PEC: A Privacy-Preserving Emergency Call Scheme for Mobile Healthcare Social Networks

Xiaohui Liang, Rongxing Lu, Le Chen, Xiaodong Lin, and Xuemin (Sherman) Shen

Abstract: **In this paper, we propose a privacy-preserving emergency call scheme, called PEC, enabling patients in life-threatening emergencies to fast and accurately transmit emergency data to the nearby helpers via mobile healthcare social networks (MHSNs). Once an emergency happens, the personal digital assistant (PDA) of the patient runs the PEC to collect the emergency data including emergency location, patient health record, as well as patient physiological condition. The PEC then generates an emergency call with the emergency data inside and epidemically disseminates it to every user in the patient's neighborhood. If a physician happens to be nearby, the PEC ensures the time used to notify the physician of the emergency is the shortest. We show via theoretical analysis that the PEC is able to provide fine-grained access control on the emergency data, where the access policy is set by patients themselves. Moreover, the PEC can withstand multiple types of attacks, such as identity theft attack, forgery attack, and collusion attack. We also devise an effective revocation mechanism to make the revocable PEC (rPEC) resistant to inside attacks. In addition, we demonstrate via simulation that the PEC can significantly reduce the response time of emergency care in MHSNs.**

Index Terms: **Fine-grained access control, mobile healthcare social network, privacy preservation, revocation.**

I. INTRODUCTION

From the "List of causes of death by rate" [1], heart disease and stroke are the causes of 50 percent of deaths worldwide, and car accidents cause an additional 600,000 deaths per year. Most heart and stroke survivors and car accident survivors suffer long-term disabilities. Research studies [2]–[4] conclude that early and specialized pre-hospital acute medical treatment contributes to emergency case survival and a rapid response of emergency care results in dramatically improving the outcome of patients. In practice, the current healthcare system accommodates emergency medical services (EMS) [5] which are dedicated to provide pre-hospital acute medical treatment and/or transport definitive care to patients with illnesses and injuries which the patient or the medical practitioner believes constitute to a medical emergency. The services normally require a central trusted authority (TA) to help allocating the emergency resources, as shown in Fig. 1. After receiving an emergency call from the witness, ambulance personnels following the instructions provided by hospital experts are sent to first handle the emergency situations and take the patients to hospital as soon as possible. We call such system a centralized emergency response system. In addition, the system is further improved in terms of reducing the response time. For example, international medical health organization (IMHO) allows patients to directly transmit the emergency data to a remote hospital via general packet radio service (GPRS), global system for mobile communications (GSM), or third generation of mobile telephony (3G) links so that the hospital could find a physician near to the emergency location to provide emergency care. However, the centralized emergency response system might not be stable if either the centralized available medical resources are pretty limited or the emergency location is very faraway from the medical resources. In this paper, we address the emergency response problem from "mobile healthcare social network (MHSN)" perspective: Enabling a patient to locally search for the nearby physicians via a self-organized manner.

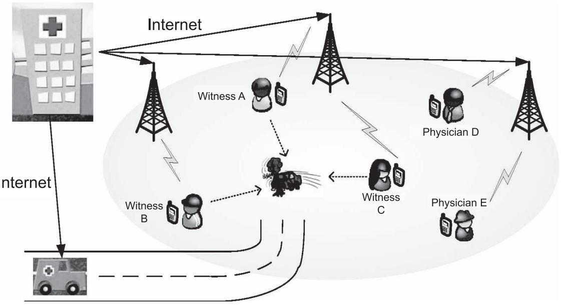


Fig. 1. A centralized emergency response system.

Mobile healthcare social network [6]–[9], serving as a mobile community platform for healthcare purposes, extends the traditional centralized healthcare system by placing great emphasis on user self-organized and social interactivities. An essential capability offered by MHSN is to allow mobile patients to search, recognize, and interact with physicians who locate in their physical vicinity. As shown in Fig. 2, each user of MHSN is equipped with a personal digital assistant (PDA) and able to wirelessly connect to an one-hop neighboring user without the involvement of any third party. In MHSN, some users are patients equipped with wireless body sensors that can be used to monitor body physiological condition, and they need medical services in the emergency situation. Some physicians or paramedics are capable of providing medical services to patients who are in need of emergency care.

A decentralized emergency response system designed in MHSN can reduce the response time compared to the centralized emergency response system. Firstly, patients can use the decentralized emergency response system as an auxiliary tool

Manuscript received October 10, 2010.

The research is financially supported by the Ontario Research Fund for Research Excellence (ORF-RE), Canada.

X. Liang, R. Lu, L. Chen, and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1, email: {x27liang, rxlu, xshen}@bbcr.uwaterloo.ca, chenle0213@gmail.com.

X. Lin is with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, Ontario, Canada, L1H 7K4, email: xiaodong.lin@uoit.ca.

1229-2370/11/$10.00 © 2011 KICS

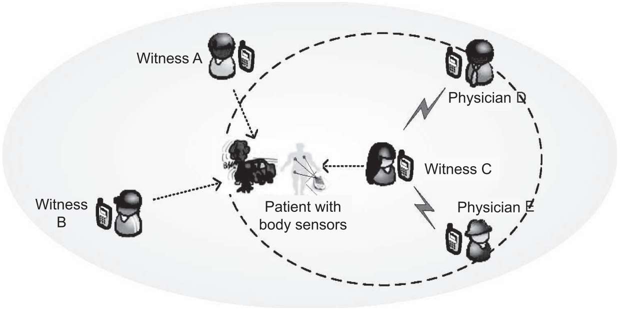


Fig. 2. A decentralized emergency response system in an MHSN.

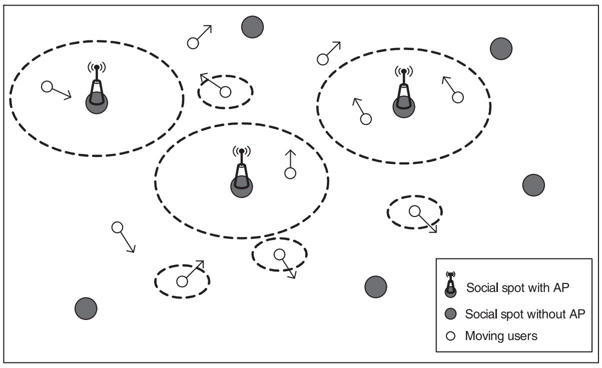


Fig. 3. Network model.

to locally find the nearest physician, while waiting for the ambulance or someone who might be sent from a faraway location. Secondly, it prevents a single point failure of the centralized services when the centralized available resources are pretty limited or the centralized control system is down. Thirdly, it does not require a well-structured network to support long-distance communication. As a result, the decentralized emergency response system could possibly have short transmission delay and consume less transmission power. Notably, for the decentralized emergency response system, though the medical equipments may not be available, the body sensors deployed in, on or around that patient's body can intelligently and continuously collect physiological condition and provide certain body-related information for local medical measures. The decentralized emergency response system increases patient safety, but this system poses new challenging issues on the security and privacy of personal health information (PHI) [10]–[12].

In this paper, we consider the following research issues in designing a privacy-preserving emergency call (PEC) scheme in MHSNs. Since the availability of emergency data wherever medical services are required maybe critical to save lives, the PEC should guarantee that emergency data is always available if it is needed. A quick access to emergency data must be provided to assist nearby physicians in finding the emergency location within a short time and carrying out accurate medical measures using emergency data as a source of reference. Meanwhile, any inappropriate disclosure of emergency data to malicious users may enable them to track private behaviors and seriously violate personal privacy. This would result in a difficulty in encouraging privacy-aware patients to use the system. Specifically, in the emergency situation, patients should not expose their identification information to untrustworthy users but share enough medical information with the arrived physicians or paramedics. The PEC thus needs to support a fine-grained access control of emergency data [13], [14]. Additionally, the PEC must ensure the integrity and authenticity of the transmitted emergency data and have an effective revocation mechanism in order to evict the malicious users out of the network.

The main contributions of this paper are threefold.

