Information Sciences 314 (2015) 255–276

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks

Jun Zhou [a], Zhenfu Cao [a,b,*], Xiaolei Dong [a,b,*], Naixue Xiong [c], Athanasios V. Vasilakos [d]

[a] Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China
[b] Software Engineering Institute, East China Normal University, Shanghai, China
[c] School of Computer Science, Colorado Technical University, USA
[d] Department of Electrical and Computer Engineering, National Technical University of Athens, Greece

ARTICLE INFO

Article history:
Received 25 August 2013
Received in revised form 26 August 2014
Accepted 7 September 2014
Available online 17 September 2014

Keywords:
Key management
Cloud-assisted WBAN
Mobile attack
Security
Privacy
M-healthcare social network

ABSTRACT

Cloud-assisted wireless body area networks (WBANs) significantly facilitate efficient patient treatment of high quality, unfortunately in the meanwhile greatly challenge the patient's data confidentiality and privacy. The existing work mainly focused on the traditional scenario where patients securely stay indoors. In this paper, we consider a more practical situation of cloud-assisted WBANs in m-healthcare social networks where patients traverse among blocks outdoors and WBANs are more vulnerable to sophisticated attacks including even node compromise attack. To solve the problem, a secure and privacy-preserving key management scheme resilient to both time-based and location-based mobile attacks is proposed by the cooperation of the mobile patients in the same social group for both hierarchical and distributed environment. It also protects patient's identity privacy, sensor deployment privacy and location privacy by exploiting the blinding technique and embedding human body's symmetric structure into Blom's symmetric key mechanism with modified proactive secret sharing. Especially, the computationally-intensive privacy-preserving key material updating is outsourced to the cloud server and the unchanged pairwise keys after key material updating dramatically saves the resources for energy-constrained WBANs. Finally, the security analysis and simulation results show our scheme far outperforms the previous ones in terms of resisting mobile attacks and storage, computation and communication overhead.

1. Introduction

M-healthcare social network has been increasingly adopted by healthcare providers all over the world owing to its great convenience and efficiency brought about to both patients and healthcare providers [16,20,31]. Wireless body area networks (WBANs) are pre-deployed on, in and/or around patients to monitor and collect personal health information (PHI) timely. The body sensors, the body sensor deployed locations and their work mode are determined by the diseases suffered from by the patients. The PHI monitored by WBANs can be efficiently collected to the patient's hand-held data sink (PDAs),

* Corresponding authors at: Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China.
E-mail addresses: zhoujun_tdt@sjtu.edu.cn (J. Zhou), zfcao@cs.sjtu.edu.cn (Z. Cao), dong-xl@cs.sjtu.edu.cn (X. Dong), nxiong@coloradotech.edu (N. Xiong), vasilako@ath.forthnet.gr (A.V. Vasilakos).

http://dx.doi.org/10.1016/j.ins.2014.09.003
0020-0255/

transmitted through the internet and accessed by the authorized physicians in healthcare providers to give precise medical treatment. Owing to the large number of patients and the high frequency of PHI sampling, a huge amount of medical data is required to be scalably stored and computed on demand. The cloud computing system can satisfy the above-mentioned requirements, and well bridge the resource-constrained body sensors and the supercomputers (cloud servers) to push the storage and computationally-intensive tasks to the cloud side, prolonging the lifetime of the body sensors and providing auxiliary medical services in a "pay-per-use" manner. More significantly, the personal health information is extremely private for the patients and required to be well protected from exposure to both the unauthorized entities (malicious adversaries) and the honest-but-curious cloud servers that would perfectly execute the protocol specifications, but simultaneously extract secret information of personal health information and/or kinds of patients' privacy from the interactions with the patients and the healthcare provider.

However, lacking an appropriate security or privacy mechanism, personal health information will be exposed to various kinds of threats such as eavesdropping, modifying and injecting messages to result in wrong medical diagnosis and treatment, spoofing the patients' identities/locations to mislead the medical rescue and even sponsoring node compromise attack to extract all the private medical information stored in the resource-constrained body sensors. Therefore, it is crucial to guarantee both the patients' personal health data security and identity/location privacy in WBANs before m-healthcare social network is widely adopted and reaches its full flourish. Due to the vulnerability about data confidentiality and patient privacy in WBANs, key management in WBANs has provided a convincing solution to secure the wireless communication channels for m-healthcare social networks.

Key management in wireless sensor networks has been thoroughly studied and a series of protocols have been proposed to establish the secure communication between sensor nodes such as E–G scheme [11], q-composite scheme [6] and Zhou's scheme [48]. However, it is necessary in the traditional solutions to perform key material pre-distribution before key agreement, which takes considerable storage and computational overhead on body sensors and violates the principle of "plug-and-play" on resource-constrained WBANs. The existing key exchange schemes [2,8,22,26,32,37,41,43–47] proposed in WBANs mainly focused on exploiting the underlying biometric characteristics to establish the authenticated pairwise keys between body sensors. Unfortunately, only the static environment where the patients are conventionally assumed to securely stay at home or hospital is considered, neglecting a more practical scenario where the patients experiencing ECG or EEG examinations can behave as the ordinary persons moving outdoors from time to time and place to place. More seriously, in the latter situation, since the mobile patients are exposed in public, both the body sensors and data sinks (PDAs) of their WBANs are vulnerable to sophisticated cyber attacks and even node compromise attack.

On the other hand, to realize the lightweight key updating for cloud-assisted WBANs, it is required to devise a secure and efficient privacy preserving outsourcing computation scheme supporting both addition and multiplication operations. However, quite a number of outsourcing computation schemes only support one kind of computation (either addition or multiplication operation) and the existing outsourcing computation supporting both computations heavily depends on the fully homomorphic encryptions which bring about huge amount of computational cost out of the tolerance of WBANs. Therefore, how to devise a lightweight secure and privacy preserving key management for cloud-assisted WBANs in m-healthcare social networks is still a challenging problem.

In this paper, by taking advantage of the cooperation among the patients suffering from the same diseases who are generally assumed to constitute a social group for discussing the shared health conditions, exchanging medical care experiences, and providing mutual supports with privacy preservation for each other, a secure and privacy-preserving key management scheme for cloud-assisted WBANs in m-healthcare social networks resilient to both time-based and location-based mobile attacks is proposed in the hierarchical and distributed environments respectively. All the mobile adversaries are assumed to possess the ability to compromise fixed number of body sensors in each time period (i.e. the fixed number is no more than the threshold predefined by the underlying WBAN since once the number of compromised sensors exceeds the threshold, the adversary would be discovered by the intrusion detection system and revoked from WBAN) and can be divided into two categories. The first category is intended to compromise more than the threshold number of body sensors during different time periods from a fixed block (location) to compute all other pairwise keys established among innocent sensors; while the second category plans to achieve the same goal by compromising body sensors in a single time period from different blocks. We define the former one as time-based mobile adversary while the latter one as location-based mobile adversary. To the best of our knowledge, it is the first time to consider mobile attacks w.r.t. key management for cloud-assisted WBANs in m-healthcare social networks. The main contributions of this paper are presented as follows:

(1) A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks 4S is proposed. It can resist both time-based and location-based mobile attacks by the cooperation of the patients suffering from the same diseases in the same social group.
(2) Body's symmetric structure is integrated with the underlying Blom's symmetric key establishment mechanism to provide key materials. By exploiting the technique of proactive secret sharing, all the established pairwise keys in WBANs remain unchanged after the computationally-intensive key material updating performed by the cloud server. The property of key updating requiring no additional computation overhead on resource-constrained body sensors well adapts to WBANs.

(3) Identity privacy, body sensor deployment privacy and patient location privacy can be well protected by introducing identity blinding matrices, and embedding body sensors' deployed positions and patient's location information into the pairs of symmetric positions and the diagonal line of the private symmetric matrix (key material of the modified Blom's symmetric key establishment mechanism).
(4) It can be straightforwardly extended to the biometric characteristic based counterpart, not requiring any pre-distribution information during deployment. Security analysis and simulation results show our proposed 4S far outperforms the existing constructions in resilience and storage, computation and communication overhead.

The rest of this paper is organized as follows. In the next section, some related work is presented. In Section 3, we illustrate the network architecture and the adversary model of key establishment for cloud-assisted WBANs in m-healthcare social networks. Then, a secure and privacy-preserving key management scheme resisting mobile attacks for WBANs is proposed in Section 4, followed by the security analysis and performance evaluations in Section 5 and Section 6 respectively. Finally, we draw the conclusion in Section 7.

2. Related work

Secure and efficient pairwise key agreement in sensor networks has been profoundly studied [6,11,27–30,40,46] such as E–G scheme [11], q-composite scheme [6], Liu's and Zhou's schemes based on symmetric polynomials [28,48]. However, these symmetric key exchange schemes require a quantity of key pre-distribution materials and symmetric key computation executions. Therefore, they are not satisfied with the requirement of increasingly size-enlarged WBANs for incurring considerable latency especially in the emergent cases. In addition, excessive storage and computational overhead also do not meet the power constraint of body sensors and significantly shorten their life spans. On the other hand, the asymmetric technologies using PKC such as authenticated Diffie–Hellman key exchange scheme [5,21,42,48] are also energy-consuming and dissatisfy the lightweight requirement of WBANs.

Fortunately, a series of research work on deploying WBANs applications with integration to WBAN cloud [12–15] and constructing secure biometric-based key exchange schemes in WBANs [2,8,22,26,32,37,41,43–47] have been proposed. Fortino et al. developed SPINE2 for WBAN applications on heterogeneous sensor nodes [13,14] and further integrated cloud computing into body sensor networks [12,15]. Cherukuri et al. suggested to use physiological parameters with higher level of entropy such as blood glucose, blood pressure and body temperature to establish the key for WBANs [8]. To overcome the slight variations of the biometric traits captured at different parts of the body, a key distribution scheme based on fuzzy commitment [23] was proposed by Bao et al. to secure the key transmission with error-tolerant capability [2]. Venkatasubramanian et al. proposed PSKA [37], which allows neighboring nodes in a WBANs to agree to a symmetric cryptographic key in an authenticated manner, using the technique of fuzzy fault [36] and physiological signals without initialization or pre-deployment. Zhou et al. proposed a secure and efficient biometric based deterministic key agreement scheme BDK in WBANs [44]. It for the first time reduced the security of key agreement in WBANs to the underlying one-way trapdoor function rather than the coffer/vault size with dramatically lower computational, communication and storage overheads. All these key agreement schemes proposed above can well adapt to the usable security of a plug-n-play and largely transparent WBAN.

However, the state-of-the-art mainly emphasizes on the key agreement in WBANs w.r.t. the home environment where the security of WBANs is highly guaranteed [2,8,26,34,37]. While in reality, patients wearing WBANs for regular dynamic ECG or EEG examinations can move and behave in public the same as ordinary persons in m-healthcare social networks [7,35,38] where body sensors are exposed and much more vulnerable to sophisticated attacks and even node compromise attack. It significantly challenges our design in this new adversary model. Due to the patients' mobility, those suffering from the same disease can frequently contact with each other and share their health conditions and experiences to provide mutual support and encouragement [30]. Wang et al. proposed a security framework of body sensor networks for mobile health monitoring [39]. Ren et al. presented several techniques that can be used to monitor patients efficiently and enhance the security of m-healthcare systems in [33]. Unfortunately, further concrete constructions have not been proposed. Another challenge is that the traditional proactive key distribution techniques based on Shamir's secret key sharing [19] cannot be directly applied, since the cost of assigning each body sensor with a t-degree polynomial and the associated interpolation operations would essentially exceed the tolerance of body sensors, not to mention protecting the patients' identity and location privacy.

On the other hand, the existing outsourcing computation supporting both additive and multiplicative operations heavily relies on the fully homomorphic encryptions which also bring about huge amount of computational cost out of the tolerance of the WBANs. Gentry et al. proposed a fully homomorphic encryption using ideal lattices [17] and an i-hop homomorphic encryption by designing a re-randomizable Yao circuits [18]. Dijk et al. proposed a fully homomorphic encryption over integers [9]. However, most recently, Lauter et al. pointed out [25] that the complexity of existing fully homomorphic encryptions is still too high to be practical, even though possible number of multiplications are sacrificed for efficiency. Barbosa et al. proposed a general framework of designing delegatable homomorphic encryption with applications to secure outsourcing of computation with correctness verification [3]. Therefore, how to exploit biometric characteristics and the properties of

m-healthcare social networks to design a lightweight privacy-preserving key management scheme for cloud-assisted WBANs is the challenging problem requiring our solutions.

3. Network architecture and adversary model

3.1. Network architecture

It is assumed that the whole city is divided into various blocks in m-healthcare social networks. A great many unseverely-conditioned patients under regular medical monitoring such as electrocardiogram (ECG) and Electroencephalography (EEG) can move from block to block in public as ordinary persons [7,35,38]. Upon each patient, a WBAN is deployed and the collected personal health information will be aggregated to a mobile device, namely the data sink held by the patient. Fig. 1 illustrates the architecture of the hierarchical cloud-assisted m-healthcare social network. The whole district is divided into 12 blocks, namely $A, B, \ldots, L$. A block manager is deployed in the center of each block, responsible for collecting personal health information from local patients' mobile devices (hand-held data sinks) and transmitting it to the healthcare provider. Local patients are those currently located in the block manager's block. It is a reasonable assumption since the healthcare provider generally deploys several community healthcare centers in its adjacent blocks for convenience [20] and they can serve the function as block managers. The block manager also takes responsibility of uploading and distributing the (blinded) private key materials to and from the cloud server for local patients; while the cloud server performs the actual key updating computation.

