A NOVEL TRI-FACTOR MUTUAL AUTHENTICATION WITH BIOMETRICS FOR WIRELESS BODY SENSOR NETWORKS IN HEALTHCARE APPLICATIONS

Chen-Guang He[1, 2], Shu-Di Bao[3, 1, *], and Ye Li[1]

1. Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Nanshan Zone
Guangdong, China, 518055

2. University of Chinese Academy of Sciences, Shijingshan Zone
Beijing, China, 100049

3. School of Electron and Information Engineering
Ningbo University of Technology, Haishu Zone
Zhejiang, China, 315010

Emails: cg.he@siat.ac.cn; shudi.bao@gmail.com; ye.li@siat.ac.cn

---

Submitted: Sep. 29, 2012 ***Accepted: May 16, 2013*** ***Published: June 5, 2013***

Abstract - User authentication, as a fundamental security protocol, has been addressed with more concerns recently. Unlike normal authentication processes invoked by a user to access the network, biosensors with healthcare applications normally need to be validated automatically, followed by data transmission to the remote server without any explicit request. Hence, implied authentication procedure involved in such application scenarios shall be addressed. In this paper, a novel tri-factor user

authentication protocol with mutual access is proposed for the body sensor networks (BSN) in healthcare application. It is demonstrated that the proposed protocol has its advantages over the existing two-factor user authentication schemes.

Index terms*:* BSN, Biosensor, Mutual Authentication, Security, Pattern Vector.

I. INTRODUCTION

Wireless sensors devices are more and more widely used in various aspects of our social life, such as traffic monitoring, meteorological survey, resource protection, manufacturing and healthcare systems. With the development of sensor and network technologies, wireless sensor networks (WSN) is also by far the best fundamental infrastructure as the perception layer during the construction of the Internet of Things (IoT). In almost all cases, security of WSN is a key issue due to the fact that the sensors can be deployed in most of the environments being with the ubiquitous and widespread characteristics as well as accessed either in complex communication situation or by a remote mode. For the valuable and important data collected from the sensors in terms of battle field status, national resource analysis and health status of persons, it is unacceptable that the communication process are broken and messages are leaked or blurred being under the adversaries' attack. However, since sensors are usually configured with scanty resources including limited power energy and memory capacity, complicated cryptography methods are not feasible for securing WSN in most cases. A powerful but resource-saving security protocol is very crucial. Although there has been significant progress gained in WSN about security of link and network layers, application layer security, which is a basic requirement in many application scenarios, is more or less neglected [1]. Therefore, security is still an open issue for WSN at every level of network infrastructure, which actually becomes an urgent requirement to be met with, especially in applications of healthcare, where wireless biosensors arranged on human body to form a wireless body sensor network (BSN) to play a key role in medical and healthcare monitoring.

User authentication is deployed as a basic solution to implement the data access control, especially in the password-based authentication scheme. It is adopted for remote user authentication [2]. A pair of user identifier and password, as one kind of secure factor, can meet

the security requirement of information system to some extent. However, for critical systems such as battle environment or special applications like mobile healthcare services, it is not nearly enough. Theoretically, the more independent secure factors combined together and introduced into the scheme, the more difficult for adversaries to attack it. Consequently, more and more multi-factor user authentication schemes have been introduced [3, 4], which usually authenticate users by two distinct factors considering of the computing and management overhead. Chang and Wu [5] firstly proposed a scheme using smart card as another factor during the authentication process, and Das [1] proposed a practical two-factor user authentication protocol in WSN. In general, smart card is regarded as a physical device and issued to the user who first registers to a system with the capable of powerful computing and lager memory capacity [6].

This study focuses on the context of wireless biosensors applications for human health monitoring with mobile network access to remote services. The remainder of this paper is organized as follows. Previous works about two-factor user authentication are summarized in Section II. We introduce the application scenarios and the basis of biometric method, and then propose a mutual authentication protocol for securing communications between sensors and a remote server in Section III, followed by the protocol analysis and implementation in Section IV. Conclusions are finally given in last Section.

II. RELATED WORK

Since Chang et al [5] proposed to use a smart card to accomplish the authentication procedure, it has been studied in plenty of literatures to be applied into security protocols for access control. As far as the wireless sensor network is concerned, Benenson et al. [7] had first sketched several security issues in WSNs, especially about the access control and proposed the notion of n-authentication. Hwang and Li [8] proposed a scheme based on ID cryptosystems. Chan et al. [9] then analyzed the flaws of this scheme and indicated that it was vulnerable to the impersonation attack. Subsequently, Awasthi and Lal [10] presented a remote user authentication scheme using smart cards with forward secrecy in 2003. However, Lee et al. [11] pointed out that Awasthi's protocol was incorrect being lacking the ways to get time factor involved in verification phase. Das et al. [2] proposed their scheme and claimed that it was not necessary to maintain a password and verification table. Unfortunately, Awasthi gave an attack model [12] illustrated that anyone

could access system with an arbitrary password input, which implied Das' protocol was very vulnerable. Again, Das proposed a new protocol used two-factor user authentication scheme in 2009. Huang et al.[13] enhanced this scheme's capability of anti-eavesdropping by increasing the computing time. Kumar [14] presented an efficient framework under predetermined strict conditions, which however are assumptions over practical utilization. In 2010, Khan and Alghathbar [15] reviewed comprehensively Das' scheme for its security properties, and proposed an improved protocol which was claimed to be strong enough to resist attacks.

If user password can indicate *what you know*, then smart card indicates *what you have*. Source address analysis can guarantee *where you are* and physiological characteristic, especially based on the physiological signals sampled by biosensors from inner or outside of the body area, can directly shows *who you are*. Adams and Wiener [16] used two partial encrypted key seeds derived from a plurality of biometric input to merge a finally cipher key based on the error correction. Bhargav-Spantzel [17] proposed a two-phase authentication mechanism in which the first one consists of a two-factor biometric authentication based on zero knowledge proofs, and the second one combines several authentication factors in conjunction with the biometric features to provide a strong authentication.

Signal features of electroencephalograph (EEG) and electrocardiograph (ECG) were also proposed to be an irrefutable evidence [18, 19] for user authentication. Sufi and Khalil [20] proposed a novel method of ECG biometric generated from compressed ECG harnessing data mining techniques like feature selection and clustering. Gu et al. [21] worked out a method using photoplethysmograph (PPG) signals to distinguish human individuals in 2003. Poon [22] and Bao et al. [23] proposed and improved a scheme using interpulse intervals (IPIs) of heartbeats to generate entity identifiers (EIs) for mutual authentication among sensors in the same body area, respectively. Miao [24] and Cao et al. [25] subsequently proposed key distribution schemes with improved recognition rate of EIs. Nevertheless, authentication protocol whatever for sensors or users should also be addressed in the application layer. Recently, Shen et al. [26] design a rapid way to identify one's ECG. Overall security solutions across the multi-gateway networks are still research hotspots, and the existing studies under different network environments can be referred to each other [3, to achieve strong authentication adequately, as well as some researches of trusted signature framework [29] in wireless sensor networks.

