A Novel Biometric Algorithm to Body Sensor Networks

Chapter · January 2015

DOI: 10.1007/978-3-319-18191-2_3

CITATIONS
8

READS
270

4 authors, including:

Sandeep Pirbhulal
Norwegian University of Science and Technology
77 PUBLICATIONS **1,531** CITATIONS
SEE PROFILE

Wanqing Wu
Sun Yat-Sen University
99 PUBLICATIONS **1,806** CITATIONS
SEE PROFILE

Yuan-Ting Zhang
The Chinese University of Hong Kong
423 PUBLICATIONS **11,562** CITATIONS
SEE PROFILE

A Novel Biometric Algorithm to Body Sensor Networks

Sandeep Pirbhulal[1,2], Heye Zhang[1,2], Wanqing Wu[1,2,*], and Yuan Ting Zhang[1,2,3]

[1] Institute of Biomedical and Health Engineering, Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen, China
[2] The Key Laboratory for Health Informatics of the Chinese Academy of Sciences at Shenzhen Institutes of Advanced Technology, Shenzhen, China
[3] Research Centre for Biomedical Engineering, Chinese University of Hong Kong, Hong Kong
{sandeep,wq.wu,hy.zhang}@siat.ac.cn

Abstract. In Body Sensor Networks (BSN) several sensor nodes are attached on, inside or around human body to monitor vital sign signals such as, Electrocardiogram (ECG), Electroencephalogram (EEG), Blood pressure etc. The information from each sensor node is very significant; therefore privacy and security is very important during data transmission in BSN. The conventional cryptographic approaches make use of cryptographic keys to achieve authentication, and use of these keys not only require high resource utilization and computation time, but also consume large amount of energy, power and memory in BSN. Therefore, it is necessary to develop power efficient and less computational complex authentication technique for BSN. In this paper we design a novel biometric algorithm which is based on biometric feature Electrocardiogram (ECG) and uses Data Authentication Function (DAF) for the security of BSN instead of utilizing traditional key generation procedure. Our proposed algorithm is compared with two cryptographic authentication techniques, Data Encryption Standard (DES) which is symmetric or private-key based encryption technique and RSA (Rivest Shamir Adleman) which is asymmetric or public-key based encryption scheme. Simulation is performed in MATLAB and results explain that our algorithm is efficient in terms of transmission time utilization and average remaining energy.

Keywords: Body Sensor Network, Biometric, Electrocardiogram (ECG), Heart Rate Variability (HRV), Security.

1 Introduction

These days Wireless Sensor Networks (WSNs) technology has attracted vast attention in different domains. Wireless Body Area Networks (WBANs) or BSN is

* Corresponding author.

S.C. Mukhopadhyay (ed.), *Wearable Electronics Sensors*,
Smart Sensors, Measurement and Instrumentation 15, DOI: 10.1007/978-3-319-18191-2_3

very important application of WSNs for healthcare monitoring, which is the wireless network of different in-body, on-body and around-body associated sensor nodes. The general BSN architecture is demonstrated in Fig.1, it contains three parts as presented in S. D. Bao, et.al [1]. In the first part, BAN-Coordinator receives the vital and unique information from each sensor node, that data is the real time information of human body such as heart rate, Electrocardiogram (ECG), temperature,blood pressure, etc. That physiological data from all subjects is stored at sink (may be cellular device or PDA) and deliver that information to remote server in second part. The third part allows access to the concerned doctor or authorized person from server.

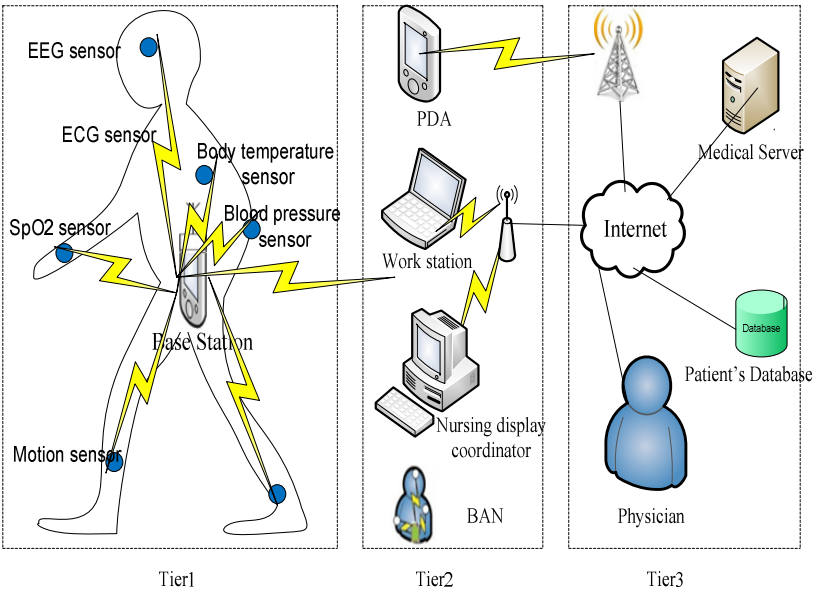


Fig. 1 Body Sensor Network Architecture [9]

The BSN is the best way for telemedicine and m-health but as sensor nodes carry very vital information, therefore data privacy is one of the major aspects in these networks. Along with privacy, data security is also the important factor. Only authorized person should access the information generated by nodes, therefore security should be implemented in all aforementioned parts of system. However, due to small size and their energy constrained nature security is very important in BSN as discussed in H. Wang, et.al [2]. Whereas, each human body has different behavior, that is why it will be difficult for attacker to hack the data. Therefore features of human body can be used to implement security in BSN.

Biometric technology is automatic detection of persons in the behavioral or physiological traits. In our research we used electrocardiogram (ECG) as a biometric characteristics. The heart beats of human body produce electrical signals

continuously and collection of these electrical currents are termed as ECG. The ECG is a unique individual trait, whereas its properties completely depend on human body and heart beats. To become ensure about ECG as a biometric feature, it is essential to know ideal biometric characteristics [3-5], as shown in Table.1.

In sensor networks many security protocols with symmetric as well as asymmetric keys are employed to obtain privacy, reliability and accuracy during data transmission C. S. lang, et.al [6]. Whereas, the BSN is the different from other ad-hoc networks because of interference in body mobility and inadequate computing resources of human body, therefore simple and efficient authentication and confidentiality techniques are very important in BSN.

Several symmetric key-based encryptions techniques have been introduced in last decade for BSN. S.D.Bao,et.al in [7], designed a symmetric key based approach , they claim that their approach is efficient to secure BSN during data transmission, but only one private key is used in whole BSN, therefore if any sensor node is compromised then private information will no more be secure as presented in C. William, et.al [8]. One solution to overcome that problem is to use multiple keys in BSN, if any one key is disclosed it will not affect the security of network. By introducing multiple keys, key management is very complex during encryption and decryption. Therefore many protocol such as; SSL (Secure Sockets Layer) utilizes private key approach during data transmission.