- We propose a privacy-preserving emergency call scheme, called PEC, adopting an attribute-based encryption technique to enable fine-grained access control of emergency data to patients. With the PEC, emergency data can be disclosed completely following the access policy predefined by the patient itself. In addition, the accompanied access control information can be computationally efficient.
- We extend the PEC to the revocable PEC, called rPEC, which enables a TA to both effectively and periodically revoke the access capabilities of inside attackers. We also consider how to prevent identity theft attacks and forgery attacks.
- We develop a custom Java simulator of the MHSN and demonstrate the effectiveness of the proposed PEC in terms of reducing response time.

The remainder of this paper is organized as follows. Section II introduces the problem formalization including the network model, the emergency data access model, the security model and the design goal. We present the PEC/rPEC in Section III, followed by the security analysis and performance evaluation in Sections IV and V, respectively. We review the related work in Section VI. Finally, we draw our conclusions in Section VII.

II. PROBLEM FORMALIZATION

In this section, we define the network model, the emergency data access model, and the security model. Then, we describe the design goal of the PEC/rPEC.

A. Network Model

We consider a typical MHSN consisting of l fixed social spots denoted by $\mathcal{S}_u = \{s_1, s_2, \cdots, s_l\}$ and k users denoted by $\mathcal{V} = \{n_1, n_2, \cdots, n_k\}$, where each user holds a PDA with the wireless transmission range tr. The social spots are defined as regions with high population density [15]. The communication between any two users n_i and n_j is bidirectional, i.e., n_i can hear n_j if and only if n_j can also hear n_i. If n_i can hear n_j, n_j is called a neighboring user of n_i. Some social spots are equipped with the access points (APs) which have wireless transmission range $tr_s > tr$, while others are not. We denote the AP corresponding to a social spot s_i by ap_i. The communication between a user n_i and an AP ap_j is unidirectional, i.e., if ap_j can hear n_j, n_j can also hear ap_j; if n_i can hear ap_j, it is not necessary that ap_j can hear n_i.

Mobility pattern: A user is associated with a set of social spots that he frequently visits. Let $\mathcal{S}_i \subseteq \mathcal{S}_u$ denote the social spot set of user n_i. The mobility pattern of each user depends on the locations of his social spots. They always move towards

Table 1. Emergency data types.

	Readable	Identifiable	Privacy-sensitive	Accessible
GI	⋆⋆⋆	⋆	⋆	⋆⋆⋆
PC	⋆⋆	⋆⋆	⋆⋆	⋆⋆
HR	⋆	⋆⋆⋆	⋆⋆⋆	⋆

their social spots and stay at the social spots for a certain amount of time.

B. Emergency Data Access Model

In an emergency data access model, we divide emergency data into three types: The general information (GI), the physiological condition (PC), and the health record (HR). The GI contains location, time, and description of the environmental condition, which can help ambulance personnel or nearby physicians to find the emergency location and arrive there within the shortest time; the PC is real-time body condition monitored by the body sensors; the HR includes family disease records and preused prescriptions which assist the arrived physicians in making accurate medical measures without complete patient profile. We denote the PC and the HR as PHI in this paper. Notably, a quick access to PHI would reduce the response time of emergency care and facilitate accurate medical measures. From the privacy preservation perspective, the access should be limited and patient self-controllable. Considering these issues, we further discuss the properties of the three types, as shown in Table 1.

We consider the GI as a non-privacy-sensitive type. The GI should be accessed by every user because it contains the critical information which helps a user to arrive at the emergency location within the shortest time. We consider the PC as a medium-privacy-sensitive type. The PC is composed of various signals, such as blood pressure and heart rhythm which are readable for those who have general medical knowledge. In this paper, the PC is considered to be accessed by physicians and paramedics. We consider the HR as a high-privacy-sensitive type. The HR contains unique and personal identifiable information of patients. The inappropriate disclosure of this type of information would pose serious threat to patient privacy. On the other hand, the HR is worth disseminating to the local physicians to prevent wrong diagnosis and inaccurate medical measures. As such, the HR is considered to be accessed by the physicians and the certified paramedics. These medical professionals have comprehensive medical knowledge to read the HR and they are trusted to preserve patient privacy. The above access policies of GI, PC, and HR are simple and straightforward. In practise, the patients are able to choose various access policies for different kinds of data type according to their own requirements.

C. Security Model

Since the mobile healthcare social network is distributed and unattended, any user possibly acts as a malicious adversary who may readily launch the security attacks to violate other users' privacy. Therefore, we consider that an adversary can compromise a fraction of users and obtain the compromised users' information. The adversary launches two types of attacks related to user privacy, one is an identity theft attack; the other one is a collusion attack. The identity theft attackers do not aim to access patient PHI, but instead they want to obtain unique identification information of patients from emergency calls. The collusion attackers do not have enough credentials to access patient PHI, but they aim to eavesdrop PHI by colluding with others.

We also consider that a forgery adversary generates a misleading emergency call with the bogus location information. This attack hardly being caught would easily exhaust network resources and ruin user trust to the healthcare services.

We further consider that an inside adversary maliciously reveal patient PHI to unauthorized entities. To resist the inside attack, a revocation mechanism controlled by a TA is normally needed to update the credentials of all non-revoked users.

D. Design Goal

Our design goal is to develop a privacy-preserving emergency call scheme which can resist all the attacks introduced in previous subsection. Specifically, the following three desirable objectives must be achieved.

D.1 Enhancing availability of PHI by using a fine-grained self-control mechanism

In an emergency situation, the access control of the PHI should completely follow the patient's willingness. In addition, the patients are able to disseminate their PHI according to fine-grained purposes in order to preserve their privacy.

D.2 Preserving identity privacy and ensuring unlinkability of the transactions

In an emergency situation, a patient must reveal his information to the nearby users in order to ask for their instant help. However, with privacy concerns, the patients would preserve the identity privacy and prevent their transactions being linked to their unique identities. On the other hand, a TA must be able to trace the emergency call and identify the corresponding patient. In this way, any malicious attacker who has generated a bogus emergency call would be detected and punished.

D.3 Effective revocation on access capabilities of inside attackers

A TA must have an effective and feasible revocation mechanism to revoke the access capabilities of the inside attackers. Once their malicious behaviors are detected, the attackers' access capabilities must be revoked.

III. PROPOSED SCHEMES

In this section, we will first introduce the design rationale, and then elaborate the PEC and the rPEC.

A. Design Rationale

In an emergency situation, a patient would forward the emergency data to nearby users aiming to locally find a physician or a paramedic as soon as possible. An effective data forwarding strategy is to let patients and relay users epidemically disseminate the emergency data. This strategy relying on the locally cooperative communications among mobile users, can increase patient safety even if the patient cannot contact to hospital or first-aid center. If a physician is in the neighbor area of the patient,

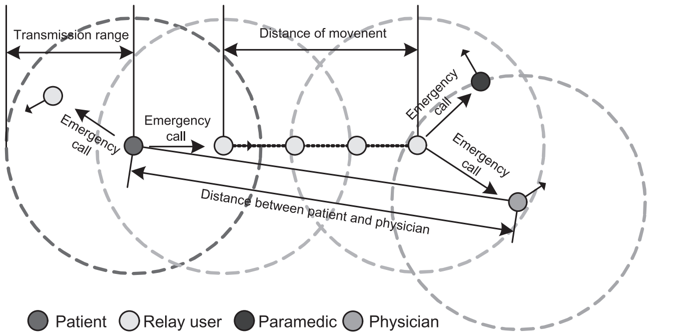


Fig. 4. A patient sends an emergency call to a paramedic or a physician.

