Secure Handshake with Symptoms-matching: The Essential to the Success of mHealthcare Social Network

Rongxing Lu[†], Xiaodong Lin[‡], Xiaohui Liang[†], and Xuemin (Sherman) Shen[†]
[†]Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada
[‡]Faculty of Business and Information Technology, University of Ontario Institute of Technology, Canada
{rxlu, x27liang, xshen}@bbcr.uwaterloo.ca; xiaodong.lin@uoit.ca

ABSTRACT

In our aging society, mHealthcare social network (MHSN) built upon wireless body sensor network (WBSN) and mobile communications provides a promising platform for the seniors who have the same symptom to exchange their experiences, give mutual support and inspiration to each other, and help forwarding their health information wirelessly to a related eHealth center. However, there exist many challenging security issues in MHSN such as how to securely identify a senior who has the same symptom, how to prevent others who don't have the symptom from knowing someone's symptom? In this paper, to tackle these challenging security issues, we propose a secure same-symptom-based handshake (SSH) scheme, and apply the provable security technique to demonstrate its security in the random oracle model. In addition, we discuss a promising application – social-based patient health information (PHI) collaborative reporting in MHSN, and conduct extensive simulations to evaluate its efficiency in terms of PHI reporting delay.

Categories and Subject Descriptors

C.2.0 [**General**]: Security and protection

General Terms

Security, Privacy

Keywords

Mobile Healthcare Social Network, Secure Handshake with Symptoms-matching, Social-based PHI Collaborative Reporting

1. INTRODUCTION

Wireless body sensor network (WBSN), as an emerging network paradigm in eHealthcare system aiming at providing patients with remote and continuous monitoring, has gathered great momentum from not only the governments but also the academia in our aging society [1]. Typically, a WBSN consists of a number of medical sensor nodes accompanied by a wireless PDA communication device, where medical sensor nodes (either implantable or wearable) are equipped on a patient to periodically collect Patient Health Information (PHI) and forward them to the PDA device, then the PDA device serving as a gateway will report these PHI to the remote eHealth center. Based on these continuous PHI, medical professionals at eHealth center can remotely monitor the patient and quickly react to those life-threatening situations such as heart attacks. Due to these promising characteristics in improving healthcare quality, eHealthcare system built upon WBSN has currently been on the cusp of major innovations and paid wide attention in North America and elsewhere. However, the flourish of eHealthcare system still hinges up the patient concerns, for example, the security issues of patient health condition information [6, 7, 8]. In general, based on whether a patient, which is equipped with medical sensor nodes, is in-bed at home/hosptial or mobile outside, eHealthcare system can be divided into two categories: in-bed eHealthcare system and mobile eHealthcare (mHealthcare) system. In this paper, we will specifically focus on the security issues in mHealthcare system.

In mHealthcare system, patient's PHI is always considered being reported to the eHealth center directly, and the primary security issue is to keep the patient's PHI secret, and only the related medical professionals at eHealth center can read them. However, due to patient's mobility, patients can often contact with each other in mHealthcare system. If two patients have the same symptom, it is possible for them to share their health condition and experiences, provide mutual support and inspiration to each other to eliminate loneliness. We call such kind of social contact as mHealthcare social network (MHSN). In our aging society, MHSN is promising and can be accepted by the sensiors. However, new security issues arisen from MHSN should be considered [6], e.g., how to securely identify a patient who has the same symptom? how to prevent others who don't have the same symptom from knowing someone's symptom?

In this paper, to address the above challenging issues in MHSN, we propose a secure same-symptom-based handshake (SSH) scheme, which allows a patient to securely share his PHI with ones who have the same symptom. Specifically, the contribution of this paper are three-fold.

- Firstly, we define the notion of mHealthcare social network (MHSN), which provides a platform for those patients who have the same symptom to exchange their

BodyNets 2010 Corfu Island, Greece

experience, and give mutual support and inspiration to each other. To the best of our knowledge, this is the *first* work to propose the promising MHSN for our aging society.

- Secondly, to guarantee the security of MHSH, we present a secure same-symptom-based handshake (SSH) scheme based on bilinear pairings [4], and apply the provable security technique [10] to validate its security in the random oracle model.

- Thirdly, we discuss a promising application — social-based PHI collaborative reporting in MHSN, and develop a custom simulation to demonstrate its substantial improvement in terms of PHI reporting delay, compared with the ordinary PHI reporting without social collaboration.

The remainder of this paper is organized as follows. In Section 2, we introduce the system model, security model, and design goal. In Section 3, we recall bilinear maps and the corresponding complex assumptions. Then, we present our secure same-illness-based handshake (SSH) scheme for MHSN and its security analysis in Section 4. In Section 5, we evaluate the performance of MHSN in terms of PHI collaborative reporting application. We discuss the related work in Section 6. Finally, we draw our conclusions in Section 7.

2. MODELS AND DESIGN GOAL

2.1 System Model

We consider a typical MHSN, which consists of a trusted authority (TA) at eHealth center and a large number of mobile patients $\mathcal{U} = \{U_1, U_2, \cdots\}$, as shown in Figure 1.

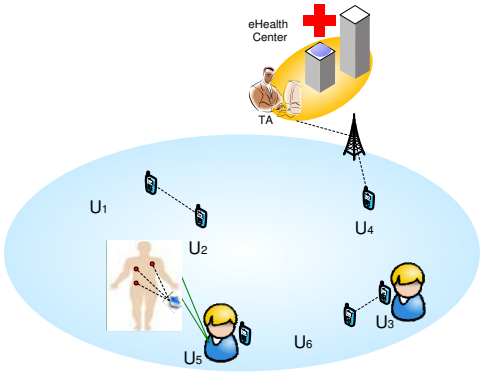


Figure 1: System model under consideration

- Trust Authority (TA): TA is a trustable and powerful entity, and located at the eHealth center. The responsibility of TA is in charge of the management of the whole eHealthcare system, for example, initializing the eHealthcare system, registering the patients at eHealth center by equipping proper body sensor nodes and key materials to patients.

- Patients $\mathcal{U}$: $\mathcal{U} = \{U_1, U_2, \cdots\}$ are a group of registered patients, each patient $U_i \in \mathcal{U}$ is equipped with implantable/wearable body sensor nodes and a wireless PDA device, which can periodically collect PHI and report them to the eHealth center for achieving better healthcare quality, where PHI including blood pressure, heart rate, etc., are closely related to the patient's symptom. Unlike in-bed patients at home or hospital, patients $\mathcal{U}$ in our model are mobile and have their sociality so that a MHSN can be formed.

