I.J.Computer Network and Information Security, **2011, 4, 53-60**
Published Online June 2011 in MECS (http://www.mecs-press.org/)

Identity Authentication and Context Privacy Preservation in Wireless Health Monitoring System

Qiming Huang, Xing Yang, Shuang Li
School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing, P.R.China
Email: qmhuangcn@gmail.com, sapphirebeijing@gmail.com, tangsfh@yahoo.com.cn

***Abstract*—Privacy preservation is an important challenge for wireless health monitoring system. This paper analyses the privacy threat types based on the wireless health monitoring system architecture, and built the key system model for identity threat and context privacy preservation based on traffic analysis threat. To resist these threat , the integrated message encryption, identity authentication and traffic context privacy preservation, based on identity-based cryptography(IBC) and identity-based signature(IBS), is carried out at one time during the process of sending, receiving and accessing the patients' health information. Extensive analysis demonstrates the effectiveness of the proposed scheme.**

***Index Terms*—Telemedicine: *privacy perservation; identity-based encryption; identity-based digital signature;* wireless health monitoring system**

I. Introduction

Time is important for the sick in emergency. There are many acute patients who live far away from hospital and they probable cannot receive immediate treatment quickly. However, in china elderly people prefer staying at their home rather than accepting guardianship in the hospital. Over the past two decades, monitoring system of wireless technology have imposed a major impact on the revolution of human's lifestyle by providing the convenience and flexibility in accessing the internet services and various types of personal communication applications. The electrocardiogram (ECG) network remote diagnosis system can cover 43.8 million people in Taiyuan so that the hospital can perceive the cardiovascular patients' data in the first time, and provide remote diagnostic services. However, in February 2005 a worldwide survey done by Harris Interactive in New York found that about 70% of the populations were very concerned about a threat to the security and privacy of personal medical information. And this situation has been deteriorating. In Christ Saint Joseph Hospital, 16,000 copies of patient information were destroyed. In Wilcox Hospital of Hawaii, there are 130,000 copies of patient health information were unlawfully obtained, even in the Hospital of Chicago University, the staff was found to sell the patient personal medical information [1].

Due to the patient health information (PHI) become digitization compared to the traditional medical care, remote medical monitoring system has also brought a series of new challenges. The most important challenge is how to ensure the patient privacy during transmission of data to avoid the threat from the attacker [2]. The patients monitored remotely will express concern about their health information, which involves unauthorized information collection, information theft, privacy leaks, forged identity impersonation and so on [3]. If the patient data cannot be protected effectively, this will bring the patient's personal immeasurable loss and mental harm [4].

This paper analyze and compare the domestic and international status quo of privacy protection technology, research from the transmission, receiving, storing and access of patient information to the entire process of privacy protection, using identity-based encryption technology (IBC) in a wireless health monitoring system, and analyze the security performance of the protocol.

II. The Health Monitoring System

The architecture block diagram of the health monitoring system is described in figure 1. Each biosensor in the patient's body area network(BAN) will include a short-range transceiver that transfers data to a small BAN gateway. The gateway, in turn, would process data and resends it to a wireless modem/router for internet delivery. Each main unit is briefly explained as follows.[14]

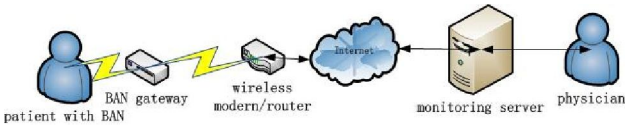

Figure 1. the health monitoring system architecture

- **Biosensor-Transceiver Pair**: Wide range of biosensors can be found in the market. Examples are sensors for heart rate, temperature, falling, bending, etc . Each sensor needs to be paired and packaged

- with a miniature low-power transceiver. As a matter of practicality, it would be much easier to use if the sensor-transceiver pair is packaged as a patch.
- **Gateway:** The gateway, would be responsible for data collection, processing and overall BAN network management. Having enough memory and processing power (a mid-size microprocessor) is inevitable. The gateway also includes two types of wireless communication: (i) a receiver to get data from biosensors and (ii) a wireless Ethernet adapter to communicate with the standard wireless router/switch.
- **Monitoring Server**: Monitoring server runs powerful back-end software to collect, analyze profile and make decisions. It is well understood that bio metrics of each individual are very much unique. Thus, for effective processing a personalized profile should be "learned" automatically by the server. This is a crucial step to minimize (and even achieves zero-level of) false positive (i.e. raising alarm for non-critical situations) and false negative (i.e. missing a critical, perhaps life-threatening situation). To do so, a combination of innovative learning and reasoning algorithms are required to interpret data properly during monitoring.