Table 1 Ideal biometric trait properties [16]

Property Name	**Detail**
Universal	Almost acquired by all or major portion of population hold
Unique	Two individuals have enough difference for identification
Everlasting	Having ability to not to change with respect to time
Measurable	convenient to obtain for an individual technically
Efficient	provide high-quality performance in terms of speed, accuracy with limited resource utilization
Adequate	acceptable to human i.e. patient as well as organization to utilize as an identifier
Unassailable	quite complicated to recreate by fake acts

In asymmetric public key encryption different keys are used for both encryption and decryption. On the one hand, it has advantage over symmetric cipher of multiple keys utilization, through this way level of security and privacy can be increased. However, on other hand these techniques are resource constrained as explained in C. C. Y. Poon, et.al [4]. Therefore asymmetric cipher is not

cost-efficient and feasible solution for BSN. Whereas, some researchers introduce the hybrid approach for symmetric and asymmetric to increase the security and privacy in BSN. C. S. lang, et.al [6], presents a hybrid technique in a more effective way to implement authentication, integrity and confidentiality, all these conventional approaches are based on public or private keys to secure human body information in BSN.

However, wavelet-domain HMM (Hidden Markov Model) based approach to secure BSN in H. Wang, et.al [2], increases the performance of network because it does not require synchronization and generation of external keys. When physiological and behavioral characteristics are used instead of external keys to implement security in WBAN is referred as biometric based authentication [10][11], they used human body features as generation of multiple keys for entity identification to implement security and privacy in WBAN during data transmission. This biometric based security increases reliability, provides rapid action and cost efficient solution as compared to conventional cryptographic key-based authentication. Therefore in modern research biometric characteristics are utilized for implementing security in WBAN.

In [12], S.D.Bao, et.al designed architecture of BSN and model to implement security by using physiological feature of human body. They used collective approach of wireless channel as well as bio-channel for data authentication. F.Miao, et.al in [13] used ECG as biometric triat to secure BSN, they used AES (Advanced Encryption standard) to generate keys from ECG for data integrity, data authentication and privacy between source and destination. The major drawback of their research was that their technique was based on asymmetric key based, which is not energy efficient and cost-effective solution.

The Physiological Signal based Key Agreement (PSKA) scheme is proposed in K. K. Venkat, et.al [14]; it uses Fuzzy vault logic between source and destination for key synchronization. In their research encoding of key is done with polynomial on source and at destination decoding procedure is utilized based on chaff points to restructure the key. There are two problems associated with that technique i) if key size is small, hacker can guess key by brute force attacks, ii) if key size is large, destination will require high computational cost for polynomial due to availability of used chaff points. In [15], GH Zhang, et.al introduced fast method to generate key from biometric feature ECG, hamming distance is used to find interval between any two generated keys. The randomness and uniqueness of keys are measured to check the accuracy of theses keys. In S. Cherukuri, et.al [16], the authors put forward a security strategy for BSN; their approach provides inexpensive and easy method for data transmission. According to S. D. Bao, et.al in [1], the IPI (Inter Pulse Interval) can be used as biometric trait for entity identification to obtain security in BSN. Lin Yao,et.al in [17], develop a data integrity and data confidentiality technique for BSN in which ECG is utilized as a biometric trait for key generation and encryption. Their research presents Syverson-van Oorschot (SVO) logic for correction and verification of results, as that technique performs well in security implementation, but is less power efficient and requires a lot of time for data authentication due to computational

complexity. Shu-Di-Bao, et.al [18], proposes Inter-pulse intervals (IPI) from ECG and Photo-plethysmogram (PPG) as biometric characteristics to accomplish security in WBAN. They support the performance of their protocol with false rejection rate and false acceptance rate. Their research claims accurate security model for WBAN, but due to complexity involved during key generation process in their designed scheme it does not provide cost efficient and energy efficient solution for data authentication in BSN.

The IPI of biometric feature PPG is used for generation of distinctive keys is studied by G. H. Zhang, et.al [19], furthermore; these keys were applied for synchronization between source and destination to execute security in WBAN. The matchless and difficult algorithm used for key generation in this paper, guarantees that accurate authentication can be obtained. However, computational complexity is the major drawback of their research, because high cost, energy and power are required to implement this technique in WBAN. S. N. Ramli, et.al [20], designs a biometric based model; it uses Message Authentication Protocol (MAC) as a key for authentication between source and destination, and omits complex key generation methods for implementing authentication in BSN. The MAC is based on R-Peak detection and Heart Rate Variability (HRV) calculation of physiological feature ECG. Their work does not discuss energy efficiency as well as power efficiency.

One of the major problem in all aforementioned research is that they used different security techniques, algorithms and models such as, PSKA based fuzzy logic, SVO etc, these all are based on key generation mechanism, which is complex and time consuming procedure, also their research do not discuss energy efficient and power efficient security approach for BSN. To remedy all these problems, we propose a novel unique algorithm based on ECG as biometric trait in which Data Authentication Function (DAF) is presented and difficult key generation procedures are excluded to secure BSN. DAF consists three basic parts; detection of QRS-complex, HRV calculation and authentication protocol. The authentication protocol is the ratio of Low Frequency-to-High Frequency ratio, and it is acting as key between source and destination to implement security in BSN. However, to further increase the security hashing algorithm SHA1 is used to hide original message before its transmission.

Rest of the paper is organized as follows. In section 2 motivation is presented, section 3 presents proposed algorithm, section 4, section 5 and section 6 include performance analysis, simulation environment and simulation and results respectively, finally paper is concluded in section 7.

2 Motivation

Body area networks (BANs) seamlessly connect miniaturized and low-power devices and biosensors that are worn on or implanted in human body. The development of BANs is emerging as one of the main research trends, particularly to collect and jointly process biological data for continuous and long-term

monitoring of health conditions. Since medical and health data are private and sensitive information that are protected by law in many countries, for example, by the Health Information and Portability Accountability Act (HIPAA) in the USA, the European Union Directive 2002/58/EC in Europe, and Law of the People's Republic of China on Medical Practitioners in China, the security of data transmission within BANs must be addressed in order for them to be widely used in real-life health applications. Although BANs share some common features with generic wireless sensor networks (WSNs), it is anticipated that the two networks should have very different security schemes [21]. WSNs have many constraints, such as low computation capability, small memory, and limited energy resources, and the security issues of them have been previously addressed in literatures. SPINS is a suite of security protocols optimized for sensor networks, where the base station accesses nodes using source routing. Differed from SPINS, Undercoffer et al. [22] proposed another protocol that relies upon broadcasts and provides a mechanism for detecting certain types of aberrant behaviours. TinySec is the first fully implemented link layer security architecture for WSNs. It generated secure packets by encrypting data using a group key shared among sensor nodes and calculating a message integrity code (MIC) for the whole packet, including the header. These security methods those were proposed or implemented for WSNs are not optimal, if not impractical, for BANs, which require a security solution that consumes even less energy and memory space than generic WSNs [21].