  – **Mobility.** We consider that each patient $U_i \in \mathcal{U}$ can move. For example, each patient $U_i \in \mathcal{U}$, who is equipped with body sensor nodes and a PDA device, can often go out for a walk. However, due to patient's mobility, there may not always exist an available Access Point (AP) for mobile patient. Therefore, only when an AP is available nearby, mobile patients can report their PHI to eHealth center via the AP, which thus is different from the in-bed patient's heathcare monitoring at home or hospital.

  – **Sociality.** In our model, different patients $\mathcal{U}$ have different sociality. Some are active, but others are not. If patients are active, they may share their health information with other patients who have the same symptom to exchange experience and give mutual support and inspiration to each other. However, if patients are not sociable, even though they often meet with each other, a social relationship based on the same symptom is still hard to establish.

  For each patient $U_i \in \mathcal{U}$, let $\mathsf{sym}(U_i)$ be the symptom that U_i have, and $\mathsf{soc}(U_i)$ be U_i's sociality, and defined as

$$\mathsf{soc}(U_i) = \begin{cases} 1, & \text{if the patient } U_i \text{ is sociable;} \\ 0, & \text{otherwise.} \end{cases}$$

  When two patients $U_i, U_j \in \mathcal{U}$ contact, the necessary conditions for establishing a social relationship based on the same symptom are as follows:

$$\begin{cases} \mathsf{soc}(U_i) = \mathsf{soc}(U_j) = 1, & U_i, U_j \text{ are sociable} \\ \mathsf{sym}(U_i) = \mathsf{sym}(U_j), & \text{have same symptom.} \end{cases}$$

.

2.2 Security Model

Patient health condition is very sensitive to the patients. Therefore, it is essential that the privacy of PHI should be controllable by the patients in a MHSN environment, i.e., without patient's consent, a patient's PHI can't be leaked to others. Specifically, the following security requirements should be ensured in a MHSN.

- *Patient's real identity should be protected in a MHSN.* Clearly, patient's identity privacy is a prerequisite of keeping PHI privacy. If all PHI are labeled with patient's real identity, patient health conditions can be easily violated.

- *Patient's PHI should be controlled by patient himself and only shared with ones who have the same symptom.* In a MHSN, the primary goal is still to securely and timely report patient's PHI to eHealth center for achieving better healthcare quality. At the same time,

some active patients could establish same-symptom-based social relationship, and self-control and share their PHI to each other for mutual support and inspiration. If two patients don't have the same symptom, their health information should not be leaked to each other.

2.3 Design Goal

With the above security model, our design goal is to develop a secure same-symptom-based handshake (SSH) scheme for MHSH, which is formally defined as follows.

Definition 1. (SSH Scheme) A secure same-symptom-based handshake (SSH) scheme consists of the following algorithms: *system setup*, *patient joining*, and *patients same-symptom-based handshaking*.

- system setup algorithm **SystemSetup**: it is a probabilistic algorithm run by TA at eHealth center, which takes as input a security parameter l and outputs the system public parameters *params* and *master key*.
- patient joining algorithm **PatientJoin**: it is an algorithm run between TA and a patient $U_i \in \mathcal{U}$, which takes as input the public parameters *params*, *master key* and the symptom $\mathsf{sym}(U_i)$ that U_i has, and outputs a pseudo-id pid_i and a corresponding private key S_i with respect to $\mathsf{sym}(U_i)$ for U_i, where the pseudo-id pid_i achieves the real identity privacy. This algorithm can be either probabilistic or deterministic.
- patients same-symptom-based handshaking algorithm **PatientsSSH**: it is an algorithm executed between two patients $U_i(pid_i)$ and $U_j(pid_j)$ who want to establish a social relationship and authenticate each other on the input pid_i, pid_j and *params*. The private input of each party is his private key S_k with respect to $\mathsf{sym}(U_k)$, where $k \in \{i, j\}$, and the output is mutual authentication and establishing a shared session key if $\mathsf{sym}(U_i) = \mathsf{sym}(U_j)$.

SSH scheme must satisfy three properties: correctness, impersonator resistance, and detector resistance.

- **Correctness.** When two honest patients $U_i, U_j \in \mathcal{U}$ run the PatientsSSH, if $\mathsf{soc}(U_i) = \mathsf{soc}(U_j) = 1$ and $\mathsf{sym}(U_i) = \mathsf{sym}(U_j)$, they can always authenticate each other as one who has the same symptom and establish a shared session key.
- **Impersonator Resistance.** The impersonator resistance is stated that, when two patients $U_i, U_j \in \mathcal{U}$ run the PatientsSSH, if $\mathsf{soc}(U_i) = \mathsf{soc}(U_j) = 1$ and $\mathsf{sym}(U_i) \neq \mathsf{sym}(U_j)$, the probability that U_i believes U_j has the same symptom $\mathsf{soc}(U_i)$ is negligible.
- **Detector Resistance.** The detector resistance is stated that, when two patients $U_i, U_j \in \mathcal{U}$ run the PatientsSSH, if $\mathsf{soc}(U_i) = \mathsf{soc}(U_j) = 1$ and $\mathsf{sym}(U_i) \neq \mathsf{sym}(U_j)$, U_j has no idea on what symptom $\mathsf{sym}(U_i)$ that U_i has.

Only when a MHSN is reinforeced by a secure SSH scheme, it can be widely accepted by the patients and step into its flourish stage.

3. BILINEAR MAPS AND COMPLEX ASSUMPTIONS

3.1 Notations

Let $\mathbb{N} = \{1, 2, 3, \ldots\}$ denote the set of natural numbers. If $l \in \mathbb{N}$, then 1^l is the string of l 1s. If x, y are two strings, then $|x|$ is the length of x and $x\|y$ is the concatenation of x and y. If S is a finite set, $s \xleftarrow{R} S$ denotes sampling an element x uniformly at random from S. And if $\mathcal{A}$ is a randomized algorithm, $y \leftarrow \mathcal{A}(x_1, x_2, \ldots)$ means that $\mathcal{A}$ has inputs $x_1, x_2, \ldots$ and outputs y.

3.2 Bilinear Maps

Let $\mathbb{G}$ be a cyclic additive group generated by P, whose order is a large prime q, and $\mathbb{G}_T$ be a cyclic multiplicative group with the same order q. An *admissible* bilinear pairing $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a map with the following properties:

1. *Bilinearity:* For all $P, Q \in \mathbb{G}$ and any $a, b \in \mathbb{Z}_q^*$, we have $e(aP, bQ) = e(P, Q)^{ab}$;
2. *Non-degeneracy:* There exist $P, Q \in \mathbb{G}$ such that $e(P, Q) \neq 1_{\mathbb{G}_T}$;
3. *Computability:* There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in \mathbb{G}$.

Such an *admissible* bilinear pairing $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ can be implemented by the modified Weil or Tate pairings [4].