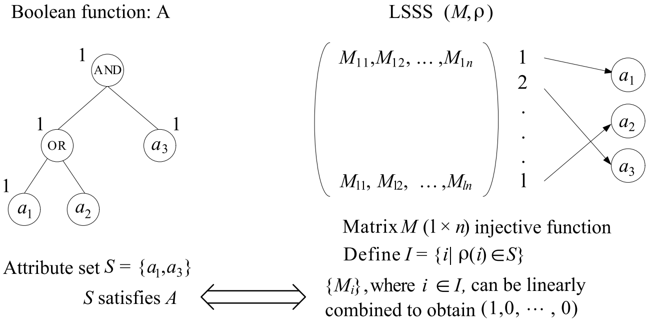

Boolean function: A
1
AND
1
OR
1
a_3
1
a_1
a_2
LSSS (M,ρ)
$M_{11},M_{12}, \ldots ,M_{1n}$
$M_{l1}, M_{l2}, \ldots ,M_{ln}$
1
2
.
.
.
l
a_1
a_2
a_3
Matrix M ($l \times n$) injective function
Define $I = \{i \mid \rho(i) \in S\}$
Attribute set $S = \{a_1,a_3\}$
S satisfies A
$\{M_i\}$, where $i \in I$, can be linearly combined to obtain $(1,0, \cdots, 0)$

Fig. 5. An attribute set satisfying a linear secret sharing structure.

this strategy will ensure that the physician receives the emergency call within the shortest time. As shown in Fig. 4, a relay user forwards the emergency call to a paramedic and a physician when that user moves to another location. In this case, the opportunistic contact and the mobility of users are critical factors to the PEC performance. We define two performance metrics: *Response time* and *receiving delay*. The response time denotes a time period from the emergency occurrence to the first physician's arrival at the emergency location, and the receiving delay denotes a time period from the emergency occurrence to the reception of the emergency call by the first physician. The *running delay* of a physician denotes a time period from his reception of the emergency call to his arrival at the emergency location.

The emergency data in the PEC includes the following components.

- Location (LOC): It contains the emergency location information which can be measured by a global positioning system (GPS) of the patient PDA.
- Incident (INC): It contains a general description of the environment where the emergency occurs.
- Time (TIME): It contains the exact time when the emergency occurs.
- Group Signature (GS): It is generated by using a patient's credential. The signed message is a concatenation of three components "LOC||INC||TIME".
- Access Control (AC): It contains two ciphertexts corresponding to two randomly-selected symmetric keys. An attribute-based encryption scheme is used to provide a fine-grained access control to the symmetric keys.
- Information (INF): It contains the ciphertexts of the PC and the HR. Two symmetric keys in "AC" are used to encrypt the PC and the HR, respectively.

B. Preliminaries

In this subsection, we define a satisfying relationship between an attribute set and a linear secret sharing structure (LSSS), which will be used in the fine-grained access control mechanism.

Suppose that a linear secret sharing structure $\mathbb{A} = (M, \rho)$ can be satisfied by an attribute set $\mathcal{S}$ as shown in Fig. 5, where M is a $l \times n$ matrix and ρ is an injective function from $\{1, \cdots, l\}$ to any attribute. Let $\mathcal{I} = \{i|\rho(i) \in \mathcal{S}\}$. Therefore, there exist constants $\{\omega_i \in \mathbb{Z}_q\}$ such that $\sum_{i\in\mathcal{I}} \omega_i M_i = (1, 0, \cdots, 0)$, where M_i is the ith row of matrix M. On the other hand, if $\mathcal{S}$ does not satisfy $\mathbb{A}$, those constants $\{\omega_i\}$ do not exist. From [16], the constants $\{\omega_i\}$ can be found in polynomial time with the size of the matrix M. Moreover, let a vector $\bar{v} = (s, r_2, \cdots, r_n)$, where $s \in \mathbb{Z}_q$ is the secret to be shared, $r_2, \cdots, r_n \in \mathbb{Z}_q$ are random numbers. The inner product $M\bar{v}^T = (\lambda_1, \cdots, \lambda_l)^T$ can be regarded as the linear secret sharing. Given an attribute set $\mathcal{S}$ and its $\mathcal{S}$ and its corresponding rows $\mathcal{I} = \{i|\rho(i) \in \mathcal{S}\}$ in the matrix M, finding $\{\omega_i \in \mathbb{Z}_q\}$ so that $\sum_{i\in\mathcal{I}} \omega_i\lambda_i = s$ is called linear secret reconstruction.

C. PEC Description

The PEC includes four phases: Initialization, registration, emergency call generation, and emergency call verification. Note that a TA will be involved in the initialization and registration phases.

Initialization Phase: Let $\mathbb{G}$ and $\mathbb{G}_T$ be two finite cyclic groups of the same large prime order q. Suppose $\mathbb{G}$ and $\mathbb{G}_T$ are equipped with a pairing, i.e., a non-degenerated and efficiently computable bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ such that i) $\forall g, h \in \mathbb{G}, \forall a, b \in \mathbb{Z}_q, e(g^a, h^b) = e(g, h)^{ab}$; and ii) $\exists g \in \mathbb{G}$, $e(g, g)$ has order q in $\mathbb{G}_T$ [16].

As the first step of the initialization phase, the TA chooses a generator g of $\mathbb{G}$, a secure cryptographic hash function $H : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$, the random numbers $\alpha, a, b \in \mathbb{Z}_q^*$, and computes $T{=}e(g, g)^\alpha$, $A{=}g^a$, $B{=}g^b$. TA then setups a group signature scheme including key generate algorithm `GS.KGen`, signing algorithm `GS.Sign`, verification algorithm `GS.Verify`, and trace algorithm `GS.Trace` [17], [18]. TA also setups a standard symmetric key encryption scheme [19] including encryption algorithm `SE.Enc`, and decryption algorithm `SE.Dec`. Let GPK denote the group public key, and TK the trace key of the group signature scheme. With these settings, the TA keeps the master keys (α, a, b) and the trace key TK secretly and publishes the public parameter $\mathsf{pub} = (q, g, \mathbb{G}, \mathbb{G}_T, e, H, T, A, B, GPK)$.

Registration Phase: If a user is either a paramedic or a physician who is capable of providing the medical services in the emergency situation, the TA authorizes their access capabilities by assigning the secret keys according to their attributes.

(1) The TA first assigns a new identity u_{id} to the user. If the user is a physician with an attribute $\{phy\}$, the TA computes the secret key K_{phy} as

$$\langle K, K_1^{(1)}, K_1^{(2)} \rangle = \langle g^\alpha g^t, r_1, g^{\frac{t}{a+br_1+H(phy)}} \rangle$$

where $t, r_1 \in \mathbb{Z}_q^*$ are the unique random numbers;

if the user is a paramedic with an attribute $\{par\}$, the TA computes the secret key K_{par} as

$$\langle K, K_1^{(1)}, K_1^{(2)} \rangle = \langle g^{\alpha} g^{t}, r_1, g^{\frac{t}{a+br_1+H(par)}} \rangle$$

where $t, r_1 \in \mathbb{Z}_q^*$ are the unique random numbers;

if the user is a certified paramedic with an attribute set $\{cer, par\}$, the TA computes the secret key K_{cpar} as

$$\begin{aligned}&\langle K, K_1^{(1)}, K_1^{(2)}, K_2^{(1)}, K_2^{(2)} \rangle \\ &= \langle g^{\alpha} g^{t}, r_1, g^{\frac{t}{a+br_1+H(par)}}, r_2, g^{\frac{t}{a+br_2+H(cer)}} \rangle\end{aligned}$$

where $t, r_1, r_2 \in \mathbb{Z}_q^*$ are the unique random numbers. The TA then delivers the secret key to the user through a secret channel. In the considered scenario, a paramedic with cer can access HR while a paramedic without cer cannot.

(2) If a user is a patient who needs the medical services for possible emergency situation, the TA uses algorithm `GS.KGen` to issue a group secret key and delivers the key to the patient through a secure channel.

Emergency call generation phase: The emergency call generation is started by a detection of the abnormal physiological condition from body sensors. This condition can be pre-implanted into the patient's PDA with the instructions of the medical professionals. Let patient n_i denote a user who has an emergency situation. The patient n_i's PDA generates an emergency call according to the following steps.

(1) The PDA intelligently collects the general information including the emergency location, the general description of environment, and the exact time of emergency's occurrence. Then, the PDA uses the algorithm `GS.Sign` to generate a group signature on "LOC||INC||TIME." The group signature will be put into the "GS" component.