In distributed cloud-assisted m-healthcare social networks, private personal health information and key updating materials are transmitted cooperatively by the patients themselves without the help of block managers. All the patients suffering the same disease with their mobile devices (data sinks) in each other's transmission range maintain the social group for data transferring and key updating (i.e. the patients suffering from the same disease can frequently contact with each other in the same social group to share their health conditions, medical care experiences and providing mutual supports without privacy

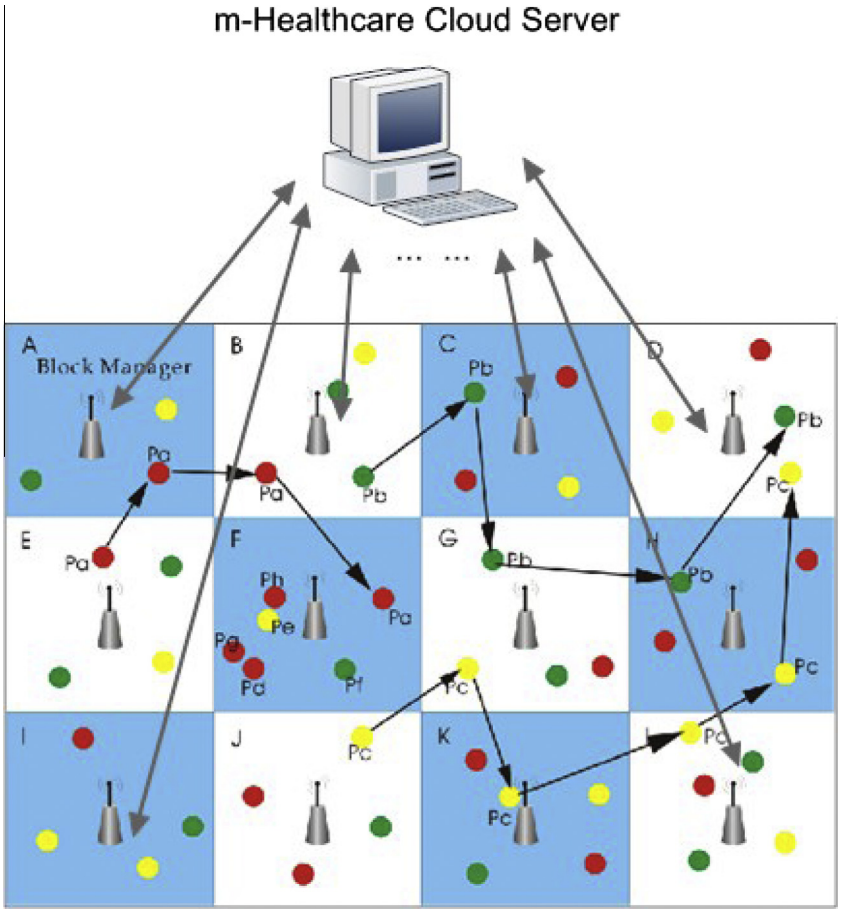

Fig. 1. Architecture of cloud-assisted m-healthcare social networks.

leakage). For example, in Fig. 1, the moving routine of patient P_a can be described as $E \rightarrow A \rightarrow B \rightarrow F$. Patients with the same color represent those that are suffering from the same disease (possessing the same symptoms) and the WBANs deployed on them are under the same work mode (i.e. monitoring the same set of physiological characteristics and possessing the same sensor deployment positions).

3.2. Adversary model

In cloud-assisted m-healthcare social networks, since the mobile patients behave as the ordinary persons in the open area, it is assumed that the energy-constrained body sensors are vulnerable to a variety of attacks and even node compromise attack. The adversary can sponsor compromise attack by extracting from PDAs all the private information including the secret key used to encrypt the PHI, the private key to generate signatures and other key establishment materials, re-programming the PDAs or replacing them with malicious ones under the control of the adversary. If a body senor is compromised by an adversary, all the key materials stored in it will be exposed. The resource-constrained mobile device held by each patient is less vulnerable to the mobile attacks and the block managers are full of resources and cannot be compromised by the adversary since the community healthcare centers can always be trusted. It is also assumed that there exists a secure communication channel established among data sinks and block managers through authenticated Diffie–Hellman key exchange protocol [5]. Now, we can formally define two kinds of mobile attacks as follows.

3.2.1. Time-based mobile attack

Assuming even though the adversary sponsors time-based mobile attacks on one specific patient in time slots $t_1, t_2, \ldots, t_n$ in one fixed block L, he can still not have any knowledge about the pairwise keys established between the innocent body sensors. $\mathbb{C}_{t_i,L}(i = 1, 2, \ldots, n)$ denotes the set of compromised body sensors during each time slot t_i in one specific block L. It is assumed that $|\mathbb{C}_{t_i,L}| \leqslant \lambda$ and $\lambda + 1$ is the threshold of the underlying pairwise key establishment scheme. If no less than threshold number of body sensors were compromised, all the pairwise keys would be exposed. In the cloud-assisted WBANs, there exist efficient intrusion detection mechanisms [1,24] to guarantee that once no less than threshold number of body sensors are compromised in one specific time slot, the compromised body sensors would be revoked from the underlying WBANs and can never be further exploited by the adversary to derive the pairwise keys established among the innocent body sensors. Therefore, time-based mobile attack is a new kind of attack trying to compromise the pairwise keys established among innocent body sensors without being discovered by existing intrusion detection mechanisms. Specifically speaking, even though the mobile adversary is restricted to compromise $|\mathbb{C}_{t_i,L}| \leqslant \lambda$ body sensors in each time slot, he tries to combine the private key materials extracted from the compromised body sensors in a series of different time slots satisfying $\sum_{i=1}^{n} |\mathbb{C}_{t_i,L}| \geqslant \lambda + 1$ (the threshold) to deduce the innocent pairwise keys in WBANs. It is defined that a pairwise key establishment scheme in WBANs is unconditionally secure against time-based mobile attack, if and only if

$$H\left(Key_{\mathbb{N}\setminus\mathbb{C}_{t_1,L}\bigcup\cdots\bigcup\mathbb{C}_{t_n,L}} | Key_{\mathbb{C}_{t_1,L}\bigcup\cdots\bigcup\mathbb{C}_{t_n,L}}\right) = H(Key_{\mathbb{N}\setminus\mathbb{C}_{t_1,L}\bigcup\cdots\bigcup\mathbb{C}_{t_n,L}}), \tag{1}$$

where $H(\cdot)$ here represents the information entropy, $\mathbb{N}$ denotes the set of body sensors deployed on the patient and $\mathbb{N} \setminus \mathbb{C}_{t_1,L} \bigcup \cdots \bigcup \mathbb{C}_{t_n,L}$ denotes the set including all the elements not in set $\mathbb{C}_{t_1,L} \bigcup \cdots \bigcup \mathbb{C}_{t_n,L}$ but in set $\mathbb{N}$, namely the set of innocent body sensors. Eq. (1) illustrates the knowledge the time-based mobile adversary exploited in the sets of compromised body sensors $\mathbb{C}_{t_1,L}, \ldots, \mathbb{C}_{t_n,L}$ in a series of time slots $t_1, \ldots, t_n$ from one specific block L cannot provide him any additional information to deduce the pairwise keys established among innocent body sensors.

3.2.2. Location-based mobile attack

Assuming the patient moves among different blocks $l_1, l_2, \ldots, l_n$ in one specific time slot T, even though the adversary sponsors location-based mobile attacks to one specific patient in blocks $l_1, l_2, \ldots, l_n$ in one specific time slot T, he can still not have any knowledge about the pairwise keys established between innocent body sensors. $\mathbb{C}_{l_i,T}(i = 1, 2, \ldots, n)$ denotes the set of compromised sensors in each block l_i during one specific time slot T. It is assumed that $|\mathbb{C}_{l_i,T}| \leqslant \lambda$ to prevent being detected by the intrusion mechanism [1,24] in WBANs and $\lambda + 1$ is the threshold of the underlying pairwise key establishment scheme. If no less than threshold number of body sensors were compromised, all the pairwise keys would be exposed. As a counterpart of the time-based mobile attack, the location-based mobile attack aims to combine the private key materials extracted from the compromised body sensors in a series of different locations (blocks) satisfying $\sum_{i=1}^{n} |\mathbb{C}_{l_i,T}| \geqslant \lambda + 1$ (the threshold) to deduce the innocent pairwise keys in WBANs without being caught by existing intrusion detection mechanisms. It is defined that a pairwise key establishment scheme in WBANs is unconditionally secure against location-based mobile attack, if and only if

$$H(Key_{\mathbb{N}\setminus\mathbb{C}_{l_1,T}\bigcup\cdots\bigcup\mathbb{C}_{l_n,T}} | Key_{\mathbb{C}_{l_1,T}\bigcup\cdots\bigcup\mathbb{C}_{l_n,T}}) = H(Key_{\mathbb{N}\setminus\mathbb{C}_{l_1,T}\bigcup\cdots\bigcup\mathbb{C}_{l_n,T}}), \tag{2}$$

where $H(\cdot)$ here represents the information entropy, $\mathbb{N}$ denotes the set of body sensors deployed on the patient and $\mathbb{N} \setminus \mathbb{C}_{l_1,T} \bigcup \cdots \bigcup \mathbb{C}_{l_n,T}$ denotes the set including all the elements not in set $\mathbb{C}_{l_1,T} \bigcup \cdots \bigcup \mathbb{C}_{l_n,T}$ but in set $\mathbb{N}$, namely the set of innocent body sensors. Eq. (2) illustrates the knowledge the location-based mobile adversary exploited in the sets of

compromised body sensors $\mathbb{C}_{l_1,T},\ldots,\mathbb{C}_{l_n,T}$ from a series of time blocks $l_1,\ldots,l_n$ in one specific time slot T cannot provide him any additional information to deduce the pairwise keys established among innocent body sensors. It is observed that the definition of the mobile adversary simultaneously launching two kinds of mobile attacks can be straightforwardly derived and the threshold can be adjusted according to the attacks sponsored by the adversary and the security level required by the system.

4. Our scheme

In this section, for cloud-assisted WBANs in m-healthcare social networks, pairwise key establishment, pairwise key updating for both time-based and location-based attacks, pairwise key updating for switching work mode, pairwise key updating in the distributed environment and group key agreement in WBANs are respectively proposed.

4.1. Pairwise key establishment

Our scheme is constructed by integrating the body's symmetric structure with the underlying Blom's symmetric key construction [4]. Fig. 2 illustrates the pairwise key establishment for WBANs in our construction. Due to body's symmetric structure, body sensors for medical cares such as ECG and EEG are generally deployed symmetrically on patients to monitor the vital signs [7,35,38]. For the scenarios where body sensors are required to be deployed asymmetrically, we can simply duplicate one data element into its correspondingly symmetric position in the private symmetric matrix D_{P_s}. (i.e. if only one body sensor is deployed on the left chest for medical care, it is required to pad $H_0(CHEST)$ to both elements $D_{P_s}(i,j)$ and $D_{P_s}(j,i)$ such that $D_{P_s}(i,j)=D_{P_s}(j,i)=H_0(CHEST)$ to compose the private symmetric matrix D_{P_s} as explained below). The patients suffering from the same disease can constitute a social group to communicate with each other for discussing their medical care experiences and provide mutual support. (i.e. it is noted that since they are suffering from the same disease, it is likely for them to well protect the privacy of each other. For the consideration of utilization and privacy preservation, patients suffering from different diseases are not allowed to communicate with each other). Patients belonging to the same social group have their WBANs working under the same mode with their body sensors deployed on the same positions. It is assumed that there are N patients $P_s(s=1,2,\ldots,N)$ suffering from the same disease and the associated data sinks are denoted by $DS_s(s=1,2,\ldots,N)$. The pairwise key establishment scheme can be described as follows. Table 1 illustrates the notations used in our construction.

Step 1. Before a set of N_s body sensors $BSR_{s,k}(k\in\{1,\ldots,N_s\})$ is deployed on patient P_s for specific diseases, the physician stores the symmetric sensor position information into the private symmetric matrix D_{P_s} in the hand-held data sink owned by the patient as follows. Taking the ECG monitoring for example, a pair of body sensors would be deployed respectively on the

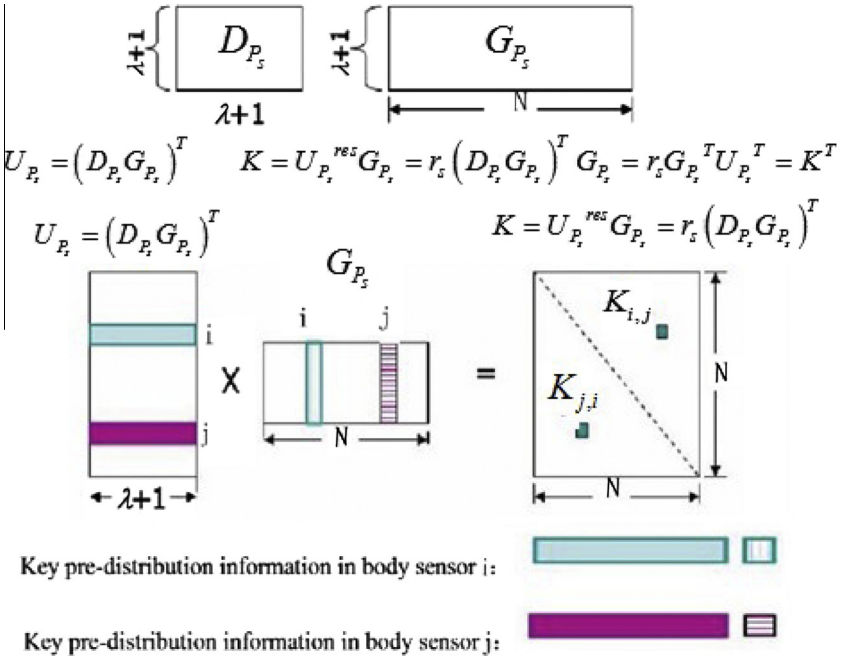

Fig. 2. Pairwise key establishment for WBANs.