3.3 Complex Assumptions

In the following, we define the quantitative notion of the complexity of the problems underlying the proposed SSH scheme, namely the Decisional Bilinear Diffie-Hellman (DBDH) Problem, and the Successive-Power DBDH (SPDBDH) Problem [5].

Definition 2. (DBDH Problem) The DBDH problem in $\mathbb{G}$ is as follows: Given an element P of $\mathbb{G}$, a tuple (xP, yP, zP, V) for unknown $x, y, z \in \mathbb{Z}_q^*$ and $V \in \mathbb{G}_T$, decide whether $V = e(P, P)^{xyz}$ or a random element R drawn from $\mathbb{G}_T$.

Definition 3. (k-SPDBDH Problem) The k-SPDBDH problem in $\mathbb{G}$ is as follows: Given an element P of $\mathbb{G}$, a tuple $(xP, yP, zP, V, \frac{z}{x}P, \frac{z}{x^2}P, \cdots, \frac{z}{x^k}P)$ for unknown $x, y, z \in \mathbb{Z}_q^*$ and $V \in \mathbb{G}_T$, decide whether $V = e(P, P)^{xyz}$ or a random element R drawn from $\mathbb{G}_T$.

Definition 4. (k-SPDBDH Assumption) Let $\mathcal{A}$ be an adversary that takes an input of $(xP, yP, zP, V, \frac{z}{x}P, \frac{z}{x^2}P, \cdots, \frac{z}{x^k}P)$ for unknown $x, y, z \in \mathbb{Z}_q^*$ and $V \in \mathbb{G}_T$, and returns a bit $b' \in \{0, 1\}$. We consider the following random experiments.

Experiment $\mathbf{Exp}_{\mathcal{A}}^{k-\mathrm{SPDBDH}}$
$x, y, z \xleftarrow{R} \mathbb{Z}_q^*; R \xleftarrow{R} \mathbb{G}_T$
$\widetilde{b} \leftarrow \{0, 1\}$
if $\widetilde{b} = 0$, then $V = e(P, P)^{xyz}$; else if $\widetilde{b} = 1$ then $V = R$
$\widetilde{b}' \leftarrow \mathcal{A}\left(\begin{array}{c} xP, yP, zP, V \\ \frac{z}{x}P, \frac{z}{x^2}P, \cdots, \frac{z}{x^k}P \end{array}\right)$
return 1 if $\widetilde{b}' = \widetilde{b}$, 0 otherwise

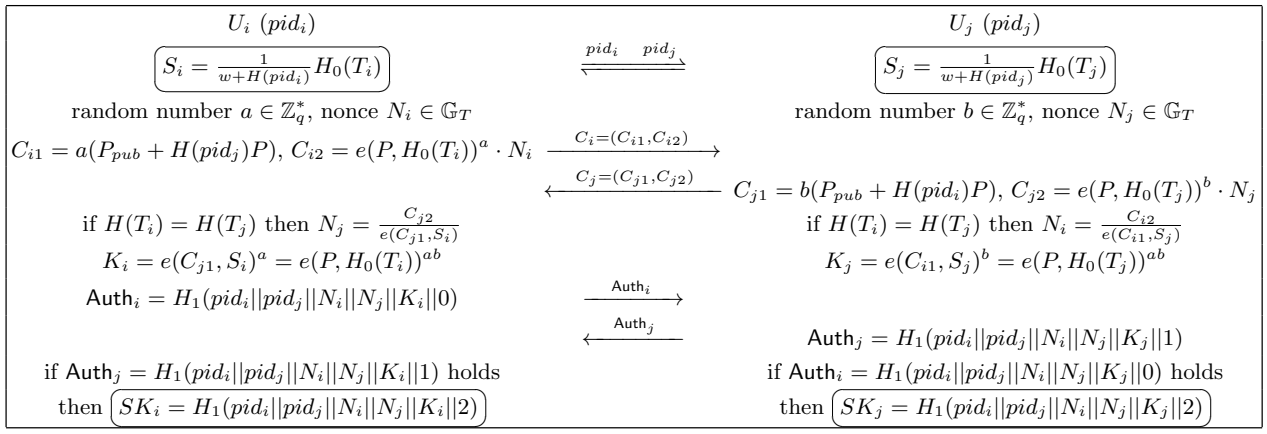


Figure 2: Proposed Secure Same-symptom-based Handshake (SSH) Scheme

We then define the advantage of $\mathcal{A}$ via

$$\mathbf{Adv}_{\mathcal{A}}^{k-\mathrm{SPDBDH}} = \left| \Pr\left[\mathbf{Exp}_{\mathcal{A}}^{k-\mathrm{SPDBDH}} = 1 | \widetilde{b} = 0\right] - \Pr\left[\mathbf{Exp}_{\mathcal{A}}^{k-\mathrm{SPDBDH}} = 1 | \widetilde{b} = 1\right] \right| \geq \epsilon$$

Let $\tau \in \mathbb{N}$ and $\epsilon \in [0,1]$. We say that the k-SPDBDH is (τ, ϵ)-secure if no adversary $\mathcal{A}$ running in time τ has an advantage $\mathbf{Adv}_{\mathcal{A}}^{k-\mathrm{SPDBDH}} \geq \epsilon$.

Note that the k-SPDBDH problem has been proved to be intractable for generic adversary, and the detailed proof can be refer to [5].

4. PROPOSED SSH SCHEME FOR MOBILE HEALTH SOCIAL NETWORK

In this section, we propose our secure same-symptom-based handshake (SSH) scheme, followed by its security analysis in MHSN.

4.1 Description of The Proposed Scheme

Our proposed SSH scheme is dedicated for MHSN, which mainly consists of three parts: SystemSetup, PatientJoin, and PatientsSSH.

SystemSetup: Given the security parameter l, the bilinear map groups $(\mathbb{G}, \mathbb{G}_T, e, P)$ of order q are chosen, where $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, P is a generator of $\mathbb{G}$ and q is a large prime with $|q| = l$. Then, the trust authority (TA) chooses a random number $w \in \mathbb{Z}_q^*$ as the *master key*, and computes the corresponding $P_{pub} = wP$. In addition, TA chooses three secure cryptographic hash functions H, H_0, and H_1, where $H : \{0,1\}^* \to \mathbb{Z}_q^*$, $H_0 : \{0,1\}^* \to \mathbb{G}$, and $H_1 : \{0,1\}^* \to \mathbb{Z}_q^*$. Let $\mathcal{T} = \{T_1, T_2, T_3, \cdots\}$ be a set of symptoms, each $T_i \in \mathbb{G}_T$ denotes a kind of symptom, as shown in the figure below.

T_1	diabetes
T_2	heart disease
T_3	high blood pressure
$\vdots$	$\vdots$

After that, TA sets the system public parameters *params* as $(\mathbb{G}, \mathbb{G}_T, e, P, P_{pub}, H, H_0, H_1, \mathcal{T})$.