III. APPLICATION SCENARIOS AND PROTOCOL

a. Application Requirements

Before illustrate our work, any symbol and its meaning used in this paper are shown in Table 1 .

Table 1: List of notions and symbols used in the proposed protocol

Symbols		**Notions**
BSn		Body Sensor nodes
SE		Sever End
MGW		Mobile Gateway node
User	O_i	The i^{th} pattern of Owner
	S_j	The j^{th} body sensor node
	U_k	The k^{th} User
PW_k		Password of the k^{th} user
PV_i		Pattern Vector of the i^{th} owner
ID_k		Login ID of the k^{th} user
CID		Compound Identifier
x_a		A different session key according to different applications pre-stored in the MGW and BSn
K		A symmetric Key, permanent
h(.)		One-way hash function
||		Bitwise concatenation
$\oplus$		XOR operation
A→B:M		A sends M to B through an unsecure channel

$A \Rightarrow B:M$	A sends M to B through a secure channel

Contemporary mobile devices are getting more and more powerful and intelligent that can act as a key gateway node which connects monitoring sensor nodes with a remote server. In many cases, a mobile device can also be regarded as a sharing device among a certain group of people, e.g. a whole family or a clinic unit. Similar to general User-Gateway-Sensor structures, the 3-layer infrastructure for mobile healthcare systems consists of Server End (SE), Mobile Gateway (MGW) and Body Sensor nodes (BSn). However, the SE always plays a dual role, passive and active, in which the former is providing services when the MGW invokes requests and the latter can accesses the sensors actively after being authenticated by the MGW. Mutual login must be introduced into SE, which is logging or logged in. Furthermore, people who want to check their health status from SE or BSn via mobile devices directly should be permitted after being authenticated. Though a pair of user identifier and password is the traditional method for this purpose, inputting password is sometimes inconvenient or even impossible with biometric characteristics outside the body, such as fingerprint for a physically disabled person. Hence, using more general biometrics as a kind of authentication factors is needed.

The Figure 1 shows a typical application scenario under our requirement specifications. Proposed protocol would be implemented over these real equipments. A mini hotter, which is placed on the one's chest, can measure people's heart beat and breathe rate, described as ECG and PPG signals. IPIs can be generated from this information. A specialized application built in mobile can receives the data from these nodes by Bluetooth, generated a group of pattern vectors, and then transmits them to the server end for the sake of comparing with the legal/registered pattern vectors stored previously. Obviously, mobile plays a gateway at that time, and smart card id and user/password are also can be opted to enhance the security strength of the whole system if necessary. That's the reason why this scheme is so called tri-factor authentication: a pair of username with password, a smart card with build-in variable security parameters to protect session and some kind of biometric features such as IPI pattern vectors.

b. Pattern Vectors Generation

As aforementioned, using biometrics methods to distinguish one bio entity from the others is getting more and more popular. According to our experiments, original ECG signals are

differentiable for different entities after necessary process of data fusion, just like shown in Figure 2.

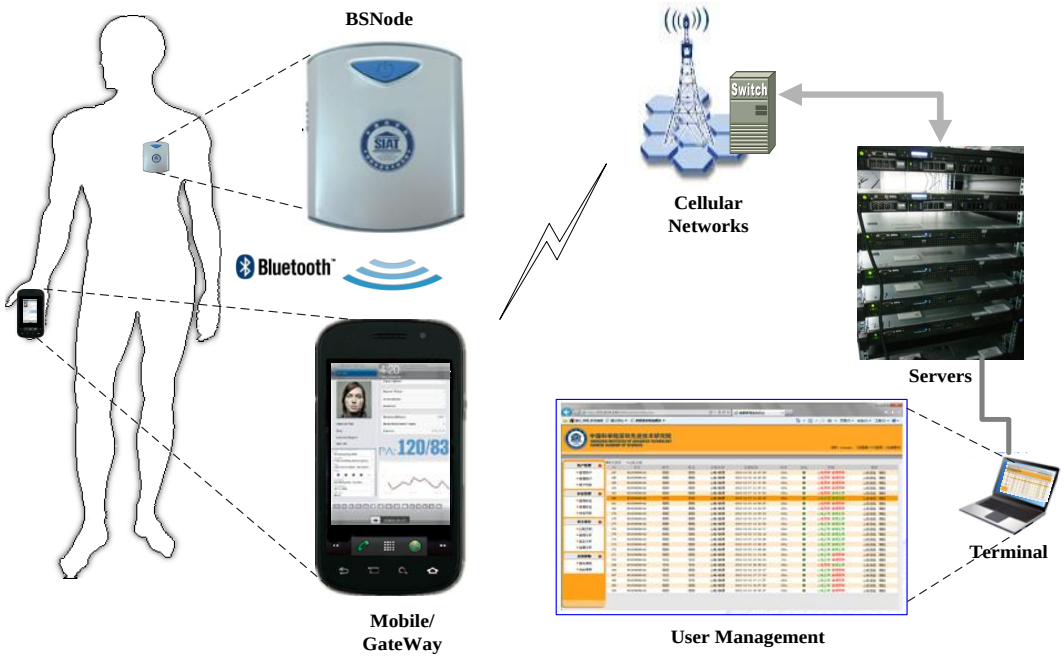


Figure 1. Application scenario of our protocol implemented

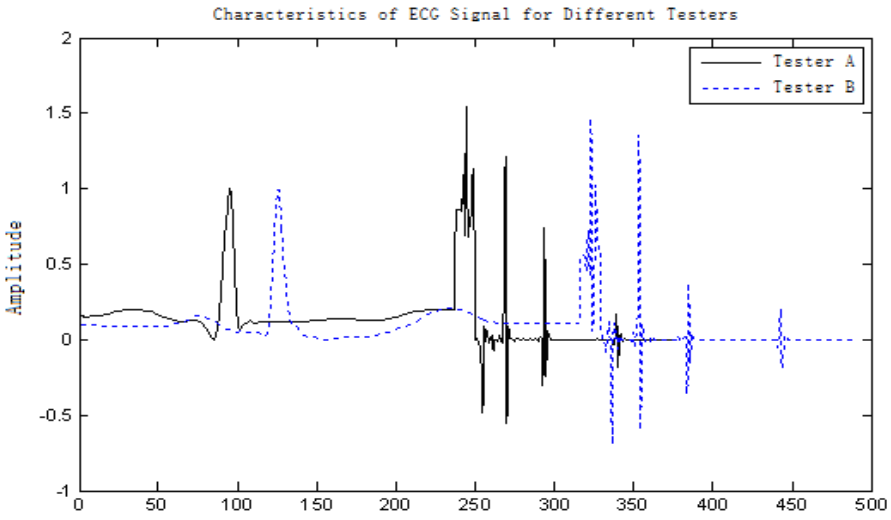


Figure 2. Characteristics of ECG signal for different testers

However, it is very hard to identify directly by wave shape in machine context, and we need to sample and convert it to digital entity identifier that appropriate for computer processing. Overall, the two categories of entity identifier generation scheme with biometrics ways are based on the