III. Problem Formalization

A. System Model

The design of the Health Monitoring System come with a lot of emerged challenges,. The government has established stringent regulations to ensure the security and privacy of patients' Personal Health Information(PHI) are properly protected, for example, HIPAA[15]. However, if an observer knows that a patient often sends his/her PHI to a specific physician, the observer can correctly guess the patient's disease with a high probability.

To preserve the context privacy, the Health Monitoring System is organized by a trusted authority(TA). The system model includes the registered patients, physicians, Electric Health Records(EHR) database in the monitoring server and TA, as shown in figure 3. Patient Alice, after registering himself/herself to TA, can get the some body sensor devices suitable to him/her, and then deploy a body body network at home so that PHI can be collected and sent to the EHR database and physicians.

B. Adversary Model

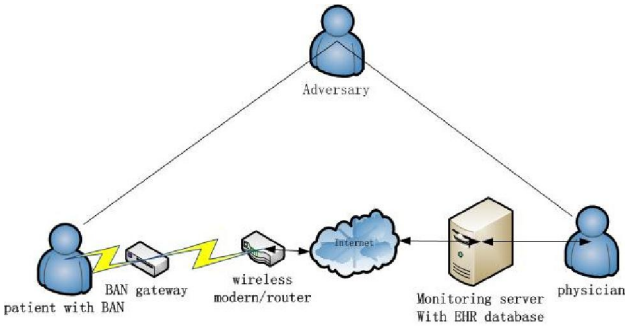

Figure 2. the health monitoring system with a adversary

These are three types of the threat[16]: mis-use of Patient identities, unauthenrized access and modification of PHI in the health monitoring system in figure 2. we consider three types of adversary: the Patient himself or herself, insiders (authorized EHR users, staff of the EHR organization, or staff of other mHealth support systems), and outsiders (third parties who act without authorization).

- Identity threat. There are three concerns here. First, the Patient may lose (or share) their identity credentials, enabling others to have access to their PHI in the EHR (or in their MN). Second, insiders may use Patient identities for medical fraud, for example, by submitting fraudulent insurance claims [16];the result can be financially or even medically damaging to the Patient. Furthermore, in the growing problem of medical identity theft, outsiders (or insiders) may use a Patient's identity to obtain medical services [17], potentially with financial or medical damage to the Patient. Finally, in some settings (such as research) Patient identities are removed from the PHI, and the risk is that an outsider may combine the de-identified data with data from another source to re-identify the Patients, that is, to re-link Patient identity to their PHI [18].
- Access threats. we explore threats related to unauthorized access to PHI, whether in the MN or the EHR. The first threat comes from the Patient himself or herself, because (under the definition of health information privacy) the Patient has a right to control the collection, use, and disclosure of PHI; if the Patient fails to express their consent consistent with their actual preference, for whatever reason, they may allow broader-than-intended collection, access or disclosure; Insiders may "peek" at Patient data, out of curiosity, or with the intent to harm the Patient (e.g., an employer who snoops on employer-provided EHR and fires workers with expensive conditions) [19], [20]. Outsiders may break into Patient records, which may lead to embarrassment (e.g., exposing a Patient's psychiatric data to his divorced spouse) [21]; Several of these threats involve the modification of health records. In a EHR, Patients (or insiders [19]) may mistakenly modify their data if the access-control policies are too permissive, or if the mechanisms too easily allow mistakes. Insiders may modify PHI intentionally, to obtain reimbursement via insurance fraud [22]. Outsiders may also modify a Patient's PHI, for fraud

or malice [21].