PatientJoin: When a patient $U_i \in \mathcal{U}$ wants to join into the eHealthcare system for better healthcare quality, he will first take a medical examination at eHealth center and register himself with the TA by the following procedures:

- Based on the medical examination results, TA knows U_i has the symptom $T_i \in \mathcal{T}$. Then, TA chooses some proper implantable/wearable body sensor nodes for U_i, and also equips U_i with a PDA device. In such a way, the PDA device can aggregate the patient health information (PHI) from body nodes, and report them to the eHealth center. In order to keep the confidentiality of PHI, U_i can use $H_0(T_i)$ as the public key to encrypt the PHI [4]. Then, only the medical professionals who have the corresponding private key $wH_0(T_i)$ at eHealth center can recover them.
- In order to keep the patient U_i's privacy, TA assigns a pesudo-id pid_i and a corresponding private key $S_i = \frac{1}{w+H(pid_i)} H_0(T_i)$ related to the symptom T_i to U_i[1]. With these key materials, U_i can involve himself in a secure MHSN.

PatientsSSH: Assume that two patients $U_i, U_j \in \mathcal{U}$ are sociable, i.e., $\mathsf{soc}(U_i) = \mathsf{soc}(U_j) = 1$. When they meet with each other, they will first share their pseudo-ids (pid_i, pid_j), and launch a secure same-symptom-based handshake by the following steps, as shown in Figure 2.

- **Step 1:**
  - U_i with symptom T_i, i.e., $\mathsf{sym}(U_i) = T_i$, first chooses a random number $a \in \mathbb{Z}_q^*$ and a nonce $N_i \in \mathbb{G}_T$, computes and sends $C_i = (C_{i1}, C_{i2})$ to U_j, where
  $$\begin{cases} C_{i1} = a(P_{pub} + H(pid_j)P) \\ C_{i2} = e(P, H_0(T_i))^a \cdot N_i \end{cases}$$
  - Similarly, U_j with symptom T_j, i.e., $\mathsf{sym}(U_j) = T_j$, also chooses a random number $b \in \mathbb{Z}_q^*$ and

[1]Note that if the patent user U_i have more than one kind of symptoms, he can obtain all corresponding private keys. In our current work, we consider each patient only has one kind of symptom.

a nonce $N_j \in \mathbb{G}_T$, computes and sends $C_j = (C_{j1}, C_{j2})$ to U_i, where

$$\begin{cases} C_{j1} = b(P_{pub} + H(pid_i)P) \\ C_{j2} = e(P, H_0(T_j))^b \cdot N_j \end{cases}$$

- **Step 2:**
  - After receiving $C_j = (C_{j1}, C_{j2})$, U_i uses his private key $S_i = \frac{1}{w+H(pid_i)} H_0(T_i)$ to compute (N_j, K_i), where $N_j = \frac{C_{j2}}{e(C_{j1}, S_i)}$ and $K_i = e(C_{j1}, S_i)^a$. Then, U_i sends $\mathsf{Auth}_i = H_1(pid_i||pid_j||N_i||N_j||K_i||0)$ to U_j for authentication.
  - Similarly, after receiving $C_i = (C_{i1}, C_{i2})$, U_j uses his private key $S_j = \frac{1}{w+H(pid_j)} H_0(T_j)$ to compute (N_i, K_j), where $N_i = \frac{C_{i2}}{e(C_{i1}, S_j)}$ and $K_j = e(C_{i1}, S_j)^b$. Then, U_j sends the authentication information $\mathsf{Auth}_j = H_1(pid_i||pid_j||N_i||N_j||K_i||1)$ to U_i.
- **Step 3:**
  - Upon receiving Auth_j, U_i checks whether $\mathsf{Auth}_j = H_1(pid_i||pid_j||N_i||N_j||K_i||1)$. If it holds, U_i believes that U_j has the same symptom with him. Then, he computes the shared session key
  $$SK_i = H_1(pid_i||pid_j||N_i||N_j||K_i||2)$$
  - Similarly, on receiving Auth_i, U_j checks whether $\mathsf{Auth}_i = H_1(pid_i||pid_j||N_i||N_j||K_j||0)$. If it holds, U_j is convinced that U_i also has the same symptom with him. Then, he also computes the shared session key
  $$SK_j = H_1(pid_i||pid_j||N_i||N_j||K_j||2)$$

Correctness. If U_i and U_j have the same symptom, i.e., $\mathsf{sym}(U_i) = \mathsf{sym}(U_j) = T_i$, then

$$N_j = \frac{C_{j2}}{e(C_{j1}, S_i)} = \frac{e(P, H_0(T_i))^b \cdot N_j}{e(b(P_{pub} + H(pid_i)P), \frac{1}{w+H(pid_i)} H_0(T_i))} = \frac{e(P, H_0(T_i))^b \cdot N_j}{e(P, H_0(T_i))^b}$$

$$N_i = \frac{C_{i2}}{e(C_{i1}, S_j)} = \frac{e(P, H_0(T_i))^a \cdot N_i}{e(a(P_{pub} + H(pid_j)P), \frac{1}{w+H(pid_j)} H_0(T_i))} = \frac{e(P, H_0(T_i))^a \cdot N_j}{e(P, H_0(T_i))^a}$$

can be correctly recovered, and

$$K_i = e(C_{j1}, S_i)^a = e(P, H_0(T_i))^{ab} = e(C_{i1}, S_j)^b = K_j$$

are also identified. Then, both Auth_i and Auth_j are valid, and the session key $SK_i = SK_j$ are established. However, if $\mathsf{sym}(U_i) \neq \mathsf{sym}(U_j)$, the relations $K_i \neq K_j$ and $SK_i \neq SK_j$ are obvious. Therefore, the correctness of the proposed SSH scheme follows.

Mobile Healthcare Social Network. Once the SSH is successful, the patients U_i and U_j can use the shared session key to securely exchange their PHI and experiences, and give mutual support and inspiration to each other. Due to these promising functionalities, MHSN can be widely accepted by patients. In addition, because the Access Point (AP) is not always available for a patient in mobile environment, those active patients, based on the same-symptom-based social relationship, can also help each other to relay their PHI. In such a way, the PHI reporting delay can be reduced. The details of social-based PHI collaborative reporting algorithm is described in Algorithm 1.