Table 1
Notations in our scheme.

Notation	Description
D_{P_s}	$(\lambda+1,\lambda+1)$-Private symmetric matrix storing location and body sensor deployment information of patient P_s
DS_s	Hand-held data sink on patient P_s
$P_{s,k}$	The k-th body sensors deployed on patient P_s
H_0, H_1	Hash functions mapping $\{0,1\}^* \to \mathbb{G}_p$ and $\{0,1\}^* \to \mathbb{G}_p^{\lambda+1}$ Respectively
G_{P_s}	$(\lambda+1, N_s)$-Public identity matrix for N
U_{P_s}	$(N_s,\lambda+1)$-Private initial key material matrix
$U_{P_s}^{res}$	$(N_s,\lambda+1)$-Blinded key material matrix
$K(i,j)$	The element at the i-th row and j-th column of matrix key matrix K

left and right chest of the patient two at a time [7,38]. There exists a hash function $H_0 : \{0,1\}^* \to \mathbb{G}_p$ mapping the string 'CHEST' to a pair of symmetric elements in the private matrix D_{P_s}.

$$D_{P_s}(i,j) = D_{P_s}(j,i) = H_0(Loc_{BSR_{s,k}}), \tag{3}$$

where $Loc_{BSN_{s,k}}, D_{P_s}(i,j)(i \neq j \wedge i,j \in \{1,\ldots,\lambda+1\})$ denotes each body sensor's position information on patient P_s and the element located at the intersection of the i-th row and j-th column in D_{P_s}. The unfilled pairs of symmetric elements in D_{P_s} are not associated to any body sensors, initially randomized by the same value $D_{P_s}(i,j)(i \neq j) = D_{P_s}(j,i) = r_{i,j \in_R} \mathbb{G}_p$ and reserved for the future use.

Step 2. Each data sink DS_s determines the patient P_s's block location by GPS service. Then, the location information of the patient, namely the block where the mobile patient is located, can be represented by the $\lambda+1$ elements in the diagonal line of the private symmetric matrix D_{P_s} as follows

$$D_{P_s}(i,j)(i = j \wedge i,j \in [1,\lambda+1]) = H_1(Loc_{P_s}), \tag{4}$$

where Loc_{P_s} represents the patient's block location information and $H_1 : \{0,1\}^* \to \mathbb{G}_p^{\lambda+1}$ maps patient's location information to $\lambda+1$ elements in the diagonal line of D_{P_s}. Until now, the private symmetric matrix D_{P_s} has been completely constructed. The mobile patients suffering from the same disease in each block possess the same D_{P_s}.

Step 3. The data sink calculates the initial key material matrix as $U_{P_s} = (D_{P_s} G_{P_s})^T$, where the columns of G_{P_s} represent the identities of body sensors. It is noted that though deployed on different patients, body sensors located on the same body position under the same work mode have the identical identities (i.e. they are serving the same function of monitoring specific healthcare information such as heartbeat). The block manager can differentiate the personal health information from different mobile patients by concatenating the patient identities (i.e. the identities of the mobile data sinks) with the identities of the body sensors.

Step 4. Each data sink DS_s selects a private key $r_s \in \mathbb{G}_p (s = 1,2,\ldots,N)$ and computes the blinded private key material matrix $U_{P_s}^{res}$ as follows.

$$U_{P_s}^{res} = r_s U_{P_s} (s = 1,2,\cdots,N). \tag{5}$$

By introducing the private keys $r_s \in \mathbb{G}_p (s = 1,2,\ldots,N)$, the established pairwise keys will vary from patient to patient suffering from the same disease in each block. Then, each body sensor can be privately pre-distributed by one corresponding row in $U_{P_s}^{res}$.

Step 5. Body sensors i and j can establish pairwise keys according to Blom's symmetric key construction [4] as follows,

$$K(i,j) = U_{P_s}^{res}(i) G_{P_s}(j) = U_{P_s}^{res}(j) G_{P_s}(i) = K(j,i), \tag{6}$$

where $U_{P_s}^{res}(i), G_{P_s}(j), K$ denotes the i-th row, j-th column in $U_{P_s}^{res}, G_{P_s}$ and the key matrix respectively. The identity of the data sink DS_s can also be included in the matrix G_{P_s} to allow it to establish pairwise keys with body sensors.

Remark 1. The security of the proposed pairwise key establishment scheme can be straightforwardly derived from the Blom's symmetric key construction [4]. The purpose of using r_s is to protect the body sensors deployed at the same position as the compromised one on other patients suffering from the same disease from exposure. Furthermore, the secure communication channel among data sinks and block managers can be utilized to securely realize the cross-patient communication within the same social group of mobile patients suffering from the same diseases afterwards. Finally, our scheme can be directly applied on the biometric based constructions if we replace the location information in D_{P_s} by the biometrically measured values. It can still works since the biometrically measured values such as the interval pulse and blood pressure are also symmetrically distributed on pairs of patient body positions and for different patients suffering from the same disease, the values of the same biometrically measured characteristic would fall into a specific range [7,35,38] with a high probability. The techniques in [2,8,37] can be utilized to tackle the problem of biometric data discrepancy and no pre-distribution is needed for WBAN deployment.

4.2. Pairwise key updating for mobile attacks

The pairwise key updating in our scheme can be divided into two cases resisting time-based mobile attacks and location-based mobile attacks. It is assumed that the block manager (i.e. the community healthcare center) knows the diseases of his local patients, therefore the private symmetric matrix D_{P_s} of each local patient can be appropriately assigned in the registration phase when he enters the block. It is noted that the community healthcare center (block manager) is only required to generate the identity blinding matrices for mobile patients and relieved (off-line) from the computationally-intensive key updating which is performed by the cloud server. In this subsection, both the key updating schemes resilient to time-based and location-based mobile compromise attacks are proposed in a hierarchical architecture. It will be observed in our extension to the distributed environment, the block manager can be completely avoided to the off-line status in the key updating. We believe both hierarchical and distributed constructions are valuable depending on different m-healthcare social network models. The symptoms-matching patients suffering from the same disease are reasonably assumed to constitute a social group and have the incentive to cooperatively fulfill the task of key updating [39].

4.2.1. Updating for time-based mobile attacks

In key updating for time-based mobile attacks in cloud-assisted WBANs, our goal is to invalidate the combination of private key materials extracted from the compromised body sensors in a series of different time slots to effectively deduce the established pairwise keys among innocent body sensors by exploiting the technique of proactive secret sharing. Besides, all kinds of patient's privacy is required to be well protected and the computationally-intensive key updating is outsourced to the cloud server to significantly save energy for resource-constrained body sensors. The details are described as follows.

Every time one patient P_s stays in one specific block b for a time period T, this updating process will be triggered. It is also assumed that there are N_d patients suffering from the same disease in a specific block and constituting a social group. Therefore, these N_d patients share the same original private symmetric matrix D_{P_s} and each body sensor deployed on each patient shares the same identity column in the identity matrix G_{P_s}. The block manager firstly selects a random identity blinding matrix $G'_{P_s}(s = 1, 2, \ldots, N_d)$ for each patient, satisfying the condition that $\sum_{s=1}^{N_d} G'_{P_s} = O_{(\lambda+1)\times N_s}$ where $O_{(\lambda+1)\times N_s}$ is the zero matrix of the size $(\lambda + 1) \times N_s$ (N_s is the number of body sensors constituting one specific WBAN). Next, the block manager sends the identity blinding matrix G'_{P_s} to each mobile patient P_s in the encryption form encoded by the authenticated symmetric key established by the block healthcare manager BM_b and the data sink DS_s by [5].

Then, each data sink DS_s (representing the mobile patient P_s) randomly selects $r_{c,s} \in_R \mathbb{G}_p$ and computes the blinded key materials as follows,

$$D_{P_s}^{b,bld} = r_{c,s} D_{P_s}, G_{P_s}^{b,bld} = r_{c,s}(G_{P_s} + G'_{P_s}), \tag{7}$$

and transmits them to the cloud server for key updating.

After that, the cloud server calculates the updated key materials for WBANs deployed on the N_d patients as follows,

$$U_{P_s}^{b,bld} = (D_{P_s}^{b,bld} G_{P_s}^{b,bld})^T = (D_{P_s}^{b,bld} r_{c,s}(G_{P_s} + G'_{P_s}))^T (s = 1, 2, \ldots, N_d), \tag{8}$$

and sends $(U_{P_s}^{b,bld}, MAC(U_{P_s}^{b,bld}))(s = 1, 2, \ldots, N_d)$ to each data sink $DS_s(s = 1, 2, \ldots, N_d)$ through the underlying pre-established secure and authenticated communication channel between the cloud server and each data sink DS_s [5], where $MAC(\cdot)$ is the message authentication code for integrity check.

Finally, after checking the message integrity, each data sink DS_s recovers the original updated U'_{P_s}, computes the blinded private key material matrix $U_{P_s}^{\prime,res}$ for patient P_s as follows,

$$U_{P_s}^{b'} = U_{P_s}^{b,bld} (r_{c,s}^2)^{-1}, U_{P_s}^{b',res} = r_s U_{P_s}^{b'}, \tag{9}$$

and sends the updated row in $U_{P_s}^{b',res}$ with the same row number in U_{P_s} encrypted by the pairwise keys to each body sensor deployed on its patient as follows,

$$DS_s \rightarrow BSR_{s,k} : E_{k_{DS_s - BSR_{s,k}}}(U_{P_s}^{b',res}(k) \| MAC(U_{P_s}^{b',res}(k))), \tag{10}$$

where $k_{DS_s - BSR_{s,k}}$ represents the pairwise key established between data sink DS_s and body sensor $BSR_{s,k}$. Until now, the key material updating resilient to time-based mobile attacks has been fulfilled.

What deserves our attention is that performing the key material updating procedure described above does maintain the established pairwise keys among body sensors the same as before. Therefore, it is unnecessary for body sensors to re-establish updated pairwise keys. Only in this way, can we achieve the goals of resisting time-based mobile attacks and saving the computational cost of pairwise key updating simultaneously, which is critical to energy-constrained WBANs. The correctness of the process of key material updating for cloud-assisted WBANs can be verified by the cooperation of the mobile patients in the same social group suffering from the same disease in the same block, since they can correctly recover the initial key material matrix U_{P_s} as follows,

$$U'_{P_s}=\frac{1}{N_d}\sum_{s=1}^{N_d}U^{b'}_{P_s}=\frac{1}{N_d}\sum_{s=1}^{N_d}U^{b,bld}_{P_s}(r^2_{c,s})^{-1}=\frac{1}{N_d}\sum_{s=1}^{N_d}(r_{c,s}D_{P_s}r_{c,s}(G_{P_s}+G'_{P_s}))^T(r^2_{c,s})^{-1}=\frac{1}{N_d}\sum_{s=1}^{N_d}D_{P_s}(G_{P_s}+G'_{P_s})=\frac{1}{N_d}\sum_{s=1}^{N_d}D_{P_s}G_{P_s}+\frac{1}{N}D_{P_s}\sum_{s=1}^{N}G'_{P_s}$$
$$\left(Provided\ that\ \sum_{s=1}^{N_d}G'_{P_s}=O\right)=\frac{1}{N_d}\sum_{s=1}^{N_d}D_{P_s}G_{P_s}=\frac{1}{N_d}N_dU_{P_s}=U_{P_s}. \tag{11}$$

Therefore, we can conclude that after updating, the original private key material matrix $U^{res}_{P_s}$ for each mobile patient P_s can still remain unchanged, so does the resultant pairwise keys established among body sensors.

4.2.2. Updating for location-based mobile attacks

In key updating for location-based mobile attacks in cloud-assisted WBANs, our goal is to invalidate the combination of private key materials extracted from the compromised body sensors in a series of different locations (blocks) to effectively deduce the established pairwise keys among innocent body sensors by exploiting the technique of proactive secret sharing. Besides, all kinds of patient's privacy is required to be well protected and the computationally-intensive key updating is outsourced to the cloud server to significantly save energy for resource-constrained body sensors. The details are described as follows.