A unique feature of this solution is the generation of random keys by physiological data (i.e. a biometric approach) for securing communication. Our research aims to produce cost efficient (by offering less computational complexity and low resources utilization), time efficient (by requiring less transmission time for processing as complex keys are being omitted), energy and power efficient (by demanding less energy and power consumption) as well as accurate authentication model for BSN. The beauty of our algorithm is that it eradicates conventional procedure of key generation and uses biometric feature i.e. ECG as authentication protocol to secure transmission between nodes in BSNs.

3 Proposed Algorithm

In our research, we extended the work of S. N. Ramli, et.al [20], the block diagram of our proposed algorithm for data authentication in BSN is shown in Fig. 2. The authentication protocol mentioned in Data Authentication Function (DAF), is acting as a key, once this key matches between source and destination than message can be transmitted. In case receiver does not match statistically, transmission will not get start and message will be discarded as shown in demonstrated in Fig. 2.

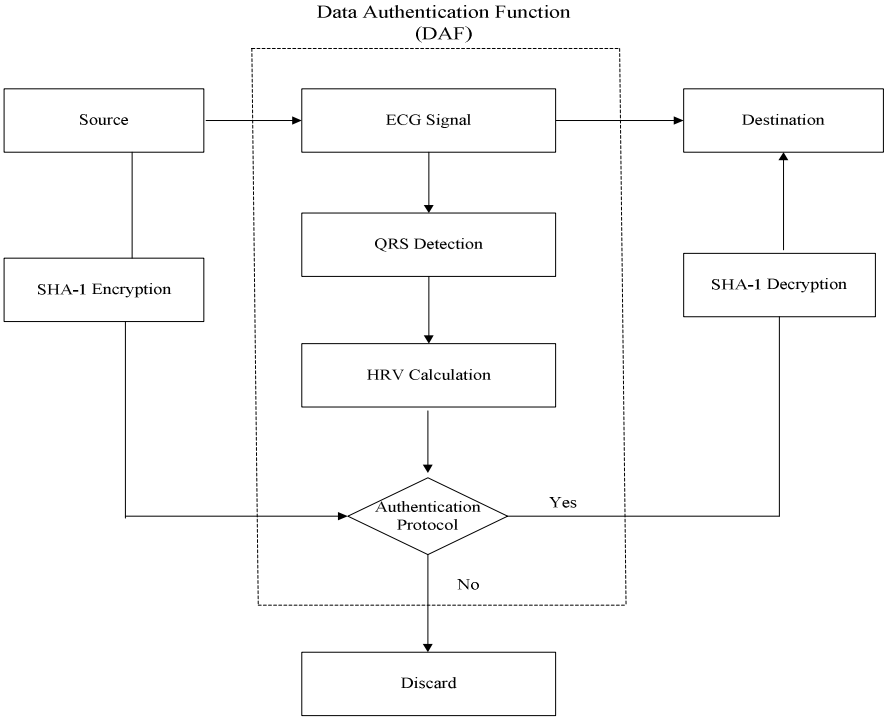


Fig. 2 Block diagram of Biometric-based Proposed Algorithm

Our proposed algorithm is simple because it eliminates the use of complex key-based techniques. As in BSN those methods not only require high computational cost for keys management and its distribution, but also consume a lot of time, energy and power during data transmission. Although by using DAF, data reliability and accuracy can be achieved, but to increase the level of security before sending patient's data to DAF for authentication, our proposed algorithm utilizes SHA-1 hashing scheme for encryption of original message. This hashing technique is very simple, easy to apply and less complex in managing keys, therefore it provides low cost encryption.

3.1 Data Authentication Function (DAF)

The Data Authentication Function (DAF) is shown in Fig.2, which includes three main parts; QRS detection; HRV calculation; and authentication protocol. The authentication protocol used in DAF is responsible to make decision either to transmit data to destination or discard the message initiated from source. ECG is used as biometric trait for authentication in our proposed algorithm.

3.1.1 Wearable System for Biosignal Collection

Electrical considerations for the system platform are driven by its use model. It must perform at least as well as commercially available devices, with a small and comfortable form factor. It must be able to record ECG continuously for at least one week. Dry noncontact electrodes work based on the capacitive coupling between the skin and the conductive disc which leads to the polarization of the electrode, causing displacement current to flow for a while. The proposed capacitive coupling based is composed of a conductive textile fabric electrode, clothes and the skin of the subject, as shown in Fig.3. To achieve strong capacitive coupling, we can increase the area of contact, use a thin insulator layer or include an insulator with a high dielectric constant. Dry noncontact electrodes are sensitive to motion artifacts, but show better behavior in terms of decreased skin irritation.

We design a measuring device to extract ECG signal from a textile electrode (Fig. 1). The measuring device of ECG and breathing signal is constructed using filtering and amplification circuit, and its block diagram as shown in Fig.1. The device consisted of a common part and a differential separation filter for sensing ECG signal and breathing activity respectively. The common part was composed of two buffers, which functioned as an impedance of the capacitive coupling with low impedance required by the subsequent circuitry. Operational amplifier ICs with high input resistance were used in the present study. The differential separation filter described in the subsection A and a driven-right-leg (DRL) circuit. The differential separation filter separated the input signal into high frequency component containing ECG signal (>1Hz) and low frequency component including breathing signal (<1Hz). The separation filter was constructed of two sets of subtracter, amplifiers and integrators. The book diagram in circuit was employed in order to reduce common mode noise mainly due to power line interference.

The differential separation filter separated the input signal into sets of subtracters, amplifiers and integrators according to DC suppression circuit. The part for sensing ECG signal consisted of an instrumentation amplifier, a high-pass filter(HPF), a low pass filter(LPF) and two inverting amplifiers. The circuit elements of the HPF and the LPF were designed in order to obtain a cutoff frequency of 5 and 40Hz, respectively. Although electrocardiograph for diagnostic purpose requires a bandwidth from 0.01 to 100Hz, we narrowed the bandwidth of the developed part for obtaining breathing activity. And the part for sensing breathing signal is constructed of a high-pass filter (HPF of 0.1Hz).

