PH}, ID_{PH})$ reveals neither PK_{PH} nor ID_{PH}. [20] has proven that the PEKS scheme is semantically secure under chosen keyword attack in the random oracle model under the Bilinear Diffie-Hellman (BDH) assumption (PEKS-IND-CPA security). Thus it does not reveal any information about ID_{PH}, even under the strong attack.

Here we discuss the security of $PEKS(PK_{PH}, ID_{PH})$ with respect to PK_{PH}. We are going to prove that the PEKS scheme in [20] is an anoymous encryption under chosen keyword attack (we call it PEKS-ANO-CPA). That is, a strong attacker cannot infer the information PK_{PH}.

First, refering to [36], PEKS-ANO-CPA is formallly defined using the following game between a challenger and an attacker $\mathcal{A}$:

1. The challenger takes the security parameter k and generates system parameter $param$ and master-key s. It gives $param$ to the attacker $\mathcal{A}$.
2. The challenger generates (PK_0, SK_0), (PK_1, SK_1) and sends the attacker $\mathcal{A}$ the two public keys PK_0 and PK_1.
3. The attacker $\mathcal{A}$ sends a keyword W to the challenger.
4. The challenger picks a random $b \in \{0,1\}$ and gives the attacker $\mathcal{A}$ the challenge ciphertext $PEKS(PK_b, W)$.

The advantage of $\mathcal{A}$ in above game is

$$Adv_{\mathcal{A}}(k) = \Pr[b'=1|b=1]\text{-}\Pr[b'=1|b=0] \tag{13}$$

Definition 3 (PEKS-ANO-CPA). A PEKS scheme is PEKS-ANO-CPA secure if for any polynomial time attacker $\mathcal{A}$ the advantage function $Adv_{\mathcal{A}}(k)$ is a negligible function.

Intuitively, note that $PEKS(PK_b, W) = [g^r, H_2(t)] = [A, B]$ has two part $A = g^r$ and $B = H_2(t)$. First, r is chosen uniformly at random from Z_q^* by the challenger, thus for any element $\tilde{g} \in G^*$, $Pr[A = \tilde{g}] = 1/|G^*|$. Second, for any element $\tilde{x} \in Z_q^*$, $Pr[B = \tilde{x}] = 1/|Z_q^*|$ in the random oracle model. Therefore, in both $b = 0$ and $b = 1$ cases of the game, the challenge ciphertext $PEKS(PK_b, W)$ has exactly the same distribution. In fact, we have the following theorem, the formal proof of this theorem can refer to the proof of Lemma 4.3 and Theorem 4.4 in [37].

Theorem 1. The PEKS scheme in [20] is PEKS-ANO-CPA secure under the BDH assumption in the random oracle model.

Based on the above analysis, $PEKS(PK_{PH}, ID_{PH})$ indeed does not reveal any information about both PK_{PH} and ID_{PH} to a strong attacker. Therefore from the PHI packet transmitted

over the VANET and the health center, the attacker cannot infer to any information about the destination. Suppose there are n physicians in the health center, combining with the broadcast technique, every physician has $1/n$ possibility of being the destination from the attacker's point of view, even through the attacker colludes with the insiders (the L/A-vehicle and the DB does not know any information about the recipient, either). Therefore, the context privacy is achieved in SVC under.

6. Performance Evaluation

6.1 Computation Overhead

We choose the Type A pairing of PBC Library [38] and jPBC Library [39] which is implemented on the curve $y^2 = x^3 + x$ over the field F_p with 512 bits p and the embedding degree is 2 for our system. G is a subgroup of the curve $E(F_p)$ and G_T is a subgroup of the field F_{q^2}. Thus the size of the elements in G and G_T is 512 + 1 bits (using point compression) and 1024 bits, respectively. The order q of G and G_T is 160 bits. We analyze the computation overhead using the benchmarks from PBC and jPBC on the following simulation platforms:

- WBAN gateway: we use a smartphone HTC Desire HD A9191 with Qualcomm QSD8225 1GHz CPU and 1.5GB ROM, Android 2.2 to simulate the WBAN gateway, on which programming with jPBC Library.
- A-vehicle, DB and PH: we use a PC with Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GHz, 3GB RAM, Ubuntu 10.04 to simulate A-vehicle, DB and PH, on which programming with PBC Library.