(2) The PDA chooses two random symmetric keys k_1 and k_2, where k_1 is used for encrypting patient n_i's PC and k_2 is used for encrypting patient n_i's HR. We suppose that the patient n_i sets the access structure of the PC as "phy OR par" and the access structure of the HR as "phy OR (cer AND par)." As mentioned in Section III-B, the access structure "phy OR par" and "phy OR (cer AND par)" can be mapped to LSSSes (M_1, ρ_1) and (M_2, ρ_2) respectively, where

$$M_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \rho_1 : \begin{array}{ccc} 1 & \rightarrow & phy \\ 2 & \rightarrow & par, \end{array}$$

$$M_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix}, \rho_2 : \begin{array}{ccc} 1 & \rightarrow & phy \\ 2 & \rightarrow & par \\ 3 & \rightarrow & cer. \end{array}$$

Then, the PDA encrypts the symmetric keys with the access structures: i) It sets $\vec{v}_1 = (s_1), \vec{v}_2 = (s_2, u_1)$, where s_1, s_2, and u_1 are randomly selected from $\mathbb{Z}_q^*$; ii) it computes $\vec{\lambda}_1 = (\lambda_{1,1}, \lambda_{1,2}) = (\vec{v}_1(M_1)_1, \vec{v}_1(M_1)_2)$ and $\vec{\lambda}_2 = (\lambda_{2,1}, \lambda_{2,2}, \lambda_{2,3}) = (\vec{v}_2(M_2)_1, \vec{v}_2(M_2)_2, \vec{v}_2(M_2)_3)$, where $(M_x)_y$ represent the y-th row of matrix M_x; iii) it computes C_1 and C_2 as follows and puts them into the "AC" component.

$$C_1 = (M_1, \rho_1, k_1 \oplus T^{s_1}, g^{s_1}, [(Ag^{H(\rho_1(i))})^{\lambda_{1,i}}, B^{\lambda_{1,i}}]_{i=1,2}),$$

$$C_2 = (M_2, \rho_2, k_2 \oplus T^{s_2}, g^{s_2}, [(Ag^{H(\rho_2(j))})^{\lambda_{2,j}}, B^{\lambda_{2,j}}]_{j=1,2,3}).$$

(3) The PDA uses k_1 to encrypt the PC and uses k_2 to encrypt the HR using `SE.Enc`. The ciphertexts $C_1 = \texttt{SE.Enc}_{k_1}(\text{PC})$ and $C_2 = \texttt{SE.Enc}_{k_2}(\text{HR})$ will be put into the "INF" component.

(4) Finally, the PDA generates the emergency call EmC

$$\text{EmC} = \text{“LOC} \,\|\, \text{INC} \,\|\, \text{TIME} \,\|\, \text{GS} \,\|\, \text{AC} \,\|\, \text{INF.”}$$

and epidemically disseminates the EmC to the neighboring users and APs.

Emergency call verification phase: User n_j receives the EmC from patient n_i and executes the following steps, where a PDA represents user n_j's PDA:

(1) The PDA verifies the group signature "GS" by using algorithm `GS.Verify`. If the verification passes, user n_j confirms the information "LOC||INC||TIME." As an emergency response, user n_j firstly makes a phone call (e.g., dialing 911) to report the emergency to the hospital/first-aid center. Then, the PDA executes the step (2).

(2) The PDA checks the "TIME" component: If the time period from the time of emergency occurrence to the time that user n_j receives it, is larger than a threshold value $T_{invalid}$, the emergency call is invalid and would be discarded. If the emergency call is still valid, the PDA forwards the EmC to the neighboring users. In addition, if the PDA is able to access the symmetric keys of "AC," it executes the following steps.

- The access structure of the PC is phy OR par. If user n_j is a physician, it could use K_{phy} to decrypt C_1 as follows:

  $$k_1 = (k_1 \oplus T^{s_1}) \oplus \frac{e(K, g^{s_1})}{e((Ag^{H(\rho_1(1))})^{\lambda_{1,1}} B^{K_1^{(1)} \lambda_{1,1}}, K_1^{(2)})}$$

  and PC $= \texttt{SE.Dec}_{k_1}(C_1)$, where $\lambda_{1,1} = s_1$ and $\rho_1(1) = phy$.

- The access structure of the HR is phy OR (cer AND par). If user n_j is a certified paramedic, it could use K_{cpar} to decrypt C_2:

  $$\begin{aligned}k_2 &= (k_2 \oplus T^{s_2}) \\ &\oplus \frac{e(K, g^{s_2}) e((Ag^{H(\rho_2(3))})^{\lambda_{2,3}} B^{K_2^{(1)} \lambda_{2,3}}, K_2^2)}{e((Ag^{H(\rho_2(2))})^{\lambda_{2,2}} B^{K_1^{(1)} \lambda_{2,2}}, K_1^{(2)})}\end{aligned}$$

  and HR $= \texttt{SE.Dec}_{k_2}(C_2)$, where $\lambda_{2,2} = s_1 + u_1$, $\lambda_{2,3} = u_1$, $\rho_2(2) = par$, and $\rho_2(3) = cer$.

If user n_j successfully decrypts the PHI, user n_j capable of providing medical services would go straight to the emergency location.

D. Revocation Mechanism

The revocation mechanism makes the system robust even if registered users launch inside attacks. In this subsection, we extend the PEC to a revocable PEC (rPEC) by using the technique from [20]. In the rPEC, if the TA identifies a user who has revealed patient PHI to unauthorized entities, the TA can revoke the access capability. Specifically, the rPEC has the following changes.

Initialization Phase: The TA appends two random numbers $v, y \in \mathbb{Z}_q^*$ to its master keys, and publishes $V = g^v$ and

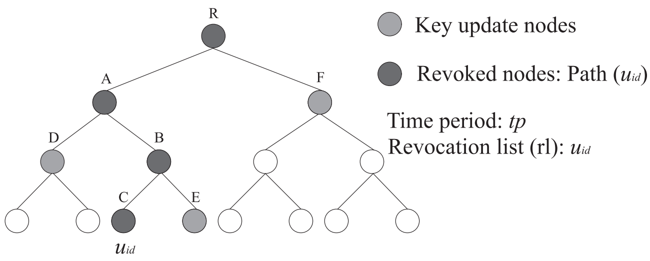

R
A
F
D
B
C
E
u_{id}
Key update nodes
Revoked nodes: Path (u_{id})
Time period: *tp*
Revocation list (rl): u_{id}

Fig. 6. Revocation tree.

a secure cryptographic hash function $\mathcal{H} : \{0,1\}^* \rightarrow \mathbb{G}$. The TA then builds a binary revocation tree $\mathcal{T}$ (an example with height 3 is shown in Fig. 6). When a user registers to the system with a unique identifier u_{id}, the TA maps u_{id} to a vacant leaf node, e.g., node C. Node C is then occupied. Let $Path(u_{id}) = \mathcal{X}_{u_{id}} = \{R, A, B, C\}$ denote the path from node C to the root R. For any $x \in \mathcal{X}_{u_{id}}$, if a_x is undefined, the TA randomly selects $a_x, r_x \in \mathbb{Z}_q^*$ and associates a_x with node x. For different users, a_x is the same but r_x is different.

Registration Phase: If a physician with u_{id}, a additional secret key K_{id}^* is generated as follows:

$$K_{id}^* = (x, d_x, D_x)_{x \in \mathcal{X}_{u_{id}}} = (x, r_x, g^{\frac{a_x \mathcal{H}(u_{id}) + t'}{a + r_x b + v}})_{x \in \mathcal{X}_{u_{id}}}$$

where $t' \in \mathbb{Z}_q^*$ is a unique random number.

Suppose that the physician has a secret key $K_{phy} = \langle K, K_1^{(1)}, K_1^{(2)} \rangle$ of the PEC. The rPEC assigns the physician with a modified secret key $K_{id} = \langle Kg^{t'}, K_1^{(1)}, K_1^{(2)}, K_{id}^* \rangle$.