Every time one patient P_s moves into a new block b^{new} represented by $Loc'_{P_s}=b^{new}$, the data sink DS_s establishes an authenticated symmetric key with the new block healthcare manager $BM_{b^{new}}$ by [5]. It is assumed that there are $N_{d'}$ patients including P_s in block b^{new} suffering from the same disease and constituting a social group. To help the newly coming mobile patients wearing sets of body sensors to fulfill key updating, $BM_{b^{new}}$ selects an additional identity blinding matrix G''_{P_s} satisfying $\sum_{i=1}^{N_{d'}}G'_{P_i}+G''_{P_s}=O_{(\lambda+1)\times N_s}$. Next, the new block manager $BM_{b^{new}}$ sends the identity blinding matrix G''_{P_s} to each mobile patient P_s in the encryption form encoded by the authenticated symmetric key established by the block healthcare manager $BM_{b^{new}}$ and the data sink DS_s by [5].

Then, the data sink DS_s determines the new block's location information by GPS services, randomly selects $r'_{c,s}\in_R\mathbb{G}_p$ and updates the key materials as follows,

$$D'_{P_s}(i,j)(i=j\wedge i,j\in\{1,\ldots,\lambda+1\})=H_1(Loc'_{P_s}), \tag{12}$$
$$D^{b^{new},bld}_{P_s}=r'_{c,s}D'_{P_s},G^{b^{new},bld}_{P_s}=r_{c,s}(G'_{P_s}+G''_{P_s}), \tag{13}$$

and transmits them together with the blinding ratio $\rho=r'_{c,s}r^{-1}_{c,s}$ to the cloud server.

After that, the cloud server incrementally calculates the updated key materials for WBANs deployed on the $N_{d'}$ patients as follows,

$$U^{b^{new},bld}_{P_s}(i,j)=\rho(U^{b,bld}_{P_s}(i,j)-D^{b,bld}_{P_s}(j,j)G^{b,bld}_{P_s}(j,i))+D^{b^{new},bld}_{P_s}(j,j)G^{b^{new},bld}_{P_s}(j,i), \tag{14}$$

where $i\in\{1,\ldots,N_{d'}\},j\in\{1,\ldots,\lambda+1\}$, and sends $(U^{b^{new},bld}_{P_s},MAC(U^{b^{new},bld}_{P_s}))$ $(s=1,2,\ldots,N_{d'})$ to each data sink $DS_s(s=1,2,\cdots,N_{d'})$ through the underlying pre-established secure and authenticated communication channel between the cloud server and each data sink DS_s [5].

Finally after checking the message integrity, each data sink DS_s recovers the original updated $U^{b^{new}}_{P_s}$, computes the blinded private key material matrix $U^{b^{new},res}_{P_s}$ for patient P_s as follows,

$$U^{b^{new}}_{P_s}=r'^{-1}_{c,s}U^{b^{new},bld}_{P_s},U^{b^{new},res}_{P_s}=r_sU^{b^{new}}_{P_s}, \tag{15}$$

and sends the updated key materials encrypted by the established pairwise key to each body sensor.

$$DS_s\rightarrow BSR_{s,k}:E_{k_{DS_s-BSR_{s,k}}}(U^{b^{new},res}_{P_s}(k)\|MAC(U^{b^{new},res}_{P_s}(k))). \tag{16}$$

where $k_{DS_s-BSR_{s,k}}$ represents the pairwise key established between data sink DS_s and body sensor $BSR_{s,k}$. Until now, the key material updating resilient to location-based mobile attacks in the new block b^{new} has been fulfilled. The correctness can be proved in the same way as the key updating for time-based mobile attacks.

Every time one patient P_s moves into a new block, the number of patients who are suffering from the same disease in the existing block b will decrease by one. Therefore, the key updating would also be performed in the existing block to tackle the problem of patient leaving. It is assumed that the identity blinding matrix of patient P_s in the existing block is G'_{P_s}. When he leaves the block, the block manager will update the key materials as follows,

$$G^{b,\prime\prime}_{P_i}=G'_{P_i}+\frac{1}{N_d-1}G'_{P_s}(i=1,2,\ldots,N_d-1). \tag{17}$$

Next, the new block manager BM_b sends the identity blinding matrix $G^{b,\prime\prime}_{P_i}$ to each mobile patient P_i in the encryption form encoded by the authenticated symmetric key established by the block healthcare manager BM_b and the data sink DS_s by [5].

Then, each data sink DS_i computes the blinded key materials as follows,

$$D^{b,\prime\prime,bld}_{P_i}=D^{b,bld}_{P_i},G^{b,\prime\prime,bld}_{P_i}=G^{b,bld}_{P_i}+r_{c,i}G^{b,\prime\prime}_{P_i}, \tag{18}$$

and transmits them to the cloud server for key updating, where $r_{c,i} \in_R \mathbb{G}_p$ is the blinding factor randomly and previously selected by the data sink DS_i in the key updating resilient to time-based mobile attack.

After that, the cloud server calculates the updated key materials for WBANs deployed on the $N_d - 1$ patients as follows,

$$U_{P_i}^{b,\prime\prime,bld} = (D_{P_i}^{b,\prime\prime,bld} G_{P_i}^{b,\prime\prime,bld})^T = (D_{P_i}^{b,bld} (G_{P_i}^{b,bld} + r_{c,i} G_{P_i}^{b,\prime\prime}))^T (i = 1, 2, \ldots, N_d - 1), \tag{19}$$

and sends $(U_{P_i}^{b,\prime\prime,bld}, MAC(U_{P_i}^{b,\prime\prime,bld}))(i = 1, 2, \ldots, N_d - 1)$ to each data sink $DS_i (i = 1, 2, \ldots, N_d - 1)$ through the underlying pre-established secure and authenticated communication channel between the cloud server and each data sink DS_s [5].

Finally, after checking the message integrity, each data sink DS_i recovers the original updated $U_{P_i}^{b,\prime\prime}$, computes the blinded private key material matrix $U_{P_i}^{b,\prime\prime,res}$ for patient P_i as follows,

$$U_{P_i}^{b,\prime\prime} = U_{P_i}^{b,\prime\prime,bld} (r_{c,i}^2)^{-1}, U_{P_i}^{b,\prime\prime,res} = r_i U_{P_i}^{b,\prime\prime}, \tag{20}$$

where $r_i \in_R \mathbb{G}_p$ is the pairwise key blinding element privately kept by DS_i and sends the updated row in $U_{P_i}^{b,\prime\prime,res}$ with the same row number in U_{P_i} encrypted by the pairwise keys to each body sensor deployed on its patient as follows,

$$DS_i \rightarrow BSR_{i,k} : E_{k_{DS_i - BSR_{i,k}}} (U_{P_i}^{b,\prime\prime,res}(k) \| MAC(U_{P_s}^{b,\prime\prime,res}(k))), \tag{21}$$

where $k_{DS_i - BSR_{i,k}}$ represents the pairwise key established between data sink DS_i and body sensor $BSR_{i,k}$. Until now, the key material updating resilient to location-based mobile attacks in the existing block b has been fulfilled. The correctness can be straightforwardly proved in the same way as the key updating for time-based mobile attacks.

4.3. Pairwise key updating for switching WBANs work mode

In practice, to comprehensively monitor the health condition of a specific patient, it is necessary for physicians to perform a series of physical examinations such as ECG and EEG through a unique set of body sensors. Therefore, to adapt to each kind of examination, the data sink is necessary to securely and efficiently switch the underlying WBANs from one work mode to another. Body sensors are also necessary to join the current WBANs for some medical purposes and to be revoked for their malicious behaviors (being compromised). In each situation described above, the position information of the associated body sensors embedded in the original private symmetric matrix D_{P_s} and the corresponding established pairwiese key should be updated.

Before depicting the updating process in detail, we will briefly explain the concrete construction of the private symmetric matrix D_{P_s}. It is well known that the $\lambda + 1$ elements in the diagonal line cooperate to represent patient P_s's location information. Therefore, there are $N_E = (\lambda + 1)^2 - (\lambda + 1) = \lambda^2 + \lambda$ elements corresponding to $\frac{\lambda^2 + \lambda}{2}$ symmetric positions left for body sensors' deployment. If we want to reserve some positions for future use, the relationship between the threshold number λ and the number of body sensors N_{BSR} deployed on each patient can be described as follows,

$$N_{BSR} \leqslant \lambda^2 + \lambda. \tag{22}$$

It can be obviously observed in Fig. 3 that the relationship between the number of body sensors deployed on each patient and the threshold is reasonable and well adapts to the reality. The fact is that the more body sensors deployed on the patient, the larger the probability of successfully launching node compromise attack would be. Therefore, a larger threshold should be selected for security consideration. On the other hand, if it is detected that the number of compromised sensors approaches the threshold, we can set it as a larger number λ' and remains N_{BSR} constant. In this case, additional

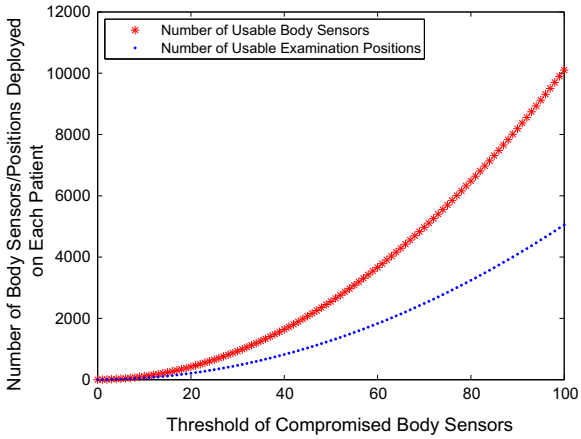

Fig. 3. Relationship between number of deployed body sensors and threshold.

$\lambda'^2+\lambda'-(\lambda^2+\lambda)$ elements are reserved for future use and vice versa. In this way, each element in the original private symmetric matrix D_{P_s} except the ones in the diagonal line corresponds to a specific position of a body senor on the patient. Now, the key updating for switching work mode can be described as follows.

Without loss of generality, it is assumed that one body sensor on the mobile patient P_s currently located in block b is re-deployed from $Loc_{P_{s,k}}$ to $Loc'_{P_{s,k}}$ during the process of switching work mode, where $Loc_{P_{s,k}}$ and $Loc'_{P_{s,k}}$ are associated to elements $D_{P_s}(i,j)=D_{P_s}(j,i)$ and $D_{P_s}(x,y)=D_{P_s}(y,x)$ respectively. For $x\neq y\wedge x,y\in\{1,\ldots,\lambda+1\}$, the data sink DS_s firstly computes

$$D^{b,upd}_{P_s}(x,y)=D^{b,upd}_{P_s}(y,x)=H_0(Loc'_{P_{s,k}}). \tag{23}$$

Then, DS_s generates a random number $r_{i,j}\in_R\mathbb{G}_p$ and sends the blinded key updating materials $D^{b,bld}_{P_s}, G^{b,bld}_{P_s}$ to the cloud server the same as the key updating for time-based mobile attacks presented in Section 4.2. Besides, the data sink DS_s also submits the following blinded key updating materials

$$\begin{aligned} &D^{b,bld,upd}_{P_s}(x,y)=D^{b,bld,upd}_{P_s}(y,x)=r_{c,s}D_{P_s}(x,y)=r_{c,s}H_0(Loc'_{P_{s,k}}),\\ &D^{b,bld,upd}_{P_s}(i,j)=D^{b,bld,upd}_{P_s}(j,i)=r_{c,s}r_{i,j}, \end{aligned} \tag{24}$$

where $r_{c,s}\in_R\mathbb{G}_p$ is the same as the blinding factor in the key updating for time-based mobile attack presented in Section 4.2.

After receiving the blinded key updating materials, for $k\in\{1,\ldots,N_s\}$ (N_s is the current number of body sensors deployed on patient P_s), the cloud server updates the key material as follows,

$$U^{b,bld,upd}_{P_s}(k,i)=U^{b,bld}_{P_s}(k,i)-D^{b,bld}_{P_s}(i,j)G^{b,bld}_{P_s}(j,k)+D^{b,bld,upd}_{P_s}(i,j)G^{b,bld}_{P_s}(j,k), \tag{25}$$

$$U^{b,bld,upd}_{P_s}(k,j)=U^{b,bld}_{P_s}(k,j)-D^{b,bld}_{P_s}(j,i)G^{b,bld}_{P_s}(i,k)+D^{b,bld,upd}_{P_s}(j,i)G^{b,bld}_{P_s}(i,k), \tag{26}$$

$$U^{b,bld,upd}_{P_s}(k,x)=U^{b,bld}_{P_s}(k,x)+D^{b,bld,upd}_{P_s}(x,y)G^{b,bld}_{P_s}(y,k)-D^{b,bld}_{P_s}(x,y)G^{b,bld}_{P_s}(y,k), \tag{27}$$

$$U^{b,bld,upd}_{P_s}(k,y)=U^{b,bld}_{P_s}(k,y)+D^{b,bld,upd}_{P_s}(y,x)G^{b,bld}_{P_s}(x,k)-D^{b,bld}_{P_s}(y,x)G^{b,bld}_{P_s}(x,k). \tag{28}$$

and sends the updated elements in $U^{b,bld,upd}_{P_s}$ mentioned above together with their message authentication codes to the data sink DS_s through the underlying pre-established secure and authenticated communication channel between the cloud server and each data sink DS_s [5].