Note that we only count the computation overhead for pairing and exponentiation in G. Other computations such as hashing, addition/multiplication in Z_q^* are negligible compared with the two computations. The measured results on the PC and on the smartphone are given in **Table 2** and **Table 3**, respectively. The preprocessing applies to the pairings with one constant G element and the exponentiations with the constant base.

Table 2. Benchmark of PBC on PC

Notation	Computation	Time Cost
C_p	pairing without preprocessing	2.7 ms
C_{pp}	pairing with preprocessing	1.1 ms
C_e	exponentiation without preprocessing	3.5 ms
C_{pe}	exponentiation with preprocessing	0.3 ms

Table 3. Benchmark of jPBC on smartphone

Notation	Computation	Time Cost
C_{jp}	pairing without preprocessing	491 ms
C_{jpp}	pairing with preprocessing	245 ms
C_{je}	exponentiation without preprocessing	260 ms
C_{jpe}	exponentiation with preprocessing	30 ms

Table 4. The computation cost in a WBAN to A-vehicle process

WBAN gateway	$3C_{jpp}+C_{jp}+C_{je}+2C_{jpe}=1.5\text{s}$
A-vehicle	$2C_{pe}+2C_{pp}+C_e=6.3\text{ms}$

Table 4 gives the computation cost of each side in a WBAN to A-vehicle process. Specifically, the A-vehicle first broadcasts the beacon message, it needs $2C_{pe}$ to compute (X,Y). Then the WBAN gateway costs $3C_{jpp}+C_{jp}+C_{je}$ to check the beacon message. After that, the gateway runs $2C_{jpe}$ to generates σ_{PA} in the PHI packet. Note that we do not count the computation overhead of *Data* because it can be pre-computed before the A-vehicle comes. Finally, the A-vehicle takes $2C_{pp}+C_e$ to verify σ_{PA}. Thus for the gateway the total computation overhead is $3C_{jpp}+C_{jp}+C_{je}+2C_{jpe}=1.5\text{s}$ and $2C_{pe}+2C_{pp}+C_e=6.3\text{ms}$ for the A-vehicle in this process.

In the process from A-vehicle to DB, suppose that DB receives $cert_{LV_i}|_{i=1}^{n}$ and $(X_i',Y_i')|_{i=1}^{n}$ in a time window. For the public-key certificates, if there is no forged one among them, it only needs $2C_{pp}=2.2\text{ms}$ for DB to batch verify them. If there are k forged signatures, the computation overhead is $(k+2)log(n/k)+4k-2$ by using binary authentication algorithm [35]. In contrast, if DB individually verifies $cert_{LV_i}$ for $i=1$ to $i=n$, the computation overhead is $2nC_{pp}$. For the signatures, if all of them were signed by legitimate A-vehicles, the computation overhead for DB to batch verify them is $C_{pp}+nC_p+nC_e$, and if there exist k forged signatures, it is $[(k/2+1)log(n/k)+2k-1]C_{pp}+nC_p+nC_e$. In contrast, if DB individually verifies them, the computation overhead is $nC_{pp}+nC_p+nC_e$. **Fig. 3** gives the computation overhead compare between individual verification and batch verification with different k/n of $cert_{LV_i}|_{i=1}^{n}$ and $(X_i',Y_i')|_{i=1}^{n}$.

In the last process, suppose that the PH with ID_{PH} receives n PHI packets. For each packet, she/he takes one C_{pp} to test whether this packet is sent to her/him, thus the total computation overhead is nC_{pp}. Given n=1000, then the computation overhead is only 1.1 s.

Base on the above analysis, we conclude that the computation overhead of SVC is very acceptable.