- Disclosure threats. we explore threats related to the disclosure of PHI, including data at rest and data in transit. We now survey work related to secure data transmission, device presence, and device compromise and theft. There are four fundamental challenges in secure transmission. First, the adversary may inspect the wireless-network packets and obtain sensitive medical data; Second, even if the wireless-network traffic is encrypted, in some settings it is possible for a clever adversary to use traffic analysis to determine characteristics of the traffic [23]. Third, the adversary may use physical-layer or link-layer fingerprinting methods to identify the device type. Fourth, because the wireless medium is open, an active adversary may inject frames or may selectively interfere with (cause collisions with) wireless frames.

C. Privacy Problem Statement

The health monitoring systems have many characteristics that make them more vulnerable to the privacy attack than other scenarios. In the health monitoring system, it should be ensured that the correct Patient is being sensed, that data is sent to the authentic information systems, and that only authorized personnel have access to the sensor data, so the identity authentication for patients, physician and EHR database is basis privacy requirement.

We can divide the privacy issues in health monitoring systems into two categories: content oriented privacy and contextual privacy [24], [25]. It is not difficult to withstand not only the content oriented privacy attacks due to many cryptographic techniques such as available encryption algorithms [26]. Contextual privacy means an adversary has the ability to link the source and the destination of a message in the system. If an adversary can link the patient with a specific physician, then the patient privacy will be disclosed. This is disclosure threats to broke the secure transmission.

Time is important for the sick in emergency. Identity authentication and context privacy preservation should be carried out with the encrypted message transportation. This is the research object of this paper.

IV. Related Work

Yang Guo-qing, Wang Dan, etc. built the security system model of remote transmission for medical information [5], using the public key infrastructure to complete the encryption and authentication of the information. But in the large-scale distributed network, the inconvenience problems from the update and remove of digital certificate need to be considered. Hu Jian-li, Li Xiao-hua, Zhou Bin proposed the security model of electronic medical records transmission [6], which uses document integrity monitoring, asymmetric encryption and decryption processing and the time stamp mechanism to guarantee the secure transmission of electronic medical records. M. Layouni, K. Verslype et al proposed privacy protection for remote monitoring of medical care [7]. Achieved the automated examine and approved process through the patient's pre-configuring, they applied symmetric encryption and RSA algorithms to complete the encryption and authentication for patient information. The U.S. government has also established stringent regulations to ensure that the security of patients' PHI is properly protected, for example HIPAA [8].

Generally, to achieve contextual privacy, the existing approaches can be categorized into two types: one is *by protecting the source location privacy*, and the other is *by protecting the destination location privacy*.

By protecting the source location privacy, the relation between the source and the destination can be cut off, and then the contextual privacy is achieved. Kamat et al. [11] provided two new techniques to provide efficient source location privacy. One technique is called *routing with fake sources*, and the other is called *phantom single path routing*. In the routing with fake sources, when a source wants to send data, several fake sources, which are away the real source, are involved. Then, both the real and fake sources send data at the same time. Clearly, this technique can provide location privacy against local eavesdropping. However, it is not suitable for health monitoring systems. In real life, since the locations of different patients are scattered, when a patient wants to send data, it is not reasonable to assume that he can inform other patients to participate. In *phantom single-path routing*, after a data is generated by the source, it will walk a random path before reaching the destination. By walking a random path, the source data can prevent the local eavesdropping. Another technique, called cyclic entrapment [13], is very similar to the phantom single-path routing, which deals with the local eavesdropping by creating looping pathes at various places. Although the above techniques can deal with non global eavesdropping, they are still not suitable for the defined health monitoring system, since the tricks used in these techniques are not effective to a strong global eavesdropper. To deal with the global eavesdropping, Mehta et al. [12] proposed two new techniques: *periodical collect* and *source simulation*. However, the *periodical collect* should send dummy packets and thus could cause large data delivery latency. Therefore, it is not suitable for the real health monitoring system. Although the source simulation method provides practical tradeoffs between privacy, communication cost and latency, it will bring inconvenience to the patient since a set of virtual objects should be simulated. On the other hand, the global eavesdropping they considered is confined to the weak global adversary.