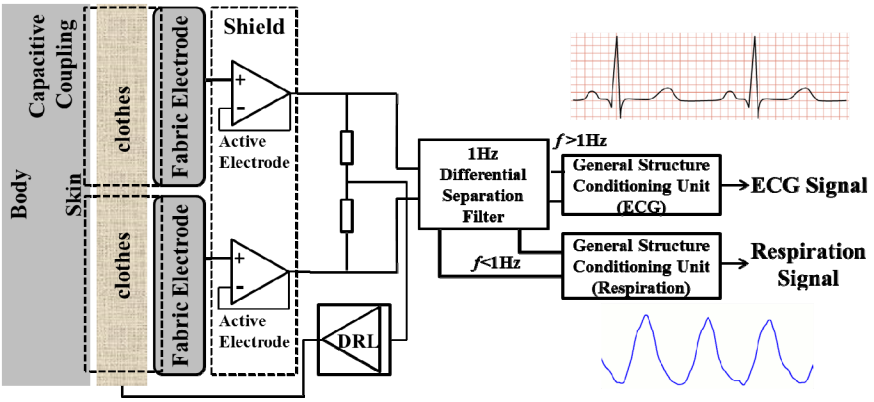


Fig. 3 Block diagram of capacitive measurement system

3.1.2 HRV-Calculation

Software platform is responsible for extracting bio-information from raw data and for calculating the corresponding characteristic parameters of the bio-signal to provide HRV based key for the proposed algorithm. Physiological signals are usually weak and easily corrupted by various kinds of noise (power line interference, electrode contact noise, baseline drift, instrumentation noise, motion artifacts, electrosurgical noise, and other less significant noise sources), which cannot be filtered completely by the hardware platform. Therefore, a digital 60-Hz notch filter for minimizing the power line interference, a finite impulse response (FIR) band-pass filter for correcting baseline wander, a multi-scale mathematical morphology (3M) filter for eliminating motion artifacts and power line interference, and a differential operation method (DOM) for smoothing and normalizing have been integrated into the software. In order to measure the HRV, an adaptive QRS detect algorithm, which was easy to implement on a simple, real-time device developed by our laboratory in a previous study, has been adopted to extract RR interval series for HRV analysis, with 99.3% detection rate. The calculated time domain(Mean RR, SDNN, rMSSD, pNN50), frequency domains (VLF, absolute and normalized LF, HF, total power), geometric (TINN, HRV TI) and nonlinear measures (Poincare plot, Detrended fluctuation analysis) of HRV are obtained according to the standards of measurement, proposed by the Task Force of the European Society of Cardiology and the North American Society of Pacing and Electrophysiology, which describes the detail of physiological correlates of HRV and calculation methods.

3.1.3 Autentication Protocol

The LF/HF ratio approach is used for decision either data transmission will be carried out or not. It will act as key, if source and destination both matches by authentication protocol then original information generated from sender can be

transmitted to receiver. But before sending data to DAF, this data is encrypted by using low cost hashing algorithm to increase the level of security.

There are two methods to evaluate HRV. The first one is evaluation of HRV in time domain by investigating ECG's RR intervals chain. However, second method is based on frequency domain analysis of ECG, in which same spectrum of identical RR intervals are analyzed. The frequency domain approach has following benefits in comparison with time domain approach

i) Their results could be presented with the absolute value (magnitude) of variability as power spectrum function.
ii) Same spectrum of identical RR intervals is analyzed, and it decomposes chain of successive RR intervals as addition of functions of sinusoidal with different frequencies and amplitudes.
iii) The frequency specific fluctuations of signals can be studied by analyzing its power spectrum or frequency
iv) The spectral analysis displays fluctuations of heart rate at different frequencies, Fast Fourier Transformation (FFT) and Autoregressive modelings (AR) are renowned methods for its analyzing.

Due to these advantages, we prefer to use frequency domain approach to measure efficiency of our proposed algorithm. For conventional HRV measurements, there are three spectral components are explained [23]; a) Very Low Frequency (VLF) b) Low Frequency (LF) c) High Frequency (HF). The VLF component has range of 0.0 to 0.04 Hz and it is related to not fast regulatory methods. The range of LF component is 0.04 to 0.15 Hz; it is useful for reflecting sympathetic activity. The reflecting vagal activity is performed at HF components having range of 0.15 to 0.4Hz. The ratio between LF and HF is utilized to specify steadiness between both components of Autonomic Nervous System (ANS) action; the sympathetic and parasympathetic. The heart rate is increased and decreased by sympathetic and parasympathetic respectively. Further, statically calculated index of LF and HF can be used to calculate which factors are important for autonomic misbalance. Therefore, this ratio is utilized as authentication protocol in our proposed algorithm to reduce the computational complexity so to provide efficient approach to secure BSN.

3.1.4 DAF Algorithm

The algorithm 1 explains how DAF (Data Autentication Function) is generated by using MATLAB. It involves three basic parts QRS detection, HRV calculation and authentication protocol. In our algorithm, Pan and Tompkins approach [24-25] is used for QRS detection based on three steps: Linear filtering, non-linear transformation and threshold detection. The linear filtering is based on differentiation which is basically high-pass filtering process. It amplifies higher frequencies that are characteristic for the QRS- complex and attenuates lower

frequencies that are characteristic for P and T deflections. Consider $r[n]$ is the input raw ECG signal, and $O[n]$ is the output of linear filtering, which is the linear combination of $d_1[n]$ and $d_2[n]$, first derivative and second derivative of $r[n]$ respectively. The non-linear transformation is achieved by the combination of squaring operator and moving windows integration .The squaring operator $s[n]$ as shown in eq. (4) gives optimal output by squaring $O[n]$. In QRS complex, it performs suppression, if any difference arises due to P and T deflections and also enhances amplitude of high frequency components. The $y(n)$ represents moving window integration, it helps to make output from squaring operator further smooth. The threshold detection is essential step to discover the QRS-complex. For all value of i, where i is the number of heart beats or ECG signals involved in the ECG waveform, if outputs of non-linear transformation $y[n]$ is greater than or equal to the predetermined threshold all these outputs will be termed as QRS-complex. Once the QRS-complex is detected, next step is to determine the R-Peak, just by finding the absolute value or index of QRS-complex. In ECG, Q-to-Q intervals are the time intervals between successive heart beats during whole QRS-complex; they are also normally termed as RR intervals. However, FFT is used to determine power density spectrum by using a hanning windows (H), then we can find VLF, LF and HF. Finally, LF/HF ratio is used as authentication protocol.

3.2 Low Cost Encryption

In our research, we use SHA-1 as low cost encryption technique to increase level of authentication. Although DAF can provide authentication but for extra security, less expensive and flexible encryption technique is used in proposed algorithm as shown in Fig.2. The SHA-1 stands for Secure Hash Algorithim-1. It produces 20 bytes or 40 hexadecimal digits hash value, because it implements security in many applications and protocols, few are enlisted here Secure Sockets Layer (SSL), Internet Protocol Security (IPSec), Secure Shell (SSH) and Transport Layer Security (TLS). It is very simple and cost-effective because it does not require high resources for encryption and decryption. The proposed algorithm provides unique, accurate and efficient technique to secure BSN and its authentication is verified twice; i) by using DAF, and ii) by low cost encryption. Our designed algorithm is simple and effective and based on LF/HF ratio, as authentication protocol for implementing security in BSN.

