SPOC: A Secure and Privacy-preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency

Rongxing Lu, *Member, IEEE,* Xiaodong Lin, *Member, IEEE,* and Xuemin (Sherman) Shen, *Fellow, IEEE*

Abstract—With the pervasiveness of smart phones and the advance of wireless body sensor networks (BSNs), mobile Healthcare (m-Healthcare), which extends the operation of Healthcare provider into a pervasive environment for better health monitoring, has attracted considerable interest recently. However, the flourish of m-Healthcare still faces many challenges including information security and privacy preservation. In this paper, we propose a secure and privacy-preserving opportunistic computing framework, called SPOC, for m-Healthcare emergency. With SPOC, smart phone resources including computing power and energy can be opportunistically gathered to process the computing-intensive personal health information (PHI) during m-Healthcare emergency with minimal privacy disclosure. In specific, to leverage the PHI privacy disclosure and the high reliability of PHI process and transmission in m-Healthcare emergency, we introduce an efficient user-centric privacy access control in SPOC framework, which is based on an attribute-based access control and a new privacy-preserving scalar product computation (PPSPC) technique, and allows a medical user to decide who can participate in the opportunistic computing to assist in processing his overwhelming PHI data. Detailed security analysis shows that the proposed SPOC framework can efficiently achieve user-centric privacy access control in m-Healthcare emergency. In addition, performance evaluations via extensive simulations demonstrate the SPOC's effectiveness in term of providing high reliable PHI process and transmission while minimizing the privacy disclosure during m-Healthcare emergency.

Index Terms—Mobile-Healthcare emergency; opportunistic computing; user-centric privacy access control; PPSPC

1 Introduction

In our aging society, mobile Healthcare (m-Healthcare) system has been envisioned as an important application of pervasive computing to improve health care quality and save lives, where miniaturized wearable and implantable body sensor nodes and smartphones are utilized to provide remote healthcare monitoring to people who have chronic medical conditions such as diabetes and heart disease [1], [2], [3], [4], [5]. Specifically, in an m-Healthcare system, medical users are no longer needed to be monitored within home or hospital environments. Instead, after being equipped with smartphone and wireless body sensor network (BSN) formed by body sensor nodes, medical users can walk outside and receive the high-quality healthcare monitoring from medical professionals anytime and anywhere. For example, as shown in Fig. 1, each mobile medical user's personal health information (PHI) such as heart beat, blood sugar level, blood pressure and temperature and others, can be first collected by BSN, and then aggregated by smartphone via bluetooth. Finally, they are further transmitted to the remote healthcare center via 3G networks. Based on these collected PHI data, medical professionals at healthcare center can continuously monitor medical users' health conditions and as well quickly react to users' life-threatening situations and save their lives by dispatching ambulance and medical personnel to an emergency location in a timely fashion.

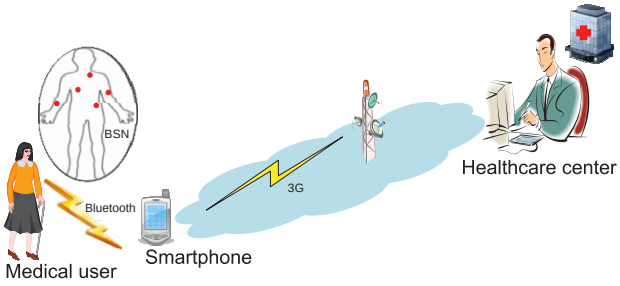


Fig. 1. Pervasive health monitoring in m-Healthcare system

Although m-Healthcare system can benefit medical users by providing high-quality pervasive healthcare monitoring, the flourish of m-Healthcare system still hinges upon how we fully understand and manage the challenges facing in m-Healthcare system, especially during a medical emergency. To clearly illustrate the challenges in m-Healthcare emergency, we consider the following scenario. In general, a medical user's PHI should be reported to the healthcare center every 5 minutes for normal remote monitoring [6]. However, when he has an emergency medical condition, for example, heart attack, his BSN becomes busy reading a variety of medical measures, such as heart rate, blood pressure, and as a result, a large amount of PHI data will be generated in a very short period of time, and they further should be reported every 10 seconds

- *R. Lu and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1 E-mail: {rxlu, xshen}@bbcr.uwaterloo.ca.*
- *X. Lin is with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, Ontario, Canada E-mail: xiaodong.lin@uoit.ca.*

for high-intensive monitoring before ambulance and medical personnel's arrival. However, since smartphone is not only used for healthcare monitoring, but also for other applications, i.e., phoning with friends, the smartphone's energy could be insufficient when an emergency takes place. Although this kind of unexpected event may happen with very low probability, i.e., 0.005, for a medical emergency, when we take into $10,000$ emergency cases into consideration, the average event number will reach 50, which is not negligible and explicitly indicates the reliability of m-Healthcare system is still challenging in emergency.

Recently, opportunistic computing, as a new pervasive computing paradigm, has received much attention [7], [8], [9], [10]. Essentially, opportunistic computing is characterized by exploiting all available computing resources in an opportunistic environment to provide a platform for the distributed execution of a computing-intensive task [10]. For example, once the execution of a task exceeds the energy and computing power available on a single node, other opportunistically contacted nodes can contribute to the execution of the original task by running a subset of task, so that the original task can be reliably performed [7]. Obviously, opportunistic computing paradigm can be applied in m-Healthcare emergency to resolve the challenging reliability issue in PHI process. However, PHI are personal information and very sensitive to medical users, once the raw PHI data are processed in opportunistic computing, the privacy of PHI would be disclosed. Therefore, how to balance the high reliability of PHI process while minimizing the PHI privacy disclosure during the opportunistic computing becomes a challenging issue in m-Healthcare emergency.

In this paper, we propose a new secure and privacy-preserving opportunistic computing framework, called SPOC, to address this challenge. With the proposed SPOC framework, each medical user in emergency can achieve the user-centric privacy access control to allow only those qualified helpers to participate in the opportunistic computing to balance the high-reliability of PHI process and minimizing PHI privacy disclosure in m-Healthcare emergency. Specifically, the main contributions of this paper are threefold.

- First, we propose SPOC, a secure and privacy-preserving opportunistic computing framework for m-Healthcare emergency. With SPOC, the resources available on other opportunistically contacted medical users' smartphones can be gathered together to deal with the computing-intensive PHI process in emergency situation. Since the PHI will be disclosed during the process in opportunistic computing, to minimize the PHI privacy disclosure, SPOC introduces a user-centric two-phase privacy access control to only allow those medical users who have similar symptoms to participate in opportunistic computing.
- Second, to achieve user-centric privacy access control in opportunistic computing, we present an efficient attribute-based access control and a novel non-homomorphic encryption based privacy-preserving scalar product computation (PPSPC) protocol, where the attributed-based access control can help a medical user in emergency to identify other medical users, and PPSPC protocol can further control only those medical users who have similar symptoms to participate in the opportunistic computing while without directly revealing users' symptoms. Note that, although PPSPC protocols have been well studied in privacy-preserving data mining [11], [12], [13], yet most of them are relying on time-consuming homomorphic encryption technique [14], [15]. To the best of our knowledge, our novel non-homomorphic encryption based PPSPC protocol is the most efficient one in terms of computational and communication overheads.
- Third, to validate the effectiveness of the proposed SPOC framework in m-Healthcare emergency, we also develop a custom simulator built in Java. Extensive simulation results show that the proposed SPOC framework can help medical users to balance the high-reliability of PHI process and minimizing the PHI privacy disclosure in m-Healthcare emergency.

The remainder of this paper is organized as follows. In Section 2, we formalize the system model and security model, and identify our design goal. Then, we present the SPOC framework in Section 3, followed by the security analysis and performance evaluation in Section 4 and Section 5, respectively. We also review some related works in Section 6. Finally, we draw our conclusions in Section 7.

2 Models and Design Goal

In this section, we formalize the system model and security model, and identify our design goal as well.

2.1 System Model

In our system model, we consider a trusted authority (TA) and a group of l medical users $\mathbb{U} = \{U_1, U_2, \cdots, U_l\}$, as shown in Fig. 2. TA is a trustable and powerful entity located at healthcare center, which is mainly responsible for the management of the whole m-Healthcare system, e.g., initializing the system, equipping proper body sensor nodes and key materials to medical users. Each medical user $U_i \in \mathbb{U}$ is equipped with personal BSN and smartphone, which can periodically collect PHI and report them to the healthcare center for achieving better health care quality. Unlike in-bed patients at home or hospital [16], [17], [18], medical users $\mathbb{U}$ in our model are considered as mobile ones, i.e., walking outside [19].