timing-domain information of physiological signals (TDPS) or frequency-domain information of physiological signals (FDPS) [23]. Our scheme takes advantage of timing information of heart-beat, so the former is proper for this solution.

Ref. [23] also analysis the characteristics of ECG and PPG signals, and gives the EI generation scheme based on IPI information. Figure 3 shows the extracted IPI information from the collected synchronous signals of ECG and PPG.

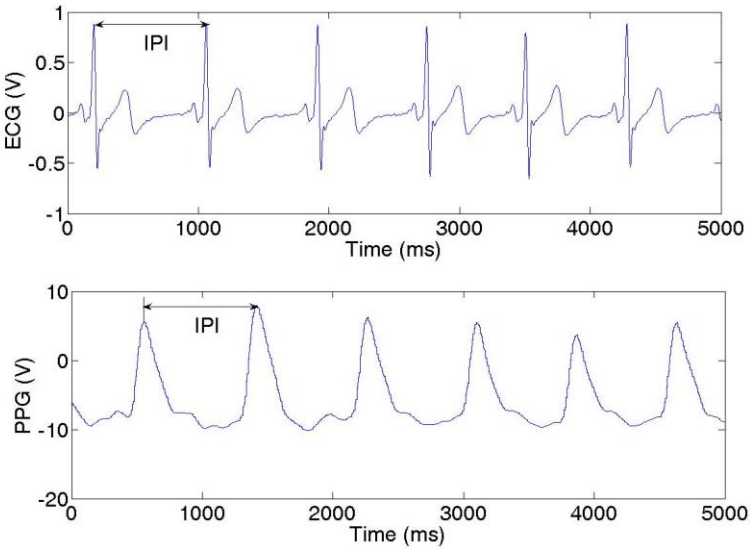


Figure 3. Extract IPI from ECG and PPG signals collected synchronously

In this EI generation scheme, based on a synchronization signal initiated by the master node, each sensor node extracts the timing-domain information by calculating a series of IPIs from its own recorded cardiovascular signal such as ECG and PPG, which can be denoted as $\{IPI_i \mid 1 \le i \le N\}$, and then deployed on the series of IPIs of each end to generate its own EI. Given N consecutive individual IPIs, a series of multi-IPIs can be obtained as follows:

$$\{ mIPI_i = \sum_{n=1}^{i} IPI_n \mid 1 \le i \le N \} \qquad (1)$$

Supposing a contraction mapping $\hat{f} : [0, 2^L) \to [0, 2^q)$, where L is a positive integer referred to as a modulo parameter, and q is a small integer. So, the random of multi-IPIs and compensation of differences among various BSnode can be achieved by this mapping, i.e., equation (2) shows us,

$$\hat{f}(m) = \left\lfloor \frac{m}{2^{(L-q)}} \right\rfloor \quad (2)$$

where $L > q$ and $\lfloor - \rfloor$ returns the largest integer less than or equal to $\frac{m}{2^{(L-q)}}$. The generated EI can be expressed as $EI = I_1 \| I_2 \ldots \| I_{L-1} \| I_N$, where I_i is generated from a corresponding $mIPI_i$ with the bit length of q. Such generated EIs have a bit length of $N \times q$. So far, we have the method to generate the pattern vectors represented by group of EIs. The recent progress about using IPIs as identifier is achieved by eliminating the error patterns [30] means the feasible of this application.

c. The Proposed Protocol

In a two-factor authentication scenario, a smart card is physically issued to the user who first registers to a system. Each user possesses a smart card for later login and authentication. Mobile USIM (Universal Subscriber Identity Module) card can be extended to load algorithms and security materials for this specific purpose. Also, a specific smartcard is another good option, e.g. USB key or SD (Secure Digital Memory) card. Based on the analysis of application requirements and disadvantages of the existing two-factor authentication scheme [1, 14, 15, 16], a novel tri-factor authentication protocol is proposed in this study.

First of all, we put forward a few facts as follows.

(1) MGW provides time synchronization services and forwards messages to SE.

(2) Whoever wants to use the system must register to MGW.

(3) IPI patterns are used as the biometric authentication factor, each of which corresponds to a 64-bit string, named PV_i, represents the i^{th} pattern vector as section b depicted. The other two factors are user ID/password and a group of secure session parameters, respectively. The latter include independent temporary secret x_a, generated by MGW as the session key and a symmetric key K preset into MGW. Both of them can be written into a smart card when starting authentications.

(4) MGW can store and make comparison of registered IPI patterns when intermittent communications scheduled between BSn and MGW. SE has more PVs than MGW, and more than one subject can be differentiated concurrently.

(5) BSn has the ability to collect IPIs and transmits a series IPIs to MGW to form a final pattern vector.

Secondly, we made a few necessary assumptions as follows:

(1) Mobile device is a gateway and also an authenticator.

(2) Seeing that secrets and biometrics are used, pattern vector is a key factor instead of password.

(3) Users in this authentication scheme are classified into two groups according to applications, where one kind of users need to input password as they are not the subject under health monitoring and thus do not have biometric patterns, and the others are subjects who need to be verified by biometric patterns directly, assuming that two categories have no intersection.

(4) Every BSn can be accessed by users via MGW authentication and provide data to requestors.

At last, the proposed protocol analyzed and divided into 4 phases, namely *request registration phase*, *login phase, authentication phase* and *security materials update phase*. Each phase is described as below.

(1) *Request Registration Phase:* sensors and owners who want to trigger the service of SE must initially register into MGW with their patterns. The other users also must be authenticated by MGW with user identifier and password. Use *User* to represent the set of $\{O_i, S_j, U_k\}$. MGW has initial ID_k, PW_k and PV_i, all set to null value initially.