Algorithm 1 Social-based PHI Collaborative Reporting

```
procedure CollaborativeReport
    patient U_i's PDA device periodically collect PHI PHI_i from body sensor nodes
    if an AP is available nearby then
        U_i directly report PHI_i to eHealth center via AP
    else if another patient U_j nearby then
        if soc(U_i) = soc(U_j) && sym(U_i) = sym(U_j) then
            U_i and U_j exchange their unreported PHI if their PDAs' storages are available. Later, before PHI_i's expiration, U_j helps reporting PHI_i when he runs into an available AP; otherwise, PHI_i will be deleted.
        end if
    end if
end procedure
```

4.2 Security Analysis

In this subsection, we will demonstrate the proposed SSH scheme to be impersonator resistant and detector resistant. Before delving into the analysis, we first show that the employed identity-based encryption ($\mathcal{IBE}$)

$$C = \begin{cases} C_1 = r(P_{pub} + H(pid)P), & \text{where } r \xleftarrow{R} \mathbb{Z}_q^* \\ C_2 = e(P, H_0(T))^r \cdot N, & T \text{ is a specific triage.} \end{cases}$$

in the SSH scheme is semantic security in the random oracle model [3].

Semantic security. To meet the requirement of SSH scheme, the identity-based encryption ($\mathcal{IBE}$) should be semantic security (indistinguishable) under selective-PID-Symptoms and chosen-plaintext attacks. Specifically, we consider an adversary $\mathcal{A}$ is first given the public parameters and selects the specific PID $pid^\star$ and symptom $T^\star$ in advance. Then, $\mathcal{A}$ is allowed to access two types queries to the key generation oracle $\mathcal{O}_K$: i) query for the challenged $pid^\star$ on other symptoms T, where $T \neq T^\star$; and ii) query for other pid, where $pid \neq pid^\star$, on the challenged $T^\star$. At some point, $\mathcal{A}$ outputs a pair of nonce $N_0, N_1 \in \mathbb{G}_T$. Then, after one nonce N_b, $b \in \{0, 1\}$, is encrypted with the challenged $pid^\star, T^\star$, the adversary $\mathcal{A}$ must decide which nonce has been encrypted.

Definition 5. (IND-sPS-CPA Secure) Let l and t be integers and ϵ be a real in $[0, 1]$. Let $\mathcal{IBE}$ be and secure encryption scheme with security parameter l, and $\mathcal{A}$ be an IND-sPS-CPA adversary against $\mathcal{IBE}$. We consider the following random experiments in the random oracle model:

Experiment $\mathbf{Exp}^{\mathsf{IND\text{-}sPS\text{-}CPA}}_{\mathcal{IBE},\mathcal{A}}(l)$
$params, masterkey \xleftarrow{R} SystemSetup(l)$
$(pid^\star, T^\star) \leftarrow \mathcal{A}$
$(N_0, N_1) \leftarrow \mathcal{A}^{\mathcal{O}_K, \mathcal{O}_H}(pid^\star, T^\star)$
$b \xleftarrow{R} \{0, 1\}$, $C \leftarrow N_b$
$b' \leftarrow \mathcal{A}^{\mathcal{O}_K, \mathcal{O}_H}(params, C, pid^\star, T^\star)$
if $b = b'$, *then return* $b^* \leftarrow 1$ *else* $b^* \leftarrow 0$
return b^*

We define the advantage probability of $\mathcal{A}$ via

$$\begin{aligned}\mathbf{Adv}^{\mathsf{IND\text{-}sPS\text{-}CPA}}_{\mathcal{IBE},\mathcal{A}}(l) &= 2\cdot \Pr\left[\mathbf{Exp}^{\mathsf{IND\text{-}sPS\text{-}CPA}}_{\mathcal{IBE},\mathcal{A}}(l)=1\right]-1\\ &= 2\cdot \Pr\left[b=b'\right]-1\end{aligned}$$

$\mathcal{IBE}$ is said to be (l,t,ϵ)-$\mathsf{IND\text{-}sPS\text{-}CPA}$ secure, if no adversary $\mathcal{A}$ running in time t has a success $\mathbf{Adv}^{\mathsf{IND\text{-}sPS\text{-}CPA}}_{\mathcal{IBE},\mathcal{A}}(l)\geq\epsilon$.

In the following theorem, we will prove that the $\mathcal{IBE}$ is IND-sPS-CPA secure under the k-SPDBDH assumption in the random oracle model, where the hash functions H, H_0 are modelled as random oracles.

Theorem 1. (IND-sPS-CPA Security) Let $k\in\mathbb{N}$ be an integer, and $\mathcal{A}$ an adversary against the $\mathcal{IBE}$ scheme in the random oracle model, where the hash functions H and H_1 behave as random oracles. Assume that $\mathcal{A}$ has the advantage probability $\mathbf{Adv}^{\mathsf{IND\text{-}sPS\text{-}CPA}}_{\mathcal{IBE},\mathcal{A}}\geq\epsilon$ to break $\mathcal{IBE}$, within the running time τ, after $q_H=k+1$, q_{H_0} and $q_K=k-1+q_{H_0}$ queries to the random oracles $\mathcal{O}_H$, $\mathcal{O}_{H_1}$, and the key generation oracle $\mathcal{O}_K$, respectively. Then, there exist $\epsilon'\in[0,1]$ and $\tau'\in\mathbb{N}$ as follows

$$\epsilon'=\mathbf{Adv}^{\mathrm{k-SPDBDH}}_{\mathcal{A}}(\tau')\geq\frac{\epsilon}{2},\qquad \tau'\leq\tau+\Theta(.) \tag{1}$$

such that the k-SPDBDH problem can be solved with probability ϵ' within time τ', where $\Theta(.)$ is the time complexity for the simulation.

Proof. We define a sequence of games $\mathbf{Game}_0$, $\mathbf{Game}_1$, $\cdots$ of modified attacks starting from the actual adversary $\mathcal{A}$ [10]. All the games operate on the same underlying probability space: the system parameters $params=(e,\mathbb{G},\mathbb{G}_T,q,P,P_{pub}=wP,H,H_0,H_1)$, the coin tosses of $\mathcal{A}$. Let

$$\left(\ \tilde{P}\in\mathbb{G}, x\tilde{P}, y\tilde{P}, z\tilde{P}, V\in\mathbb{G}_T, \frac{z}{x}\tilde{P}, \frac{z}{x^2}\tilde{P},\cdots,\frac{z}{x^k}\tilde{P}\ \right)$$

be a random instance of k-SPDBDH problem, we will use these incremental games to reduce the k-SPDBDH instance to the adversary $\mathcal{A}$ against the IND-sPS-CPA security of the $\mathcal{IBE}$ scheme.