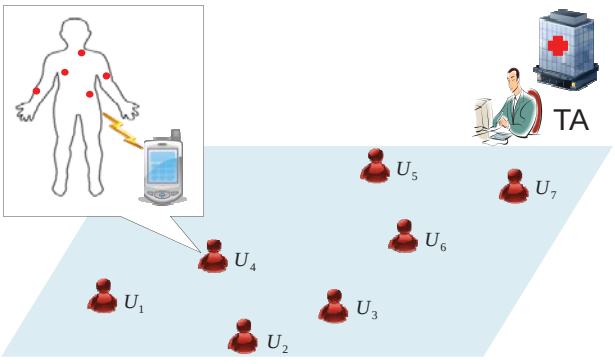


Fig. 2. System model under consideration

BSN and smartphone are two key components for the success of m-Healthcare system. In order to guarantee the high reliability of BSN and smartphone, the batteries of BSN and smartphone should be charged up everyday so that the battery energy can support daily remote monitoring task in m-Healthcare system [1], [20]. In general, since the BSN is dedicated for remote monitoring, after being charged everyday, BSN can deal with not only the normal situations but also the emergency cases in m-Healthcare. However, since the smartphone could be used for other purposes, e.g., phoning friends, surfing webpages, when an emergency suddenly takes place, the residual power of smartphone may be insufficient for high-intensive PHI process and transmission. To deal with this embarrassing situation, opportunistic computing provides a promising solution in m-Healthcare system, i.e., when other medical users find out one medical user $U_i \in \mathbb{U}$ is in emergency, they will contribute their smartphones' resources to help U_i with processing and transmitting PHI.

2.2 Security Model

Opportunistic computing can enhance the reliability for high-intensive PHI process and transmission in m-Healthcare emergency. However, since PHI is very sensitive, a medical user, even in emergency, will not expect to disclose his PHI to all passing-by medical users. Instead, he may only disclose his PHI to those medical users who have some similar symptoms with him. In this case, the emergency situation can be handled by opportunistic computing with minimal privacy disclosure. Specifically, in our security model, we essentially define two-phase privacy access control in opportunistic computing, which are required for achieving high-reliable PHI process and transmission in m-Healthcare emergency, as shown in Fig. 3.

Phase-I access control: Phase-I access control indicates that although a passing-by person has a smartphone with enough power, as a non-medical user, he is not welcomed to participate in opportunistic computing[1]. Since the opportunistic computing requires smartphones that are installed with the same medical softwares to cooperatively process the PHI, if a passing-by person is not a medical user, the lack of necessary softwares does not make him as an ideal helper. Therefore, the phase-I privacy access control is prerequisite.

Phase-II access control: Phase-II access control only allows those medical users who have some similar symptoms to participate in the opportunistic computing. The reason is that those medical users, due to with the similar symptoms, are kind of skilled to process the same type PHI. Note that, the threshold th is a user self-control parameter. When the emergency takes place at a location with high traffic, the threshold th will be set high to minimize the privacy disclosure. However, if the location has low traffic, the threshold th should be low so that the high-reliable PHI process and transmission can be first guaranteed.

1. Note that, a passing-by person can still assist in processing some physical cares before the ambulance arrives.

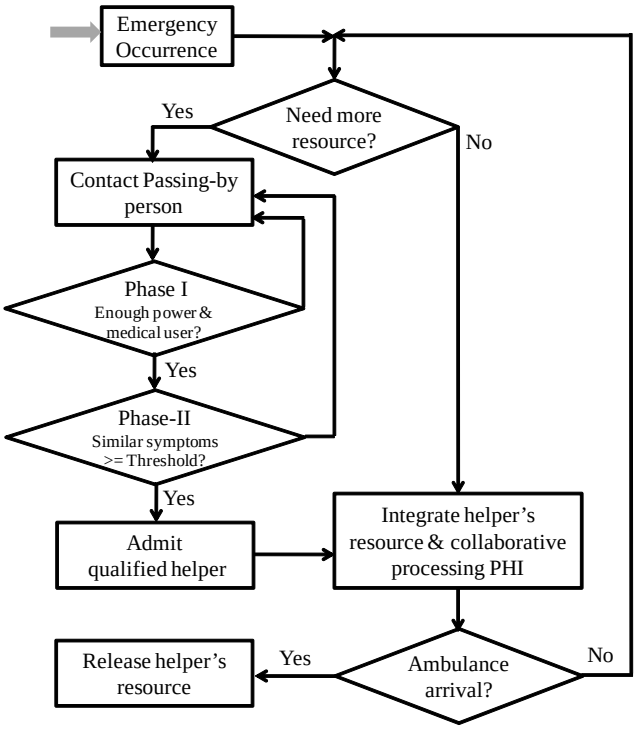


Fig. 3. Opportunistic computing with two-phase privacy access control for m-Healthcare emergency

2.3 Design Goal

Our design goal is to develop a secure and privacy-preserving opportunistic computing framework to provide high reliability of PHI process and transmission while minimizing PHI privacy disclosure in m-Healthcare emergency. Specifically, we i) apply opportunistic computing in m-Healthcare emergency to achieve high-reliability of PHI process and transmission; and ii) develop user-centric privacy access control to minimize the PHI privacy disclosure.

3 Proposed SPOC Framework

In this section, we propose our SPOC framework, which consists of three parts: system initialization, user-centric privacy access control for m-Healthcare emergency, and analysis of opportunistic computing in m-Healthcare emergency. Before describing them, we first review the bilinear pairing technique [21], [22], [23], [24], which serves as the basis of the proposed SPOC framework.

3.1 Bilinear Pairings

Let $\mathbb{G}$, $\mathbb{G}_T$ be two multiplicative cyclic groups with the same 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 $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab} \in \mathbb{G}_T$ for all $a, b \in \mathbb{Z}_q^*$ and any $g_1, g_2 \in \mathbb{G}$. In group $\mathbb{G}$, the Computational Diffie-Hellman (CDH) problem is hard, i.e., given (g, g^a, g^b) for $g \in \mathbb{G}$ and unknown $a, b \in \mathbb{Z}_q^*$, it is intractable to compute g^{ab} in a polynomial time. However, the Decisional Diffie-Hellman (DDH) problem is easy, i.e., given (g, g^a, g^b, g^c)

for $g \in \mathbb{G}$ and unknown $a, b, c \in \mathbb{Z}_q^*$, it is easy to judge whether $c = ab \bmod q$ by checking $e(g^a, g^b) \stackrel{?}{=} e(g^c, g)$. We refer to [21] for a more comprehensive description of pairing technique, and complexity assumptions.

Definition 1: A bilinear parameter generator $\mathcal{G}en$ is a probabilistic algorithm that takes a security parameter κ as input, and outputs a 5-tuple $(q, g, \mathbb{G}, \mathbb{G}_T, e)$, where q is a κ-bit prime number, $\mathbb{G}, \mathbb{G}_T$ are two groups with order q, $g \in \mathbb{G}$ is a generator, and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a non-degenerated and efficiently computable bilinear map.

3.2 Description of SPOC

3.2.1 System Initialization

For a single-authority m-Healthcare system under consideration, we assume a trusted authority (TA) located at the healthcare center will bootstrap the whole system. Specifically, given the security parameter κ, TA first generates the bilinear parameters $(q, g, \mathbb{G}, \mathbb{G}_T, e)$ by running $\mathcal{G}en(\kappa)$, and chooses a secure symmetric encryption algorithm $\mathcal{E}nc()$, i.e., AES, and two secure cryptographic hash functions H and H', where $H, H' : \{0,1\}^* \to \mathbb{Z}_q^*$. In addition, TA chooses two random numbers $(a, x) \in \mathbb{Z}_q^*$ as the master key, two random elements (h_1, h_2) in $\mathbb{G}$, and computes $b = H(a)$, $A = g^a$, and $e(g, g)^x$. Finally, TA keeps the master (a, b, x) secretly, and publishes the system parameter $params = (q, g, \mathbb{G}, \mathbb{G}_T, e, H, H', h_1, h_2, A, e(g, g)^x, \mathcal{E}nc())$.