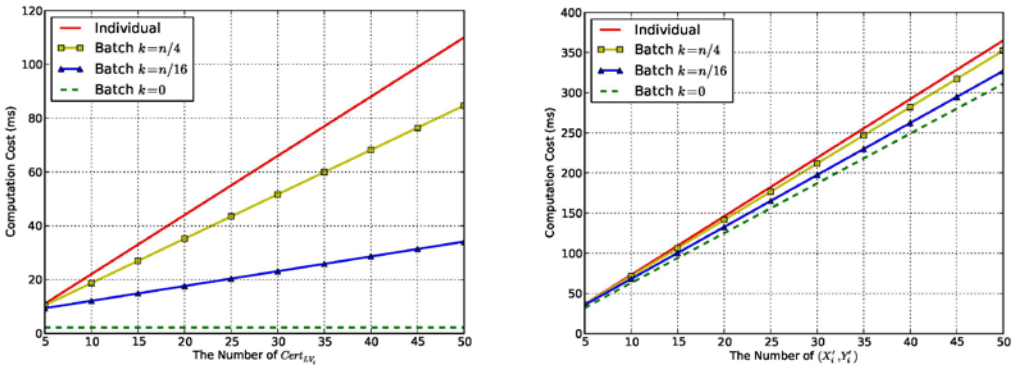


Fig. 3. The computation overhead of verifying $cert_{LV_i}|_{i=1}^{n}$ and $(X_i',Y_i')|_{i=1}^{n}$

6.1 Storage Overhead

In SVC, both DB and A-vehicles (and L-vehicles) are required to store the PHI packets. DB is a commonly powerful and resource-abundant server so that the storage overhead is not stringent. Therefore we only discuss the storage overhead of A-vehicles. For each A-vehicle, the stored contents consist of the ID, public key, and certificate of the L-vehicle, i.e., $(ID_{LV}, PK_{LV}, cert_{LV})$, a sequence of pseudonyms and private keys $(ID_{AV_i}, SK_{AV_i})|_{i=1}^{n}$ issued by the L-vehicle and a number of PHI packets $\{Data_j = g^{y_j} || C_j || A_j || B_j\}|_{j=1}^{m}$ it collected. We assume that both ID_{LV} and ID_{AV_i} are 16 bits, C_i is 120 bytes. Then the storage overhead of an A-vehicle approximately equals $130 + 68n + 268m$ bytes. This value is acceptable for the storage capability of modern vehicle (e.g., the BMW iDrive system is equipped with an on-board computer with 20 GB hard disk).

7. Related Works

In recent years, many research works have improved the development of health information transmission of remote healthcare monitoring (RHM) [3-10]. Application of IEEE 802.16/WiMAX-based broadband wireless acess technology for health information transmission (e.g., communication between an ambulance and the health center) was discussed in [3] and the followup work [4] presented a RHM system using heterogeneous wireless networks (WiMAX-based WMAN and WiFi-based WLAN). Both of the works were concerned on broadband allocation, traffic scheduling and network optimization. To improve transmission performance of RHM system, a handoff protocol between WBAN and a fixed access point (AP) was proposed in [6] to address the poor signal reception in AP when patient moves. [5] employed Reed-Solomon coding and point-coordination fucntion (PCF) to reduce the error-prone nature of wireless channel and the unpredictable delay due to the nondeterministic nature of acess to wireless medium. The problems these works researched were important in RHM, however, none of them referred to the security and privacy problems.

In the following, we review the most relevant works that are concerned on the security and privacy problems in RHM. Lin et al. proposed a strong privacy-preserving scheme for eHealth system, named SAGE [7]. The PHIs were transmitted from WBAN to a WiFi access point connected with Internet in the system, and both content privacy and contextual privacy were achieved. In SAGE, each physician and each patient share a static key, and broadcast technique combined with Hash Message Authentication Code (HMAC) was used to protect contextual privacy. HMAC is indeed more efficient than PEKS, however, the static shared keys management is a troublesome task for each physician because of the huge and dynamic number of the keys. Liang et al. presented a new RHM system model in a smart community environment [8], that was, a patient taking a walk in the smart community can use the multi-hop community network composed of smart homes instead of 3G cellular network to transmit his/her PHI so that the high cost of the latter can be economized. The privacy problems they solved in the system were identity privacy and location privacy. The same to the economic motivation, to minimize the overall health care cost in rural area, Barua et al. proposed a delay-tolerant secure long-term health care system, RCare, in which VANET was used to transmit the PHIs from Rural Access Points (RAPs) to Road-Side Units (RSUs) in the city [9]. RCare's primary concerns were on the communication in the WBAN and the incentive for the VANET. A secure communication protocol between the WBAN gateway and the sensors and a privacy-preserved incentive scheme for the VANET were presented in this work.