Protecting the destination privacy is another alternative to achieve contextual privacy. In 2007, Jian et al. [27] proposed a location privacy routing protocol, call LPR, to achieve path diversity. By combining LPR with fake packet injection, the location privacy of the receiver can be protected, and subsequently, the contextual privacy is achieved. Similar to [27], Lin X, Lu R, and Shen X, etc. [2] deal with the contextual privacy also from protecting the receiver's location privacy. They proposed a strong anti-wiretapping privacy protection system which used the IBC to encrypt based on Diffie-Hellman problem,

verify the information sent by the patient through the digital signature, and applied the broadcast mechanism for the global Network eavesdropping to achieve the objective of protecting patient privacy.

V. PRELIMINARIES

As early as 1984, Shamir first proposed the concept of IBC. Then the fellow specific program for IBC [9] was proposed by Boneh and Franklin in 2001.

IBC apply bilinear map Weil pairing. Let G_1 and G_2 be a generated additive group and a multiplicative group with the same prime order q. Discrete logarithm problem (DLP) is assumed to be hard in both G_1 and G_2. Let P denote a random generator of G_1 and $e: G_1 \times G_1 = G_2$ denote a bilinear map constructed by modified Weil pairing with the following properties:

- Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$, $\forall P, Q \in G_1$ and $\forall a, b \in Z_q^*$;
- Non-degenerate: $\exists P, Q \in G_1$ such that $e(P, Q) \neq 1$;
- Computable: there is an efficient algorithm to computing $e(P, Q), \forall P, Q \in G_1$.

VI. PATIENT PRIVACY-PRESERVATION SYSTEM

This privacy protocol includes the generation of system parameters, the registering of patients and doctors, and the transmission, reception, storage and access of patient health information (PHI). The main information transfer and key distribution is completed, according to Fig. 2, among the Trusted Authority (TA), the health monitoring server with electronic health record (EHR) database in hospital, the patient Alice and doctor Bob, shown as figure 3. Direction of the arrow in the Fig. 1 represents the direction of message transmission. The specific meaning of the symbols in this agreement is shown in Table 1.

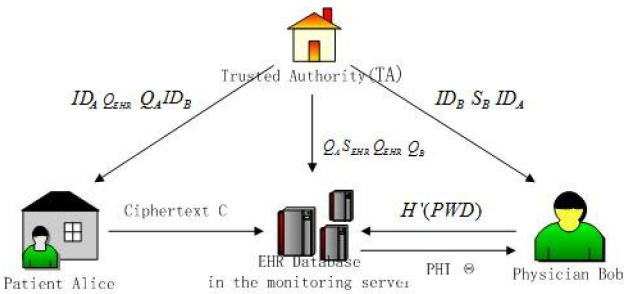

Figure 3. Information transfer in the health monitoring system

TABLE I. SYMBOL MEANING

Symbol	Explanation
A, B	Patient Alice, Physician Bob
IBC_Q	IBC encryption by Q
IBS_S	IBS signature by S
$H(g)$	Hash function
$\|$	concatenation
T	Time stamp
$\perp$	Terminal and disgard
$\oplus$	exclusive

A. System parameters generation

To establish this system, TA first initializes all required system parameters. Input the security parameters $\xi \in \mathbf{Z}^+$ to the parameter generator PG and output a tuple $(q, G_1, G_2, e, P_0, H_1)$. TA selects a random number $s_0 = \mathbf{Z}_q^*$ as a master-key and always keep its secret. Then the two hash functions $H_1: \{0,1\}^* \to G_1$ and $H_2: G_2 \to \{0,1\}^n$, and generator $P_0 \in G_1$ are chosen.

This encryption algorithm is ID-based cryptography (IBC), and the signature algorithm is ID-based signature (IBS) [10]. All the patients health information (PHI) are stored in the EHR database. The health monitoring server with EHR database received the private key $S_{EHR} = s_0 H_1(ID_{EHR})$ and the corresponding public key $Q_{EHR} = s_0 P$ from TA.

B. Physician and Patient Registration

Alice is a heart disease patient. The cardiovascular disease doctor Bob diagnoses Alice in hospital. When Alice registers in the health monitoring system, she inputs her personal information and then gets her personal identity ID_A from the health monitoring server. TA computes her private key $S_A = sH_1(ID_A)$, and transfers the corresponding public key $Q_A = sP$ to the health monitoring server. Alice gets the medical equipments of heart disease, Bob's ID, and public key Q_{EHR} of the EHR data center.