Update Phase: Let $\mathbb{X}_{tp} = \text{KUNodes}(\mathcal{T}, rl, tp)$ be the minimum coverage of nodes corresponding to non-revoked users, where rl is the revocation list at time period tp. For example, in Fig. 6, key update nodes (KUNodes) are (D, E, F) when u_{id} is revoked. A necessary condition of successful decryption by the user with u_{id} is $\mathcal{X}_{u_{id}} \cap \mathbb{X}_{tp} \neq \varnothing$. The update information can be computed as follows:

For any $x \in \mathbb{X}_{tp}$, the TA randomly selects $r'_x \in \mathbb{Z}_q^*$ and generates the update information for the time period tp as follows.

$$K_u = (x, e_x, E_x)_{x \in \mathbb{X}_{tp}} = \langle (x, r'_x, g^{\frac{a_x \mathcal{H}(tp)}{a + r'_x b + \mathcal{H}(tp)}})_{x \in \mathbb{X}_{tp}} \rangle$$

Emergency Call Generation Phase: The PDA uses (C_1^*, C_2^*) instead of (C_1, C_2) in the "AC" component.

$$\begin{aligned} C_1^* &= (M_1, \rho_1, k_1 \oplus T^{s_1}, g^{s_1}, [(Ag^{H(\rho_1(i))})^{\lambda_{1,i}}, B^{\lambda_{1,i}}]_{i=1,2}, \\ &\quad (AV)^{s_1}, (Ag^{\mathcal{H}(tp)})^{s_1}, B^{s_1}), C_2^* \\ &= (M_2, \rho_2, k_2 \oplus T^{s_2}, g^{s_2}, [(Ag^{H(\rho_2(j))})^{\lambda_{2,j}}, B^{\lambda_{2,j}}]_{j=1,2,3}, \\ &\quad (AV)^{s_2}, (Ag^{\mathcal{H}(tp)})^{s_2}, B^{s_2}) \end{aligned}$$

where $s_1, s_2 \in \mathbb{Z}_q^*$ are the random numbers.

Emergency call verification phase: If user n_j's attributes satisfy the access structure of the PC, he can obtain the value $e(g,g)^{ts_1}$ according to the PEC algorithms. In addition, if user n_j is a non-revoked user, he can find a common $a_x \in \mathcal{X}_{u_{id}} \cap \mathbb{X}_{tp}$ and obtain the values

$$e((AV)^{s_1}(B^{s_1})^{d_x}, D_x) = e(g,g)^{(a_x \mathcal{H}(u_{id}) + t')s_1},$$

$$e((Ag^{\mathcal{H}(tp)})^{s_1}(B^{s_1})^{e_x}, E_x) = e(g,g)^{(a_x \mathcal{H}(tp))s_1}.$$

Then, user n_j uses lagrange interpolation of the above two values to obtain $e(g,g)^{t' s_1}$. By computing

$$e(Kg^{t'}, g^{s_1}) / e(g^t, g^{s_1}) e(g^{t'}, g^{s_1}) = T^{s_1},$$

user n_j can obtain the symmetric key k_1 from $k_1 \oplus T^{s_1}$ and successfully decrypt the PC. Note that other registration and decryption cases are similar with the above process.

IV. SECURITY ANALYSIS

In this section, we analyze the security properties of the PEC/rPEC. Specifically, we study on how the PEC/rPEC can guarantee the availability of patient PHI in an emergency situation while preserving patient privacy. Furthermore, we show that the PEC/rPEC can effectively prevent forgery attacks and inside attacks.

The PEC/rPEC can guarantee the availability of the PHI in the emergency situation. In the PEC/rPEC, a user can choose appropriate access structures for different parts of PHI regarding to the privacy-sensitive levels, like "*phy* OR *par*" for the PC, "*phy* OR (*cer* AND *par*)" for the HR. Using the access structures consisting of the medical attributes effectively solves the access control problem for the emergency situation, since the PHI can be appropriately disclosed by the patient itself for emergency care purposes. In the PEC/rPEC, LSSS technique is adopted to implement a fine-grained access control allowing users to choose Boolean expressions as the access structures. With these expressive access structures, patients can enforce flexible access control of their PHI in the emergency situation. Therefore, the availability of the PHI is guaranteed.

The PEC/rPEC can preserve user identity privacy. The PEC/rPEC ensures that users' identities will not be exposed to any other users. In the emergency call generation phase, patient n_i would not disclose his identity to others. Instead, patient n_i uses a group signature [17] to sign the emergency data on behalf of the whole group. On the other hand, in the emergency call verification phase, user n_j directly forwards the emergency call to his neighboring users and executes a decryption operation on the PHI by itself. Therefore, user n_j would not expose its identity either.

The PEC/rPEC can ensure PHI confidentiality. The PEC/rPEC ensures that the PHI will not be disclosed to any unauthorized users. From the security analysis of work [21], to obtain $e(g,g)^s$ from $(g, X = g^x, Y = g^y, ID, X^s g^{s \cdot ID}, Y^s)$ without knowledge of $(r, g^{\frac{1}{x + ry + ID}})$ is a computational hard problem. In the PEC/rPEC, the users with the secret keys $(r, g^{\frac{t}{a + rb + H(phy)}})$ are able to compute $e(g,g)^{t\lambda}$ which is a secret share of $e(g,g)^{ts}$. When collecting enough secret shares, users can obtain $e(g,g)^{ts}$ and recover the symmetric keys from the "AC" component. However, if the users' attributes cannot satisfy the access structure, they cannot obtain the symmetric keys as well as the PHI from the emergency call. Therefore, the unnecessary disclosure of the PHI is restricted.

The PEC/rPEC can resist collusion attacks. We illustrate an example to demonstrate that the collusion attack conducted by two users cannot succeed. Suppose that two users have attribute sets $\mathcal{S}_1$ and $\mathcal{S}_2$. They cannot decrypt the symmetric key k_1 individually, since neither $\mathcal{S}_1$ nor $\mathcal{S}_2$ satisfies the access structure (M_1, ρ_1). Suppose that $\mathcal{S}_1 \cup \mathcal{S}_2$ satisfies (M_1, ρ_1) and the two users collude together trying to obtain the key k_1. Recall that the user secret key contains $(r_1, g^{\frac{t}{a+br_1+H(phy)}})$. The element t is selected independently for each user. Therefore, two users can obtain a part of shares of $e(g,g)^{t_1 s}$ and a part of shares of $e(g,g)^{t_2 s}$. The independent relation between t_1 and t_2 results in the independent relation of the secret shares. As such, the users cannot re-construct either $e(g,g)^{t_1 s}$ or $e(g,g)^{t_2 s}$, and they cannot obtain k_1 from $(k_1 \oplus e(g,g)^{t_1 s}, k_1 \oplus e(g,g)^{t_2 s})$. In conclusion, the collusion attacks cannot be successful.

The PEC/rPEC can prevent forgery attacks. In the PEC/rPEC, the TA assigns a group secret key to each user. Then, each user is able to generate an emergency call on behalf of the whole group. Without a group secret key, a non-registered user is unable to generate a valid group signature. When users receive an emergency call, they will check the group signature in the "GS" component before forwarding the emergency call. Therefore, the forgery attacks by the non-registered users cannot be successful. Moreover, the PEC can effectively resist forgery attacks by the registered users. If a registered user generates a bogus emergency call with a valid group signature, a trace key kept by the TA can be used to track the user's unique identity via the group signature. Therefore, the forgery attacks can be detected by the TA.

The rPEC can revoke malicious users. The rPEC extends the PEC with a revocation mechanism. The revocation mechanism allows the TA to revoke malicious users' access capabilities in the update phase after they have obtained the secret keys in the initialization phase. Specifically, we build a revocation tree in the update phase, as shown in Fig. 6. For the revoked user, the path of the revoked user (red nodes) has no intersection with the key update nodes (green nodes) in the revocation tree. The revoked users, with information $\{e(g,g)^{(a_x \mathcal{H}(u_{id})+t')s_1}\}_{x \in \mathcal{X}_{u_{id}}}$ and $\{e(g,g)^{a_{x'}}\mathcal{H}(tp)s_1\}_{x' \in \mathbb{X}_{tp}}$, are unable to compute $e(g,g)^{t's_1}$ because there is no overlapping between $\mathcal{X}_{u_{id}}$ and $\mathbb{X}_{tp}$ so that $a_x = a_{x'}$. Therefore, once being revoked in the time period tp, the malicious users cannot access to any PHI during that time period tp.