Step1. *User* $\Rightarrow$ MGW: ID_k, PW_k, PV_i

Step2. MGW $\Rightarrow$ *User*: $h(PW_k \| PV_i)$, $h(x_a)$, $N = h(ID_k \| h(PW_k \| PV_i) \| h(x_a)) \oplus h(K \| x_a)$

Step3. MGW $\Rightarrow$ *User*: Smart card with the parameters $\{h(.), ID_k, N, h(PW_k \| PV_i), h(x_a)\}$

(2) *Login Phase:* there are three cases that require a login: BSn→SE: Physiological information for health analysis and alarming, where the login material is IPI pattern; Owner→BSn: Physiological information for monitoring and legitimate access, where the login material is IPIs pattern; other users→BSn: login materials are user identifier and password. Note that the first two cases are implied processes, and the last case is explicit. All of these login procedures should go through the MGW to get authenticated. If the user is successfully verified with the pair of values (ID_k, PW_k) or pattern vector (PV_i) pre-stored in smart card, the following steps are then executed:

Step1. Computes $CID = h(ID_k \| h(PW_k \| PV_i) \| h(x_a)) \oplus h(h(x_a) \| T)$ and $C = h(N \| h(x_a) \| T)$, where T is the current timestamp of login activity

Step2. *User*→MGW: <CID, C, T>

(3) *Authentication Phase:* upon receiving the login request <CID, C, T> at time T_1, the MGW authenticates user by the following steps:

Step1. Validate the timestamp by checking whether $T_1 - T < \Delta T$ or not, where ΔT is the expected time interval for transmission delay. Only those requests with less than ΔT can be accepted by MGW.

Step2. Computes $h(ID_k \| h(PW_k \| PV_i) \| h(x_a))^* = CID \oplus h(h(x_a) \| T)$ and $C^* = h(h(ID_k \| h(PW_k \| PV_i) \| h(x_a))^* \oplus h(K \| x_a) \| h(x_a) \| T))$

Step3. Checks if (C^*== C) holds to accept login and continue to next steps; otherwise, rejects the request of user.

Step4. MGW computes $A = h(CID \| h(S_j \| x_a) \| T_2)$, where T_2 is current timestamp of the authentication step.

Step5. MGW→S_j: <CID, A, T_2>. A is used to verify whether the MGW is the real gateway or not, where the message originally comes from.

Step6. S_j checks the time validity with $T_3 - T_2 < \Delta T$, where T_3 is currently timestamp when S_j receives the message <CID, A, T_2> at Step5. If ΔT is expired, terminate the process or else continue to the next step.

Step7. S_j computes $A^* = h(CID \| h(S_j \| x_a) \| T_2)$ and checks if ($A==A^*$) holds to indicate the legal access to sensor node; otherwise, rejects the request.

Step8. S_j computes $M = h(h(S_j \| x_a) \| T_4)$ which is then provided to MGW for mutual authentication, where T_4 is current timestamp.

Step9. S_j → MGW: <M, T_4>.

Step10. At time T_5, upon receiving the message, MGW also checks if ($T_5 - T_4 < \Delta T$) to continue; otherwise, terminate the process.

Step11. MGW computes $M^* = h(h(S_j \| x_a) \| T_4)$ and checks if ($M==M^*$) holds to indicate the sensor S_j is legitimate and mutual authentication is accomplished

Step12. As long as the aforementioned steps successfully passed, User can start the legal access to the system.

(4) *Security Materials Update:* besides the common password, pattern vectors are additional important security materials in this protocol. We denote the new password and the pattern vector as PW^*_k and PV^*_i. When *user* wants to update his/her materials, he or she inputs his/her new materials together with the old ones into the smart card, which can be a USIM card or a SD card, where the validation about whether the original and the fresh ones are matched is carried out. If yes, the following steps are executed:

Step1. Computes $N^* = N \oplus h(ID_k \| h(PW_k \| PV_i) \| h(x_a)) \oplus h(ID_k \| h(PW^*_k \| PV^*_i) \| h(x_a))$

Step2. Smart card replaces N with N^* and $h(PW_k \| PV_i)$ with $h(PW^*_k \| PV^*_i)$

As for those out dated vectors, just remove from patterns library on the server end directly. Any fresh requisition of authentication would be process from the registration phase again. In overall, we can summarize the whole authentication procedure with sequence diagram, as shown in Figure 4.