The cardiovascular disease doctor Bob gets his identity ID_B when he fills in personal information to register the health monitoring server. Bob inputs the personal logon password PWD_B, computes the hash value $H(PWD_B)$ which is stored in EHR data center. Bob gets his private key $S_B = s_0' H_1(ID_B)$ and the corresponding public key $Q_B = s_0' P$ from TA.

C. Patient Health Information Transmission

After Alice gets the medical equipments and goes back to home, the BSN constructed by these instruments can collects her health data m. Before the information are sent to the EHR data center through internet, we need

to take corresponding encryption and sign signature to ensure that during the information transmission process it can resist the malicious attacks like decryption, tamper and forging etc. At the same time, we use time stamp technology to against replay attack. The input is the collected Alice's health information m , and the output is a ciphertext C which is ready to sent. The established process is shown in Fig. 4.

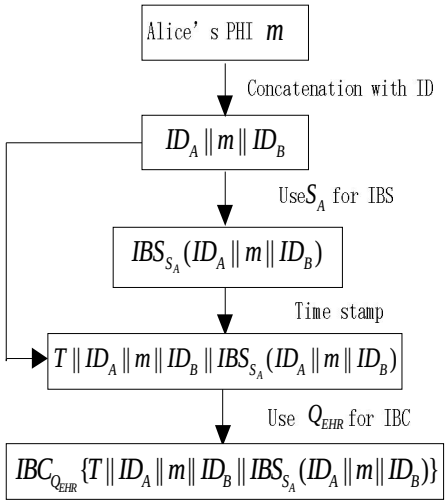

Figure 4. Patient information ready for transmission to EHR data center

D. Patient Health Information receiving and storing

Patient Alice's personal health information is transferred to the EHR data center. When EHR data center receives the ciphertext C , firstly it uses its own private key to decrypt the message and verify the legitimate identity of Alice. The message stored in the EHR data center is the ciphertext $C = IBC_{QEHR}(ID_A \| m \| ID_B)$ encrypted with the private key of the health monitoring server. Only docotor Bob can accessed Alice's health message .The process shown in Figure 5.

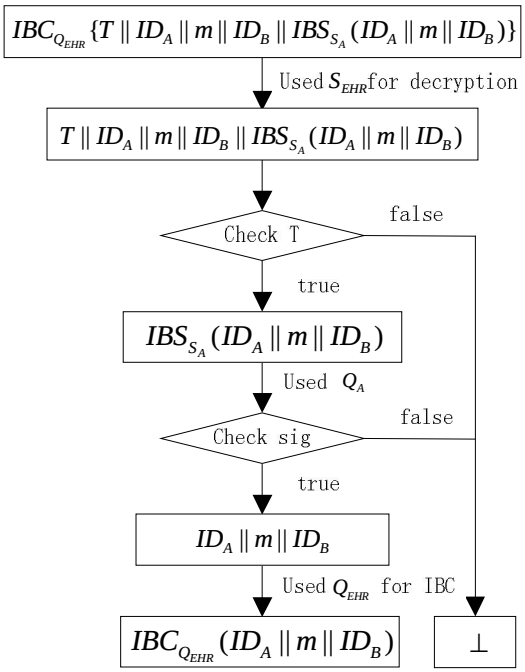

Figure 5. PHI receiving and storing

E. Patient Health Information Recovering

The health monitoring server sent a notice message which shows receiving information of the patient Alice to the doctor Bob. Registered Bob enter the health monitoring server with the password PWD_B . After the health monitoring server authenticates Bob's identity of physician based on role-based access control, Bob enters into the system and accesses the information m by querying. The process of the process is shown in Figure 6.