Assume there are total n symptom characters considered in m-Healthcare system, and each medical user's symptoms can be represented through his personal health profile, a binary vector $\vec{\mathbf{a}} = (a_1, a_2, \cdots, a_n)$ in the n-dimensional symptom character space, where $a_i \in \vec{\mathbf{a}}$ indicates a symptom character, i.e., $a_i = 1$ if the medical user has the corresponding symptom character, and $a_i = 0$ otherwise. Therefore, for each medical user $U_i \in \mathbb{U}$, when he registers himself in the healthcare center, the medical professionals at healthcare center first make medical examination for U_i, and generate U_i's personal health profile $\vec{\mathbf{a}} = (a_1, a_2, \cdots, a_n)$. Afterwards, the following steps will be performed by TA:

- Based on U_i's personal health profile $\vec{\mathbf{a}}$, TA first chooses the proper body sensor nodes to establish U_i's personal BSN, and installs the necessary medical softwares in U_i's smartphone.
- Then, TA chooses two random numbers $(t_{i1}, t_{i2}) \in \mathbb{Z}_q^*$, and computes the access control key $ak_i = (g^{x+at_{i1}}, g^{t_{i1}}, g^{t_{i2}}, h_1^{t_{i1}} h_2^{t_{i2}})$ for U_i.
- Finally, TA uses the master key b to compute the secret key $sk_i = H(U_i||b)$ for U_i.

After being equipped with the personal BSN and key materials (ak_i, sk_i), U_i can securely report his PHI to healthcare center for achieving better healthcare monitoring by the following procedure.

- U_i first chooses the current date *CDate*, computes the session key $k_i = H(sk_i||\textit{CDate})$ for one day, and distributes the session key k_i to his personal BSN and smartphone.
- Every five minutes, BSN collects the raw PHI data rPHI and reports the encrypted value $\mathcal{E}nc(k_i, \text{rPHI}||\textit{CDate})$ to the smartphone with bluetooth technology.
- Upon receiving $\mathcal{E}nc(k_i, \text{rPHI}||\textit{CDate})$, the smartphone uses k_i to recover rPHI from $\mathcal{E}nc(k_i, \text{rPHI}||\textit{CDate})$. After processing rPHI, the smartphone uses the 3G technology to report the processed PHI to healthcare center in the form of $U_i||\textit{CDate}||\mathcal{E}nc(k_i, \text{PHI}||\textit{CDate})$.
- When the TA receives $U_i||\textit{CDate}||\mathcal{E}nc(k_i, \text{PHI}||\textit{CDate})$ at the healthcare center, he first uses the master key b to compute U_i's secret key $sk_i = H(U_i||b)$, and uses sk_i to compute the current session key $k_i = H(sk_i||\textit{CDate})$. After that, TA uses k_i to recover PHI$||$*CDate* from $\mathcal{E}nc(k_i, \text{PHI}||\textit{CDate})$. If the recovered *CDate* is corrected, TA sends PHI to the medical professionals for monitoring.

3.2.2 User-Centric Privacy Access Control for m-Healthcare Emergency

When an emergency takes place in m-Healthcare, e.g., user U_0 suddenly falls down outside, the healthcare center will monitor the emergency, and immediately dispatch an ambulance and medical personnel to the emergency location. Generally, the ambulance will arrive at the scene around 20 minutes [25]. During the 20 minutes, the medical personnel needs high-intensive PHI to realtime monitor U_0. However, the power of U_0's smartphone may be not sufficient to support the high-intensive PHI process and transmission. In this case, the opportunistic computing, as shown in Fig. 3, is launched, and the following user-centric privacy access control is performed to minimize the PHI privacy disclosure in opportunistic computing.

• *Phase-I Access Control:* The goal of phase-I access control is to identify other medical users in emergency. To achieve the phase-I access control, U_0's smartphone first chooses a random number $s \in \mathbb{Z}_q^*$, computes $e(g, g)^{xs}$ and $C = (C_1, C_2, C_3)$ as

$$C_1 = g^s, C_2 = A^s \cdot h_1^{-s}, C_3 = h_2^{-s} \tag{1}$$

When user U_j passes by the emergency location, U_0 sends $C = (C_1, C_2, C_3)$ to U_j. After receiving $C = (C_1, C_2, C_3)$, U_j will perform the following steps:

- Use his access control key $ak_j = (g^{x+at_{j1}}, g^{t_{j1}}, g^{t_{j2}}, h_1^{t_{j1}} h_2^{t_{j2}})$ to compute

$$\begin{aligned} & \frac{e(C_1, g^{x+at_{j1}})}{e(g^{t_{j1}}, C_2) \cdot e(g^{t_{j2}}, C_3) \cdot e(h_1^{t_{j1}} h_2^{t_{j2}}, C_1)} \\ = & \frac{e(g^s, g^x g^{at_{j1}})}{e(g^{t_{j1}}, g^{as} \cdot h_1^{-s}) \cdot e(g^{t_{j2}}, h_2^{-s}) \cdot e(h_1^{t_{j1}} h_2^{t_{j2}}, g^s)} \\ = & \frac{e(g^s, g^x) e(g^s, g^{at_{j1}})}{e(g^{t_{j1}}, g^{as}) e(g^{t_{j1}}, h_1^{-s}) \cdot e(g^{t_{j2}}, h_2^{-s}) \cdot e(h_1^{t_{j1}} h_2^{t_{j2}}, g^s)} \\ = & \frac{e(g^s, g^x)}{e(g^s, h_1^{t_{j1}} h_2^{t_{j2}})^{-1} \cdot e(h_1^{t_{j1}} h_2^{t_{j2}}, g^s)} = e(g, g)^{xs} \end{aligned} \tag{2}$$

- Compute $\textit{Auth} = H'(e(g, g)^{xs}||\textit{timestamp})$, where *timestamp* is the current timestamp, and send back $\textit{Auth}||\textit{timestamp}$ to U_0.

When user U_0 receives $\textit{Auth}||\textit{timestamp}$ at time $\textit{timestamp}'$, he first checks the validity of the time interval between

timestamp′ and *timestamp* in order to resist the replaying attack. If $|\textit{timestamp}' - \textit{timestamp}| \leq \Delta T$, where ΔT denotes the expected valid time interval for transmission delay, U_0 accepts and processes *Auth*$||$*timestamp*, and rejects otherwise. Once *Auth*$||$*timestamp* is accepted, U_0 uses the stored $e(g,g)^{xs}$ to compute $\textit{Auth}' = H'(e(g,g)^{xs}||\textit{timestamp})$, and checks whether $\textit{Auth}' \stackrel{?}{=} \textit{Auth}$. If it does hold, U_j is authenticated as a medical user, and passes the phase-I access control.

Correctness. The correctness of the phase-I access control is obvious. If U_j is not a medical user, he cannot generate $e(g,g)^{xs}$ to produce a valid *Auth* to pass U_0's authentication. In addition, since U_0 can efficiently use the same $C = (C_1, C_2, C_3)$ and the timestamp technique to authenticate other medical users, the phase-I access control is also efficient.

Algorithm 1 Privacy-preserving Scalar Product Computation

1: **procedure** PPSPC PROTOCOL
2: **Input:** U_0's binary vector $\vec{\mathbf{a}} = (a_1, a_2, \cdots, a_n)$ and U_j's binary vector $\vec{\mathbf{b}} = (b_1, b_2, \cdots, b_n)$, where $n \leq 2^6$
3: **Output:** The scalar product $\vec{\mathbf{a}} \cdot \vec{\mathbf{b}} = \sum_{i=0}^{n} a_i \cdot b_i$

4: **Step-1:** U_0 first does the following operations:
5: choose two large primes α, β, where α is of the length $|\alpha| = 256$ bits and $\beta > (n+1) \cdot \alpha^2$, e.g., the length $|\beta| > 518$ bits if $n = 2^6$
6: set $K = 0$ and choose n positive random numbers $(c_1, c_2, c_3, \cdots, c_n)$ such that $\sum_{i=1}^{n} c_i < \alpha - n$
7: **for** each element $a_i \in \vec{\mathbf{a}}$ **do**
8: choose a random number r_i, compute $r_i \cdot \beta$ such that $|r_i \cdot \beta| \approx 1024$ bits, and calculate $k_i = r_i \cdot \beta - c_i$
9: **if** $a_i = 1$ **then**
10: $C_i = \alpha + c_i + r_i \cdot \beta, \quad K = K + k_i$
11: **else if** $a_i = 0$ **then**
12: $C_i = c_i + r_i \cdot \beta, \quad K = K + k_i$
13: **end if**
14: **end for**
15: keep (β, K) secret, and send $(\alpha, C_1, C_2, C_3, \cdots, C_n)$ to U_i
---
16: **Step-2:** U_j then executes the following operations:
17: **for** each element $b_i \in \vec{\mathbf{b}}$ **do**
18: **if** $b_i = 1$ **then**
19: $D_i = \alpha \cdot C_i = \begin{cases} \alpha^2 + c_i \cdot \alpha + r_i \cdot \alpha \cdot \beta, & \text{if } a_i = 1; \\ c_i \cdot \alpha + r_i \cdot \alpha \cdot \beta, & \text{if } a_i = 0. \end{cases}$
20: **else if** $b_i = 0$ **then**
21: $D_i = C_i = \begin{cases} \alpha + c_i + r_i \cdot \beta, & \text{if } a_i = 1; \\ c_i + r_i \cdot \beta, & \text{if } a_i = 0. \end{cases}$
22: **end if**
23: **end for**
24: compute $D = \sum_{i=1}^{n} D_i$ and return D back to U_0