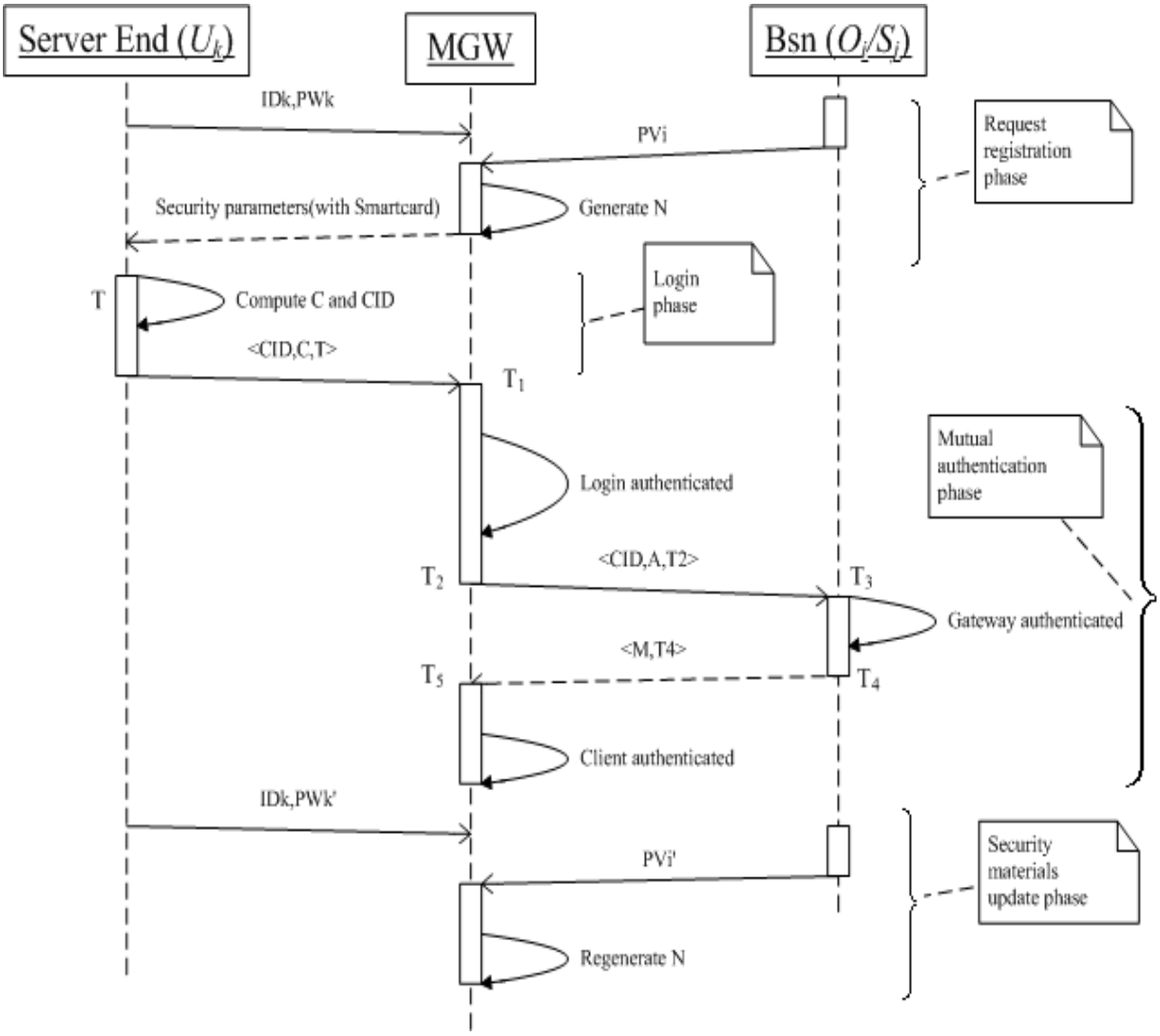


Figure 4 Sequence diagram of authentication procedure

IV. SECURITY ANAYLSIS AND IMPLEMENTATION

a. Security Analysis

Besides the security issues about *guessing, replay, stolen-verifier,* and *node-compromise* threats discussed in [6, 8, 11, 14], some further analyses about the security performance of our proposed scheme are needed after introducing pattern vector as an independent security factor.

(1) *Forgery attack or impersonation attack*. It always happens in wired and wireless networks. In our scheme, an attacker must possess the correct login information <CID, C, T> without prior legal registration phase. However, the secret x_a, user password and pattern information are all protected by $h(PW_k \| PV_i)$ and $h(x_a)$, which are impossible to be used by attackers for impersonation. Moreover, it is impossible to generate the identical PVs from biometric patterns as long as the sensing source is different.

(2) *Gateway node by-passing attack*. An attacker without passing the login from the MGW node can access the resources of sensor networks and a compromised sensor would possibly implicitly transmit malicious information to the server. To resolve this problem, x_a should be only shared between the MGW node and legitimate sensors, and keep it secret from O_i and U_k. Moreover, x_a shall be different according to the various applications.

(3) *Man-in-the-middle attacks.* Attacker who wants to intercept and modify the login message <CID, C, T> to cheat the participants of communication, it is impossible to re-calculate this message without the knowledge of x_a. Furthermore, our proposed protocol provided mutual authentication can overcome this crisis of confidence by computing $A= h(CID||h(S_j||x_a)||T_2)$ to verify the legal gateway node and $M=h(h(S_j||x_a)||T_4)$ to verify the legitimate sensors..

(4) *Insider attack*. More than 80% security issues come from the inside of networks. If privileged user controls the MGW node maliciously, all plaintext without hash protection will be leaked. Fortunately, the proposed scheme compute $N = h(ID_k \| h(PW_k \| PV_i) \| h(x_a)) \oplus h(K \| x_a)$ and no plaint text of passwords or pattern vector are directly stored.

(5) *Denial-of-service attack*. Adversary can block the message from reaching the node. From the point of the communication channel blocking, it is useless for the intruder that no responds any more if service is suspended in the public channel as well as no more information the attacker can get. However this protocol did not care the channel quality and not involved this case. From the point of the node blocking, only posses the password, pattern vector and secret of the node can be regarded as compromised and send malicious message to deny services. But these materials are protected and very hard to disclose or change arbitrarily as mentioned before, so the DoS attack by compromising node does not occur in this scheme.

b. Implementation

In our application, people can use a handy ECG collector specific developed as a biosensor to measure ones' cardiac status, as Figure 5 (a) shows. And then, a series of digital IPI information is to make up of a pattern vector to transmit to a mobile gateway by Bluetooth. Of course, mobile can recover this information to ECG wave by dedicated Android app., as shown in Figure 5 (b). For visualization, we can compute one of the PV value in MatLab 7.0 simulation environment, e.g. a 64 bits length string: A6B76C8C493E61A0, as Figure 6 shows. However, mobile or server needs not to represent it directly for the sake of security issues. Moreover, server end environment is equipped with CentOS 6.0 and MongoDB software, in which stored physiological data and users' general information.