$\mathbf{Game}_0$: This is the real attack game. In the game, the adversary $\mathcal{A}$ is fed with the system parameters $params=(e,\mathbb{G},\mathbb{G}_T,q,P,P_{pub}=wP,H,H_0,H_1)$. Let $\mathcal{PID}=\{pid_1,pid_2,\cdots,pid_{k+1}\}$ be a pseudo-id set and $\mathcal{T}=\{T_1,T_2,\cdots,T_{H_0}\}$ be a symptom set. At first, the adversary $\mathcal{A}$ chooses the challenged $pid^\star\in\mathcal{PID}$ and $T^\star\in\mathcal{T}$, then access to the random oracles $\mathcal{O}_H,\mathcal{O}_{H_0}$ and the key generation oracle $\mathcal{O}_K$ for any input either $(pid_i,T^\star)$, where $pid_i\neq pid^\star$, or $(pid^\star,T_j)$, where $T_j\neq T^\star$. At some point, the adversary $\mathcal{A}$ chooses a pair of nonce $(N_0^\star,N_1^\star)\in\mathbb{G}_T$. Then, we flip a coin $b\in\{0,1\}$ and produce the nonce $N^\star=N_b^\star$'s ciphertext $C^\star=(C_1^\star,C_2^\star)$ with respect to $(pid^\star,T^\star)$ as the challenge to the adversary $\mathcal{A}$. The challenge comes from the system parameters $P_{pub}=wP, H_0(T^\star)$ and one random number $r^\star\in\mathbb{Z}_q^*$, and $C_1^\star=r^\star\cdot(P_{pub}+H(pid^\star)P)$, $C_2^\star=e(P,H_0(T^\star))^{r^\star}\cdot N_b^\star$. Then, the adversary $\mathcal{A}$ outputs a bit $b'\in\{0,1\}$. In any $\mathbf{Game}_j$, we denote by $\mathbf{Guess}_j$ the event $b=b'$. Then, by definition, we have

$$\epsilon\leq\mathbf{Adv}^{\mathsf{IND\text{-}sPS\text{-}CPA}}_{\mathcal{IBE},\mathcal{A}}=2\Pr[b=b']-1=2\Pr[\mathbf{Guess}_0]-1 \tag{2}$$

$\mathbf{Game}_1$: In this game, we embed the random instance of k-SPDBDH problem into simulation. To achieve the perfect simulation, we use the technique in [5] for some preparatory work as follows:

▷ **PWork**$_1$

for $i=0$ **to** k
  compute $V_i=e\left(y\tilde{P},\frac{z}{x^i}\tilde{P}\right)$
choose two random numbers $t,x^\star\xleftarrow{R}\mathbb{Z}_q^*$
set $P=x\tilde{P}$ and $P_{pub}=t\tilde{P}-x^\star P$

▷ **PWork**$_2$

choose random numbers $\mathcal{X}=\{x_1,\cdots,x_k\}\xleftarrow{R}\mathbb{Z}_q^*$
establish a polynomial of degree k as
  $p(X)=\prod_{i=1}^k(tX+x_i)=\sum_{i=0}^k\rho_iX_i$ with $\rho_i\in\mathbb{Z}_q^*$
set $Q=p(\frac{1}{x})\cdot z\tilde{P}$

Since $(z\tilde{P},\frac{z}{x}\tilde{P},\frac{z}{x^2}\tilde{P},\cdots,\frac{z}{x^k}\tilde{P})$ are provided, the value of Q can be easily computed. In addition, in this game, when $P=x\tilde{P}$ and $P_{pub}=t\tilde{P}-x^\star P$, the master key w is implicitly defined as $w=\frac{t}{x}-x^\star$. Because the distribution of (P,P_{pub}) is unchanged in the eye of the adversary $\mathcal{A}$, the simulation is perfect, and we have

$$\Pr[\mathbf{Guess}_1]=\Pr[\mathbf{Guess}_0] \tag{3}$$

$\mathbf{Game}_2$: In this game, we simulate the random oracles $\mathcal{O}_H$ and $\mathcal{O}_{H_0}$, by maintaining the lists $\mathcal{H}$-List and $\mathcal{H}_0$-List to deal with the identical queries.

▷ **Sim-**$\mathcal{O}_H$

on input of a pseudo-id pid_i
  if $pid_i=pid^\star$
    set $H(pid_i)=x^\star$
    the record $(pid^\star,x^\star)$ will be added in $\mathcal{H}$-List
  else if $pid_i\neq pid^\star$
    choose a fresh x_i from $\mathcal{X}$, set $H(pid_i)=x^\star+x_i$
    the record $(pid_i,x^\star+x_i)$ will be added in $\mathcal{H}$-List
  return $H(pid_i)$

▷ **Sim-**$\mathcal{O}_{H_0}$

on input of one kind of symptom T_i
  if $T_i=T^\star$
    set $H_0(T_i)=Q$
    the record $(T^\star,Q)$ will be added in $\mathcal{H}_0$-List
  else if $T_i\neq T^\star$
    choose a fresh random number $r_i\xleftarrow{R}\mathbb{Z}_q^*$
    compute $Q_i=r_i\tilde{P}$, set $H_0(T_i)=Q_i$
    the record $(T_i,r_i,Q_i,\frac{r_i}{t}x\tilde{P})$ will be added in $\mathcal{H}_0$-List
  return $H(pid_i)$

Because the distribution of $(H(pid_i),H_0(T_i))$ is unchanged in the eye of the adversary $\mathcal{A}$, the simulation is perfect, and we have

$$\Pr[\mathbf{Guess}_2]=\Pr[\mathbf{Guess}_1] \tag{4}$$

$\mathbf{Game}_3$: In this game, we simulate the key generation oracle $\mathcal{O}_K$ to answer k queries on $(pid_i,H(T^*))$, where $pid_i\neq pid^\star$, and $q_{H_0}-1$ queries on $(pid^\star,H(T_j))$, where $T_j\neq T^\star$.

▷ **Sim-**$\mathcal{O}_K$

on input of a request Req
  if $\mathsf{Req}=(pid^\star,H(T_j))$ and $T_j\neq T^\star$
    look up the item $(T_j,r_j,Q_j,\frac{r_j}{t}x\tilde{P})$ in $\mathcal{H}_0$-List
    return $S_j=\frac{r_j}{t}x\tilde{P}$
  else if $\mathsf{Req}=(pid_i,H(T^\star))$ and $pid_i\neq pid^\star$
    look up the item $(pid_i,x^\star+x_i)$ in $\mathcal{H}$-List
    return $S_i=\frac{p(1/x)}{t/x+x_j}z\tilde{P}$

Since

$$S_j = \frac{1}{w + H_0(pid^\star)} \cdot H(T_j) = \frac{1}{t/x - x^\star + x^\star} \cdot Q_j$$
$$= \frac{x}{t} \cdot r_j \tilde{P} = \frac{r_j}{t} x\tilde{P}$$

the answer $S_j = \frac{r_j}{t} x\tilde{P}$ is a valid simulation for the query of $\mathsf{Req} = (pid^\star, H(T_j))$. At the same time, since

$$S_i = \frac{1}{w + H_0(pid_i)} \cdot H(T^\star) = \frac{1}{t/x - x^\star + x^\star + x_i} \cdot Q$$
$$= \frac{1}{t/x + x_i} \cdot p(1/x) z\tilde{P}$$

the answer $S_i = \frac{p(1/x)}{t/x+x_j} z\tilde{P}$ is also valid for the query of $\mathsf{Req} = (pid_i, H(T^\star))$. Let us define $p_i(X) = \frac{p(X)}{X+x_i}$, then $p_i(X)$ is a polynomial of degree $k-1$.