To improve the computation efficiency, Lin et al. presented CAM, a cloud-assisted privacy-preserving mobile health monitoring system [10]. In this system, both the clients' monitored data (PHIs) and the service providers' monitoring programs were placed in cloud so that the most cumbersome computation can be performed by the powerful cloud. In addition to the clients' privacy, the intellectual property of monitoring service providers, i.e. the monitoring programs, were also protected in this work.

The works above presented four different environments of RHM, a normal one in [7], smart community in [8], rural area with VANET in [9], and a cloud solution in [10]. However, as discussed in Section 1, none of these works are suitable for the disaster area because of the unpredictable network connectivity in the disaster. Note that even though [9] used VANET to transmit PHIs, the system application environment, the system model, and the security and privacy concerns are all different from SVC such that it can not be adopted in disaster area directly.

In the technical view, the batch verification in VANET was first used in [40]. In this paper, we use the similar technique to improve the efficiency at the PH's end.

8. Conclusion

In this paper, we present SVC, an RHM system working in a disaster area. Instead of using the traditional communication networks, the emerging VANET is employed to assist the PHIs transmission to eliminate the damage to communication infrastructure caused by the disaster. A two-level key management model is designed to manage the trust of vehicles, and under which the security of each communication process is ensured. In addition, the strong context privacy is achieved in our scheme, that is, any attacker can't link the destination and the source of a PHI packet.

References

[1] Telehealth to reach 1.8 million patients by 2017. Article (CrossRef Link).

[2] A. Tesanovic, G. Manev, M. Pechenizkiy and E. Vasilyeva, "Ehealth personalization in the next generation rpm systems," in *Proc. of 22nd IEEE International Symposium on Computer-Based Medical Systems*, pp. 1-8, 2009. Article (CrossRef Link).

[3] D. Niyato, E. Hossain and J. Diamond, "IEEE 802.16/wimax-based broadband wireless access and its application for telemedicine/e-health services," *IEEE Wireless Communications Magazine*, vol. 14, no. 1, pp. 72-83, 2007. Article (CrossRef Link).

[4] D. Niyato, E. Hossain and S. Camorlinga, "Remote patient monitoring service using heterogeneous wireless access networks: architecture and optimization," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 412-423, 2009. Article (CrossRef Link).

[5] K. Kang, K. J. Park, J. J. Song and C. H. Yoon, L. Sha, "A medical-grade wireless architecture for remote electrocardiography," *IEEE Transactions on Information Technology in Biomedicine*, vol. 15, no. 2, pp. 260-267, 2011. Article (CrossRef Link).

[6] S. Gonzalez-Valenzuela, M. Chen and V. C. Leung, "Mobility support for health monitoring t home using wearable sensors," *IEEE Transactions on Information Technology in Biomedicine*, vol. 15, no. 4, pp. 539-549, 2011. Article (CrossRef Link).

[7] X. Lin, R. Lu, X. Shen, Y. Nemoto and N. Kato, "Sage: a strong privacy-preserving scheme against global eavesdropping for ehealth systems," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp.365-378, 2009. Article (CrossRef Link).

[8] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, "Enabling pervasive healthcare with privacy preservation in smart community," in *Proc. of IEEE International Conference on Communications*, pp. 3451-3455, 2012. Article (CrossRef Link).