(a) ECG collector (b) Mobile with ECG wave recovery

Figure 5. BSn and MGW

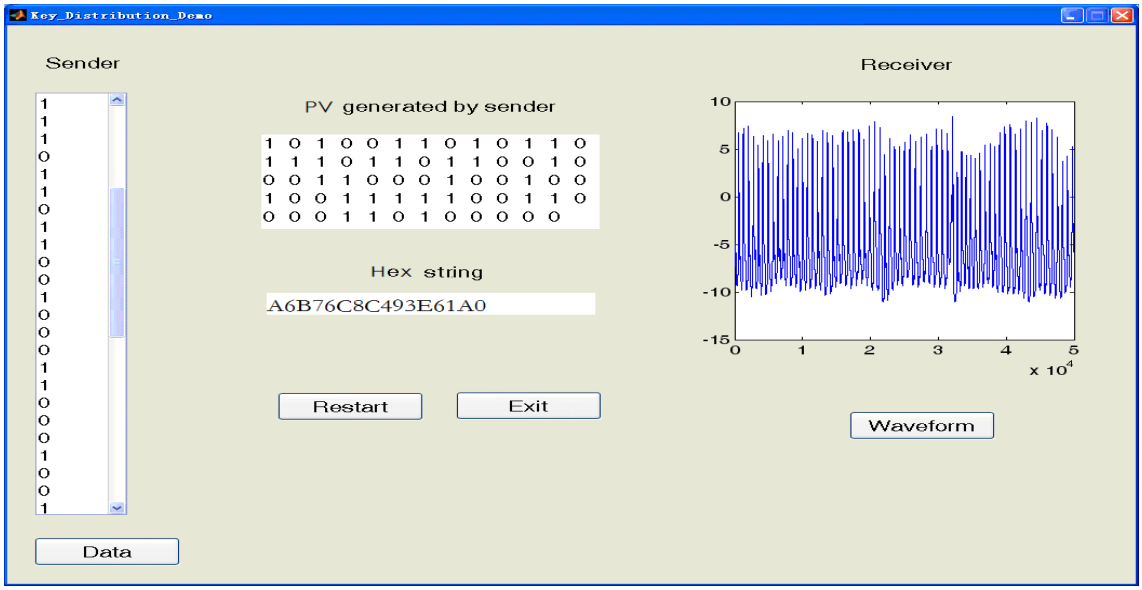
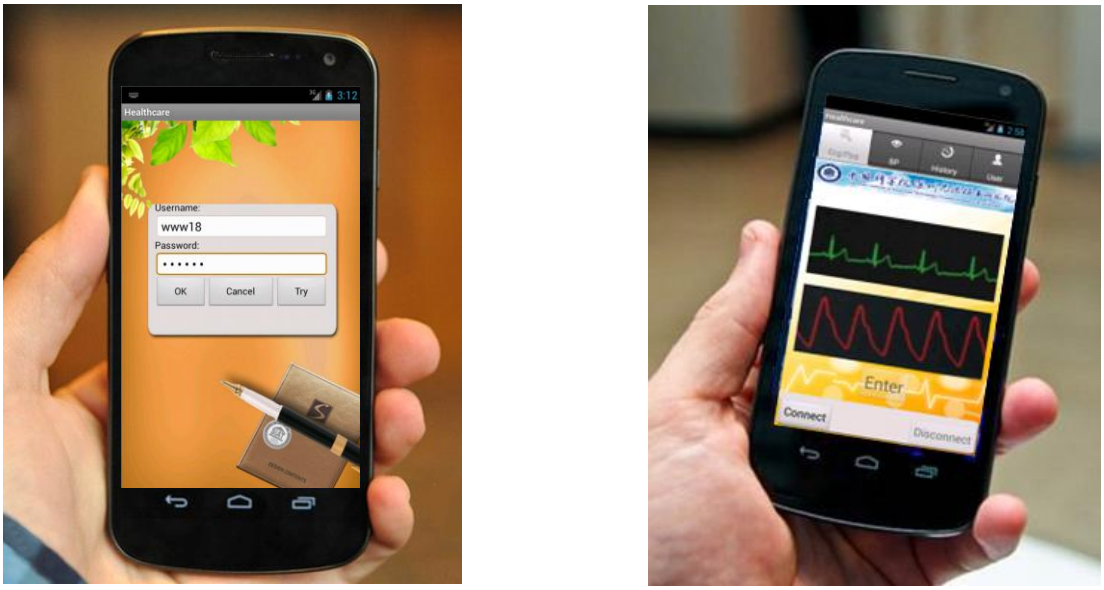


Figure 6. Simulation of PV pattern represented as a 64-bit string

For a fresh user, he or she must also transfer his/her PV to back-end server as well as stored in MGW if he/she want to be a frequent legitimate user. So, a fresh user can register to server with a smart card recorded with PV string and user id/password (optional) to follow-up login stage. We utilize SD card within a validation program to simulate the smart card functions. Hence, after this user's pattern vector string is generated and stored, he or she can login to MGW with optional ID and password with the interface and validate the PV while connecting to the physiological sensor (ECG collector) via Bluetooth, as shown in Figure 7(a) and (b), respectively. Here, mobile is regarded as an authenticator as well as a mobile gateway to transfer data between sensors and back-end server.

Figure 8 shows the whole classes relationships of Android app which act as a data acquisitor and authenticator. *LoginActivity* called *AuthenActivity* not only by validating via ID/password but also by smart card information which *IdentifyService* provided. Furthermore, *StartActivity* has three activities are optional for user: one is *MainActivity*, one is HistoryActivity, and the rest one is *UpdateActivity*. The first class is utilized for main businesses such as ECG and PPG generating and showing (*ECGPPGActivity* and *ECGPPGView*) as well as initiating connection of Bluetooth with *DeviceDiscovery*, which is responsible for finding the available Bluetooth devices and list them by *ListViewAdapte*. After then *GetBlueDataService* called *HandleThread* to receive and

save data dynamically with a dedicated queue data structure implemented by class of *CircularQueue*.



(a) Login interface on MGW (b) Connecting to the server to validate PV

Figure 7. Login progress and validating via Bluetooth connecting

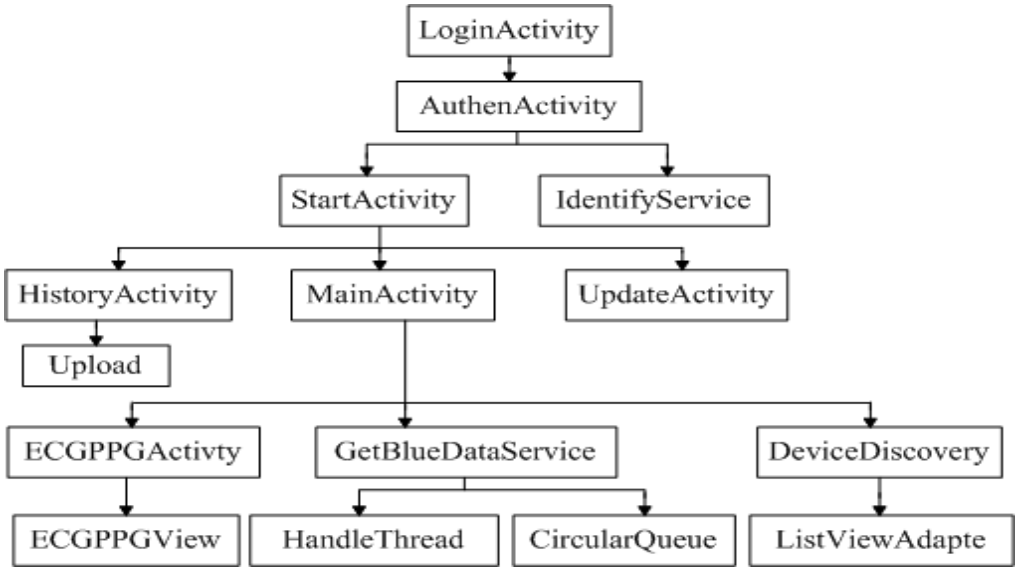


Figure 8. Relationships of Android app classes in MGW

In additon, back-end server plays another key role during authentication. All of registered user information including common data, physiological data authentication data are all stored in NoSQL database on the remote server. For example, a testing user's storage status can be seen in

Figure 9 Smart card is assigned to this user previously with the stored value of "smartcard_id" attribute which indicates where can be found about the user's legal privileges to handle device, own security materials and common keys. If the value of "smartcard_id" of current smart card is not consistent with the previous registered to the MGW, the authentication procedure should be terminated. With the correct smart card, the authentication routine can fetch the corresponding pre-set K and temporary session key x_a by this id to process authentication procedure.