25: **Step-3:** U_0 continues to do the following operations:
26: compute $E = D + K \bmod \beta$
27: **return** $\frac{E - (E \bmod \alpha^2)}{\alpha^2}$ as the scalar product $\vec{\mathbf{a}} \cdot \vec{\mathbf{b}} = \sum_{i=0}^{n} a_i \cdot b_i$
28: **end procedure**

• *Phase-II Access Control:* Once U_j passes the phase-I access control, U_0 and U_j continue to perform the phase-II access control to check whether they have some similar symptoms. Suppose the personal health profiles of medical users U_0, U_j are $\vec{\mathbf{a}} = (a_1, a_2, \cdots, a_n)$ and $\vec{\mathbf{b}} = (b_1, b_2, \cdots, b_n)$, respectively. U_0 first defines an expected threshold th for the number of common symptom characters. Then, in order to compute $\vec{\mathbf{a}} \cdot \vec{\mathbf{b}}$ in a privacy-preserving way, U_0 and U_j invoke our newly designed PPSPC protocol in Algorithm 1. Since the PPSPC protocol ensures neither U_0 nor U_j will disclose their personal healthcare profiles to each other during the computation of $\vec{\mathbf{a}} \cdot \vec{\mathbf{b}}$, it can efficiently achieve privacy-preserving access control. For example, if the returned value $\vec{\mathbf{a}} \cdot \vec{\mathbf{b}} \geq th$, U_j passes the phase-II access control and becomes a qualified helper. Then, U_0 assigns the current session key $k_0 = H(sk_0||\textit{CDate})$ to U_j. With the session key k_0, U_j can decrypt and process the raw PHI sent from U_0's personal BSN, and also transmit the processed PHI to healthcare center to reduce the burden of U_0's smartphone. However, if the returned value $\vec{\mathbf{a}} \cdot \vec{\mathbf{b}} < th$, U_j is not a qualified helper to participate in opportunistic computing. Note that the threshold th is not fixed, if the residual power of U_0's smartphone can last a little long time, th can be set relatively high to minimize the PHI privacy disclosure. However, if the residual power is little, th can be set low so as to firstly guarantee the reliability of high-intensive PHI process and transmission.

Correctness of PPSPC Protocol. The correctness of our proposed PPSPC protocol can be clearly illustrated by the following typical example. Assume two binary vectors are $\vec{\mathbf{a}} = (a_1, a_2, a_3, a_4, a_5) = (1, 1, 0, 0, 1)$ and $\vec{\mathbf{b}} = (b_1, b_2, b_3, b_4, b_5) = (1, 0, 1, 0, 1)$. After Step-1 is performed, we have $C_1 = \alpha + c_1 + r_1 \cdot \beta$, $C_2 = \alpha + c_2 + r_2 \cdot \beta$, $C_3 = c_3 + r_3 \cdot \beta$, $C_4 = c_4 + r_4 \cdot \beta$, and $C_5 = \alpha + c_5 + r_5 \cdot \beta$.

After Step-2 is executed, we have $D_1 = \alpha^2 + c_1 \cdot \alpha + r_1 \cdot \alpha \cdot \beta$, $D_2 = \alpha + c_2 + r_2 \cdot \beta$, $D_3 = c_3 \cdot \alpha + r_3 \cdot \alpha \cdot \beta$, $D_4 = c_4 + r_4 \cdot \beta$, $D_5 = \alpha^2 + c_5 \cdot \alpha + r_5 \cdot \alpha \cdot \beta$, and $D = \sum_{i=1}^{5} D_i$.

Based on the returned D and the secret $K = \sum_{i=1}^{5} k_i$, the value of E can be calculated in Step-3 as

$$\begin{aligned} & E = D + K = \textstyle\sum_{i=1}^{5}(D_i + k_i) \\ = \; & [\alpha^2 + c_1 \cdot (\alpha - 1) + r_1 \cdot \alpha \cdot \beta + c_1 + k_1] + (\alpha + \\ & r_2 \cdot \beta + c_2 + k_2) + [c_3 \cdot (\alpha - 1) + r_3 \cdot \alpha \cdot \beta + c_3 + \\ & k_3] + (r_4 \cdot \beta + c_4 + k_4) + [\alpha^2 + c_5 \cdot (\alpha - 1) + \\ & r_5 \cdot \alpha \cdot \beta + c_5 + k_5] \bmod \beta \\ = \; & [\alpha^2 + c_1 \cdot (\alpha - 1) + r_1 \cdot (\alpha + 1) \cdot \beta] + (r_2 \cdot 2 \cdot \beta \\ & + \alpha) + [c_3 \cdot (\alpha - 1) + r_3 \cdot (\alpha + 1) \cdot \beta] + r_4 \cdot 2 \cdot \beta \\ & + [\alpha^2 + c_5 \cdot (\alpha - 1) + r_5 \cdot (\alpha + 1) \cdot \beta] \bmod \beta \\ = \; & 2 \cdot \alpha^2 + \alpha + (c_1 + c_3 + c_5) \cdot (\alpha - 1) \bmod \beta \end{aligned} \tag{3}$$

Since $\alpha - n = \alpha - 5 > \sum_{i=1}^{n} c_i = \sum_{i=1}^{5} c_i$, $\beta > (n+1) \cdot \alpha^2 = 6 \cdot \alpha^2$ when $n = 5$, the value

$$\begin{aligned} & 2 \cdot \alpha^2 + \alpha + (c_1 + c_3 + c_5) \cdot (\alpha - 1) \\ < \; & 2 \cdot \alpha^2 + \alpha + \textstyle\sum_{i=1}^{5} c_i \cdot \alpha < 2 \cdot \alpha^2 + \alpha(1 + \alpha - 5) \\ < \; & 2 \cdot \alpha^2 + \alpha^2 = 3 \cdot \alpha^2 < \beta \end{aligned} \tag{4}$$

Therefore, we can remove "$\bmod \beta$" from Eq.(3) and have

$$\begin{aligned} E = & 2 \cdot \alpha^2 + \alpha + (c_1 + c_3 + c_5) \cdot (\alpha - 1) \bmod \beta \\ = & 2 \cdot \alpha^2 + \alpha + (c_1 + c_3 + c_5) \cdot (\alpha - 1) \end{aligned} \tag{5}$$

Again, since $\alpha + (c_1 + c_3 + c_5) \cdot (\alpha - 1) < \alpha^2$, we have

$$\frac{E - (E \bmod \alpha^2)}{\alpha^2} = \frac{2 \cdot \alpha^2}{\alpha^2} = 2 \tag{6}$$

According to the line-19 in Algorithm 1, only when both a_i and b_i are 1, an α^2 can be produced. Then, the coefficient of α^2 is just the required scalar product $\vec{\mathbf{a}} \cdot \vec{\mathbf{b}}$. As a result, the correctness of PPSPC protocol is verified.

Extension of PPSPC protocol. Although Algorithm 1 deals with the PPSPC for binary vectors, it can be easily extended

for the generalized vector's PPSPC. For example, to calculate the PPSPC of the generalized vectors $\vec{\mathbf{a}} = (a_1, a_2, \cdots, a_n)$, $\vec{\mathbf{b}} = (b_1, b_2, \cdots, b_n)$, where any $a_i, b_i \in \mathbb{Z}_m$ with $2 < m < 2^8$, we only make the following modifications in Algorithm 1, and its correctness can be easily verified as well.