[9] M. Barua, X. Liang, R. Lu and X. Shen, "Rcare: extending secure health care to rural area using VANETs," *Mobile Networks and Applications*, vol. 19, no. 3, pp. 318-330, 2014. Article (CrossRef Link).
[10] H. Lin, J. Shao, C. Zhang and Y. Fang, "Cam: cloud-assisted privacy preserving mobile health monitoring," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, pp. 985-997, 2013. Article (CrossRef Link).
[11] J. Sun, X. Zhu, C. Zhang and Y. Fang, "RescueMe: location-based secure and dependable VANETs for disaster rescue," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 659-669, 2011. Article (CrossRef Link).
[12] Ponemon Institute LLC, American's opinions about healthcare privacy, 2010. Article (CrossRef Link).
[13] A. Shamir, "Identity-based cryptosystems and signature schemes," *Advances in cryptology*, pp. 47-53, 1985. Article (CrossRef Link).
[14] D. Boneh, M. Franklin, "Identity-based encryption from the weil pairing," *Advances in Cryptology—CRYPTO 2001*, pp. 213-229, 2001. Article (CrossRef Link).
[15] A. Joux, "The weil and tate pairings as building blocks for public key cryptosystems," in *Proc. of Algorithmic Number Theory*, pp. 20-32, 2002. Article (CrossRef Link).
[16] A. Fiat, "Batch RSA," *Advances in Cryptology—CRYPTO 89*, pp. 175-185, 1990. Article (CrossRef Link).
[17] D. Boneh, B. Lynn and H. Shacham, "Short signatures from weil pairing," *Advances in Cryptology—ASIACRYPT 2001*, pp. 514-532, 2001. Article (CrossRef Link).
[18] J. C. Cha and J. H. Cheon, "An identity-based signature from gap diffie-hellman groups," in *Proc. of Public key cryptography (PKC)*, pp. 18-30, 2003. Article (CrossRef Link).
[19] A. L. Ferrara, M. Green, S. Hohenberger and M. Ø. Pedersen, "Practical short signature batch verification," *Topics in Cryptology—CT-RSA 2009*, pp. 309-324, 2009. Article (CrossRef Link).
[20] D. Boneh, G. Di Crescenzo, R. Ostrovsky and G. Persiano, "Public key encryption with keyword search," *Advances in Cryptology—EUROCRYPT 2004*, pp. 506-522, 2004. Article (CrossRef Link).
[21] J. Sun, X. Zhu, C. Zhang and Y. Fang, "HCPP: cryptography based secure EHR system for patient privacy and emergency healthcare," in *Proc. of 31st International Conference on Distributed Computing Systems*, pp. 373-382, 2011. Article (CrossRef Link).
[22] M. Li, S. Yu, Y. Zheng, K. Ren and W. Lou, "Scalable and secure sharing of personal healh records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131-143, 2013. Article (CrossRef Link).
[23] H. Deng, W. Li and D. P. Agrawal, "Routing security in wireless ad hos networks," *IEEE Communications Magazine*, vol. 40, no. 10, pp. 70-75, 2002. Article (CrossRef Link).
[24] M. Li, S. Yu, J. D. Guttman and W. Lou, K. Ren, "Secure ad hoc trust initialization and key management in wireless body area networks," *ACM Transactions on Sensor Networks*, vol. 9, no. 2, 2013. Article (CrossRef Link).
[25] X. Liang, X. Li, Q. Shen, R. Lu, X. Lin, X. Shen and W. Zhuang, "Exploiting prediction to enable secure and reliable routing in wireless body area networks," in *Proc. of IEEE INFOCOM*, pp. 388-396, 2012. Article (CrossRef Link).
[26] R. A. Popa, A. J. Blumberg, H. Balakrishnan and F. H. Li, "Privacy and accountability for location-based aggregate statistics," in *Proc. of 18th ACM Conference on Computer and Communications Security*, pp. 653-666, 2011. Article (CrossRef Link).
[27] P. Kamat, Y. Zhang, W. Trappe and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in *Proc. of 25th IEEE International Conference on Distributed Computing Systems*, pp. 599-608, 2005. Article (CrossRef Link).
[28] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198-208, 1983. Article (CrossRef Link).
[29] J. Daemen and V. Rijmen, "The design of Rijndael: AES – the advanced encryption standard," *Springer*, 2002. Article (CrossRef Link).