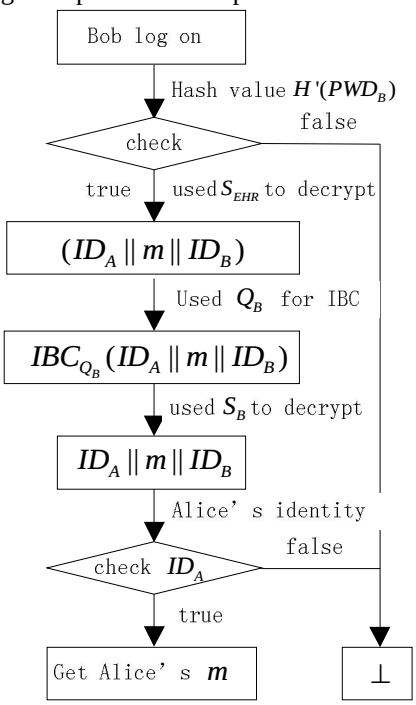

Figure 6. PHI recovered by his doctor

VII. Privacy Preservation Analisis

This privacy protection mechanism has the following safety performance.

F. Confidentiality

In this Agreement, we use encryption algorithm to protect patient information. As a basic safety protection method for the patient privacy, we apply this identity-based encryption algorithm to the patient's health information during the process of remote transmission information for patient, which can effectively resist the interception and eavesdropping by malicious attackers. The disclosure of patient privacy is prevented with encryption.

The patient's health information is guaranteed by the security of $IBC(ID_A \| m \| ID_B)$. If the ciphertext $IBC(ID_A \| m \| ID_B)$ is provably secure, so does the patient's health information.

The safety of $IBC(ID_A \| m \| ID_B)$ is based on the assumption that it is difficult to solve Bilinear Diffie-Hellman (BDH) Problem on cyclic groups which generated by parameters generater.

Let G_1 and G_2 be a generated additive group and a multiplicative group with the same prime order q. e: Let P denote a random generator of G_1 and $e: G_1 \times G_1 = G_2$ denote a bilinear map. The BDH problem of (G_1, G_2, e) is: calculating $w = e(P,P)^{abc} \in G_2$ with known parameters $(P, aP, bP, cP)^{abc}$. And $a, b, c \in Z_q^*$ are ransom.

If an adversary have a special arithmetic A(), and the probability he/she solve BDH is :

$$Pr[A(P, aP, bP, cP) = e(P,P)^{abc}] \geq \varepsilon$$

Then we define ε as superiority of the adversary.

Bilinear Diffie-Hellman (BDH) is that for any polynomial $f(x) \in Z[x]$ the polynomial-time arithmetic A() to solve BDH is less then $1/f(x)$. In another word there is not any A to solve BDH within polynomial-time.So this identity-based encryption algorithm can satisfy our need.

G. Authenticity

The patients sent remotely the health information to the EHR data centers. Then the identity-based signature scheme is used to sign the information. After the EHR Health Center receives the ciphertext message, the information is determined whether it is from a legitimately registered user by verifying the identity signature of patient. If the communication party is found as an illegal user, the process is terminated immediately so that we can resist effectively the false information or identity from an attacker to deceive the hospital. Doctors also need to be authenticated with the identity for accessing to EHR data center in order to against forgery attacks.

H. Efficiency

Integration transmission of encryption and signature for patient information are completed, achieving the effect of saving communication time. In addition, the information receiver can identify the freshness of the timestamp. The replaying attack refers to the adversary maliciously replaying some valid but old messages. If the time stamp has expired, the recipient discards the message. It can effectively resist replay attack of such models.

I. The Context Privacy

The Context Privacy is cut off the direct link between a patient and his/her physician, for attackers can get some information of patient such as what kind of illness do he/her get. Through the traffic analysis an attacker can identify the relation between patients and doctors then determine the patient's health condition. In the reference paper [2], the EHR database center broadcasts patients' encrypted information to all doctors in order to resist path eavesdropping. Our paper uses the method that physicians take the initiative to log on EHR data center to access information.

The information $IBC(ID_A \| m \| ID_B)$ in the method in our paper achieves unconditional link privacy by doctors' logging on.

Since $IBC(ID_A \| m \| ID_B)$ has been protected, the only way for the adversary A to find $IBC(ID_A \| m \| ID_B)$'s destination is by using all traffic information he obtained. However, in the eye of the adversary, each physician will get message only if they log on. It is not at the same time that the patients and doctors send or get messages. The adversary does not know the information from a certain patient transports to which doctor.