Since $(z\tilde{P}, \frac{z}{x}\tilde{P}, \frac{z}{x^2}\tilde{P}, \cdots, \frac{z}{x^k}\tilde{P})$ are given, the value of $S_i = \frac{p(1/x)}{t/x+x_j} z\tilde{P} = p_i(\frac{1}{x}) z\tilde{P}$ can be easily computed. Because the distributions of S_j, S_i are unchanged in the eye of the adversary $\mathcal{A}$, the simulation is perfect, and we have

$$\Pr[\mathbf{Guess}_3] = \Pr[\mathbf{Guess}_2] \tag{5}$$

$\mathbf{Game}_4$: In this game, we manufacture the challenge $C^\star = (C_1^\star, C_2^\star)$ by embedding the k-SPDBDH challenge $V \in \mathbb{G}_T$ in the simulation. Specifically, after flipping $b \in \{0,1\}$ and choosing a number $r^\star = \frac{y}{t} \in \mathbb{Z}_q^*$, we set the ciphertext $C_1^\star$ as

$$C_1^\star = r^\star \cdot (P_{pub} + H(pid^\star)P) = r^\star t\tilde{P} = y\tilde{P}$$

Then, the corresponding valid $C_2^\star$ should be

$$\underline{C_2^\star} = e(P, H_0(T^\star))^{r^\star} \cdot N_b^\star = e(\tilde{P}, \tilde{P})^{xp(\frac{1}{x}) z r^\star} \cdot N_b^\star$$
$$= e(\tilde{P}, \tilde{P})^{xyzp(\frac{1}{x})/t} \cdot N_b^\star$$

To solve the k-SPDBDH challenge $V \in \mathbb{G}_T$, we actually set

$$C_2^\star = V^{\rho_0/t} \cdot \prod_{i=1}^{k} V_{i-1}^{\rho_i/t} \cdot N_b^\star$$

where $\rho_0, \rho_1, \cdots$ are coefficients of $p(X)$. Then, if V in the k-SPDBDH challenge is really $e(\tilde{P}, \tilde{P})^{xyz}$, i.e., $\widetilde{b} = 0$ in the $\mathtt{Experiment}\ \mathbf{Exp}_{\mathcal{A}}^{\text{k-SPDBDH}}$, we know that

$$C_2^\star = V^{\rho_0/t} \cdot \prod_{i=1}^{k} V_{i-1}^{\rho_i/t} \cdot N_b^\star$$
$$= e(\tilde{P}, \tilde{P})^{xyz\rho_0/t} \cdot \prod_{i=1}^{k} e(\tilde{P}, \tilde{P})^{xyz\rho_i/x^i t} \cdot N_b^\star$$
$$= e(\tilde{P}, \tilde{P})^{xyzp(1/x)/t} \cdot N_b^\star = \underline{C_2^\star}$$

is a valid ciphertext. Therefore, we have

$$\Pr[\mathbf{Guess}_4 | \widetilde{b} = 0] = \Pr[\mathbf{Guess}_3]. \tag{6}$$

and

$$\Pr\left[\mathbf{Exp}_{\mathcal{A}}^{\text{k-SPDBDH}} = 1 | \widetilde{b} = 0\right] = \Pr[\mathbf{Guess}_4 | \widetilde{b} = 0] \tag{7}$$

If V in the k-SPDBDH challenge is a random element in $\mathbb{G}_T$ other than $e(\tilde{P}, \tilde{P})^{xyz}$, i.e., $\widetilde{b} = 1$ in the $\mathtt{Experiment}\ \mathbf{Exp}_{\mathcal{A}}^{\text{k-SPDBDH}}$, $C_2^\star \neq \underline{C_2^\star}$ is not a valid ciphertext, and thus is independent on b. Therefore, we will have

$$\Pr\left[\mathbf{Exp}_{\mathcal{A}}^{\text{k-SPDBDH}} = 1 | \widetilde{b} = 1\right] = \Pr[\mathbf{Guess}_4 | \widetilde{b} = 1] = \frac{1}{2}. \tag{8}$$

As a result, from Eqs. (2)-(8), we have

$$\mathbf{Adv}_{\mathcal{A}}^{\text{k-SPDBDH}} = \left| \Pr\left[\mathbf{Exp}_{\mathcal{A}}^{\text{k-SPDBDH}} = 1 | \widetilde{b} = 0\right] \right.$$
$$\left. - \Pr\left[\mathbf{Exp}_{\mathcal{A}}^{\text{k-SPDBDH}} = 1 | \widetilde{b} = 1\right] \right| \tag{9}$$
$$\geq \left| \frac{\epsilon}{2} + \frac{1}{2} - \frac{1}{2} \right| = \frac{\epsilon}{2}$$

In addition, we can obtain the claimed bound for $\tau' \leq \tau + \Theta(.)$ in the sequence games. Thus, the proof is completed. □

Theorem 2. The proposed SSH scheme is impersonator resistant.

PROOF. Based on Theorem 1, if U_j has different illness from U_i, i.e., $\mathsf{sym}(U_j) \neq \mathsf{sym}(U_i)$, U_j can't produce the valid Auth_j, thus U_i can identify U_j is not the one who has the same symptom. Thus, the impersonator resistance follows. □

Theorem 3. The proposed SSH scheme is detector resistant.

PROOF. Similarly, based on Theorem 1, if U_j has different illness from U_i, i.e., $\mathsf{sym}(U_j) \neq \mathsf{sym}(U_i)$, U_j has no private key S_j with respect to $\mathsf{sym}(U_i)$. Then, when U_j receives Auth_i from U_i, he can't determine whether it is valid or not. Therefore, U_i has no idea on what symptom U_i has. As a result, the detector resistance is achieved. □

5. PERFORMANCE EVALUATION

In this section, we use a custom simulator built in Java to study the effectiveness of MHSN in terms of PHI collaborative reporting application. The performance metric used in the evaluation is the average PHI reporting delay (PRD), which is defined as the average time between when a PHI is generated and when it is successfully relayed to the eHealth center.