5: choose two large primes α, β, where α is of the length $|\alpha| = 256$ bits and $\beta > (n \cdot m^2 + 1) \cdot \alpha^2$
6: set $K = 0$ and choose n positive random numbers $(c_1, c_2, c_3, \cdots, c_n)$ such that $m \cdot \sum_{i=1}^{n} c_i < \alpha - m \cdot n$
9: **if** $a_i \neq 0$ **then**
10: $C_i = a_i \cdot \alpha + c_i + r_i \cdot \beta, \quad K = K + k_i$
18: **if** $b_i \neq 0$ **then**
19: $D_i = b_i \cdot \alpha \cdot C_i$

3.2.3 Analysis of Opportunistic Computing in m-Healthcare Emergency

Consider the ambulance will arrive at the emergency location in the time period t. To gauge the benefits brought by opportunistic computing in m-Healthcare emergency, we analyze how many qualified helpers can participate in opportunistic computing within the time period t, and how many resources can the opportunities computing provide. Assume that the arrival of users at the emergency location follows a Poisson process $\{N(t), t \geq 0\}$ having rate λ. For a given threshold th, $N_q(t) = n$ and $N_{\bar{q}}(t) = m$ are respectively denoted as the number of qualified helpers and the number of non-qualified helpers within $[0, t]$. For any arriving user at time $\tau \in [0, t]$, the probability that the user is a qualified helper is $P(\tau)$. Then, Theorem 1 can give the expected number of qualified helpers participating in opportunistic computing within $[0, t]$.

Theorem 1: The expected number of the qualified helpers participating in opportunistic computing within $[0, t]$ is $E(N_q(t)) = \lambda t p$, where $p = \frac{1}{t}\int_0^t P(\tau)d\tau$.

Proof: Given total $N(t) = N_q(t) + N_{\bar{q}}(t) = n + m$ users arriving within time period $[0, t]$, we know the time τ is uniformly distributed in interval $[0, t]$ for any user who arrives at time τ [26]. Therefore, when defining the probability $p = P\{\text{one user arriving in } [0, t] \text{ is a qualified helper} | N(t) = n + m\}$, we have $p = \frac{1}{t}\int_0^t P(\tau)d\tau$. Since all users arrive independently, $P\{N_q(t) = n, N_{\bar{q}}(t) = m | N(t) = n + m\}$ just shows the probability that n qualified helpers' arrivals during total $n + m$ Bernoulli experiments. Therefore,

$$\begin{aligned} & P\{N_q(t) = n, N_{\bar{q}}(t) = m\} \\ = \; & P\{N_q(t) = n, N_{\bar{q}}(t) = m | N(t) = n + m\} \\ & \cdot P\{N(t) = n + m\} \\ = \; & \binom{n+m}{n} p^n (1-p)^m e^{-\lambda t} \frac{(\lambda t)^{n+m}}{(n+m)!} \\ = \; & \frac{(n+m)!}{n! \cdot m!} p^n (1-p)^m e^{-\lambda t(p+1-p)} \frac{(\lambda t)^n \cdot (\lambda t)^m}{(n+m)!} \\ = \; & e^{-\lambda t p} \frac{(\lambda t p)^n}{n!} \cdot e^{-\lambda t(1-p)} \frac{(\lambda t(1-p))^m}{m!} \end{aligned} \tag{7}$$

which indicates that both $N_q(t)$ and $N_{\bar{q}}(t)$ are independent Poisson processes with respective rate $\lambda t p$ and $\lambda t(1-p)$. As a result, the expected number of qualified helpers participating in the opportunistic computing within $[0, t]$ is $E(N_q(t)) = \lambda t p$ with $p = \frac{1}{t}\int_0^t P(\tau)d\tau$. □

Assume each qualified helper can provide η computing and power resources per unit of time, Theorem 2 further gives the expected resources that can be opportunistically provided by opportunistic computing within $[0, t]$.

Theorem 2: The expected resources that can be provided by opportunistic computing is $\frac{\lambda t^2 p}{2}\eta$ within $[0, t]$.

Proof: Suppose the k-th qualified helper arrives at time $\tau_k \in [0, t]$, where $1 \leq k \leq N_q(t)$. Then, the total resources $R(t)$ provided by all arrived qualified helpers can be expressed as $\sum_{k=1}^{N_q(t)}(t - \tau_k) \cdot \eta$. Because

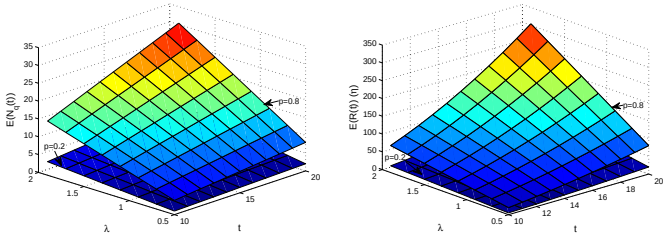
$$\begin{aligned} & E\{R(t)|N_q(t) = n\} = E\{\textstyle\sum_{k=1}^{N_q(t)}(t - \tau_k) \cdot \eta | N_q(t) = n\} \\ = \; & E\{\textstyle\sum_{k=1}^{n}(t - \tau_k) \cdot \eta | N_q(t) = n\} \\ = \; & nt\eta - E\{\textstyle\sum_{k=1}^{n} \tau_k \cdot \eta | N_q(t) = n\} = nt\eta - \frac{nt\eta}{2} = \frac{nt\eta}{2} \end{aligned} \tag{8}$$

and $E(N_q(t)) = \lambda t p$ from Theorem 1, we have the expected resources $E\{R(t)\}$ as

$$\begin{aligned} & E\{R(t)\} = \textstyle\sum_{n=0}^{\infty} (P\{N_q(t) = n\} E\{R(t)|N_q(t) = n\}) \\ = \; & \textstyle\sum_{n=0}^{\infty} P\{N_q(t) = n\} \cdot \frac{nt\eta}{2} = \frac{t\eta}{2} \cdot E(N_q(t)) = \frac{\lambda t^2 p}{2} \cdot \eta \end{aligned} \tag{9}$$

Therefore, the expected resources that can be provided by opportunistic computing is $\frac{\lambda t^2 p}{2}\eta$ within $[0, t]$. □

We plot the $E(N_q(t))$, $E(R(t))$ versus λ and t with different $p = 0.2, 0.8$ in Fig. 4. From the figure, we can see both large λ and large p can increase $E(N_q(t))$, $E(R(t))$ with the time. Therefore, when the emergency location has high traffic, i.e., enough opportunistic resources can be expected, we can set the threshold th high to reduce the probability p, so that the PHI privacy disclosure can be minimized. However, if the emergency location has low traffic, in order to guarantee the high reliability of PHI process and transmission, the threshold th should be set low to increase the probability p. In Section 5, we will conduct simulations to further evaluate the effectiveness of opportunistic computing in m-Healthcare emergency.



(a) $E(N_q(t))$ (b) $E(R(t))$

Fig. 4. $E(N_q(t))$, $E(R(t))$ versus λ and t with different p

4 Security Analysis

In this section, we analyze the security properties of the proposed SPOC framework. In specific, following the security requirements discussed earlier, our analyses will focus on how the proposed SPOC framework can achieve the user-centric privacy access control for opportunistic computing in m-Healthcare emergency.

• *The proposed SPOC framework can achieve the phase-I access control.* In the phase-I access control, the single-attribute encryption technique is employed [27]. Since $e(g, g)^{xs}$ can be recovered only by a registered medical user $U_j \in \mathbb{U}$ with his access key $ak_j = (g^{x+at_{j1}}, g^{t_{j1}}, g^{t_{j2}}, h_1^{t_{j1}} h_2^{t_{j2}})$ from $(C_1 = g^s, C_2 = A^s \cdot h_1^{-s}, C_3 = h_2^{-s})$,

if U_j can recover $e(g,g)^{xs}$, he can be authenticated as a registered medical user. In addition, the timestamp in the returned $Auth = H'(e(g,g)^{xs}||timestamp)$ can also prevent the possible replaying attack. Therefore, the phase-I access control can be achieved in the proposed SPOC framework.