We define that the advantage of *A* breaking the link privacy property is

$$Adv_A^{\log on} = \gamma.\Pr[j = j'] - 1.$$

For all adversaries *A*, if the advantage $Adv_A^{\log on}$ is negligible, we say the link privacy is achieved. If the advantage $Adv_A^{\log on}$ is exactly 0, then the link privacy is unconditional. [2]

Suppose that the numbr of doctors are γ. j' stands for the right doctor, and j satnds for the one which is choosed by the adversary. In the eye of the adversary, each doctor is equal .Therefore, $\Pr[j = j'] = \frac{1}{\Upsilon}$. Then, by definition, we have

$$Adv_A^{\log on} = \gamma.\Pr[j = j'] - 1 = \gamma.\frac{1}{\gamma} - 1 = 0$$

so the information $IBC(ID_A \| m \| ID_B)$ in the method in our paper achieves unconditional link privacy by doctors' logging on.

Therefore, to achieve high privacy, γ should be a large number. In the model of Wireless Health Monitoring System , there are many physicians. So it is reasonable to admit this method is confidential.

The transmission between patients and doctors do not have corresponding relationships. Thereby the path eavesdropping can be effectively resisted.

VIII. Conclusion

This paper proposes a protection scheme of patient privacy in wireless health monitoring system and applies IBC and IBS to complete the encryption, identity authentication and context privacy preservation for patients' health data. It resists the malicious attacks such as capture, tampering with the data confidentiality and authentication. Meanwhile, the ciphertext storage effectively protect patients' privacy information. Appropriate ways for the transmission can resist path eavesdropping. This scheme completes the encryption, authentication and context privacy preservation at one time during the transmission of patient information, which can save the communication time and allow a physician to diagnosis the patient in a timely manner.

Acknowledgment

This work is supported by the National Natural Science Foundation of China (No. 61072039), the Beijing Municipal Natural Science Foundation (No.4102040).

References

[1] Rash, M.C. Privacy concerns hinder electronic medical records. The Business Journal of the Greater Triad Area (Apr. 4, 2005).

[2] Lin X, Lu R, Shen X, Nemoto Y, Kato N.SAGE: a strong privacy preserving scheme against global eavesdropping for ehealth systems. IEEE Journal of Selected Areas of Communications.

[3] Ou, C.-M. and Ou, C. R., "A High-Level 3G Wireless PKI Solution for Secure Healthcare Communications", EuroPKI 2006, Lecture Notes in Computer Science 4043, Springer-Verlag, 2006, pp. 254-256.

[4] Yuhai Zhang, Yongyong Xu, Lei Shang, etc.An investigation into health informatics and related standards in China. International Journal of Medical Informatics[J]. 2007(76),614–620.

[5] M. Layouni, K. Verslype, M. T. Sandikkaya. Privacy-Preserving Telemonitoring for eHealth. Data and Applications Security 2009, LNCS 5645, pp. 95–110, 2009.

[6] Md. Mokammel Haque, Al-Sakib Khan Pathan, and Choong Seon Hong, Securing U-Healthcare Sensor Networks using Public Key Based Scheme, ICACT 2008：17-20.

[7] U. Sax, I. Kohane, and K.D. Mandl, "Wireless Technology Infrastructures for Authentication of Patients: PKI That Rings," J. Am. Medical Informatics Assoc., vol. 12, no. 3, pp. 263-268, 2005.

[8] Health Insurance Portability Accountability Act (HIPAA).

[9] D. Boneh and M. Franklin, Identity-based encryption from the weil pairings. Advances in Cryptology-Asiacrypt Springer-Verlag, 2001. LNCS 2248, pp.514-532.

[10] J. Cha and J. Cheon, An identity-based signature from gap diffie-hellman groups. in Prof. Practice and Theory in Public Key Cryptography– PKC'2003, Springer-Verlag, 2003. LNCS 21392567 pp. 18-30.

[11] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing sourcelocation privacy in sensor network routing", in Proc. 25th IEEE International Conference on Distributed Computing Systems - ICDCS 2005, Columbus, Ohio, USA, June 2005, pp. 599-608.