Algorithm 1. Data Authentication Function

$$
\begin{aligned}
&Algorithm\ Parameters\\
&r[n] \rightarrow raw\ ECG\ signal\\
&d_1[n] \rightarrow first\ derivative\ of\ r[n]\\
&d_2[n] \rightarrow second\ derivative\ of\ r[n]\\
&O[n] \rightarrow output\ linear\ filter(r[n])\\
&s[n] \rightarrow squaring\ operator\\
&y(n) \rightarrow moving\ window\ integeration\ output\\
&F \rightarrow output\ of\ FFT\\
&PSD \rightarrow Power\ Spectral\ Denisty\\
&HF \rightarrow High\ Frequency\\
&LF \rightarrow Low\ Frequency\\
&VLF \rightarrow Very\ Low\ Frequency\\
&a_p \rightarrow authentication\ protocol\\
&Step\ \#\ 1: Linear\ filtering\\
&d_1[n] \rightarrow diff(r[n])\\
&d_2[n] \rightarrow diff(d_1[n])\\
&O[n] \rightarrow d_1[n] + d_2[n]\\
&Step\ \#\ 2: Non-linear\ transformation\\
&s[n] \rightarrow \{O[n]\}^2 \rightarrow apply\ squaring\ operator\\
&y(n) \rightarrow \frac{1}{N}[s(n-(N-1)) + s(n-(N-2)) + \ldots\ldots\ldots + s(n)]\\
&(perform\ moving\ window\ integeration)\\
&Step\ \#\ 3: Threshold\ Detection\\
&Thershold \rightarrow \{max(y[n]) - mean(y[n])\} / 2\\
&For \rightarrow i = 1:1:b\\
&(whereas\ "b"\ is\ nunber\ of\ heartbeats\ or\ ECG\ signal\ sin\ ECG\ waveform)\\
&if \rightarrow y[n] >= Thershold\\
&QRS \rightarrow y[n]\\
&end\\
&end\\
&R-Peak\ Detection\\
&R = index(QRS)\\
&whereas R \rightarrow R-Peak\\
&For \rightarrow i = 1:1:QRS\\
&RR \rightarrow RR_{i+1} - RR_i, whereas\ RR \rightarrow RR\ interval\\
&end\\
&end\\
&Step\ \#\ 4: HRV\ Calculation\\
&i)\ Apply\ FFT\\
&F \rightarrow fft(N, H)\\
&whereas N \rightarrow index\ of\ RR, H \rightarrow hanning\ windows\\
&A = absolute(F)\\
&ii)\ Calculate\ PSD\\
&PSD \rightarrow autocorrelation(A)\\
&iii)\ output\ of\ PSD, will\ be \rightarrow VLF, LF\ and\ HF\\
&Step\ \#\ 5: Autentication\ protocol\\
&Determine \rightarrow a_p\\
&a_p \rightarrow LF\ /\ HF
\end{aligned}
$$

4 Performance Analysis

The block diagram of our proposed algorithm is shown in Fig.2, uses authentication protocol in DAF as key to achieve security in BSN, no external keys are required for data authentication; this advantage leads our algorithm toward simplicity in comparison with other traditional cryptographic approaches. However, key management and its distribution make conventional methods more complex and ineffective.

In symmetric encryption conventional schemes, only single key is used for both encryption and decryption; there are two main reasons to cause high transmission time in these approaches. Firstly, unique keys are generated for different rounds from initial key such as in 64bits DES original key, from which other 8 different keys of size 56 bits are generated. Secondly, they support only fix block size of data such as 64 bits for DES. If data is more than 64 bits, it must be divided into multiples of 64, and data is transmitted in multiple rounds.

However, for asymmetric encryption process, even more complex and time consuming algorithm is utilized for key generation and data transmission. RSA is one of the examples of public-key encryption, which uses public and private keys for encryption and decryption respectively.

To explain the efficiency of our proposed algorithm for data authentication in BSN, simulation environment with real-time data of several patients was created and parameters used in performance analysis are shown in Table 2. We used real time ECG data of 20 years old female patient, which is received by associated sensor on his body. The length of this ECG data is 258decimal values in different matrix format, and each decimal value is equal to 36 bits which means overall length in binary is 9216 bits.

In our proposed algorithm, if authentication protocol i.e. ratio of LF/HF ratio, matches between source and destination then all 9216bits will be transmitted in one round, this is the main reason to make our proposed protocol efficient. Whereas, this is not true for DES and RSA, because DES only support block size of 64bits and in RSA message of one decimal (i.e. 36 bits) value can be transmitted at a time.

a) Transmission Time

The transmission time is the amount of time required for data transmission from source to destination. It depends upon the number of rounds involved during transmission. As number of rounds increases; transmission time will increase as shown in eq. (1).

$$t = N_r \times k \tag{1}$$

Whereas t represents total transmission time, and N_r demonstrates number of rounds and complexity involved per round is denoted by k. For our proposed algorithm , $N_r = 1$ because all data is transmitted in one round, if key matches between source and destination, authentication protocol in DAF is acting as key. Due to this reason proposed algorithm requires less transmission time in data transmission, so is simple and cost-effective for implementing security in BSN.

For DES, number of rounds depends upon the initial key size and length of data generated from source. The number of rounds is directly proportional to length of data and inversely proportional to initial key size. In eq. (2) L_b, K_i represents length of data in bits and initial key size in bits, respectively.

$$N_r = \frac{L_b}{K_i} \tag{2}$$

In our simulation L_b is 9216 bits and K_i is 64 bits for DES, therefore N_r will be 144 rounds

$$N_r = \frac{L_b}{K_i} = \frac{9216}{64} = 144$$

The overall number of keys required for all rounds (N_k) depends upon N_r and keys required per round (Kr) as shown in eq. (3).

$$N_K = N_r \times Kr \tag{3}$$
$$N_K = 144 \times 8 = 1152$$

It can be visualized that DES uses 144 rounds and 1152 keys in order to achieve authentication, also this complex calculation takes longer transmission time as compared to our proposed algorithm. For RSA, number of rounds N_r equal to the length of data in decimal (L_d), in our simulation L_d is 258, therefore N_r is also 258. As transmission time depends upon number of rounds and complexity involved per round, in both conditions RSA requires more time to process complete data than our proposed algorithm and DES. Because for our proposed algorithm. DES and RSA N_r =1, N_r =144 and N_r =258, respectively.

b) Average Remaining Energy

Let E_i is the initial energy of source and destination for data transmission. The amount of energy consumed is proportional to the transmission time, larger the time required for processing; more the energy consumed. To check whether our proposed algorithm is energy efficient or not, it is necessary to determine the average remaining energy of nodes. The eq. (6) calculates average remaining energy of nodes; where, E_{rs} and E_{rd} represents remaining energy of source and destination, respectively; which depends upon data length (L_d), data rate (D) and transmitting /receiving power (T_x / R_x) as shown in eq. (4) and eq. (5).

$$E_{rs} = \sum_{j=1}^{N} [(E_i)_{(j-1)} - (T_x \times L_d / D)] \quad (4)$$

$$E_{rd} = \sum_{j=1}^{N} [(E_i)_{(j-1)} - (R_x \times L_d / D)] \quad (5)$$

$$E_{ar} = (E_{rs} + E_{rd}) / 2 \quad (6)$$

The value of E_{ar} is high for our proposed algorithm, because it requires less time for processing. Therefore, it can be said that proposed algorithm consumes less energy than DES and RSA, because it requires less transmission time than conventional methods.

c) Power Utilization

Our proposed algorithm is also power efficient, because utilization of power depends upon energy consumption and transmission time. As we explained earlier that our proposed algorithm utilizes less energy and time for data transmission, hence it can be stated that less power will be utilized to secure BSN. The amount of power utilized (P_u) can be measured by any one of following equations

$$P_u = \frac{1}{t} \sum_{i=1}^{N} [2 \times E_{(i-1)} - \frac{L_d}{D}(T_x + R_x)] \quad (7)$$

The algorithm 2 represents the performance analysis of our proposed algorithm, in which M represents the original transmitted from source, C is the cipher text generated after applying low cost encryption, where as S and D are the source and destination respectively. The authentication protocol a_p is the ratio between LF and HF, if it matches between S and D, then transmission will be started. After data transmission, total transmission time, average remaining energy and power utilization, t , E_{ar}, P_u are calculated to evaluate the performance of proposed algorithm.