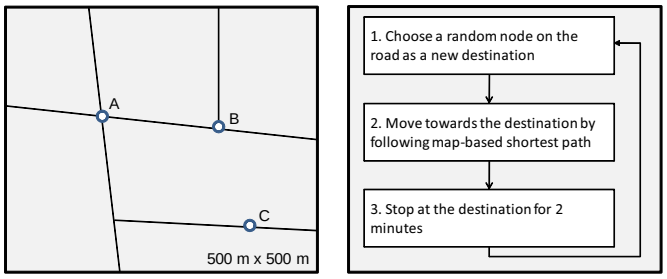
• *The proposed SPOC framework can achieve the phase-II access control.* In the phase-II access control, our novel PPSPC protocol is employed. As shown in Algorithm 1, for each $a_i \in \vec{\mathbf{a}}$, we have $C_i = \alpha + c_i + r_i\beta$ when $a_i = 1$, and $C_i = c_i + r_i\beta$ when $a_i = 0$. Since either α or 0 is masked by $c_i + r_i\beta$ in C_i, without knowing the random numbers c_i and $r_i\beta$, it is impossible to distinguish whether C_i is formed by $\alpha + c_i + r_i\beta$ or $c_i + r_i\beta$. In addition, since the random numbers $(c_i, r_i\beta)$ are individually used for one time, different C_i and C_i' are unlinkable. Therefore, each $a_i \in \vec{\mathbf{a}}$ is privacy-preserving during the scalar product computation. On the other hand, for each $b_i \in \vec{\mathbf{b}}$, we have $D_i = \alpha C_i$ when $b_i = 1$, and $D_i = C_i$ when $b_i = 0$. Obviously, this operation cannot directly hide α. However, when all D_i are summated into D, i.e., $D = \sum_{i=1}^{n} D_i$, the unknown $\sum_{i=1}^{n} c_i + r_i\beta$ will hide the operation on each D_i. As a result, each $b_i \in \vec{\mathbf{b}}$ is also privacy-preserving during the scalar product computation. Due to the correctness of Algorithm 1, the scalar product $\vec{\mathbf{a}} \cdot \vec{\mathbf{b}}$ indicates the number of same symptom characters of two personal health profiles. Once the result $\vec{\mathbf{a}} \cdot \vec{\mathbf{b}}$ is more than the threshold th, U_j is authenticated as a qualified helper, and assigned with U_0's session key k_0. Since U_j has the similar symptoms as U_0, to protect his own health information, U_j is discouraged to disclose U_0's health profiles. In such a way, U_0's PHI privacy disclosure can be minimized. As a result, the phase-II access control is also achieved in the proposed SPOC framework.

• *The proposed SPOC framework can achieve the session key's forward and backward secrecy.* In the proposed SPOC framework, once U_j has passed the phase-II access control, he can hold the session key $k_0 = H(sk_0||CDate)$ of U_0 to decrypt and process the encrypted raw PHI from $\mathcal{E}nc(k_0, \mathrm{rPHI}||CDate)$. However, since the one-wayness of the hash function $H()$, the secret key sk_0 cannot be inversely obtained from $k_0 = H(sk_0||CDate)$. Moreover, since the session key $k_0 = H(sk_0||CDate)$ is date-dependent, i.e., U_0 will utilize unlinkable session key everyday. Therefore, even though U_j gets the session key k_0 in m-Healthcare emergency, he cannot use it to derive U_0's previous and/or future session keys. As a result, the session key's forward and backward secrecy is also satisfied in the proposed SPOC framework.

From the above security analysis, we can see the proposed SPOC framework can indeed achieve the user-centric privacy access control of opportunistic computing in m-Healthcare emergency.

5 Performance Evaluation

In this section, we evaluate the performance of the proposed SPOC framework using a custom simulator built in Java. The simulator implements the application layer under the assumptions that the communications between smartphones and the communications between BSNs and smartphones are always workable when they are within each other's transmission ranges. The performance metrics used in the evaluation are 1) the average number of qualified helpers (NQH), which indicates how many qualified helpers can participate in the opportunistic computing within a given time period, and 2) the average resource consumption ratio (RCR), which is defined as the fraction of the resources consumed by the medical user in emergency to the total resources consumed in opportunistic computing for PHI process within a given time period. Both NGH and RCR can be used to examine the effectiveness of the proposed SPOC framework with user-centric privacy access control of opportunistic computing in m-Healthcare emergency.



(a) Simulation area (b) Mobility model

Fig. 5. Simulation area and mobility model under consideration

5.1 Simulation Setup

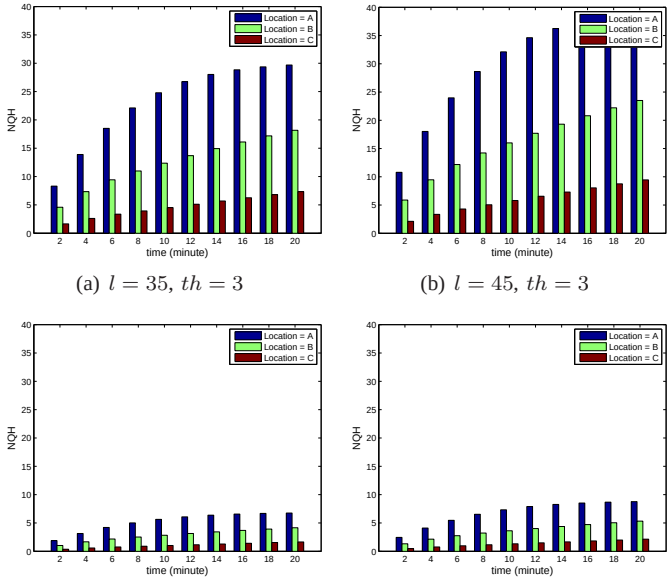
In the simulations, total l users $\mathbb{U} = \{U_0, U_1, \cdots, U_{l-1}\}$ are first uniformly deployed in an interest area of $500\ m \times 500\ m$, as shown in Fig. 5(a). Each user $U_i \in \mathbb{U}$ is equipped with his personal BSN and a smartphone with a transmission radius of 20 meters, and independently moves along the road with the velocity $v \in [0.5, 1.2] m/s$ in the area by following the mobility model described in Fig. 5(b). Assume that the symptom character space $n = 16$, each user is randomly assigned 6-8 symptom characters. Let the emergency of user U_0 take place at time $t = 0$, he sets the threshold th as $\{3, 5\}$, and waits the qualified helpers participating in the opportunistic computing before the ambulance arrives in 20 minutes. Note that, in the simulations, we consider all users will stop when they meet U_0's emergency, and only the qualified helpers will participate in the opportunistic computing. To eliminate the influence of initial system state, a warm-up period of first 10 minutes is used. In addition, we consider U_0's emergency takes place at three locations, A, B, and C, in the map to examine how the factors l, th affect the NGH and RCR at different locations. The detailed parameter settings are summarized in Table 1.

TABLE 1
Simulation Settings

Parameter	Setting
Simulation area	500 m $\times$ 500 m
Simulation warm-up, duration	10 minutes, 20 minutes
Number, velocity of users	$l = \{40, 60\}$, $v = 0.5 - 1.2$ m/s
Similarity threshold	$th = \{3, 5\}$
Transmission of smartphone, BSN	20 m, 20 m
Raw PHI data generation interval	every 10 seconds
Emergency location	A, B, and C

In the following, we run the simulations with different parameter settings. For each setting, the simulation lasts for 20 minutes (excluding the warm-up time), and the average performance results over 10000 runs are reported.

5.2 Simulation Results



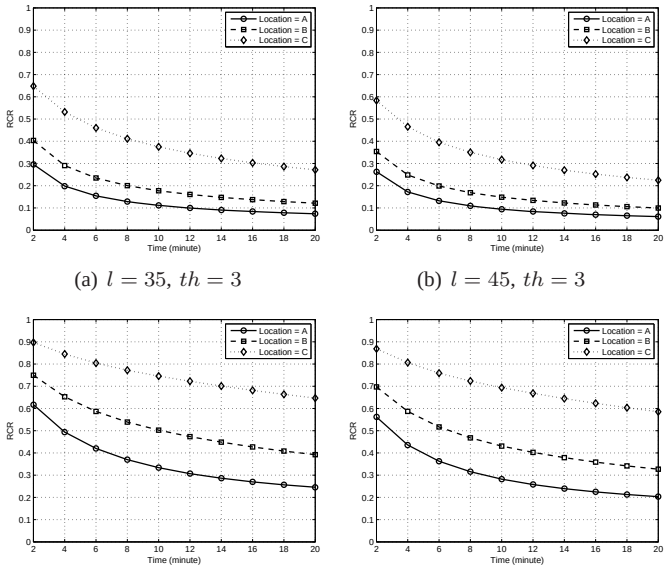
(a) $l = 35$, $th = 3$ (b) $l = 45$, $th = 3$

(c) $l = 35$, $th = 5$ (d) $l = 45$, $th = 5$

Fig. 6. NQH varying with time under different l and th

In Fig. 6, we compare the average NQHs at locations A, B and C varying with time from 2 minutes to 20 minutes under different user number l and threshold th. From the figure, we can see, with the increase of time, the average NQH will also increase, especially for the location A. The reason is that, when all users move in the simulation area by following the same mobility model, location A will have higher traffic than locations B and C. In addition, when the user number l in the simulation area increases, the user arrival rate at locations A, B, and C also increase. Then, the average NQH increases as well. By further observing the differences of the average NQH under thresholds $th = 3$ and $th = 5$, we can see the average NQH under $th = 5$ is much lower than that under $th = 3$, which indicates that, in order to minimize the privacy disclosure in opportunistic computing, the larger threshold should be chosen.