Finally, after checking the message integrity, the data sink DS_s recovers the original updated $U^{b,upd}_{P_s}$, computes the blinded private key material matrix $U^{b,upd,res}_{P_s}$ as follows,

$$U^{b,upd}_{P_s}=(r^2_{c,s})^{-1}U^{b,bld,upd}_{P_s}, U^{b,upd,res}_{P_s}=r_sU^{b,upd}_{P_s}, \tag{29}$$

where $r_s\in_R\mathbb{G}_p$ is the pairwise key blinding factor for the patient P_s, and sends the updated key materials encrypted by the established pairwise keys to each body sensor as follows,

$$DS_s\rightarrow BSR_{s,k}: E_{k_{DS_s-BSR_{s,k}}}(U^{b,upd,res}_{P_s}(k)\|MAC(U^{b,upd,res}_{P_s}(k))). \tag{30}$$

Until now, the key updating for switching a WBAN work mode has been fulfilled and all the body sensors can update their established pairwise keys according to our proposed key establishment mechanism in Section 4.1.

4.4. Extension to pairwise key updating in distributed environment

Without loss of generality, we will explain the distributed pairwise key updating resisting time-based mobile attacks. For example, the block manager BM_b is not required, and all the key material updating is fulfilled by the cooperation of the mobile patients suffering from the same disease and constituting a m-healthcare social group in block b. Other two cases for resisting location-based mobile attacks resemble it. It is assumed that there exist N_d patients suffering from the same disease, and the data sinks are $DS_i(i=1,2,\ldots,N_d)$, respectively. All N_d data sinks are assumed to have negotiated a group key by the secure and authenticated group key agreement protocol [5], and we focus on how to resist the mobile compromise attacks from the outside of the symptom-matching social group. The distributed pairwise key updating can be described as follows.

Each data sink $DS_s(s=1,2,\ldots,N_d)$ respectively sends the identity blinding matrices $G'_{P_{s,i}}(i=1,2,\ldots,s-1,s+1,\ldots,N_d)$ encrypted by the group key k_{GS} to other mobile patients suffering from the same disease and belonging to the same social group. After deciphering the identity blinding matrices from other data sinks, the data sink DS_i will compute its own identity blinding matrix G'_{P_i} as follows,

$$G'_{P_s}=\sum_{j=1,j\neq s}^{N_d}G'_{P_{s,j}}-\sum_{j=1,j\neq s}^{N_d}G'_{P_{j,s}}. \tag{31}$$

Then, it uploads the blinded identity matrices $G_{P_s}^{bd,bld} = r_{c,s}(G_{P_s} + G'_{P_s})$ to the cloud server, where $r_{c,s} \in_R \mathbb{G}_p$ is randomly selected by DS_s. The following steps of key material updating in cloud-assisted WBANs and the correctness proof resemble the ones resilient to time-based mobile attacks in the architectural environment described in Section 4.2. The unchanged pairwise key after updating is still maintained to save computational cost for energy-constrained WBANs.

4.5. Group key agreement

It is assumed that $BSR_{s,k}(k \in \{1, \ldots, N_s\})$ are N_s body sensors deployed on the patient P_s negotiating a group key associated to the session SID_j in WBANs. Firstly, each body sensor $BSR_{s,k}$ computes the pairwise keys $K^0_{BSR_{s_{k,k-1}}}$ and $K^0_{BSR_{s_{k,k+1}}}$ between two neighbor nodes and itself. After that, it computes the value

$$K^0_{BSR_s}(k,k) = \sum_{\theta=1}^{\lambda+1} U^0_{P_s}(k,\theta) G^0_{P_s}(\theta,k). \tag{32}$$

Finally, each body sensor $BSR_{s,k}$ transmits $K^0_{BSR_s}(k,k)$ encrypted by established pair-wise keys to its two neighbors respectively, and uses the DB protocol [10] to accomplish the following steps of group key agreement. The established group key in WBANs is required to meet the following properties: (a) group key secrecy, (b) forward security, and (c) backward security. Consequently, it is necessary to update the group key whenever there are body sensors revoked from the network for energy-exhausting, being compromised by adversaries and joining/leaving the underlying WBAN. After successfully joining or abolished in session j, other innocent body sensors can update their private key information, respectively exploiting the distributed key updating mechanism presented in Section 4.4, transmit the updated contributory key information $K^{j+1}_{BSR_{s_{k,k}}}$ to its neighboring nodes in the encrypted form, and have the session number SID_j updated to SID_{j+1}. The following steps of group key updating resemble the process of group key establishment in DB protocol [10].

5. Security analysis

Theorem 1 (Correctness). *The proposed secure and privacy-preserving key management scheme for cloud-assisted WBANs in m-healthcare social networks (4S) maintains all the pairwise keys established among body sensors constant after key updating in both architectural and distributed scenarios.*

Proof. In the cloud-assisted WBANs, the cloud server assists the mobile patient to fulfill the computationally-intensive key updating under a "pay-per-use" mode, which means there exists great incentive for the cloud server to cheat on the updated key material results. Therefore, it is necessary to devise a correctness verification mechanism for the mobile patients to check the outputs from the cloud server. The verification mechanisms have been proposed after the key updating protocols w.r.t each scenario explained in the previous section, and the corresponding correctness can be straightforwardly derived. □

Theorem 2. *The Proposed 4S is Unconditional Secure against Time-based Mobile Adversaries.*

Proof. In our scheme, every time the patient stays in one fixed block L for a certain time period T, the mutual identity blinding process and corresponding key material updating will be triggered in cloud-assisted WBANs and fulfilled by the cooperation of the mobile patients in the same social group. Therefore, the key materials, the time-based mobile adversary obtained in different time slots, cannot be combined to derive the authentic pairwise keys established among innocent body sensors. Without loss of generality, it is assumed that the adversary has successfully compromised λ_i and λ_{i+1} body sensors during time slots t_i and t_{i+1}, respectively, which can be represented as follows,

$$\left|\mathbb{C}_{t_i,L}\right| = \lambda_i \leqslant \lambda \wedge \left|\mathbb{C}_{t_{i+1},L}\right| = \lambda_{i+1} \leqslant \lambda \wedge \lambda_i + \lambda_{i+1} \geqslant \lambda + 1. \tag{33}$$

From $\mathbb{C}_{t_i,L}$, the adversary can obtain the following information $U^{t_i}_{P_s}(j)(j = 1, 2, \ldots, \lambda_i)$. Since the Blom's symmetric key construction [4] is linearly independent with $\lambda + 1$, all the pairwise keys are uniquely determined by every $\lambda + 1$ rows of $U^{t_i}_{P_s}$. The knowledge of less than $\lambda + 1$, namely λ_i compromised pairwise keys can only reveal λ_i columns in the pairwise key matrix $K^{t_i}_{P_s}$, leaving any information about the pairwise keys established between innocent nodes absolutely unobtained. The case in the time slot t_{i+1} resembles it.

Then, we will claim that even the adversary combines the private information of the pairwise keys, compromised from the mobile patients in the same social group during different time slots, it will still be impossible for him to obtain any information about the pairwise keys, established among innocent body sensors. The fact is that the identity blinding matrices, selected in different time slots, cannot be combined to recover the authentic initial key materials $U^{t_i}_{P_s}$ or $U^{t_{i+1}}_{P_s}$ since

$$\sum_{s=1}^{\lambda_i} G'^{,t_i,L}_{P_s} + \sum_{s=\lambda_i+1}^{\lambda_i+\lambda_{i+1}-1} G'^{,t_{i+1},L}_{P_s} \neq O_{(\lambda+1)\times N_s}. \tag{34}$$

Therefore, without loss of generality, we can conclude the Eq. (1) in Section 2

$$H\left(Key_{\mathbb{N}\setminus\mathbb{C}_{t_1,L}\bigcup\cdots\bigcup\mathbb{C}_{t_n,L}}|Key_{\mathbb{C}_{t_1,L}\bigcup\cdots\bigcup\mathbb{C}_{t_n,L}}\right)=H(Key_{\mathbb{N}\setminus\mathbb{C}_{t_1,L}\bigcup\cdots\bigcup\mathbb{C}_{t_n,L}}). \tag{35}$$

This completes the proof. □

Theorem 3. *The Proposed 4S is Unconditional Secure against Location-based Mobile Adversaries.*

Proof. Every time when the patient moves into a new block, the location information, stored in the diagonal line of the original private symmetric matrix D_{P_s}, will be updated. In addition to the identity re-blinding performed cooperatively by the patients suffering from the same disease and constituting the same social group in the new block, even more than the threshold number of body sensors are compromised during a single time slot from different blocks, the probability of the pairwise key exposure among innocent body sensors still remains zero. Resembling the proof of Theorem 2, assuming

$$\left|\mathbb{C}_{T,l_i}\right|=\lambda_i\leqslant\lambda\wedge\left|\mathbb{C}_{T,l_{i+1}}\right|=\lambda_{i+1}\leqslant\lambda\wedge\lambda_i+\lambda_{i+1}\geqslant\lambda+1, \tag{36}$$

we have

$$\sum_{s=1}^{\lambda_i}G'^{,l_i,T}_{P_s}+\sum_{s=\lambda_i+1}^{\lambda_i+\lambda_{i+1}-1}G'^{,l_{i+1},T}_{P_s}\neq O_{(\lambda+1)\times N_s}. \tag{37}$$

Therefore, without loss of generality, we can conclude the Eq. (2) in Section 2

$$H(Key_{\mathbb{N}\setminus\mathbb{C}_{l_1,T}\bigcup\cdots\bigcup\mathbb{C}_{l_n,T}}|Key_{\mathbb{C}_{l_1,T}\bigcup\cdots\bigcup\mathbb{C}_{l_n,T}})=H(Key_{\mathbb{N}\setminus\mathbb{C}_{l_1,T}\bigcup\cdots\bigcup\mathbb{C}_{l_n,T}}). \tag{38}$$

This completes the proof. □

The privacy issue has been increasingly emphasized on in the key agreement in WBANs, since the adversary can infer the diseases of the patients from the specific identities and positions of body sensors deployed on them [31]. In our scheme, the identity privacy, sensor deployment privacy and location privacy refer to the identities of both the sensors and the patient (i.e. represented by the identity of the mobile data sink), the sensors' deployed positions and the block location of the patient can be simultaneously well protected. No less than the threshold number $(\lambda+1)$ of body sensors can cooperatively work out the deployed positions of themselves on the patient P_s as well as the dynamic block location information of the patient. The fact is that the threshold number of body sensors are able to recover D_{P_s} by utilizing the knowledge of $U_{P_s}(s=1,2,\ldots,\lambda+1)$, since the underlying Blom's symmetric key construction [4] is linearly independent with $\lambda+1$. However, the collusion of whatever kind of mobile adversaries cannot obtain any position or location information w.r.t the body sensors or the patient P_s within their attacking ability of λ-restriction defined in Section 2. Besides, the identity blinding matrices are also utilized as an efficient anonymization method to protect both the identities of body sensors and the patient. After key updating, it is impossible for the adversaries to link the pseudonyms of a specific body sensor or the patient with its original identities. Only in this way, the sensor deployment privacy, location privacy and identity privacy can be all protected.

Additionally, it is generally assumed that the in cloud-assisted WBANs, the cloud server performs the key updating in the honest-but-curious mode, where it perfectly complies with the protocol specifications, but tries to extract the private information (i.e. the identity privacy, the sensor deployment privacy, and the location privacy mentioned above that significantly relevant to the mobile patient's private health information) from the interactions with the patients. Therefore, it is also required to devise a secure and efficient mechanism to prevent these private information from the exposure to the cloud server. In our proposed scheme, without loss of generality, we take the key updating for time-based mobile attacks for example. Every time before the privacy key materials D_{P_s}, G_{P_s} are submitted to the cloud server by the data sink DS_s of mobile patient P_s, they are blinded by multiplying them with the blinding factor $r_{c,s}$. Consequently, the cloud server performs the key updating on the blinded key materials $D^{b,bld}_{P_s}, G^{b,bld}_{P_s}$ and without the knowledge of the blinding factor $r_{c,s}$ privately kept by DS_s, it cannot derive the patient's private information.

6. Performance analysis

In this section, the efficiency of our proposed secure and efficient privacy preserving key management scheme for cloud-assisted WBANs in m-healthcare social networks (4S) is analyzed from the storage overhead, computational overhead, and the communication overhead. Then, the key connectivity and the resilience to mobile attacks are extensively simulated to verify the efficiency and the practicability of our proposed construction.