5 Simulation Environment

MATLAB is used in our simulation. It is assumed that initial energy is 1 joule for both source and destination. It is considered that transmission power, receiving power and data rate as -25dbm, -95dbm and 256Kbps, respectively. A comparative analysis of proposed algorithm based on ECG as biometric trait and two conventional cryptographic security approaches; Data Encryption Standard (DES) which is symmetric or private-key based encryption technique and RSA (Rivest Shamir Adleman) which is an asymmetric or public-key based encryption method. In this research real time data of ECG from physioNet including two data bases; MIT-BIH Normal Sinus Rhythm Database (nsrdb) and MIT-BIH long-Term ECG Database (ltdb) was used. Overall we have analyzed ECG data of 20 patients in between age of 20 to 80.

Table 2 List of abbreviations used in performance analysis

Abbreviation	Detail	Abbreviation	Detail
t	total simulation time	L_b	data length in binary
k	complexity per round	E_i	Initial energy
N_r	number of rounds	E_{rs}	Remaining energy from source
N_k	overall keys required for all rounds	E_{rd}	remaining energy for destination
Kr	number of keys required per round	E_{ar}	average remaining energy
K_i	initial key size	T_x	transmission power
L_d	data length in decimal	R_x	reception power
D	data rate	P_u	Power utilized

Algorithm 2. Performance Analysis

```
Alg orithm parameters
M → orignal message
C → ciephertext
S → sourcenode
D → destinationnode
a_p → autenticationprotocol
LF / HF → LowFrequencytoHighFrequencyRatio
Ear → Average Remaining Energy
P_tr → TotalPower Required
t → TransmissionTime
Step # 1 : Low cost Encryption
C → E(M)
Step # 2 : DataTransmissionand Reception
i) Stranmits → C
ii) if → S.a_p = D.a_p
whereas, a_p → LF / HF
Drecieves → C
DdecryptsCtogetback → M, whereasM = D(C)
end
Step # 3 : PerformanceEvaluation
i) Determine → t
ii) Determine → E_ar
iii) Determine → P_tr
```

6 Experimental Results

The Fig.4 represents ECG waveform of 20 years old subject (female). The grid interval used in this waveform is 0.2 seconds and amplitude is 0.5 mV, a 12-bit Analog-to-Digital converter sampling at 128Hz frequency is used to get digital signal. The RR-interval representation at different time durations of mentioned subject is shown in Fig. 5, this time interval is distance between two consecutive R-peaks. The Figs.5 (a), 5(b) and 5(c) exploit the RR-interval for time duration of 1minute, 1hour and for complete wave respectively. The Fig.6 demonstrates histogram of RR-interval for different time durations. The Figs.6 (a), 6(b) and 6(c) explain histogram for RR-interval representation for time duration of 1minute, 1hour and for complete wave, respectively.

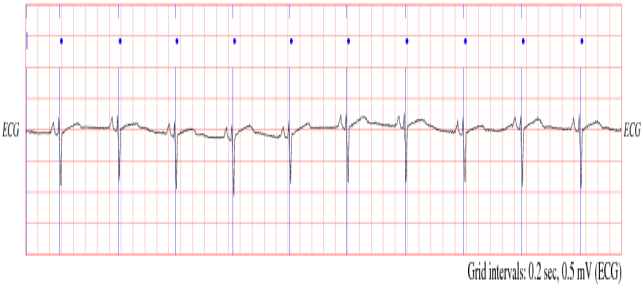
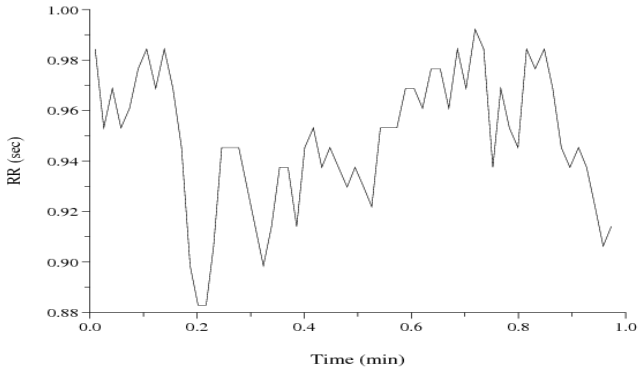
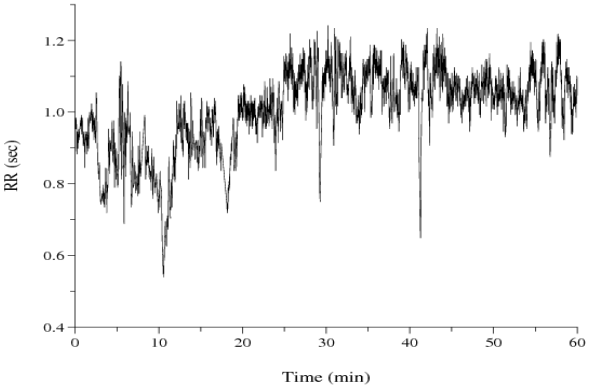