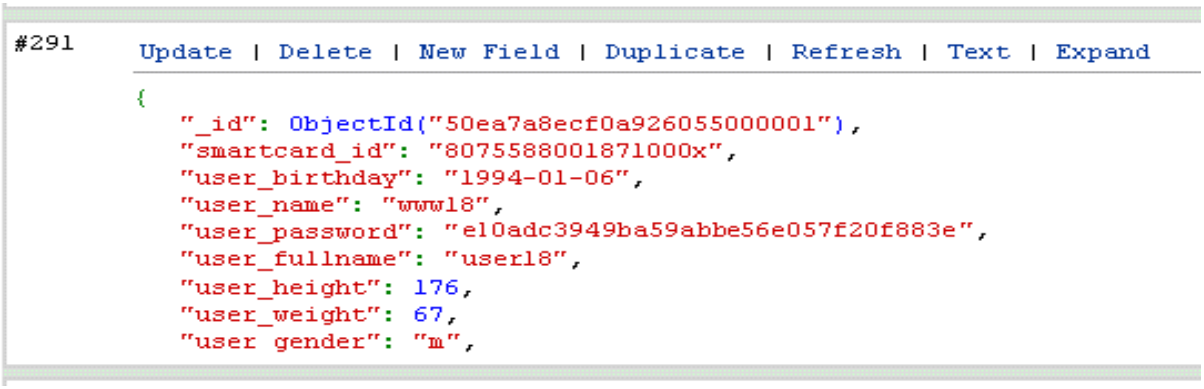


Figure 9. User information stored in database

Successively, the authentication event is lunched and recorded into another data collection, as Figure 10 shows. This item recorded the corresponding user's PPG and ECG information. Therefore, the routine can seek the registered user's detail by the id, e.g., "UserId: ObjectId("50ea7a8ecf0a926055000001")", to proceed with the following mutual authentication.

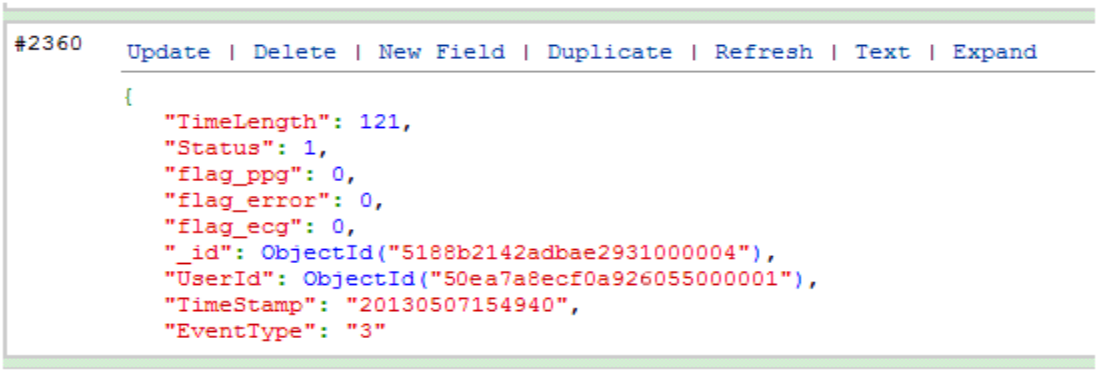


Figure 10. Details of event collection

For any illegal user, at least one of the three factors is absent: Anyone who's PV is not to be registered before, or can not match with the original one stored in database, as well as failing to compute secure proof in smart card, the whole authentication is failure. After analysis in segment

Section IV.(a), the adversaries is also hard to attack this proposed scheme without legal PV information, although the password or temporary session key may be comprised.

V. CONCLUSIONS

The security issues in BSN are paid more close attention with the popularization of biosensors applications. In addition to the traditional user-name/password pairs for user authentication, another novel method is to exploit the physiological characteristics readily available at individual sensors in BSN for entity identifier generation to enhance the subsequent authentication process. Through the analysis of special security requirements for wireless body sensor networks with healthcare applications, we have proposed a protocol in this study to unify these cases with the set of *User* concept and construct a compound identifier to form a universal authentication material for the sake of convenience. Thanks to the special characteristic of physiological signals, e.g. ECG and PPG, more authentication factors like IPI pattern vectors besides user password can be deployed to increase the security level in addition to the secret x_a and symmetric keys in the existing protocols. As a result, a novel tri-factor user authentication with mutual access can thus be designed specially for the sensor networks involved in healthcare applications. A real application system is also implemented with this mechanism. By bonding biometric and passwords, it has been proved that the security of the resultant authentication transaction is stronger than one or two-factor authentication schemes due to the independence among these multiple factors. The cryptanalysis of this protocol also indicates that the ability of resisting against attacks is strong and flexible enough.

ACKNOWLEDGEMENT

This work was supported in part by the National S&T Major Project of China (No. 2011ZX03005-001), National Natural Science Foundation of Youth Science Foundation (No. 61102087), and the Key Basic Research Program of Shenzhen (No. JC201005270257A)...

REFERENCES

[1] M. L Das, "Two-Factor User Authentication in Wireless Sensor Networks", IEEE Transaction on Wireless Communication, Vol.8, no.3, pp. 25-31, March 2009.

[2] M. L. Das, A. Saxena, and V. P. Gulati, "A Dynamic ID-based Remote User Authentication Scheme", IEEE Transactions on Consumer Electronics, Vol. 50, no. 2, pp.629-631, May 2004.

[3] A. Tiwari, Sudip Sanyal, A. Abraham, S. J. Knapskog, and Sugata Sanyal, "A Multi-Factor Security Protocol for Wireless Payment Secure Web Authentication Using Mobile Devices", Proceedings of the IADIS Int'l. Conference on Applied Computing, pp. 160-167, Salamanca, Spain, February 17-20, 2007.

[4] D. Glynos, P. Kotzanikolaou and C. Douligeris, "Preventing Impersonation Attacks in MANET with Multi-factor Authentication", Proc. of *WiOpt'05***,** pp. 59-64, Trentino, Venezuela, 2005.