The rPEC can revoke collusion attacks by non-revoked users and revoked users. We show that the revoked users cannot generate any information helpful to non-revoked users' decryption. In the initialization phase of rPEC, user n_j's secret key contains an element $g^{\alpha} g^{t} g^{t'}$, where t, t' are two unique random numbers. If revoked, the user n_j can obtain $e(g,g)^{ts}$ but cannot obtain $e(g,g)^{t's}$ in the decryption. The element g^{α} is mixed with user n_j's unique and random element $g^{t'}$. Therefore, user n_j cannot provide any help for other users' decryption. The rPEC ensures that the revoked users cannot provide any help for the non-revoked users' decryption.

V. PERFORMANCE EVALUATION

A. Decryption Efficiency

In this subsection, we evaluate the decryption algorithms of both the PEC and the scheme [16] (called WAT) in terms of the computational time cost (CC) and the communication overhead (CO). We do not consider the performance of the encryption algorithms. This is because most operations of the encryption can be pre-computed. Therefore, we focus on the decryption algorithms which may cause the delay to the response time of emergency care. The communication time cost and computational overhead of the two schemes are given in the Table 2, where $\mathbf{T_{exp}}$ and $\mathbf{T_{pair}}$ denote the time cost spent on a modular exponentiation and a bilinear pairing computation, respectively. $\mathcal{I}$ is defined in subsection III-B.

Table 2. Comparison of decryption algorithms.

	WAT [16]	PEC
CC	$(2\lvert\mathcal{I}\rvert+1)\mathbf{T_{pair}} + \lvert\mathcal{I}\rvert\mathbf{T_{exp}}$	$(\lvert\mathcal{I}\rvert+1)\mathbf{T_{pair}} + \lvert\mathcal{I}\rvert\mathbf{T_{exp}}$
CO	$\lvert M\rvert + \lvert\rho\rvert + 2l\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$\lvert M\rvert + \lvert\rho\rvert + 2l\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$

Table 2 shows that the decryption algorithm of the PEC consumes only half of the computational time on pairing in comparison to that of the WAT, while the communication overhead of two schemes are the same.

B. Revocation Efficiency

In this subsection, we evaluate the revocation mechanisms of both the PEC and the scheme [22] (called YRL). The details are given in Table 3, where k is the number of total users who have access capabilities and r is the number of revoked users.

Table 3. Comparison of revocation algorithms.

	YRL[22]	rPEC
Secure channel from PKG to users	Need	No need
The amount of update information	$O(k-r)$	$\leq O(k-r)$
The authentication times of system public key	Many	One
Synchronization	Hard	Easy
Collusion attacks by revoked/Non-revoked users	Yes	No

Specifically, we compare the rPEC and the YRL from the following five aspects:

1) The revocation mechanism of the YRL relies on a permanent secure channel. By using this channel, the private key generator (PKG) sends the update information to all the non-revoked users. Although the ciphertext-policy attribute-based encryption (CPABE) could be applied for removing such secure channel, the attributes and policies of CPABE for non-revoked users would complicate the scheme. In contrast, the rPEC requires a broadcast channel to publish the update information which would be more practical and easy to implement.
2) In the YRL, the amount of update information in each period is $O(k-r)$, while in the rPEC, the amount of information as given below is much less.

$$\begin{cases} O(1), & \text{if } r = 0 \\ O(rlog(\frac{k}{r})) & \text{if } 1 < r \leq k/2 \\ O(k-r) & \text{if } k/2 < r \leq k \end{cases}$$

3) The YRL requires the system public key to be changed in each period, and thus a sender needs to frequently authenticate the updated system public key. But in the

Table 4. Simulation settings.

Parameters	Value
The size of interest area	1000 m × 1000 m
Number of users	$k = \{20, 40, 60, 80, \cdots, 200\}$
User average velocity	$v = 2$ m/sec
Number of physicians	PN $= \{1, 3, 5\}$
Physician accelerated velocity	5 m/sec
PDA transmission range	$tr = \{50, 30\}$ m
Numbers of social spots and APs	$(l = 10, 5)$
AP transmission range	$tr_s = 100$ m

rPEC, the system public key remains the same all the time, and users do one-time authentication in the initialization phase.

4) In YRL, the PKG determines the update period by sending a signal to senders and receivers. This may cause an inconsistence between encryption and decryption operations if a receiver still uses the old secret keys while a sender encrypts the message under the update system public key. However, in the rPEC, each update period is tagged with a time stamp so that the senders and receivers would use the same time stamp to keep synchronous.
5) In the YRL, the revocation mechanism cannot resist the collusion attack since the update information is the same for both the revoked users and the non-revoked users. The non-revoked users can help the revoked users to decrypt the ciphertexts. To prevent this attack, in the rPEC, the update information is published to all the users but it is only useful to non-revoked users.

C. Simulations

In order to evaluate the response time of the proposed scheme, we have conducted a set of custom simulations of the MHSN. In the following subsections, we first detail our simulation settings, and then present the simulation results.

C.1 Simulation settings

We consider a typical mobile healthcare social network, where 20 to 200 users equipped with PDAs are uniformly deployed in an interest area $1,000$ m $\times$ $1,000$ m. The PDAs enable users to communicate with each other at a distance of 50 m or 100 m. 1 to 5 users are considered as the physicians. Before receiving an emergency call, the physicians behave exactly the same as other users. 10 social spots, denoted by a set $\mathcal{S}_u$, are randomly deployed into the interest area and each user has a fixed social spot set $\mathcal{S}_i \subset \mathcal{S}_u$, where $6 \leq |\mathcal{S}_i| \leq 10$. There are 5 access points (AP) deployed at 5 random social spots, and the wireless transmission range of an AP is 100 meters. The simulation settings are detailed in Table 4.

Mobility pattern: Each user randomly chooses a social spot from its social spot set, and arrives there along the shortest path. After arriving at the social spot, the user spends at most 2 minutes there and repeats the above process.

Emergency situation: Suppose that a patient n_i suddenly has an emergency and he loses his mobility at all. The patient n_i's PDA will epidemically disseminate an emergency call to the neighboring users until the first nearby physician/paramedic arrives at the emergency location. When user n_j receives patient n_i's emergency call, user n_j will disseminate the emergency data to his neighboring users. If user n_j is a physician, he will accelerate his velocity to 5 m/sec and go straight to the emergency location. The APs are well connected to each other. If an AP receives patient n_i's emergency call, it will transmit the emergency call to other APs at once. Meanwhile, if an AP receives the emergency call, it disseminates the emergency call to all nearby users in its transmission range, assisting patient n_i in finding a nearby physician as soon as possible.

We perform the simulations with varying numbers of total users $[20, 200]$, varying numbers of physicians $[1, 5]$, and varying PDA transmission ranges $(50\text{m}, 30\text{m})$. For each case, we take 200 samples and evaluate average response time and average receiving delay as defined in Section III-A.