However, since the high reliability of PHI process is expected in m-Healthcare emergency, minimizing the privacy disclosure in opportunistic computing is not always the first priority. In Fig. 7, we plot the corresponding RCR varying with the time under different user number l and threshold th. From the figure, we can observe both high-traffic location, i.e., location A, and large number of users, i.e., $l = 45$, can reduce the U_0's RCR. However, the RCR under $th = 5$ is higher than that under $th = 3$. Therefore, once U_0 sets the threshold $th = 5$ while the residual energy in his smartphone is not enough, his smartphone cannot support high-reliability of PHI process and transmission before the ambulance arrives. This indicates U_0 should carefully choose the threshold th



(a) $l = 35$, $th = 3$ (b) $l = 45$, $th = 3$

(c) $l = 35$, $th = 5$ (d) $l = 45$, $th = 5$

Fig. 7. RCR varying with time under different l and th

to balance the high reliability of PHI process and privacy disclosure. For example, if the emergency takes place at a high traffic location and the residual energy in U_0's smartphone is not too low, U_0 can choose a relative high threshold to minimize the privacy disclosure. However, if the emergency location has low traffic and the smartphone's energy is also insufficient, th should be as low to first fit the high-reliability of PHI process and transmission in m-Healthcare emergency.

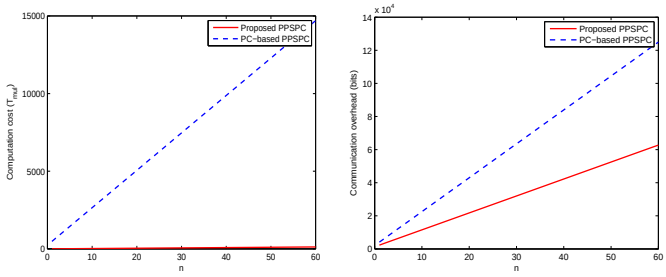
6 Related Works

Opportunistic computing: The study of opportunistic computing has gained the great interest from the research community recently, and we briefly review some of them related to our work [7], [8], [9], [10]. In [7], Avvenuti et al. introduce the opportunistic computing paradigm in wireless sensor network to solve the problem of storing and executing an application that exceeds the memory resources available on a single sensor node. Especially, their solution is based on the idea of partitioning the application code into a number of opportunistically cooperating modules, and each node contributes to the execution of the original application by running a subset of the application tasks and providing service to the neighboring nodes. In [8], Passarella et al. evaluate the performance of service execution in opportunistic computing. Specifically, they first abstract resources in pervasive computing as services, that are opportunistically contributed by providers and invoked by seekers. Then, they present a complete analytical model to depict the service invocation process between seekers and providers, and derive the optimal number of replicas to be spawned on encountered nodes, in order to minimize the execution time and optimize the computational and bandwidth resources used.

Although [7] and [8] are important for understanding how the opportunistic computing paradigm work when resources available on different nodes can be opportunistically gathered

together to provide richer functionality, they have not considered the potential security and privacy issues existing in the opportunistic computing paradigm [9], [10]. Different from the above works, our proposed SPOC framework aims at the security and privacy issues, and develops a user-centric privacy access control of opportunistic computing in m-Healthcare emergency.

Privacy-preserving scalar product computation: Research on privacy-preserving scalar product computation (PPSPC) has been conducted for privacy-preserving data mining [28], [12], [11], [29], and as well for secure friend discovery in mobile social networks quite recently [30], [31], [32]. Initially, PPSPC protocol was designed by involving a semi-trusted party [28]. Later, to remove the semi-trusted party, many PPSPC protocols without a third party were proposed [12], [11], [29], [13]. However, they are relying on time-consuming "homomorphic encryption" [14] and/or "add vector protocol", and are not quite efficient[2]. In our proposed SPOC framework, we present a new PPSPC protocol, which does not use any "homomorphic encryption", but is very efficient in terms of computational and communication costs, i.e., the computational cost only takes $2n$ multiplications (*mul*), and the communication cost is only $(n+1)\cdot 1024 + 256$ bits. Let T_{mul}, T_{exp} denote the time needed to execute a modulus multiplication and a modulus exponentiation, respectively. When we roughly estimate $T_{exp} \approx 240 T_{mul}$ [33], we use Fig. 8 to compare the computation and communication costs of the proposed PPSPC protocol and the popular Paillier Cryptosystem (PC)-based PPSPC protocol described in Fig. 9. From Fig. 8, we can obviously observe that our proposed PPSPC protocol is much efficient, especially in computation costs. To the best of our knowledge, our proposed PPSPC is the most efficient privacy-preserving scalar product computation protocol till now.



(a) Computation comparison (b) Communication comparison

Fig. 8. Computation and communication comparisons between the proposed PPSPC and the PC-based PPSPC varying with n

7 Conclusions

In this paper, we have proposed a secure and privacy-preserving opportunistic computing (SPOC) framework for m-Healthcare emergency, which mainly exploits how to use opportunistic computing to achieve high reliability of PHI process and transmission in emergency while minimizing the privacy disclosure during the opportunistic computing. Detailed security analysis shows that the proposed SPOC framework can achieve the efficient user-centric privacy access control. In addition, through extensive performance evaluation, we have also demonstrated the proposed SPOC framework can balance the high-intensive PHI process and transmission and minimizing the PHI privacy disclosure in m-Healthcare emergency. In our future work, we intend to carry on smartphone based experiments to further verify the effectiveness of the proposed SPOC framework. In addition, we will also exploit the security issues of PPSPC with internal attackers, where the internal attackers will not honestly follow the protocol.

2. Although the PPSPC protocol in [29] is not based on homomorphic encryption, the description of protocol is incorrect, as noted in [13].

The currently popular Paillier Cryptosystem (PC)-based PPSPC is described as follows. Given the Paillier cryptosystem $\mathcal{E}(x) = g^x r^N \bmod N^2$ [14], where $N = pq$ and the base g are public, U_0 keeps (p, q) secretly and performs the following steps with U_j: *i*) for each element $a_i \in \vec{\mathbf{a}} = (a_1, a_2, \cdots, a_n)$, U_0 first uses a random number r_i to encrypt a_i as $\mathcal{E}(a_i) = g^{a_i} r_i^N \bmod N^2$. Then, U_0 sends $\mathcal{E}(\vec{\mathbf{a}}) = (\mathcal{E}(a_1), \mathcal{E}(a_2), \cdots, \mathcal{E}(a_n))$ to U_j; and *ii*) after receiving $\mathcal{E}(\vec{\mathbf{a}}) = (\mathcal{E}(a_1), \mathcal{E}(a_2), \cdots, \mathcal{E}(a_n))$, U_j uses his vector $\vec{\mathbf{b}} = (b_1, b_2, \cdots, b_n)$ to compute $\mathcal{E}(\vec{\mathbf{a}} \cdot \vec{\mathbf{b}})$ as

$$\begin{aligned} &\prod_{i=1}^{n} \mathcal{E}(a_i)^{b_i} \equiv \prod_{i=1}^{n} \left(g^{a_i} r_i^N\right)^{b_i} \equiv \prod_{i=1}^{n} g^{a_i b_i} \left(r_i^{\ b_i}\right)^N \\ \equiv\ & g^{\sum_{i=1}^{n} a_i \cdot b_i} \cdot \left(\prod_{i=1}^{n} \left(r_i^{\ b_i}\right)\right)^N \bmod N^2 = \mathcal{E}\left(\sum_{i=1}^{n} a_i \cdot b_i\right) \\ =\ & \mathcal{E}(\vec{\mathbf{a}} \cdot \vec{\mathbf{b}}) \end{aligned}$$

and returns $\mathcal{E}(\vec{\mathbf{a}} \cdot \vec{\mathbf{b}})$ back to U_0; *iii*) upon receiving $\mathcal{E}(\vec{\mathbf{a}} \cdot \vec{\mathbf{b}})$, U_0 uses the secret (p, q) to recover $\vec{\mathbf{a}} \cdot \vec{\mathbf{b}}$ from $\mathcal{E}(\vec{\mathbf{a}} \cdot \vec{\mathbf{b}})$.