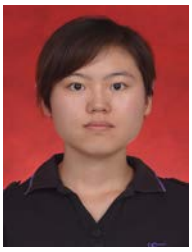
[30] W. Mao, “Modern cryptography: theory and practice,” *Prentice Hall PTR*, 2003. Article (CrossRef Link).
[31] Z. Zhu and G. Cao, “Toward privacy preserving and collusion resistance in a location proof updating system,” *IEEE Transactions on Mobile Computing*, vol. 12, no. 1, pp. 51-64, 2013. Article (CrossRef Link).
[32] R. Lu, X. Lin, X. Shen, “Spring: a social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks,” in *Proc. of IEEE INFOCOM*, pp. 1-9, 2010. Article (CrossRef Link).
[33] R. Lu, X. Lin, H. Zhu, X. Shen and B. Preiss, “Pi: a practical incentive protocol for delay tolerant networks,” *IEEE Transactions on Wireless Communications*, vol. 9, no. 4, pp. 1483-1493, 2010. Article (CrossRef Link).
[34] U. Shevade, H. H. Song, L. Qiu and Y. Zhang, “Incentive-aware routing in DTNs,” *IEEE International Conference on Network Protocols*, pp. 238-247, 2008. Article (CrossRef Link).
[35] Y. Jiang, M. Shi, X. Shen and C. Lin, “Bat: a robust signature scheme for vehicular networks using binary authentication tree,” *IEEE Transactions on Wireless Communications*, vol. 8, no. 4, pp. 1974-1983, 2009. Article (CrossRef Link).
[36] M. Bellare, A. Boldyreva, A. Desai and D. Pointcheval, “Key-privacy in public-key encryption,” *Advances in Cryptology—ASIACRYPT 2001*, pp. 566-582, 2001. Article (CrossRef Link).
[37] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, “Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extension,” *Advances in Cryptology–CRYPTO 2005*, pp. 205-222, 2005. Article (CrossRef Link).
[38] The pairing based cryptography library (PBC). Article (CrossRef Link).
[39] The java pairing based cryptography library (jPBC). Article (CrossRef Link).
[40] C. Zhang, R. Lu, X. Lin, P.H. Ho and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. of IEEE INFOCOM*, 2008. Article (CrossRef Link).
[41] C. Zhang, P.H. Ho and J. Tapolcai, "On batch verification with group testing for vehicular communications," *Wireless Networks*, vol. 17, no. 8, pp. 1851-1865, 2011. Article (CrossRef Link).
[42] X. Lin, R. Lu, C. Zhang, H. Zhu, P. Ho and X. Shen, "Security in vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 88-95, 2008. Article (CrossRef Link).

Xuefeng Liu is a postdoctor of Xidian University, China. He received his B.S. and Ph.D. degrees in information security from Xidian University, in 2007 and 2013, respectively. His research interests lie in the fields of cloud computing security and applied cryptography.

Hanyu Quan received the M.S. degree in cryptography and the B.S. degree in information security from Xidian University. He is currently working toward the Ph.D. degree in Xidian University. His research interests include the security and privacy issues in cloud computing and big data.

Yuqing Zhang is a professor and supervisor of Ph.D. students of Graduate University of Chinese Academy of Sciences. He received his B.S. and M.S. degree in computer science from Xidian University, China, in 1987 and 1990 respectively. He received his Ph.D degree in Cryptography from Xidian University in 2000. His research interests include cryptography, wireless security and trust management.

Qianqian Zhao received her BSc degree information and computing science from Henan University, China, in 2009. She is currently working torward the Ph.D degree in Information Security, Department of Communication Engineering, Xidian University. Her research interests include cryptography, wireless security, cloud computing security, and social networks.



Ling Liu received her B.E. Degree in information security from Xidian University, China, 2013. She has been in Xidian University for her Ph.D degree since 2013. Her research interests include privacy issues in cloud computing, wireless security and applied cryptography.