Fig. 4 ECG waveform of 20years female patient

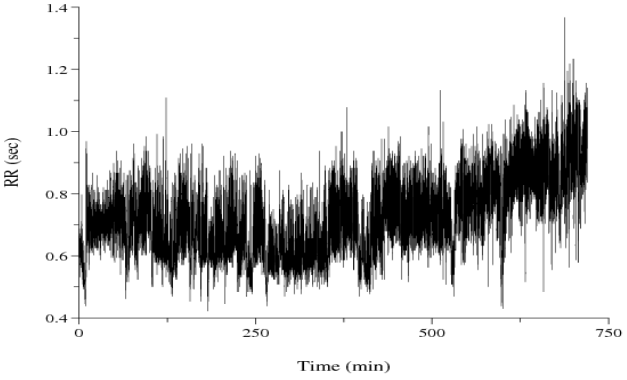
The RR-intervals are further used to determine HRV by using different time domain as well as frequency domain approaches. The ratio LF/HF is used as authentication protocol between source and destination in our proposed algorithm to provide efficient solution to secure BSN as shown in Figs. 7, 8 and 9. Our proposed algorithm eliminates the need of complex key generation procedure, which is more cost-effective and efficient approach that existing techniques for data authentication in BSN as shown in Table 3. Fig.7 shows total amount of transmission time required for proposed algorithm, DES and RSA is 0.214 ms, 3.40ms and 6.40 ms respectively. From results it can be analyzed that proposed algorithm consumes less time than traditional cryptographic techniques during transmission. In parallel with more transmission time consumption, the key generation procedure for two cryptographic techniques consumes more resources, such as, transmission time execution. Fig.8, shows the average remaining energy of our proposed algorithm, DES and RSA of 0.998 joules, 0.963 joules and 0.932 joules respectively. The implementation of proposed algorithm is simple and easy than DES and RSA, therefore it requires less time and energy than both conventional techniques. Total power consumed by proposed algorithm, DES and RSA during data transmission is 9.64mW, 10.05mW and 10.10mW respectively, as shown in Fig.9. Hence, we can say that our proposed algorithm is power-efficient than DES, and RSA.



(a)

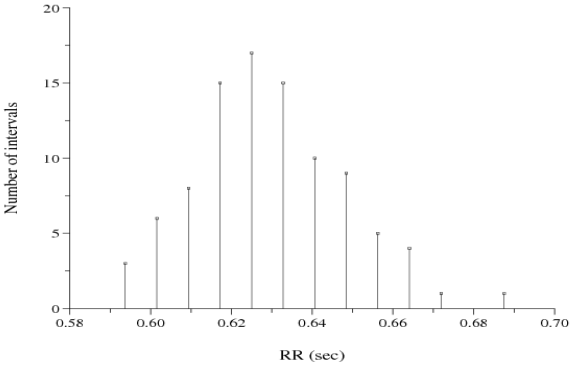


(b)

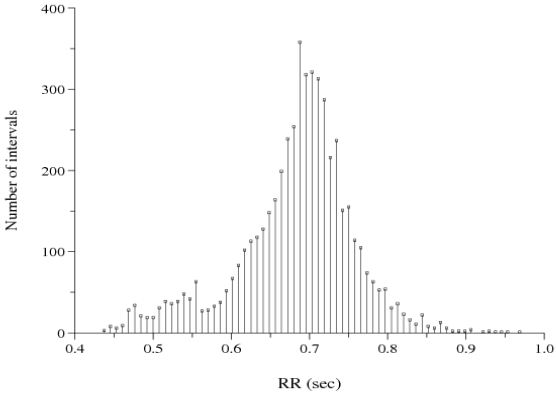


(c)

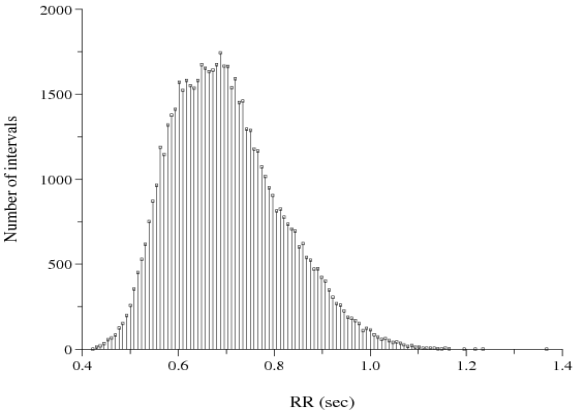
Fig. 5 RR-Interval representation (a) RR-interval for 1minute, (b) RR-interval for 1hour, and (c) RR-interval for complete wave



(a)



(b)



(c)

Fig. 6 Histogram representation of RR-interval (a) Histogram representation of RR-interval for 1minute, (b) Histogram representation of RR-interval for 1hour and (c) Histogram representation of RR-interval for complete wave

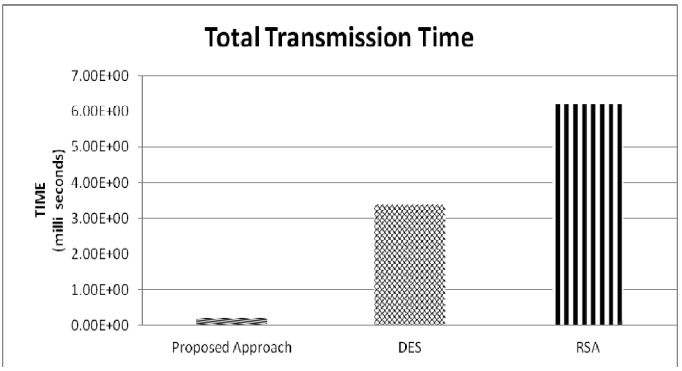


Fig. 7 Total transmission time

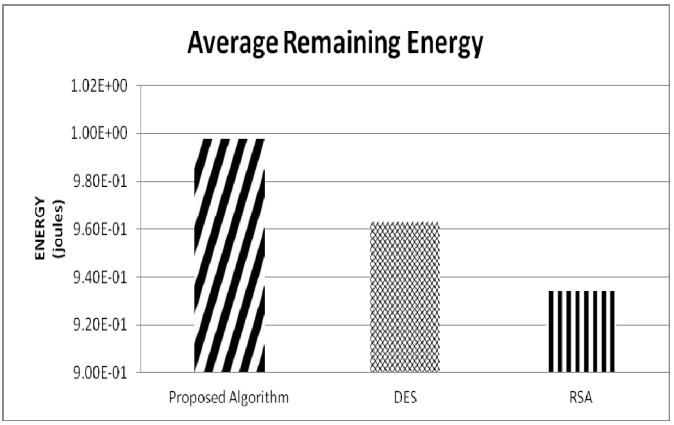


Fig. 8 Average Remaining Energy

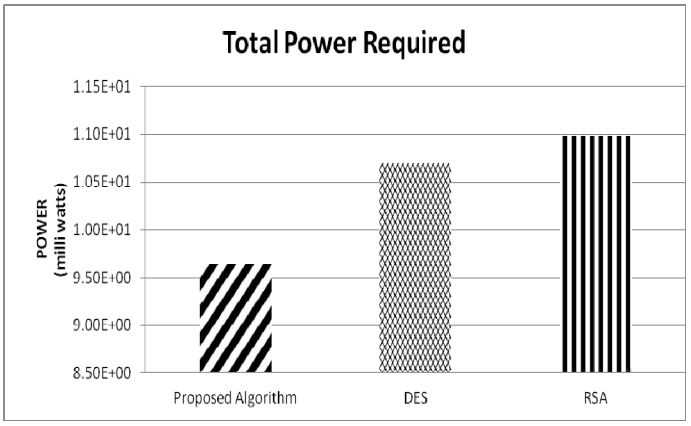


Fig. 9 Total Power required

Table 3 Comparison between proposed algorithm, DES and RSA

	Transmission Time (ms)	Average Remaining Energy(Joules)	Power Utilization (mW)
Proposed Algorithm (Biometric-based)	0.214	0.998	9.64
DES(Symmetric Encryption Approach)	3.40	0.963	10.07
RSA(Asymmetric-Encryption Approach)	6.20	0.934	10.10