6.1. Storage, computation, and communication overhead

Our scheme provides an efficient privacy-preserving key agreement scheme for cloud-assisted WBANs in m-healthcare social networks in terms of the storage, computation and communication cost on body sensors. In the process of pairwise

key establishment and updating, it is required for each body sensor to store one row in the blinded key material matrix $U_{P_s}^{res}$. Since the underlying Blom's symmetric key construction [4] is a deterministic proposal, there exists no additional communication cost in pairwise key establishment. For each body sensor that wants to establish a shared key with another, the only operation required is to perform a multiplication between two vectors of the size $\lambda + 1$. In the process of key updating, it is necessary for each body sensor to receive a row in the updated key material matrices $U_{P_s}^{b',res}$ ($U_{P_s}^{b^{new},res}$ or $U_{P_i}^{b,\prime\prime,res}$) after blinding. However, there exists no additional computational overhead for key updating, since each kind of key updating resisting time-based or location-based mobile attacks, maintains the established pairwise key unchanged by extending the technique of proactive secret sharing. It merely makes the private key materials be blinded, to prevent the mobile adversaries from obtaining any useful information, to deduce the pairwise keys established among innocent body sensors. It is significant in saving the computational cost for energy-constrained WBANs, and allocating it to the side of cloud server that are more powered. In the E–G scheme [11] and the q-composite scheme [6], the storage and computational overhead increase linearly to the size of the key rings pre-distributed in each body sensor, respectively represented by k and m. t represents the degree of the pre-distribution polynomial selected in [28]. In PSKA scheme [37], the storage overhead increases linearly to the total number of polynomial points m, chaff points n, and the degree of the polynomial λ, chosen by each body sensor, and the communication cost is linear to $m + n$. Since it is required for each body sensor to perform Lagrange interpolation in the operation of unlocking vault, the computation complexity would increase linearly to the square of λ. Table 2 illustrates the storage, computation, and communication overhead on resource-constrained body sensors of the E–G scheme [11], the Liu's scheme [28], the q-composite scheme [6], the Blom's symmetric key construction [4], the PSKA scheme [37], and ours. It obviously shows that our scheme far outperforms the others.

6.2. Evaluation and simulation results

We evaluate the effectiveness of the proposed secure key management scheme for the cloud-assisted WBANs in m-healthcare social networks, in terms of its resilience to mobile attacks. Resilience is negatively related to the probability of the pairwise key exposure among the innocent body sensors. The lower the probability of innocent sensors' pairwise key exposure is, the higher the resilience will be. Table 3 illustrates the parameters we adopted in practical simulations.

In our evaluation, it is assumed that the mobile adversary sponsors attack randomly. It means the adversary cannot possess in advance the knowledge of the health condition of each patient, namely the diseases each patient is suffering from. Therefore, when the mobile adversary prepares to compromise a body sensor, it is absolutely impossible for him to know whether the host (patient) of this sensor is suffering from the same disease (belonging to the same social group) as the patients, from whom he has compromised body sensors before, except a random guess at the successful probability of $Prob_{\cdot com}(\beta)$. In another word, each time the probability of effective compromise, namely the mobile adversary successfully compromise a body sensor, that can be used for inferring the established pairwise keys among innocent WBANs, is $Prob_{\cdot com}(\beta)$. The reason is that only the mobile patients in the same social group (suffering the same disease and being located in the same block) share the same private key material matrix $U_{P_s}^{b'}$, taking key updating for time-based mobile attack for example. Now, once a body sensor is compromised, a blinded row in the blinded private key material matrix $U_{P_s}^{b',res}$ is obtained by the adversary. To recover the original private key material matrix $U_{P_s}^{b'}$ and compromise the innocent nodes, it is necessary for the adversaries to further attack the data sink, namely the mobile device held by each patient, to obtain the private key r_s. We assume he can fulfill this task and recover the associated row in $U_{P_s}^{b'}$ at the probability of $Prob_{\cdot DS}(\alpha)$.

Table 2
Comparison of storage, communication and computation overhead.

Schemes	Storage	Comm.	Comp.
E-G [11]	$O(k)$	$O(2)$	$O(k)$
q-Composite [6]	$O(m)$	$O(2)$	$O(m)$
Liu [28]	$O(t)$	$O(2)$	$O(t)$
Blom [4]	$O(\lambda)$	$O(\lambda)$	$O(\lambda)$
PSKA [37]	$O(m+n+\lambda)$	$O(m+n)$	$O(\lambda^2)$
Ours	$O(\lambda)$	$O(\lambda)$	$O(\lambda)$

Table 3
Notations for our simulation.

Notation	Description
$Prob_{\cdot DS}(\alpha)$	Probability of data sinks' compromise
$Prob_{\cdot BSR}(\gamma)$	Probability of body sensors' compromise
λ	Threshold set for WBANs w.r.t each patient
$Prob_{\cdot com}(\beta)$	Probability of patients suffering from the same disease in each block
N	Average number of patients located in each block

Then, the adversary wants to de-blind it, and recover the associated row in the private initial key material matrix U_{P_s}. Since there are βN identity blinding matrices adopted in the anonymization algorithm, it is required for the adversary to compromise at least $\beta N - 1$ data sinks, deployed on the patients suffering from the same disease. Only in this way, the adversary can recover one authentic row in U_{P_s}. If we denote the probability of successfully compromising a body sensor, and the threshold of WBANs as $Prob_{\cdot BSR}(\gamma)$ and λ respectively, we can conclude that the mobile adversary can obtain the established pairwise keys among the innocent body sensors at the following probability

$$Prob_{\cdot InnocentBSR}^{compromise} = (\alpha\beta)^{\beta N-1}\gamma^{\lambda+1}. \tag{39}$$

Now, we can further consider a more sophisticated situation that one patient is suffering from more than one disease, which is also practical in the reality. It is assumed that there exist m kinds of different diseases in each block. $\beta_i (i = 1, 2, \ldots, m)$ represents the probability of the patients suffering from disease i in each block and it can be computed as $\beta_i = \frac{|\mathbb{A}_i|}{N}$, where $\mathbb{A}_i$ and $|\mathbb{A}_i| (i = 1, 2, \ldots, m)$ represent the set of patients suffering from disease i and its corresponding size, respectively. $\mathbb{A}_j \bigcap \mathbb{A}_k$ is denoted as the set of patients, suffering from diseases j and k simultaneously. Then, assuming each kind of disease is infected independently, the probability of a patient to suffer from at least one disease can be described as follows,

$$\beta_{total} = \sum_{i=1}^{m}\beta_i - \sum_{i=1}^{|\mathbb{A}_j \bigcap \mathbb{A}_k|}\beta_{\mathbb{A}_j \bigcap \mathbb{A}_k} + \cdots + (-1)^{m+1}\beta_{\mathbb{A}_1 \bigcap \mathbb{A}_2 \bigcap \cdots \bigcap \mathbb{A}_m}. \tag{40}$$

Finally, we can derive the successful probability for the mobile adversary to obtain the established pairwise keys among innocent body sensors as follows,

$$Prob_{\cdot InnocentBSR}^{compromise,total} = (\alpha\beta_{total})^{\beta_{total}N-1}\gamma^{\lambda+1}. \tag{41}$$

In our simulation, we use a custom simulator built in Java to evaluate the resilience to the mobile attack of our scheme. 180 patients and 9 block managers are initially and uniformly deployed in an area of 500×500 m, as shown in a similar network architecture illustrated in Fig. 1, Section 2. A secure and authenticated communication channel is established between the mobile patient and the medical cloud server. Each patient P_s is equipped with a set of 260 wearable smart micro body sensors and a mobile device PDA with a transmission radius of 20 meters to simulate the m-healthcare social networks. Then, we simulate our scheme in the following four facets.

Firstly, we evaluate the key connectivity at the initialization phase. It is assumed that P, s, S and k, m, s' represent the sizes of the key pool and the key ring in the E–G scheme [11], the Liu's scheme [28] and the q-composite scheme [6], respectively. q, t, t', λ represent the threshold in the q-composite scheme [6], the Liu's scheme [28], the PSKA [37] and the Blom's symmetric key construction [4], respectively. Fig. 4 shows that the key connectivity of our scheme at the initialization phase remains 100%, and far outperforms other schemes [6,11,28,37], regardless of the size of key rings, since the underlying Blom's symmetric key construction [4] is a deterministic one. Therefore, we can conclude that our scheme costs the least time to successfully establish the same number of pairwise keys for WBANs. This characteristic well adapts to m-healthcare social networks, especially in the emergent cases, where the PHI is required to be collected timely through the secure communication channels among body sensors [46].

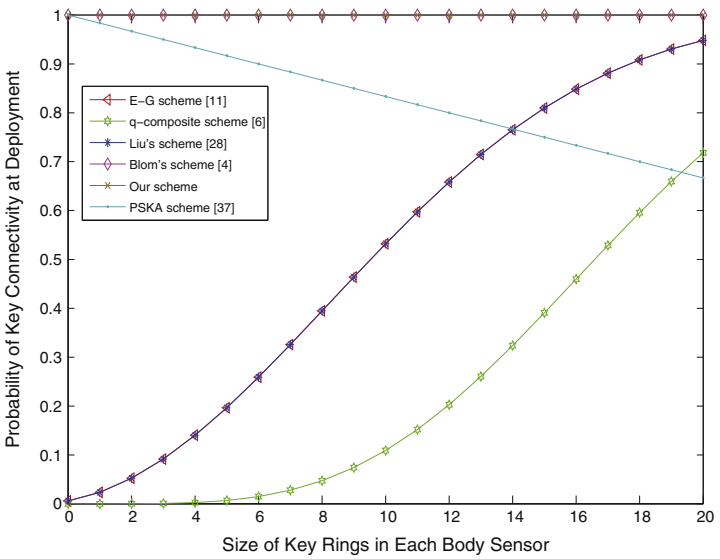

Fig. 4. Comparison of key connectivity at deployment ($S = s = P = 170$, $q = 2$).

Then, we make a comparison between previous schemes [6,11,28,37] and ours in terms of the resilience to mobile attacks, as the number of compromised body sensors increases. For comparison convenience, consider the adversaries in the associated schemes [6,11,28,37] possess the same attacking ability, that they can compromise at most λ body sensors in each time slot from one specific patient. Fig. 5 shows the probability of the key exposure in mobile attacks of the E-G scheme [11], the Liu's scheme [28], the q-composite scheme [6], the Blom's symmetric key construction [4], the PSKA scheme [37], and ours. Taking the threshold $\lambda = 40$ for example, as the number of compromised body senors increases, even exceeds the threshold, the probability of key exposure in our scheme remains nearly zero, and obtains almost 100% resilience. By comparison, it is obvious that our scheme far outperforms others. In the probabilistic schemes [6,11], once the number of compromised sensors increases, the fraction of the affected communication links in the rest of WBANs increases very fast. The reason is that in probabilistic schemes, it is probable for one single key to be pre-distributed in a number of body sensors' key rings and be used by several different pairs of sensors as a pairwise key. Consequently, some body sensors' compromise can make the pairwise keys established between innocent sensors exposed. Since there exists no key updating approaches in schemes [4,28,37], when the mobile adversary compromised more than the threshold number of body sensors, all the pairwise keys, established among innocent body sensors, will be exposed.

Thirdly, we evaluate the resilience to mobile attacks of our scheme towards $Prob_{\cdot com}(\beta), Prob_{\cdot DS}(\alpha), Prob_{\cdot BSR}(\gamma)$, and N with the variation of threshold λ. Fig. 6 shows that $Prob_{\cdot InnocentBSR}^{compromise}$ decreases dramatically fast to nearly zero, as the ratio of the patients affected by the same disease increases, since more and more mobile patients in the same social group can cooperate to fulfill the task of mutual blinding in key material updating. Finally when $Prob_{\cdot com}(\beta)$ grows continuously above a certain ratio, $Prob_{\cdot InnocentBSR}^{compromise}$ slightly grows accordingly, since when the number of patients suffering from the same disease exceeds some threshold, the exposure of one body sensor deployed on some patient means that more innocent sensors deployed on

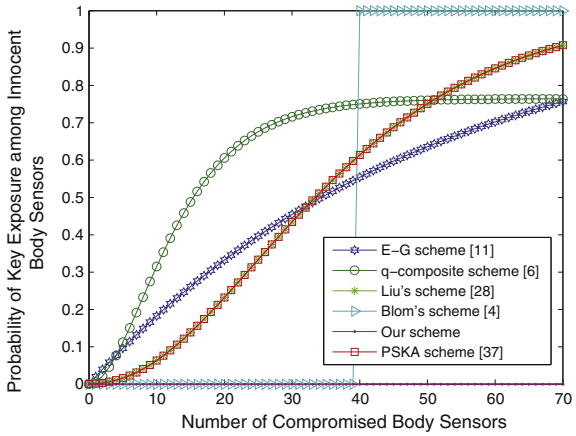

Fig. 5. Comparison of key exposure in compromise attacks ($q = 2, k = m = s' = 20, S = s = P = 170, t = t' = \lambda = 40$).

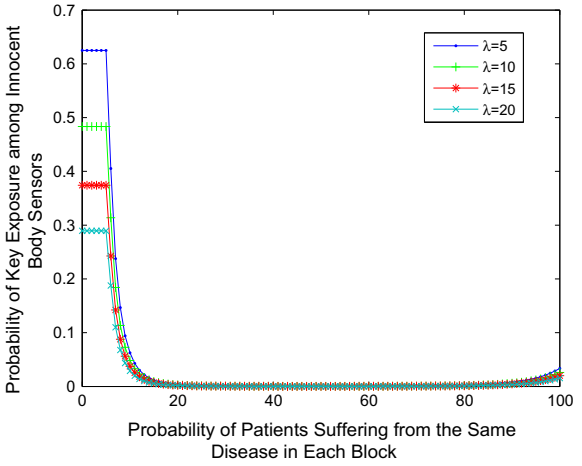

Fig. 6. The resilience to mobile adversaries towards λ and β ($\alpha = 0.85, \gamma = 0.95, N = 20$).

other patients in the same social group will be affected and compromised afterwards. The reason is that more and more patients are sharing the same private initial key material matrix U_{P_s} in each block. Figs. 7 and 8 show that $Prob._{InnocentBSR}^{compromise}$ grows as $Prob._{DS}(\alpha)$ and $Prob._{BSR}(\gamma)$ increases. However in Fig. 9, $Prob._{InnocentBSR}^{compromise}$ decreases when the number of patients located in each block increases. There is a common characteristic in Figs. 6–9 that the higher the threshold becomes, the lower $Prob._{InnocentBSR}^{compromise}$ will be, and the resilience will also become increasingly higher. We can adjust threshold λ to make a tradeoff between the resilience and efficiency according to different situations.