[5] C. C. Chang and T. C. Wu, "Remote Password Authentication with Smart Cards", IEE Proceedings-E of Computers and Digital Techniques, Vol. 138, Iss. 3, pp. 165-168, May 1991,

[6] K. Wong, Y. Zheng, J. Cao, and S. Wang, "A Dynamic User Authentication Scheme for Wireless Sensor Networks", Proceedings of IEEE Int'l. Conference. on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), Vol. 1, Taichung, Taiwan, Jun 5-7, 2006.

[7] Z. Benenson, F. Gartner, and D. Kesdogan, "User Authentication in sensor network (extended abstract)", Proc. of *Informatics'04,* Workshop on Sensor Networks, Ulm, German, September 2004.

[8]. M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards", IEEE Transactions. on Consumer Electron, Vol. 46, Iss. 1. pp.28-30, 2000.

[9] C. K. Chan and L. M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards", IEEE Transactions. on Consumer Electron, Vol. 46, Iss. 4, pp. 992-993, 2000.

[10] A. K. Awasthi and S. Lal, "A Remote User Authntication Scheme Using Smart Cards with Forward Secrecy", IEEE Transactions. on Consumer Electronics, Vol. 49, Iss. 4, pp. 1246-1248, 2003.

[11] S. W. Lee, H. S. Kim, and K. Y. Yoo, "Comment on 'A Remote User Authentication Scheme using Smart Cards with Forward Secrecy' ", IEEE Transactions. on Consumer Electronics, Vol. 50, Iss. 2, pp. 576-577, May 2004.

[12] A. K. Awasthi, "Comment on 'A Dynamic ID-based Remote User Authentication Scheme' ", Transc. on Cryptology Vol.1, Iss. 2, pp. 15-16, Aug. 2004.

[13] H. F. Huang, Y. F. Chang, and C. H. Liu, "Enhancement of Two-Factor User Authentication in Wireless Sensor Networks", Proceedings. of the 6th IEEE Int'l. Conference. on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), pp. 27-30, Darmstadt, German, October 15-17, 2010.

[14]. P. Kumar, M. Sain, and H. J. Lee, "An Efficient Two-Factor User Authentication Framework for Wireless Sensor Networks", Proceedings. of the 13rd IEEE Int'l. Conference. on Advanced Communication Technology (ICACT), pp.574-578, Phoenix Park, R. Korea, 2011.

[15] M. K. Khan and K. Alghathbar, "Cryptanalysis and Security Improvement of 'Two-Factor User Authentication in Wireless Sensor Networks' ", Journal of Sensors, Vol.10, pp. 2450-2459, 2010.

[16] C. Adams and M. J. Wiener, Multi-Factor Biometric Authenticating Device and Method, U.S. Patent 6,363,485, Mar 26**,** 2002.

[17] A. Bhargav-Spantzel, A. C. Squicciarini, S. Modi, M. Young, E. Bertino, and S. J. Elliott, "Privacy Preserving Multi-Factor Authentication with Biometrics", Journal of Computer Security Vol. 15, no. 5, pp. 529-560, 2007.

[18] R. B. Paranjape, J. Mahovsky, L. Benedicenti, and Z. Koles, "The Elechoencephalogram as a Biometric", Proc. Canadian Conference on Electrical and Computer Engineering, pp. 1363-1366, Toronto, Canada, May 13-16, 2001.

[19] L. Biel, O. Pettersson, L. Philipson, and P. Wide, "ECG Analysis: A New Approach in Human Identification", IEEE Transactions on Instrumentation and Measurement, Vol. 50, Iss.3, pp. 808-812, 2001.

[20] F. Sufi and I. Khalil, "Faster Person Identification Using Compressed ECG in Time Critical Wireless Telecardiology Applications", Journal of Network and Computer Applications, Vol. 34, pp. 282-293, 2011.

[21] Y. Y. Gu, Y. Zhang, and Y. T. Zhang, "A Novel Biometric Approach in Human Verification by Photoplethysmographic Signals", Proceedings of the 4th Annual IEEE Conference on Information Technology Applications in Biomedicine, pp. 13-14, Birmingham, U.K., April 24-26, 2003.

[22] C. C. Y. Poon, Y. T. Zhang and S. D. Bao, "A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and m-Health", IEEE Communications Magazine, Vol. 44, no.4, pp.73–81, 2006.

[23] S. D. Bao, C. C. Y. Poon, Y. T. Zhang, and L. F. Shen, "Using the Timing Information of Heartbeats as the Entity Identity to Secure Medical Body Sensor Networks", IEEE Transactions on Information Technology in Biomedicine, Vol.12, Iss. 6, pp. 772-779, Nov. 2008.

[24] F. Miao, S. D. Bao, and Y. Li, "A Modified Fuzzy Vault Scheme for Biometrics-Based Body Sensor Networks Security", Proc. of the 53rd *IEEE GLOBECOM 2010*, pp.1-5, Miami, USA, Dec. 6-10, 2010.

[25] C. Z. Cao, C. G. He, S. D. Bao, and Ye Li, "Improvement of fuzzy vault scheme for securing key distribution in body sensor network", Proceedings of 33rd IEEE Int'l Conference Engineering in Medicine and Biology Society (EMBC'11), pp. 3563-3567, Boston, USA, August 30–September 3, 2011.

[26] J. Shen, S. D. Bao, L. C. Yang, and Y. Li, "The PLR-DTW Method for ECG Based Biometric Identification", Proceedings of 33rd IEEE Int'l Conference Engineering in Medicine and Biology Society (EMBC'11), pp. 5248-5251, Boston, USA, August 30–September 3, 2011

[27] K. Singh and V. Muthukkumarasamy, "Authenticated Key Establishment Protocols for a Home Health Care System". Proceedings of the IEEE Int'l Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), pp. 353-358, Melbourne, Australia, Dec 3-6, 2007.

[28] C. G. He, S. D. Bao, "An Encryption Algorithm Based on Chaotic System for 3G Security Authentication", Proc. 2nd IEEE Youth Conference on Information, Computing and Telecommunications, pp. 351–354, Beijing, China, Nov 28-20, 2010.

[29] Z. Li, X. Xu and Z. Fan, "Light Weight Trusted ID-Based Signcryption Scheme for Wireless Sensor Networks", International Journal on Smart Sensing and Intelligent Systems, Vol. 5, no.4, pp.799-810, 2012.

[30] T. Hong, S. D. Bao, Y. T. Zhang, Y. Li and P. Yang. "An Improved Scheme of IPI-based Entity Identifier Generation for Securing Body Sensor Networks", Proceedings of 33rd IEEE Int'l Conference Engineering in Medicine and Biology Society (EMBC'11), pp. 1519-1522, Boston, USA, August 30–September 3, 2011.