Xu and Hua *EURASIP Journal on Information Security* (2016) 2016:5
DOI 10.1186/s13635-015-0024-x

EURASIP Journal on Information Security
a SpringerOpen Journal

RESEARCH Open Access

Secured ECG signal transmission for human emotional stress classification in wireless body area networks

Hansong Xu and Kun Hua[*]

Abstract

Information security is key important when we are trying to interconnect the wireless body sensor network with the healthcare social network via mobile facilities. In this paper, we specially work on a secured electrocardiogram (ECG) signal transmission scheme to prevent further injuries for patients with heart diseases from human emotional stress. We proposed a dynamic encryption method via biometric information among frequency spectrums of ECG signals, which can guarantee both high classification rate (>90 %) and system energy efficiency. At the same time, cooperative relays are applied for an additional spatial diversity gains. Simulation results show that the improved transmission rate and signal power capacity can lower the probability of data intercept (LPI) and detection (LPD) by taking the advantages of both temporal and spatial diversities. The network security thereby can be further improved.

Keywords: Stress classification, Wireless Body Area Network (WBAN), Signal encryption, Cooperative relay, Electrocardiogram (ECG)

1 Introduction

Over the last few decades, smart devices have improved digital signal communication performances greatly, and thus brought us numerous benefits in our daily lives. State-of-the-art smartphones are equipped with advanced processors, which provide high speed data transmission rate, efficiency usage of battery life, and multi-task running ability. In wireless communication network, such features promise high quality information delivery, efficient energy cost, and low bit error rate, etc. For smartphones based on signal encryption and transmission, traditional encryption methods, such as “RSA,” are too slow for the computational process and are limited for key generation. While, in this paper, a time-varying encryption method “dynamic AES” is proposed, where its symmetric key is selected from dynamic key sets, which are generated from the changing biometric information of electrocardiogram (ECG) signals. Through this “dynamic AES” encryption scheme, the security and robustness of the wireless transmission is improved greatly.

Meanwhile, we use cooperative relays to improve data transmission quality [1] and constrain the probability of intercept and detection. In our work, low probability of intercept can be achieved by increasing the spatial and temporal diversity of the transmission, and low probability of detection can be realized by multiplexing among multiple virtual multiple-input and multiple-output (MIMO) channels [2]. At the same time, the battery energy efficiency is also guaranteed by sharing transmission power cost with cooperative relays.

Indexed body health condition information can be shown as a certain form of continual signals, which are called “biomedical signals.” Biomedical signal analysis can provide us a probability of estimation for our health condition from both physical and mental sides, which mainly focuses on skin temperature (ST), electromyogram (EMG), blood pressure (BP), ECG, etc. Among those signals, ST is a physiological signal, which is often used to indicate stress conditions and is similar to BP, but BP is often applied to measure different levels of stresses during induce stress level task [3, 4]. For EMG and ECG signals, the former is used more on-body movement control or pain identification and monitoring

[*] Correspondence: khua@ltu.edu
Electrical and Computer Engineering Department, Lawrence Technological University, Southfield 48075, USA

through muscles. The latter is used more for heart activity monitoring and heart information carrier. ECG signal carries heart activity information, which can be analyzed for stress level detection, identification, and predication [3, 5].

Emotional stress may cause lots of diseases for human beings, such as the following: mental illness, disorders, etc. Being under a stress environment for a long time or accidentally attacked by strong emotional stress may cause serious problems on both physical and mental issues, especially for patients. Thus, the general structure of proposed scheme is shown in Fig. 1 and 2. Processes of ECG signal in the Wireless Body Area Network (WBAN) are shown in the steps 1–3: (1) ECG signal collection by on-body sensors, (2) artifacts and machine noise removal by low frequency pass filter (LPF) and High frequency pass filter (HPF), and (3) features extraction and stress level identification. Then, the transmission of pre-processed ECG signal is shown as steps 4 and 5: (4) pre-processed signal encryption [6] and (5) cooperative relay as MIMO for encrypted signal transmission under noise channel.

The remainder of this paper is organized as follows: Section II reviews relevant literature. The proposed dynamic ECG signal encryption scheme with cooperative relayed network is studied in Section III. Simulation results are given and analyzed in Section IV, and Section V summarizes our research conclusions.

2 Peer work review

For stress level identification assessment, Paper [3], introduced ST for stress level change identification and monitoring. In their work, a plenty of experiments have been placed for stress level classification through ST parameters. They induced stress levels to healthy volunteers by using Stroop color test for different stress levels and received the accuracy rate of 88 %.

In 2012, paper [7] applied statistical features from ECG signals for stress level identification and classification, which is considered as a better technique. In their paper, the stress was induced by the method called "MAT" [8, 9], which was designed to increase stress level from one to another, gradually from "normal" to "low stress level," then "medium stress level" and finally "strong stress level." Then, using "DWT" for statistical features extraction, in which "DWT" was able to decompose the ECG signal both in time and frequency domain.

ECG signals are more meaningful at the frequency range of 0–0.5 Hz, which was separated into three frequency ranges (VLF, LF, HF) [7] for stress classification. Meanwhile, paper [5] used wavelet transform for ECG signal decomposition and feature extraction; totally, six statistical features in combinations of LF, HF, and LF/HF give a best of 96.41 % classification accuracy rate.