Next, we further evaluate the resilience to mobile attacks towards $Prob._{DS}(\alpha), Prob._{BSR}(\gamma), \lambda$, and N with the variation of $Prob._{com}(\beta)$. Figs. 10 and 11 illustrate that $Prob._{InnocentBSR}^{compromise}$ grows as $Prob._{DS}(\alpha)$ or $Prob._{BSR}(\gamma)$ increases, respectively. On the other hand, Figs. 12 and 13 suggest that $Prob._{InnocentBSR}^{compromise}$ decreases, as the threshold λ and N increase. The common characteristic among Figs. 10–13 is that $Prob._{InnocentBSR}^{compromise}$ decreases firstly, and increases afterwards as $Prob._{com}(\beta)$ grows continuously. The reason is the same as what we explained in the previous simulation. These simulation results presented here demonstrate our key agreement scheme well adapts to the cloud-assisted WBANs in m-healthcare social networks.

Fourthly, we evaluate the resilience to mobile attacks of our scheme towards $Prob._{DS}(\alpha), Prob._{BSR}(\gamma), \lambda$, and N with the variation of $Prob._{com}(\beta)$ in the situation that the patients in each block are suffering from different kinds of diseases. Without loss of generality, β_1 and β_2 represent the probabilities of the patients suffering from disease one and disease two, respectively. The common characteristic in Figs. 14–17 is that $Prob._{InnocentBSR}^{compromise,total}$ increases as β_1, β_2 grow, since the probability of the mobile adversary's effective compromise increases when kinds of diseases break out simultaneously. Fortunately, as shown in Figs. 14 and 15, when $Prob._{DS}(\alpha)$ and $Prob._{BSR}(\gamma)$ are below 50% and 80%, respectively, $Prob._{InnocentBSR}^{compromise,total}$ remains nearly zero. From Figs. 16 and 17, we can see even β_1 and β_2 increase significantly, when the threshold and the number of the patients located in each block are adjusted to no less than about 70 and 20, respectively, $Prob._{InnocentBSR}^{compromise,total}$ will decrease to nearly zero

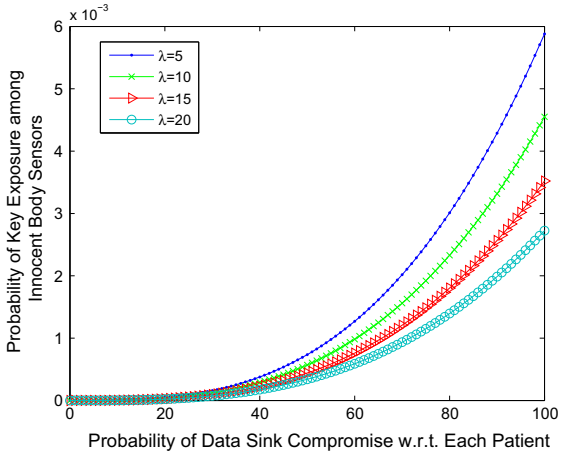

Fig. 7. The resilience to mobile adversaries towards λ and α ($\beta = 0.2, \gamma = 0.95, N = 20$).

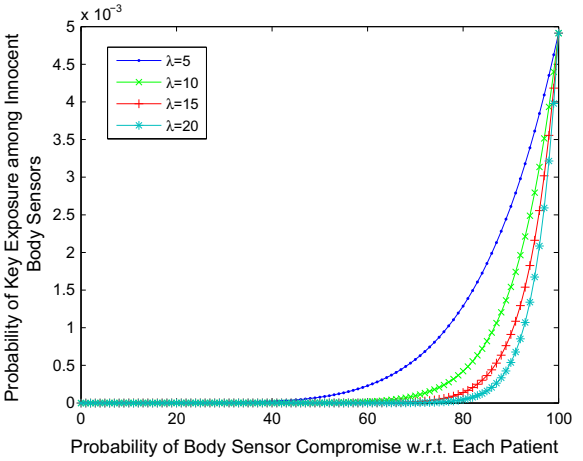

Fig. 8. The resilience to mobile adversaries towards λ and γ ($\beta = 0.2, \alpha = 0.85, N = 20$).

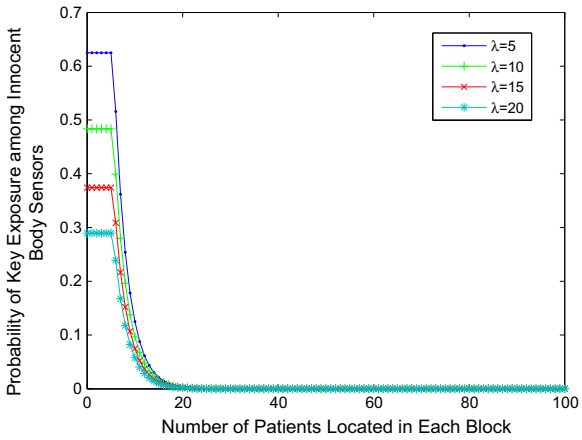

Fig. 9. The resilience to mobile adversaries towards λ and N ($\beta = 0.2, \gamma = 0.95, \alpha = 0.85$).

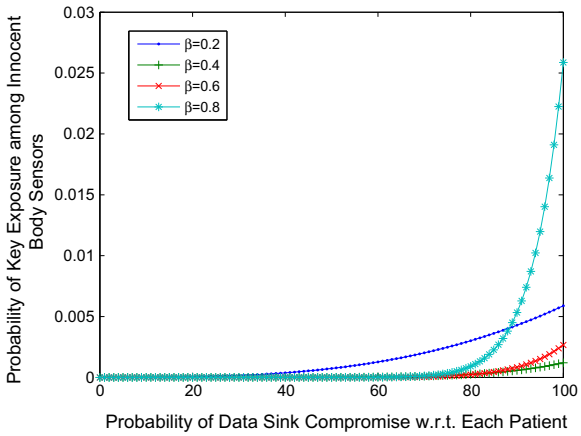

Fig. 10. The resilience to mobile adversaries towards β and α ($\lambda = 5, \gamma = 0.95, N = 20$).

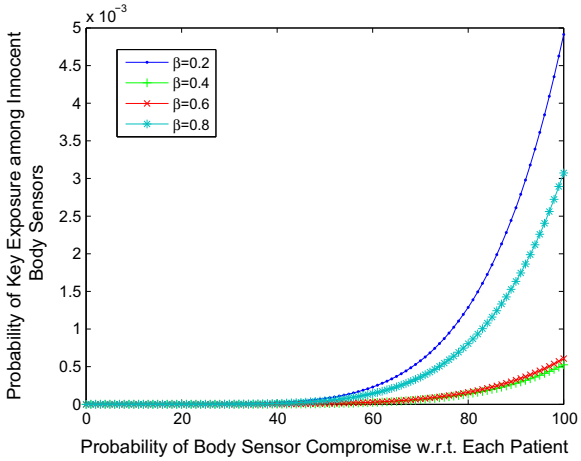

Fig. 11. The resilience to mobile adversaries towards β and γ ($\lambda = 5, \alpha = 0.85, N = 20$).

in a very short time faster than the speed, at which it increases as $Prob_{\cdot DS}(\alpha)$ and $Prob_{\cdot BSR}(\gamma)$ increase in Figs. 14 and 15. In this way, we can control security level according to the body sensor compromise attacks, sponsored by the mobile adversaries by adapting the parameters λ and N flexibly.

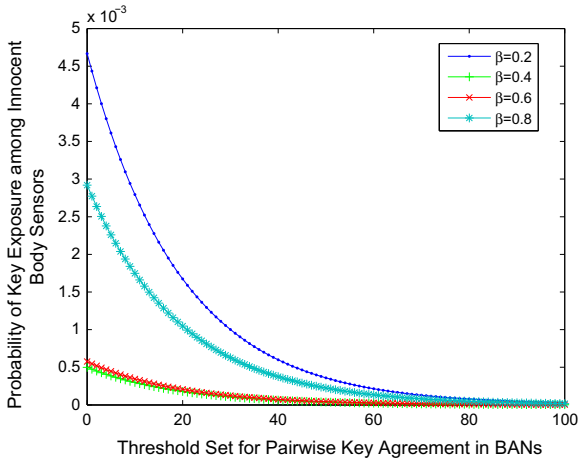

Fig. 12. The resilience to mobile adversaries towards β and λ ($\gamma = 0.95, \alpha = 0.85, N = 20$).

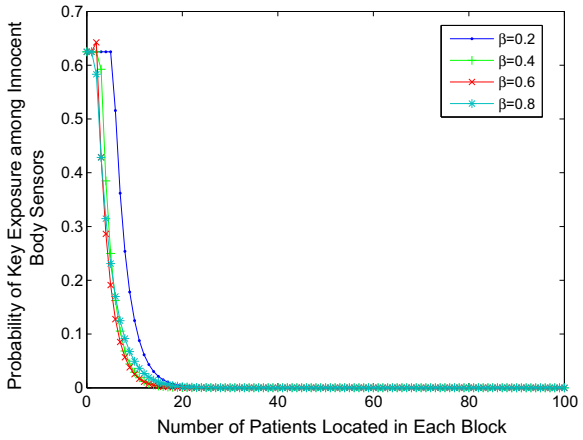

Fig. 13. The resilience to mobile adversaries towards β and N ($\lambda = 5, \alpha = 0.85, \gamma = 0.95$).

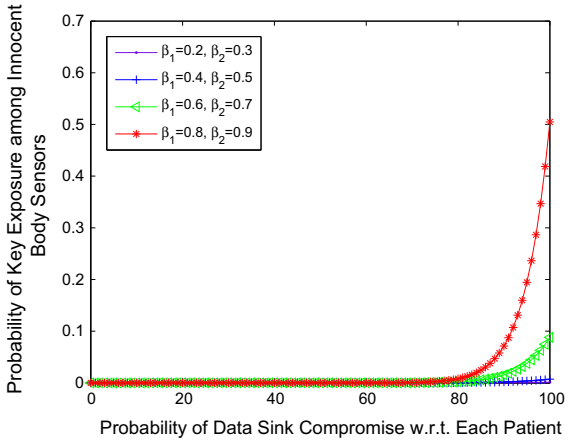

Fig. 14. The resilience to mobile adversaries towards β_1, β_2 and α ($\lambda = 5, \gamma = 0.95, N = 20$).

Finally, we perform a comparison by adjusting the threshold λ to make a tradeoff between the resilience and efficiency. Fig. 18 firstly illustrates the probability of key exposure among innocent body sensors and the computational cost of pairwise key agreement in WBANs, respectively decreases and increases as the threshold increases. Additionally, it can be observed

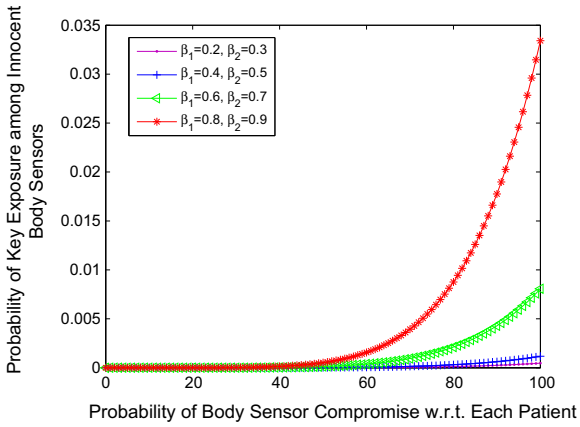

Fig. 15. The resilience to mobile adversaries towards β_1, β_2 and γ ($\lambda = 5, \alpha = 0.85, N = 20$).

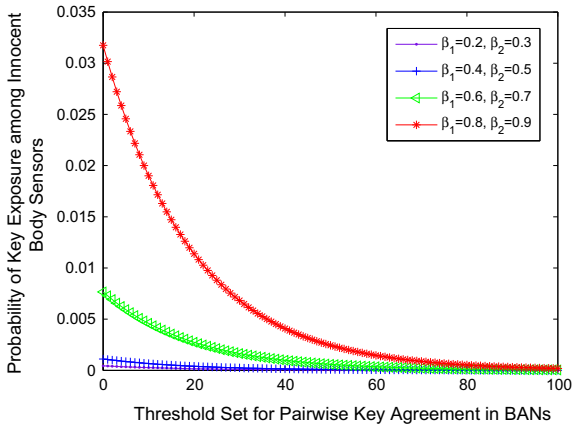

Fig. 16. The resilience to mobile adversaries towards β_1, β_2 and λ ($\gamma = 0.95, \alpha = 0.85, N = 20$).