C.2 Simulation results

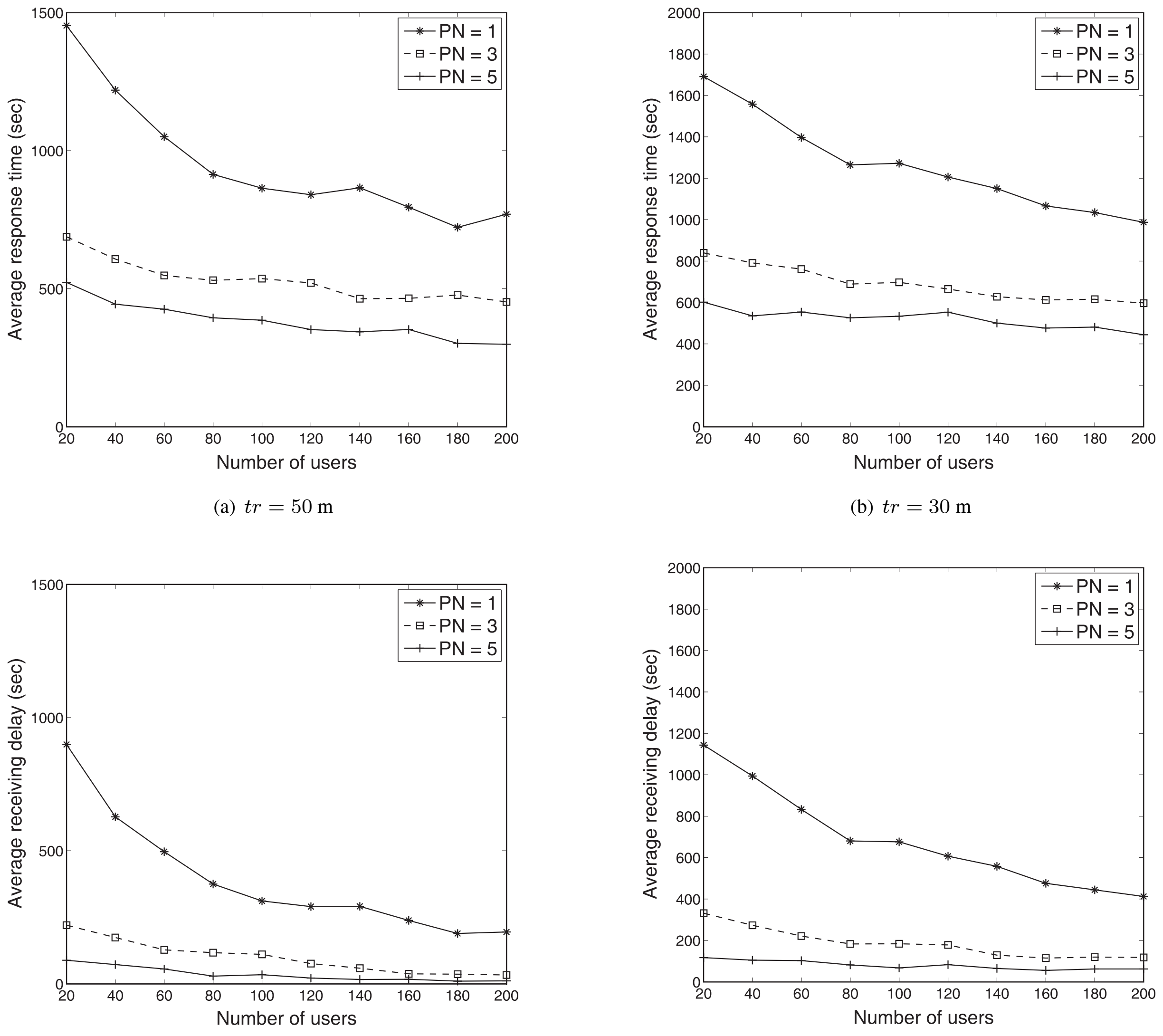
As shown in Fig. 7, if the number of users increase, the response time and the receiving delay would be significantly reduced. This is because the emergency call can be forwarded to a physician more quickly if more users are involved in the cooperative communication.

Figs. 7(a) and 7(b) plot the response timein in terms of number of total users for two cases $tr = 50$ and $tr = 30$. From the Fig. 7(a), in case of PN $= 1$, the response time that the first physician arrives at the emergency location would be 1453.08 seconds at maximum or 522.69 seconds at minimum. From Fig. 7(a), if the number of users is fixed to 200, we can further observe that the response time would vary from 769.75 seconds to 298.97 seconds as the number of physicians increases from 1 to 5. When the number of physicians increases, the probability that a physician is physically close to the emergency location increases. In this case, the receiving delay and running delay both decrease and correspondingly the response time would also decrease. By comparing Figs. 7(a) to 7(b), if the PDA transmission range is reduced from 50 m to 30 m, the response time would increase. The larger transmission range would make more users well connected for more effective dissemination.

Figs. 7(c) and 7(d) plot the receiving delay in terms of number of total users for two cases $tr = 50$ and $tr = 30$. It can be seen that if PN $= 5$, the receiving delay is less than 100 seconds; if PN $= 3$ and the number of users is larger than 100, the receiving delay is less than 200 seconds. However, the corresponding response time are still around 500 seconds. For these cases, a more effective way to reduce the response time is to increase the physician accelerated velocity which is set to 5 m/sec in the simulations. By doing so, the decentralized emergency response system would be very effective. For other cases like PN $= 1$ or the number of total users is very small, the receiving delay would also lead a large increase of the response time. As such, when the receiving delay of user self-organized communications cannot be significantly reduced, the decentralized/centralized emergency response systems should be used together to increase patient safety.

C.3 Computational delay

After presenting the simulation results, we reconsider the computational delay taken by the PEC algorithm. Notably, if



(a) $tr = 50$ m

(b) $tr = 30$ m

(c) $tr = 50$ m

(d) $tr = 30$ m

Fig. 7. Simulation results.

a physician arrives at the emergency location without the decrypted patient PHI, a medical measure using insufficient patient information may endanger patient life in the emergency situation. The time efficiency of the PEC decryption algorithm is thus critical. Generally, the time consumed on processing a cryptographic algorithm is determined by the computational power of the hardware installed in the PDA. Based on the recent works [23], a pairing operation takes $\mathbf{T_{pair}} = 550$ ms on a PDA equipped with a 416 MHz processor [23]. Recall that the decryption algorithm of the PEC takes $|\mathcal{I}|\mathbf{T_{pair}} + \mathbf{1}$ pairings, where $|\mathcal{I}|$ is the number of attributes used for decryption. Therefore, the time used to decrypt the symmetric keys is less than 10 seconds if $|\mathcal{I}| < 10$. On the other hand, from Fig. 7, the average running delay $(= \mathrm{responsetime} - \mathrm{receivingdelay})$ is larger than 100 seconds. This ensures that the physician can obtain the patient's PHI before arriving at the emergency location in most cases. In other words, if adopting the access policies in Section II-B, the time used for decryption would not lead an increasing delay to the response time.

VI. RELATED WORK

There have been a lot of research efforts on the security and privacy issues of the healthcare system [10], [13], [14], [24]–[27].

To design a fine-grained and self access control of the PHI in the healthcare system has attracted a great attention. Currim *et al.* [25] developed an algorithm to evaluate ad-hoc user queries against database policies. They also considered some of the limitations of the fine-grained access control mechanisms, and proposed an efficient approach to answer user queries and prevent linkability of transactions. Dillema *et al.* [26] designed a rendezvous-based access control for medical records in the pre-hospital environment, which uses a simple cryptographic access control method that provides access to medical record if and only if the patient and the health worker meet in the physical world. Similar to the PEC, their system provides local access to the PHI without the involvement of the centralized system. However, in their design, they did not consider how to control the access to the physiological condition monitored by body sensors, and their central-controllable access policy cannot be directly applied to emergency situation. *Principle of self care*, is another desired property of the healthcare system from patient perspective, which has been studied recently [13], [14], [27]: Data collected in a ubiquitous monitoring environment must be processed and stored in a personal healthcare system under the self-control of patient. Inspired by these novel ideas, the PEC enables a fine-grained and self access control of emergency data for a patient in the emergency situation, where the emergency data includes the emergency location computed by a GPS device, the health records pre-stored in the PDA and the physiological condition instantly monitored by the body sensors.

Ciphertext-policy attribute-based encryption scheme allows a sender to disseminate the privacy-sensitive information according to an access structure which can be expressed as a boolean function consisting of (OR, AND) gates between attributes. The decryption of a receiver is successful if and only if the attributes associated with the receiver satisfy the access structure. The first implementation of CPABE is developed by Bethencourt *et al.* [28], and later several other works [29], [30] are appeared to improve the algorithm efficiency or achieve the high security-level. Recently, Waters [16] presented an expressive, efficient and provably secure scheme, called WAT. Compared to the WAT, the PEC has a more efficient decryption algorithm in terms of computational time cost.

Group signature [17], [18], a typical identity anonymous technique, provides anonymity and central traceability at the same time, i.e., a group signature can be verified on behalf of the group by any other users, but it can be traced to a real identity only by the TA. The PEC adopts this technique to prevent the forgery attacks and preserve identity privacy.

The revocation mechanism has been well studied in traditional public key infrastructure. However, in the setting of identity-based encryption (IBE), most revocation mechanisms [31], [32] are not very efficient; they require a large amount of update information. Boldyreva *et al.* [20] proposed an efficient mechanism for IBE by leveraging the size of user private key and the amount of update information. With this mechanism, the PEC allows the TA to effectively revoke the access capabilities of the malicious users with small update information.