Computational cost. For binary vectors $(\vec{\mathbf{a}}, \vec{\mathbf{b}})$, U_0 should take at least n exponentiations to compute $\mathcal{E}(\vec{\mathbf{a}})$. Then, U_j takes around $(n-1)$ multiplications to calculate $\mathcal{E}(\vec{\mathbf{a}} \cdot \vec{\mathbf{b}})$. Finally, U_0 takes one more exponentiation to recover $\vec{\mathbf{a}} \cdot \vec{\mathbf{b}}$. Therefore, the computational cost is around $(n+1) \cdot T_{exp} + (n-1) \cdot T_{mul}$. Note that, if $(\vec{\mathbf{a}}, \vec{\mathbf{b}})$ are generalized vectors, the computational cost should be $(3n+1) \cdot T_{exp} + (n-1) \cdot T_{mul}$.

Communication cost. The security of the Paillier cryptosystem relies on the unknown factorization of modulus $N = pq$. When $N = pq$ is set as 1024, each $\mathcal{E}(a_i)$ and $\mathcal{E}(\vec{\mathbf{a}} \cdot \vec{\mathbf{b}})$ will be expanded to 2048 bits, and then the communication cost will be $(n+1) \cdot 2048$ bits.

Fig. 9. Description of Paillier Cryptosystem (PC)-based PPSPC

References

[1] A. Toninelli, R. Montanari, and A. Corradi, "Enabling secure service discovery in mobile healthcare enterprise networks," *IEEE Wireless Communications*, vol. 16, pp. 24–32, 2009.

[2] 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'10*, Corfu Island, Greece, 2010.

[3] Y. Ren, R. W. N. Pazzi, and A. Boukerche, "Monitoring patients via a secure and mobile healthcare system," *IEEE Wireless Communications*, vol. 17, pp. 59–65, 2010.

[4] R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for mhealthcare social network," *MONET*, vol. 16, no. 6, pp. 683–694, 2011.

[5] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed System*, to appear.

[6] M. R. Yuce, S. W. P. Ng, N. L. Myo, J. Y. Khan, and W. Liu, "Wireless body sensor network using medical implant band," *Journal of Medical Systems*, vol. 31, no. 6, pp. 467–474, 2007.

[7] M. Avvenuti, P. Corsini, P. Masci, and A. Vecchio, "Opportunistic computing for wireless sensor networks," in *IEEE Proc. of MASS'07*, pp. 1–6.

[8] A. Passarella, M. Conti, E. Borgia, and M. Kumar, "Performance evaluation of service execution in opportunistic computing," in *Proc. of ACM MSWIM '10*, 2010, pp. 291–298.

[9] M. Conti, S. Giordano, M. May, and A. Passarella, "From opportunistic networks to opportunistic computing," *IEEE Communications Magazine*, vol. 48, pp. 126–139, September 2010.

[10] M. Conti and M. Kumar, "Opportunities in opportunistic computing," *IEEE Computer*, vol. 43, no. 1, pp. 42–50, 2010.

[11] W. Du and M. Atallah, "Privacy-preserving cooperative statistical analysis," in *Proc. of ACSAC '01*, 2001, pp. 102–111.

[12] J. Vaidya and C. Clifton, "Privacy preserving association rule mining in vertically partitioned data," in *Proc. of ACM KDD'02*, pp. 639–644.

[13] A. Amirbekyan and V. Estivill-Castro, "A new efficient privacy-preserving scalar product protocol," in *Proc. of AusDM '07*, pp. 209–214.

[14] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. of EUROCRYPT'99*, 1999, pp. 223–238.

[15] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel Distributed and Systems*, to appear.

[16] 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.

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

[18] J. Sun and Y. Fang, "Cross-domain data sharing in distributed electronic health record systems," *IEEE Transactions on Parallel Distributed and Systems*, vol. 21, no. 6, pp. 754–764, 2010.

[19] "Exercise and walking is great for the alzheimer's and dementia patient's physical and emotional health," http://free-alzheimers-support.com/wordpress/2010/06/exercise-and-walking/, June 2010.

[20] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "Grs: The green, reliability, and security of emerging machine to machine communications," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 28–35, 2011.

[21] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Proc. of CRYPTO'01*, 2001, pp. 213–229.

[22] X. Lin, X. Sun, P. Ho, and X. Shen, "Gsis: A secure and privacy preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, pp. 3442–3456, 2007.

[23] R. Lu, X. Lin, H. Zhu, , and X. Shen, "An intelligent secure and privacy-preserving parking scheme through vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, pp. 2772–2785, 2010.

[24] R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," *IEEE Transactions on Vehicular Technology*, vol. 61, pp. 86–96, 2012.

[25] http://www.uaproperty.com/articles/In-Ukraine-ambulance-come-patient-10-minutes.html.

[26] S. Ross, *Introduction to Probability Models, Ninth Edition*, 2007.

[27] X. Lin, R. Lu, X. Liang, and X. Shen, "STAP: A social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in vanets," in *Proc. of INFOCOM'11*, 2011, pp. 2147–2155.

[28] W. Du and Z. Zhan, "Building decision tree classifier on private data," in *Proc. of CRPIT '14*, ser. CRPIT '14, 2002, pp. 1–8.

[29] I. Ioannidis, A. Grama, and M. Atallah, "A secure protocol for computing dot-products in clustered and distributed environments," in *Proc. of ICPP '02*, 2002, pp. 379 – 384.

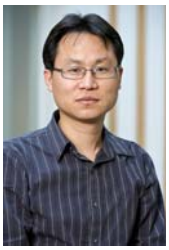
[30] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in *Prof. of INFOCOM'11*, 2011, pp. 1647–1655.

[31] R. Zhang, Y. Zhang, J. Sun, and G. Yan, "Fine-grained private matching for proximity-based mobile social networking," in *Prof. of INFOCOM'12*, 2012, pp. 1–9.

[32] M. Li, N. Cao, S. Yu, and W. Lou, "Findu: Privacy-preserving personal profile matching in mobile social networks," in *INFOCOM*, 2011, pp. 2435–2443.

[33] K.-H. Huang, Y.-F. Chung, C.-H. Liu, F. Lai, and T.-S. Chen, "Efficient migration for mobile computing in distributed networks," *Computer Standards & Interfaces*, vol. 31, no. 1, pp. 40–47, 2009.

Rongxing Lu (S'09-M'11) received the Ph.D. degree in computer science from Shanghai Jiao Tong University, Shanghai, China in 2006 and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2008. He is currently a Postdoctoral Fellow with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and trusted computing.



Xiaodong Lin (S'07-M'09) 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, and software security. Dr. Lin 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 IEEE International Conference on Computer Communications and Networks (ICCCN 2009) and the IEEE International Conference on Communications (ICC 2007) - Computer and Communications Security Symposium.

Xuemin (Sherman) Shen (M'97-SM'02-F'09) received the B.Sc.(1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a Professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo, Canada. He was the Associate Chair for Graduate Studies from 2004 to 2008. Dr. Shen's research focuses on resource management in interconnected wireless/wired networks, wireless network security, wireless body area networks, vehicular ad hoc and sensor networks. He is a co-author/editor of six books, and has published more than 600 papers and book chapters in wireless communications and networks, control and filtering. Dr. Shen served as the Technical Program Committee Chair for IEEE VTC'10 Fall, the Symposia Chair for IEEE ICC'10, the Tutorial Chair for IEEE VTC'11 Spring and IEEE ICC'08, the Technical Program Committee Chair for IEEE Globecom'07, the General Co-Chair for Chinacom'07 and QShine'06, the Chair for IEEE Communications Society Technical Committee on Wireless Communications, and P2P Communications and Networking. He also serves/served as the Editor-in-Chief for IEEE Network, Peer-to-Peer Networking and Application, and IET Communications; a Founding Area Editor for IEEE Transactions on Wireless Communications; an Associate Editor for IEEE Transactions on Vehicular Technology, Computer Networks, and ACM/Wireless Networks, etc.; and the Guest Editor for IEEE JSAC, IEEE Wireless Communications, IEEE Communications Magazine, and ACM Mobile Networks and Applications, etc. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004, 2007 and 2010 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. Dr. Shen is a registered Professional Engineer of Ontario, Canada, an IEEE Fellow, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, and a Distinguished Lecturer of IEEE Vehicular Technology Society and Communications Society.