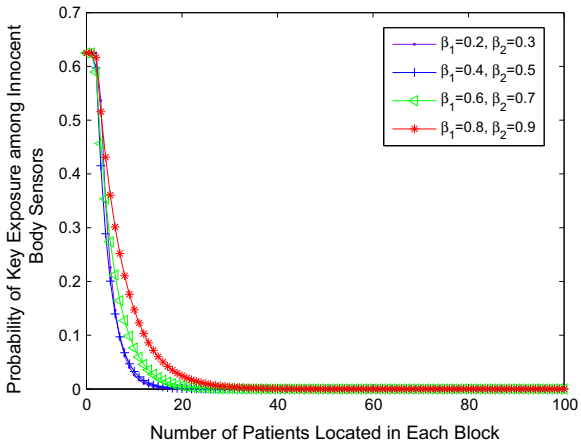

Fig. 17. The resilience to mobile adversaries towards β_1, β_2 and N ($\lambda = 5, \alpha = 0.85, \gamma = 0.95$).

that we can achieve the optimized tradeoff between the resilience and efficiency by setting the threshold λ, respectively as about 35, 10 and 25 when the probability of patients suffering from the same disease in each block is respectively assumed to be 20%, 50% and 80%.

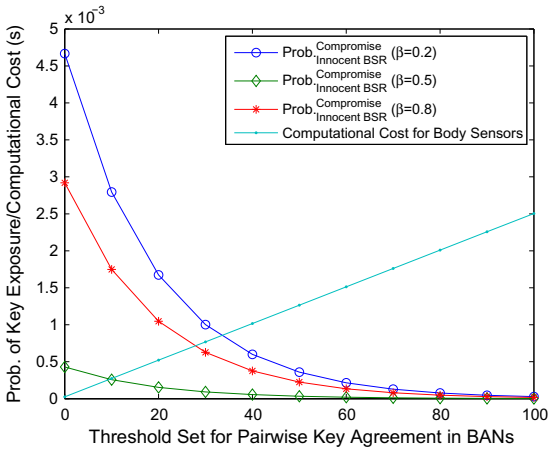

Fig. 18. The tradeoff between resilience and efficiency by adjusting the threshold λ ($\gamma = 0.95, \alpha = 0.85, N = 20$).

Therefore, we can conclude that our proposed secure and privacy-preserving key management scheme 4S well adapts to cloud-assisted WBANs in m-healthcare social networks.

7. Conclusions

A secure and privacy-preserving key management scheme for cloud-assisted WBANs, resilient to mobile attacks in m-healthcare social networks, is proposed in this paper. It significantly develops the adversary model of the existing work to a more practical situation, where the patients are allowed to behave as ordinary persons outdoors and are exposed to various sophisticated attacks. Then, it gives the formal definitions of time-based and location-based mobile sensor compromise attacks, proposes corresponding constructions, and proves their security and privacy. In a word, our scheme possesses the following characteristics: Firstly, it can resist two kinds of mobile attacks and protect the mobile patient's identity privacy, sensor deployment privacy and location privacy in both hierarchical and distributed environment efficiently, by introducing the identity blinding factor and extending the technique of proactive secret sharing. Especially, in our scheme, the computationally-intensive key material updating is outsourced to the cloud server with patient's privacy preservation, and the unchanged pairwise keys after key material updating significantly save computational cost for energy-constrained WBANs. Furthermore, the body's symmetric structure is integrated with the underlying Blom's symmetric key establishment mechanism to provide key materials, not requiring any pre-distributed information at deployment. Finally, simulation results show that our scheme far outperforms the previous ones in terms of resilience and efficiency. How to deal with the patients' selfishness in cooperation to resist mobile compromise attacks and integrate the incentive mechanisms into the m-healthcare social networks to stimulate such collabration, is in the scope of our future research.

Acknowledgments

This work was supported by the National Program on Key Basic Research Project (973 Program)-China and National Natural Science Foundation of China-China under Grant 2012CB723401, 61161140320, 61371083, 61373154 and 61033014.

References

[1] I.F. Akyildiz, W. Su, Y. Sankarsubramaniam, E. Cayirci, A survey on sensor networks, IEEE Commun. Mag. (2002) 102–114.
[2] S.D. Bao, C.C.Y. Poon, Y.T. Zhang, L.F. Shen, Using the timing information of hearbeats as an entity identifier to secure body sensor network, IEEE Trans. Inf. Technol. Biomed. 12 (6) (2008) 772–779.
[3] M. Barbosa, P. Farshim, Delegatable homomorphic encryption with applications to secure outsourcing of computation, in: CT-RSA 2012, LNCS 7178, Springer, Heidelberg, 2012, pp. 296–312.
[4] R. Blom, An optimal class of symmetric key generation systems, in: Eurocrypt 1984, LNCS209, Springer, 1985, pp. 335–338.
[5] E. Bresson, O. Chevassut, D. Pointcheval, J.J. Quisquater, Provably authenticated group Diffie–Hellman key exchange, in: ACM CCS '01, November 2001, pp. 255–264.
[6] H. Chan, A. Perrig, D. Song, Random key distribution schemes for sensor networks, in: IEEE Symposium on Security and Privacy, 2003, pp. 197–213.
[7] C. Chen, S. Pan, P. Kinget, ECG Measurement System. <http://www.cisl.columbia.edu/kinget_group/student_projects/ECG%20Report/E6001%20ECG%20final%20report.htm>.
[8] S. Cherukuri, K.K. Venkatasubramanian, S.K.S. Gupta, BioSec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body, in: Proc. IEEE Int'l Conf. Parallel Processing Wksp., October 2003, pp. 432–439.
[9] M.V. Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan, Fully homomorphic encryption over the integers, in: EUROCRYPT, 2010, LNCS 6110, Springer, 2010, pp. 24–43.
[10] R. Dutta, R. Barua, Provably secure constant round contributory group key agreement in dynamic setting, IEEE Trans. Inf. Theory 54 (5) (2008) 2007–2025.

[11] L. Eschenauer, V. Gl igor, A key management scheme for distributed sensor networks, in: Proc. of the 9th ACM Conf. on Computer and Communication Security, ACM Press, New York, 2002.
[12] G. Fortino, G. Di Fa tta, Engineering large-scale body area networks applications, in: 8th International Conference on Body Area Networks (BodyNets 2013), ACM Press, Boston, USA, 2013. September 30–October 2.
[13] G. Fortino, A. Guerrieri, R. Giannantonio, F. Bellifemine, SPINE2: developing BSN applications on heterogeneous sensor nodes, in: Proc. of IEEE Symposium on Industrial Embedded Systems (SIES'09), Special Session on Wireless Health, Lausanne (Switzerland), 8–10 July 2009.
[14] G. Fortino, A. Guerrieri, R. Giannantonio, F. Bellifemine, Platform-independent development of collaborative WBSN applications: SPINE2, in: Proc. of. IEEE International Conference on Systems, Man, and Cybernetics (SMC 2009), San Antonio (Texas, USA), Oct. 11-14, 2009.
[15] G. Fortino, M. Pathan, G. Di Fatta, BodyCloud: integration of cloud computing and body sensor networks, in: IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom 2012), Taipei, Taiwan, December 3–6, 2012.
[16] L. Gatzoulis, I. Iakovidis, Wearable and portable E-health systems, IEEE Eng. Med. Biol. Mag. 26 (5) (2007) 51–56.
[17] C. Gentry, Fully homomorphic encryption using ideal lattices, in: STOC, 2009, pp. 169–178.
[18] C. Gentry, S. Halevi, V. Vaikuntanathan, i-Hop homomorphic encryption and rerandomizable Yao circuits, in: CRYPTO, 2010,, LNCS 6223, Springer, 2010, pp. 155–172.
[19] A. Herzberg, S. Jarecki, H. Krawczyk, M. Yung, Proactive secret sharing or: how to cope with perpetual leakage, in: CRYPTO '95, LNCS963, 1995, pp. 339–352.
[20] I. Iakovidis, Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare records in Europe, Int. J. Med. Inform. 52 (1) (1998) 105–115.
[21] Y. Jiang, C. Lin, X. Shen, M. Shi, Mutual authentication and key exchange protocols for roaming services in wireless mobile networks, IEEE Trans. Wireless Commun. 5 (9) (2006) 2569–25476.
[22] A. Juels, M. Sudan, A fuzzy vault scheme, in: Proc. of IEEE Int. Symp. on Info. Theory, 2002, pp. 408.
[23] A. Juels, M. Wattenberg, A fuzzy commitment scheme, in: Proceedings of 6th ACM conference on Computer and Communication Security, 1999.
[24] I. Krontiris, T. Dimitriou, Towards intrusion detection in wireless sensor networks, in: Proc. of 13th European Wireless Conference, Paris, France, 2007.
[25] K. Lauter, M. Naehrig, V. Vaikuntanathan, Can homomorphic encryption be practical? in: ACM CCS, 2011.
[26] M. Li, S. Yu, W. Lou, K. Ren, Group device paring based secure sensor association and key management for body area networks, in: IEEE Infocom, 2010.
[27] X. Lin, R. Lu, X. Shen, Y. Nemoto, N. Kato, SAGE: a strong privacy-preserving scheme against global eavesdropping for E-health systems, IEEE J. Sel. Areas Commun. 27 (4) (2009) 365–378.
[28] D. Liu, P. Ning, Establishing pairwise keys in distributed sensor networks, in: Proc. of the 10th ACM Conf. on Computer and Communication Security, ACM Press, New York, 2003.
[29] L. Lu, Y. Liu, X. Li, Refresh: weak privacy model for RFID systems, in: IEEE INFOCOM, 2010.
[30] R. Lu, X. Lin, X. Liang, X. Shen, A secure handshake scheme with symptoms-matching for m-healthcare social network, Mob. Network Appl. (2010), http://dx.doi.org/10.1007/s11036-010-0274-2.
[31] O.G. Morchon, H. Baldus, Efficient distributed security for wireless medical sensor networks, in: International Conference on Intelligent Sensors, Sensor Networks and Information Processing, (ISSNIP), December 2008, pp. 249–254.
[32] C.C.Y. Poon, Y. Zhang, S. Bao, A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health, IEEE Commun. Mag. 44 (4) (2006) 73–81.
[33] Y. Ren, R.W.N. Pazzi, A. Boukerche, Monitoring patients via a secure and mobile healthcare system, IEEE Wirel. Commun. 17 (1) (2010) 59–65.
[34] J. Sun, Y. Fang, X. Zhu, Privacy and emergency response in E-healthcare leveraging wireless body sensor networks, IEEE Wirel. Commun. 17 (1) (2010) 66–73.
[35] M. Teplan, Fundamentals of EEG measurement, Measure. Sci. Rev. 2 (2) (2002) 1–11.
[36] K.K. Venkatasubramanian, A. Banerjee, S.K.S. Gupta, EKG-based key agreement in body sensor networks, in: Proceedings of IEEE Conference on Computer Communications Workshops, 2008.
[37] K.K. Venkatasubramanian, A. Banerjee, S.K.S. Gupta, PSKA: usable and secure key agreement scheme for body area networks, IEEE Trans. Inf Technol. Biomed. 14 (1) (2010) 60–68.
[38] E. Villalba, M.T. Arredondo, S. Guillen, E. Hoyo-Barbolla, A new solution for a heart failure monitoring system based on wearable and information technologies, in: International Workshop on Wearable and Implantable Body Sensor Networks 2006-BSN 2006, April 2006.
[39] H. Wang, H. Fang, L. Xing, M. Chen, An integrated biometric-based security framework using wavelet-domain HMM in wireless body area networks, in: ICC, 2011.
[40] K. Xing, X. Cheng from time domain to space domain: detecting replica attacks in mobile ad hoc networks, in: INFOCOM, 2010.
[41] F. Xu, Z. Qin, C.C. Tan, B. Wang, Q. Li, IMDGuard: securing implantable medical devices with the external wearable Guardian, in: IEEE INFOCOM, 2011.
[42] M. Zhang, Y. Fang, Security analysis and enhancements of 3GPP authentication and key agreement protocol, IEEE Trans. Wireless Commun. 4 (2) (2005) 734–742, 200.
[43] J. Zhou, Z. Cao, TIS: a threshold incentive scheme for secure and reliable data forwarding in vehicular delay tolerant networks, in: IEEE GLOBECOM, 2012.
[44] J. Zhou, Z. Cao, X. Dong, BDK: secure and efficient biometric based deterministic key agreement in wireless body area networks, in: 8th International Conference on Body Area Networks (BodyNets 2013), Boston, Massachusetts, United States, September 30–October 2, 2013.
[45] J. Zhou, Z. Cao, X. Dong, X. Lin, A.V. Vasilakos, Securing m-healthcare social networks: challenges, countermeasures and future directions, IEEE Wirel. Commun. 20 (4) (2013) 12–21.
[46] J. Zhou, M. He, An improved distributed key management scheme in wireless sensor networks, in: 9th. International Workshop of Information Security Applications 2008-WISA 2008, September, 2008.
[47] J. Zhou, X. Lin, X. Dong, Z. Cao, PSMPA: patient self-controllable and multi-level privacy-preserving cooperative authentication in distributed m-healthcare cloud computing system, IEEE Trans. Parallel Distrib. Syst. (in press).
[48] Y. Zhou, Y. Fang, Scalable and deterministic key agreement for large scale networks, IEEE Trans. Wireless Commun. 6 (12) (2007) 4366–4373.