VII. CONCLUSIONS

We have proposed a privacy-preserving emergency call scheme, called PEC, to implement a decentralized emergency response system for a rapid response of emergency care in the mobile healthcare social network. We have demonstrated that the PEC not only preserves users' privacy in terms of hiding their identities and avoiding unnecessary disclosure of the PHI, but also resists the forgery and collusion attacks. We have further extended the PEC, i.e., rPEC, to be more efficient and feasible to enable a TA to revoke the access capabilities of malicious users. For our future work, we will develop a prototype decentralized emergency response system to evaluate the effectiveness and workability of the PEC/rPEC, and explore more practical issues related to the decentralized emergency response system.

REFERENCES

[1] List of causes of death by rate. [Online]. Available: http://en.wikipedia.org/wiki/List_of_causes_of_death_by_rate

[2] S. Pavlopoulos, E. Kyriacou, A. Berler, S. Dembeyiotis, and D. Koutsouris, "A novel emergency telemedicine system based on wireless communication technology-ambulance," *IEEE Trans. Inf. Technol. Biomed.*, vol. 2, no. 4, pp. 261–267, 1998.

[3] T. Y. Kim, A. Coenen, and N. Hardiker, "A quality improvement model for healthcare terminologies," *J. Biomed. Informat.*, 2010.

[4] N. Razack, "Time is critical in treating stroke victims." [Online]. Available:http://www2.tbo.com/content/2010/may/05/071105/timeiscritical-in-treating-stroke-victims/life-health/, 2010

[5] Emergency medical services. [Online]. Available: http://en.wikipedia.org/wiki/Emergency_medical_services

[6] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure handshake with symptoms-matching: The essential to the success of mhealthcare social network," in *Proc. BodyNets*, 2010.

[7] D. Meltzer, J. Chung, P. Khalili, E. Marlowa, V. Arora, G. Schumock, and R. Burt, "Exploring the use of social network methods in designing healthcare quality improvement teams," in *Proc. Soc. Sci. Med.*, vol. 71, no. 6, 2010, pp. 1119–1130.

[8] M. Domingo, "Managing healthcare through social networks," in *Proc. IEEE Comput. Mag.*, vol. 43, no. 7, 2010, pp. 20–25.

[9] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," in *Proc. Comput. Netw.*, vol. 54, no. 15, 2010, pp. 2688–2710.

[10] K. Malasri and L. Wang, "Addressing security in medical sensor networks," in *Proc. HealthNet*, 2007, pp. 7–12.

[11] A. Mohan, D. Bauer, D. M. Blough, M. Ahamad, B. Bamba, R. Krishnan, L. Liu, D. Mashima, and B. Palanisamy, "A patient-centric, attribute-based, source-verifiable framework for health record sharing," *Technique Reports*. [Online]. Available: http://www.cercs.gatech.edu/tech-reports/tr2009/git-cercs-09-11.pdf, 2009

[12] A. Mohan and D. M. Blough, "An attribute-based authorization policy framework with dynamic conflict resolution," in *Proc. IDtrust*, 2010, pp. 37–50.

[13] X. Liang, R. Lu, X. Lin, and X. Shen, "Patient self-controllable access policy on phi in ehealthcare systems," in *Proc. Advances in Health Informat. Conf.*, 2010.

[14] K. J. Leonard, "One patient, one record: Report on one-day symposium to promote patient ehealth," in *Proc. Technique Reports*. [Online]. Available:http://patientdestiny.typepad.com/OPOR%20Report%20-%20Ottawa.pdf, 2010

[15] M. Kim, D. Kotz, and S. Kim, "Extracting a mobility model from real user traces," in *Proc. IEEE INFOCOM*, 2006, pp. 1–13.

[16] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Proc. Cryptology ePrint Archive: Report 2008/290*, 2008.

[17] X. Liang, Z. Cao, J. Shao, and H. Lin, "Short group signature without random oracles," in *Proc. ICICS*, 2007, pp. 69–82.

[18] X. Boyen and B. Waters, "Full-domain subgroup hiding and constant-size group signatures," in *Proc. PKC*, 2007, pp. 1-15.

[19] J. Daemen and V. Rijmen, *The Design of Rijndael: AES–The Advanced Encryption Standard*. Springer, 2002.

[20] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proc. ACM CCS*, 2008, pp. 417–426.

[21] D. Boneh and X. Boyen, "Efficient selective-id secure identity-based encryption without random oracles," in *Proc. EUROCRYPT*, 2004, pp. 223–238.

[22] S. Yu, K. Ren, and W. Lou, "Fdac: Toward fine-grained distributed data access control in wireless sensor networks," in *Proc. IEEE INFOCOM*, 2009, pp. 963–971.

[23] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 51–58, 2010.

[24] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: A strong privacy-preserving scheme against global eavesdropping for ehealth systems," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 4, pp. 365–378, 2009.

[25] F. Currim, E. Jung, X. Xiao, and I. Jo, "Privacy policy enforcement for health information data access," in *Proc. WiMD*, 2009, pp. 39–44.

[26] F. W. Dillema and S. Lupetti, "Rendezvous-based access control for medical records in the pre-hospital environment," in *Proc. HealthNet*, 2007, pp. 1–6.

[27] J. Kim, A. Beresford, and F. Stajano, "Towards a security policy for ubiquitous healthcare systems (position paper)," in *Proc. ICUCT*, 2006, pp. 263–272.

[28] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Security and Privacy*, 2007, pp. 321–334.

[29] L. Cheung and C. Newport, "Provably secure ciphertext policy abe," in *Proc. ACM Conf. Comput. Commun. Security*, 2007, pp. 456–465.

[30] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in *Proc. ICALP (2)*, 2008, pp. 579–591.

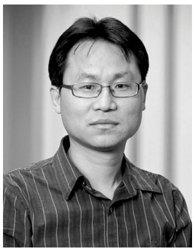
[31] D. Boneh, X. Ding, G. Tsudik, and M. Wong, "A method for fast revocation of public key certificates and security capabilities," in *Proc. USENIX Security Symp.*, 2001, pp. 22–22.

[32] B. Libert and J.-J. Quisquater, "Efficient revocation and threshold pairing based cryptosystems," in *Proc. ACM Symp. Principles of Distributed Comput.*, 2003, pp. 163–171.

Xiaohui Liang is currently working toward a Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is currently a Research Assistant with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include network security and privacy, applied cryptography, and e-healthcare system.

Rongxing Lu is currently working toward a Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is currently a Research Assistant with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and trusted computing.

Le Chen is currently working as a Visiting Scholar with the Broadband Communications Research (BBCR) Group, Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is also working toward a Ph.D. degree with the Department of Computer Science and Engineering, Shanghai Jiao Tong University. His research interests include wireless network security, applied cryptography, and key agreement.



Xiaodong Lin received the Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1998 and the Ph.D. degree (with Outstanding Achievement in Graduate Studies Award) in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2008. He is currently an assistant Professor of Information Security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON, Canada. His research interests include wireless network security, applied cryptography, computer forensics, software security, and wireless networking and mobile computing. He was the recipient of a Natural Sciences and Engineering Research Council of Canada (NSERC) Canada Graduate Scholarships (CGS) Doctoral and the Best Paper Awards of the 18th International Conference on Computer Communications and Networks (ICCCN 2009), the 5th International Conference on Body Area Networks (BodyNets 2010), and IEEE International Conference on Communications (ICC 2007).

Xuemin (Sherman) Shen received a B.Sc.(1982) degree from Dalian Maritime University, China, and M.Sc. (1987), and Ph.D. degrees (1990) from Rutgers University, New Jersey, all in electrical engineering. He is a Professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo. His research focuses on mobility and resource management, UWB wireless networks, wireless network security, and vehicular ad hoc and sensor networks. He served as an Area Editor for IEEE Transactions on Wireless Communications and Editor-in- Chief for Peer-to- Peer Networks and Applications. He is a Fellow of Engineering Institute of Canada, a registered Professional Engineer of Ontario, Canada, and a Distinguished Lecturer of the IEEE Communications Society.