[12] K. Mehta, D. Liu, and M. Wright, "Location privacy in sensor networks against a global eavesdropper", in Proc. IEEE International Conference on Network Protocols, 2007 - ICNP 2007, Beijing, China, 2007, pp. 314-323.

[13] Y. Ouyang, Z. Le, G. Chen, J. Ford, and F. Makedon, "Entrapping adversaries for source protection in sensor networks", in *Proc. International* Symposium on on Word of Wireless, Mobile and Multimedia Networks *(WoWMoM)*, pp. 23 -24, June 2006.

[14] *Shinyoung Lim, Tae Hwan Oh, Young B. Choi, Tamil Lakshman, Security issues on wireless body area network for remote healthcare monitoring,* 2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing.

[15] Health Insurance Portability Accountability Act (HIPAA).

[16] P. Dixon, "Medical identity theft: The information crime that can kill you," The World Privacy Forum, May 2006. Available at http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf

[17] M. E. Johnson, "Data hemorrhages in the health-care sector," in Financial Cryptography and Data Security. Springer-Verlag, Feb. 2009. DOI 10.1007/978-3-642-03549-4 5

[18] B. Malin, "Re-identification of familial database records," in AMIA Annual Symposium Proc.. AMIA, Nov. 2006, pp. 524–528. Available at http://view.ncbi.nlm.nih.gov/pubmed/17238396

[19] S. Sinclair and S. W. Smith, "Preventative directions for insider threat mitigation via access control," in Insider Attack and Cyber Security: Beyond the Hacker. Springer-Verlag, 2008, vol. 39, pp. 173–202. DOI 10.1007/978-0-387-77322-3 10

[20] A. Appari and M. E. Johnson, "Information security and privacy in healthcare: Current state of research," Proc. Workshop on Information Security and Privacy (WISP), Aug. 2008. Available at http://www.ists.dartmouth.edu/library/416.pdf

[21] E. Messmer, "Health care organizations see cyberattacks as growing threat," Network World, Feb. 2008. Available at http://tinyurl.com/66b2pv

[22] P. Dixon, "Medical identity theft: The information crime that can kill you," The World Privacy Forum, May 2006. Available at http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf

[23] C. V. Wright, F. Monrose, and G. M. Masson, "On inferring application protocol behaviors in encrypted network traffic," Journal of Machine Learning Research, vol. 7, pp. 2745–2769, Dec. 2006. Available at http://portal.acm.org/citation.cfm?id=1248547.1248647

[24] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing sourcelocation privacy in sensor network routing", in *Proc. 25th IEEE International Conference on Distributed Computing Systems - ICDCS 2005*, Columbus, Ohio, USA, June 2005, pp. 599-608.

[25] K. Mehta, D. Liu, and M. Wright, "Location privacy in sensor networks against a global eavesdropper", in *Proc. IEEE International Conference on Network Protocols, 2007 - ICNP 2007*, Beijing, China, 2007, pp.314-323.

[26] W. Mao, *Modern Cryptography: Theory and Practice*, Prentice Hall PTR, 2003.
[27] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "Protecting receiver-location privacy in wireless sensor networks", *Proc. IEEE INFOCOM 2007*, Anchorage, Alaska, USA, May 2007.

Qiming Huang received the B.S. degree from Jilin University, Changchun, P.R.China, in 1989, and the Ph.D degree in Huazhong University of Science and Technology, Wuhan, P.R.China, in 1998, was a post doctoral fellow at Computer Science and Technology Department in Zhejiang University, Hanzhou, P.R.China, until 2001. He is currently an associated professor of School of Computer and Communication Engineering at USTB, Beijing, P.R.China. His research interests include security and privacy of Internet of Things, Cloud Computing and Artificial Intelligence. He has authored or coauthored more than 30 journal papers and conference papers.

Xing Yang received the M.S. degree from Communication Engineering Department at USTB in 2010.

He was a student of Communication Engineering Department at USTB.

Shuang Li received the B.S. degree from Agricultural University of Hebei, Baoding, P.R.China, in 2010.

She was a M.S. student of Communication Engineering Department at USTB.