7 Conclusion

This paper presents one efficient and cost-effective algorithm based on ECG as biometric characteristics to attain security and privacy in BSN, whereas ECG is used as biometric feature. The real-time data of ECG from physiobank is used in simulation; we utilized two data bases namely MIT-BIH Normal Sinus Rhythm Database (nsrdb) and MIT-BIH long-Term ECG Database (ltdb) to carry out experiments. The real-time ECG data of 20 patients of the age in between 20 to 80 is received from both databases. The aim of our research is to minimize time consumption during key generation mechanism in conventional methods. Therefore, we utilize the ECG as biometric feature to implement security; the Data Authentication Function (DAF) is applied in our proposed algorithm instead of generation of complex keys. The DAF involves three major steps i) detection of QRS-complex iii) to calculate Heart Rate Variability v)the LF/HF ratio is used as authentication protocol, the output of authentication protocol is acting as key between source and destination in our research paper. Transmission between source and destination will only begin if this ratio LF/HF matches, otherwise message will be discarded. Although DAF provides the authentication, but to raise the further level of security, we added low cost hashing encryption scheme in our research. The source performs encryption of message by SHA1, before processing to DAF. Simulation results show that our proposed scheme outperforms symmetric encryption based technique DES and asymmetric encryption based algorithm RSA. Finally, it can be concluded by simulation results that our proposed algorithm requires less transmission time than DES and RSA as, 0.214 ms, 3.40ms and 6.40 ms, respectively. Average remaining energy of our proposed algorithm, DES and RSA is 0.998 joules, 0.963 joules and 0.932 joules respectively. Total power required by proposed algorithm is 9.64mW which is lower than DES and RSA with total power consumption of 10.05mW and 10.10mW respectively. As fewer resources are required during data transmission, therefore our proposed algorithm claims to offer cost-efficient solution than conventional approaches for security of BSN.

References

[1] Bao, S.D., Zhang, Y.T., Shen, L.F.: Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems. In: Proc. 27th Annual Conf. IEEE-EMBS, Shanghai, China (September 2005)

[2] Wang, H., Fang, H., Xing, L., Chen, M.: An Integrated Biometric-Based Security Framework Using Wavelet- Domain HMM in Wireless Body Area Networks (WBAN). In: 2011 IICC, pp. 1–5 (June 2011)

[3] Challa, N., Cam, H., Sikri, M.: Secure and Efficient Data Transmission over Body Sensor and Wireless Networks. Eurasip Journal on Advances in Signal Processing (2008)

[4] Poon, C.C.Y., Bao, S.D., Zhang, Y.T.: A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and M-health. To appear in IEEE Communications Magazine (April 2006)

[5] Uludag, U., et al.: Biometric Cryptosystems: Issues and Challenges. Proc. IEEE 92(6), 948–960 (2004)

[6] Lang, C.S., Lee, D.G., Han, L.-W., Park, L.H.: Hybrid security protocol for wireless body area networks. Wireless Communications and Mobile Computing, 277–288 (2011)

[7] Bao, S.-D., Shen, L.-F., Zhang, Y.-T.: A Novel Key Distribution of Body Area Networks for Telemedicine. In: IEEE International Workshop on Biomedical Circuits & Systems (2004)

[8] William, C., Tan, C.C., Wang, H.: Body Sensor Network Security: An Identity-Based Cryptography Approach. Security, 148–153 (2008)

[9] Chen, M., Gonzalez, S.: Body area networks: A survey. MONET (2010)

[10] Jain, A.K., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Trans. Circ. Syst. Video Technol. 14(1), 4–20 (2004)

[11] Reid, P.: Biometrics for Network Security, pp. 4–5. Prentice-Hall, Englewood Cliffs (2004)

[12] Bao, S.-D., Zhang, Y.-T., Shen, L.-F.: A Design Proposal of Security Architecture for MedicalBody Sensor Networks. In: Proceedings of the International Workshop on Wearable and Implantable Body Sensor Networks (2006)

[13] Miao, F., Jiang, L., Li, Y., Zhang, Y.-T.: A Novel Biometrics Based Security Solution for Body Sensor Networks. In: 2nd International Conference on Biomedical Engineering and Informatics, BMEI (2009)

[14] Venkatasubramanian, K.K., Banerjee, A., Gupta, S.K.S.: PSKA: usable and secure key agreement scheme for body area networks. IEEE Transactions on Information Technology in Biomedicine 14(1), 60–68 (2010)

[15] Zhang, G.H., Poon, C.C.Y., Zhang, Y.T.: A Fast Key Generation Method based on Dynamic Biometrics to Secure Wireless Body Sensor Networks for p-Health. In: 32nd Annual International Conference of the IEEE EMBS (2010)

[16] Cherukuri, S., Venkatasubramanian, K.K., Gupta, S.K.S.: 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 6-9, pp. 432–439 (2003)

[17] Yao, L., Liu, B., Wu, G., Yao, K., Wang, J.: A Biometric Key Establishment Protocol for Body Area Networks. Hindawi Publishing Corporation International Journal of Distributed Sensor Networks 2011, 1–10

[18] Bao, S.-D., Poon, C.C.Y., Zhang, Y.-T., Shen, L.-F.: Using the Timing Information of Heartbeats as an Entity Identifier to Secure Body Sensor Network. IEEE Transaction on Information Technology in Biomedicine 12(6) (November 2008)
[19] Zhang, G.H., Poon, C.C.Y., Li, Y., Zhang, Y.T.: A Biometric Method to Secure Telemedicine Systems. In: 31st Annual International Conference of the IEEE EMBS, Minneapolis, Minnesota, USA, September 2-6 (2009)
[20] Ramila, S.N., Ahmed, R., Abdollah, M.F., Dutkiewicz, E.: A Biometric-based Security for Data Authentication in Wireless Body Area Network (WBAN) (2013)
[21] Zhang, G.H., Poon, C.C.Y., Zhang, Y.T.: A Review on Body Area Networks Security for Healthcare. ISRN Communications and Networking 2011, 1–8 (2011)
[22] Undercoffer, J., Avancha, S., Joshi, A., Pinkston, J.: Security for sensor networks. In: Proceedings of the CADIP Research Symposium (2002)
[23] Jovic, A., Bogunovic, N.: Feature set extension for heart rate variability analysis by using non-linear, statistical and geometric measures. In: Proceedings of the ITI 2009 31st International Conference on Information Technology Interfaces, pp. 35–40 (June 2009)
[24] Pan, J., Tompkins, W.J.: A real-time QRS detection algorithm. IEEE Trans. Biomed. Eng. 32(3), 230–236 (1985)
[25] Hamilton, P.S., Tompkins, W.J.: Quantitative investigation of Qrs detection rules using the Mit/Bih arrhythmia database. IEEE Trans. Biomed. Eng. 33(12), 1157–1165 (1986)