5.1 Simulation Settings

In the simulation, 80 mobile patients and 5 APs are first uniformly deployed in an area of 1,000 m × 1,000 m, as shown in Fig. 3-(a). Each patient U_i equipped with implantable/wearable body sensor nodes and a PDA device with a transmission radius of 30 meters to simulate a MHSN. Among these patients, 40 patients have the symptom T_1 and form group $\mathcal{G}_1$, and the other 40 patients have the symptom T_2 and form group $\mathcal{G}_2$. Let $\rho = \frac{\text{the number of sociable patients}}{\text{the number of patients in group}}$ be the social ratio of a group. In the simulation, we assume both $\mathcal{G}_1$ and $\mathcal{G}_2$ have the same social ratio $\rho = [0, 0.1, 0.2, 0.3, 0.4]$. Since each AP has a reliable and fast connection with the eHealth center, we consider the time when a PHI is relayed to AP roughly as the time when it reaches the eHealth center in the simulation.

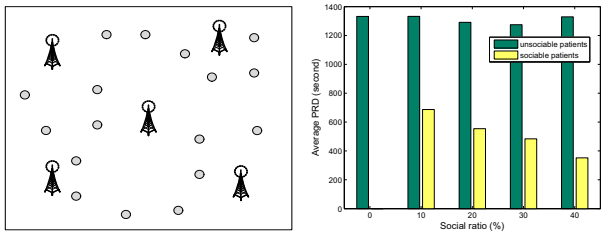
Mobility model. The performance of PHI reporting is highly contingent upon the mobility of patients. Here, we assume all patients follow the same *mobility model*. Specifically, each patient first randomly chooses a destination in the area, and gets there using the shortest route with the

velocity $v = 1 \pm 0.3$ m/s. After reaching the destination, with 2-minute pause time, the patient randomly chooses a new destination and repeats the above.

The detailed parameter settings in the simulations are summarized in Table 1. We perform the experiments for the specified social ratio ρ varying from 0 to 0.4 with increment of 0.1. For each case, we run the simulation 10 times, and the average PRD is reported.

Table 1: Simulation Settings

Parameter	Setting
Simulation area	$1,000$ m $\times$ $1,000$ m
Simulation duration	120 minutes
Number of APs, patients in $\mathcal{G}_1$, $\mathcal{G}_2$	5, 40, 40
Patient velocity	1 ± 0.3 m/s
Social ratio	$\rho = [0, 0.1, 0.2, 0.3, 0.4]$
PDA storage, transmission	100 M, 50 m
PHI generation interval, size	10 minutes, 5 Kbytes



(a) simulation area (b) simulation result

Figure 3: Simulation area and result with average PRD in different social ratios within 120 minutes

5.2 Simulation Results

Fig. 3-(b) shows the average PRD between the sociable patients and unsociable patients within 120 minutes with different social ratios. From the figure, we can see the average PRD of sociable patients is obviously less than those of unsociable patients. The higher the social ratio ρ, the lower the PRD. These results demonstrate that the MHSN has positive affect on PRD, and can be accepted by the mobile patients.

6. RELATED WORK

Research on mobile social network (MSN) has grown tremendously recently. A typical example is pocket switched network (PSN), which can be regarded as one kind of MSN where users can exchange data related movie, news, and any interesting information etc. using their PDA device. However, most existing works on PSN are geared towards new communication architecture, protocol, or fundamental analysis, but pay less attention on security issues in social connection [9]. Because eHealthcare systems take particularly attention on security and privacy issues, ordinary PSN can't be directly applied to MHSN, if the security issue, i.e., secure handshake, is not resolved.

Secret handshake was introduced recently by Balfanz et al [2], is a useful cryptographic mechanism which allows two members of the same group to authenticate each other secretly. Therefore, secret handshake mechanism can certainly be applied to PSN to achieve MHSN. Over the past years, several secret handshake schemes have been proposed [12, 11]. However, due to lack of provable security, some of them are shown insecure, and other signature-based schemes are not efficient. Our proposed same-symptom-based handshake (SSH) scheme belongs to the secret handshake, but it is dedicated to mHealthcare system. Most importantly, it is efficient and provably secure.

7. CONCLUSION

Secure same-symptom-based handshake (SSH) is of vital importance to the success of MHSN, yet it hasn't been paid great attention. In this paper, based on the bilinear pairings, we have proposed an efficient SSH scheme for MHSN. With the provable security technique, the proposed SSH scheme has been demonstrated to be secure in the MHSN scenarios. Since the proposed SSH scheme won't disclose each other's symptom information if two patients don't have same symptom, MHSN can be widely accepted by patients, so that they can enjoy the benefits brought by MHSN, such as eliminating the loneliness in our aging society and collaborative PHI reporting in mobile environment.

8. REFERENCES

[1] Appari, A., Johnson, M. E., and Anthony, D. L. HIPAA compliance in home health: A neo-institutional theoretic perspective. In *SPIMACS '09* (2009), pp. 13–20.

[2] Balfanz, D., Durfee, G., Shankar, N., Smetters, D., Staddon, J., and Wong, H. Secret handshake from pairing-based key agreements. In *IEEE S&P '93* (2003), pp. 180–196.

[3] Bellare, M., and Rogaway, P. Random oracles are practical: A paradigm for designing efficient protocols. In *CCS '93* (1993), pp. 62–73.

[4] Boneh, D., and Franklin, M. Identity-based encryption from the weil pairing. *SIAM J. Comput. 32*, 3 (2003), 586–615.

[5] Izabachene, M., and Pointcheval, D. New anonymity notions for identity-based encryption. In *SCN '08* (2008), LNCS 5229, pp. 375–391.

[6] Kotz, D., Avancha, S., and Baxi, A. A privacy framework for mobile health and home-care systems. In *SPIMACS '09* (Chicago, Illinois, USA), pp. 1–12.

[7] Liang, X., Lu, R., Lin, X., and Shen, X. Patient self-controllable access policy on PHI in ehealthcare systems. In *AHIC 2010* (Kitchener, Ontario, Canada).

[8] Lin, X., Lu, R., Shen, X., Nemoto, Y., and Kato, N. SAGE: A strong privacy-preserving scheme against global eavesdropping for ehealth systems. *IEEE J. Selected Areas of Communications 27* (2009), 365–378.

[9] Pietilainen, A.-K., and Diot, C. Social pocket switched networks. In *INFOCOM'09* (Rio de Janeiro, Brazil, 2009), pp. 403–404.

[10] Shoup, V. OAEP reconsidered. *J. of Cryptology 15*, 4 (2002), 223–249.

[11] Su, R. On the security of a novel and efficient unlinkable secret handshakes scheme. *IEEE Comm. Letters. 13*, 9 (2009), 712–713.

[12] Zhou, L., Susilo, W., and Mu, Y. Three-move secret handshakes. In *ISPEC 2006* (2006), LNCS 3903, pp. 332–342.