From wired to wireless communication, security problem is increasingly severe because of the publicly shared bandwidth and open access in wireless network. Paper

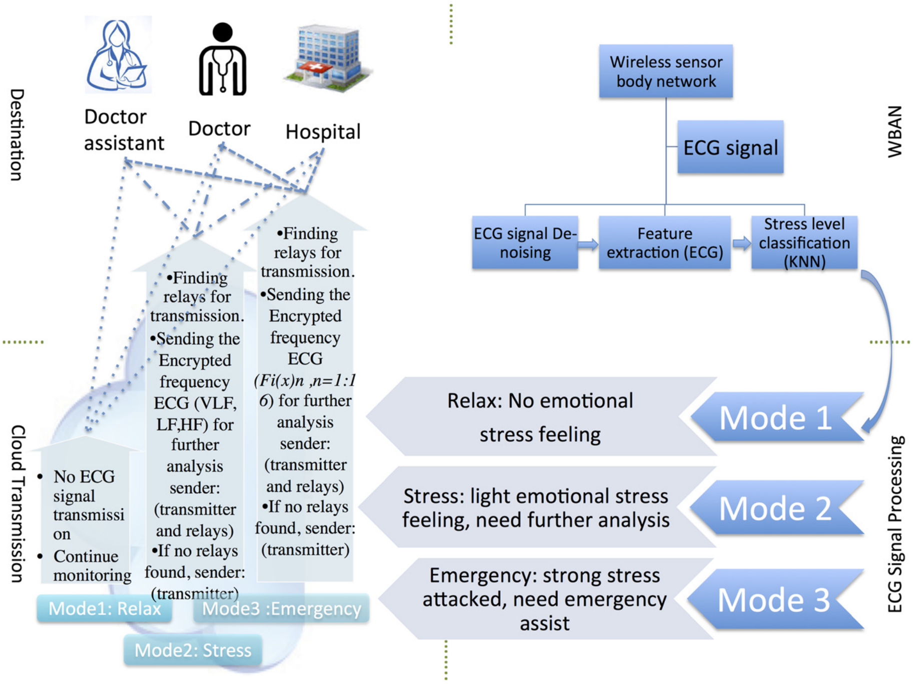

Destination
Doctor assistant
Doctor
Hospital
Cloud Transmission
• No ECG signal transmissi on
• Continue monitoring
•Finding relays for transmission.
•Sending the Encrypted frequency ECG (VLF, LF,HF) for further analysis sender: (transmitter and relays)
•If no relays found, sender: (transmitter)
•Finding relays for transmission.
•Sending the Encrypted frequency ECG (Fi(x)n ,n=1:16) for further analysis sender: (transmitter and relays)
•If no relays found, sender: (transmitter)
Mode1: Relax
Mode3 :Emergency
Mode2: Stress
Wireless sensor body network
ECG signal
ECG signal De-noising
Feature extraction (ECG)
Stress level classification (KNN)
WBAN
Relax: No emotional stress feeling
Mode 1
Stress: light emotional stress feeling, need further analysis
Mode 2
Emergency: strong stress attacked, need emergency assist
Mode 3
ECG Signal Processing

Fig. 1 General structure of proposed work

[6] proposed a biometric-information-based key distribution for WBSN application; in their paper, the encryption method is proposed w.r.t the limitation from biomedical sensors such as the following: energy supply, computational capacity, and communication capabilities. In their work, the 128 bits symmetric keys for Advanced Encryption Standard (AES) are generated from the coefficients, where the coefficients are from fast Fourier transform (FFT) for a short period of time domain ECG.

As is well known, AES is a widespread encryption standard and works very well for WBSN-based ECG signal protection. Since DWT has already converted the temporal ECG signal into frequency domain through an efficient and also practical way, in this case, our biometric key sets are generated from the coefficients of DWT, instead of FFT on ECG signal.

Then, further research found that the improved transmission data rate and signal power are related to the higher level of transmission security in wireless communication. In paper [2], the authors investigated the information security of MIMO links (multiple-input and multiple-output) with a proposed theoretic framework; space-time communication was provided for improve the security of digital data transmission. In their work, a well-designed secure link was built to lower the probability of information intercept and detection by the eavesdroppers, such as the transmitter and destination's communication channel was informed, while the eavesdropper's channel was uninformed, putting an eavesdropper at an accordingly disadvantage.

At the same time, applying space coding over multiple transmitter and receiver antennas can also lower the data intercept and detection rates. Besides, encrypted data stream from transmitter side, which can only be decrypted by paired receiver side with time-varying biometric key. Meanwhile, the channel security was improved by applying MIMO and channel coding technologies, plus it may be applicable for several kinds of communication channels. In 2012, paper [12] considered careful physical position and smart cooperation of antennas and focused more on the specific absorption rate (SAR) performance of the increasing mobile phone terminals. In their work, the relationship of SAR with antenna position, chassis size, antenna height, etc. were evaluated.

The conclusion of peer work is shown in the following Table 1.

3 Methodology

It can be observed from Table 2 that the stress level classification can be achieved by features from frequency domain and gained outstanding classification accuracy. Continually, our approaches dealt with the real world problems and achieved reasonable gains, such as security and energy efficiency for mobile communications. To specifically address our approaches for the aforementioned solution, which is preventing further injuries on patients from strong emotional stress, we propose the following three subsections corresponding to each technique process: stress level classification scheme, state-of-the-art encryption method, and cooperative relay-based transmission.

3.1 ECG signal pre-processing and stress level classification

Figure 3 displays ECG signal '$\varphi(t)$', which is a continuous waveform. Human stress levels are able to be identified based on the curves and features.

We apply low frequency pass filter (LFP) and high frequency pass filters (HFP) to filter out the ECG signal, into frequency range 0.01–100 Hz firstly. Meanwhile, the influence of machine noises and artifacts are avoided. Then, discrete wavelet transform (DWT) is applied for further analysis, since "DWT" allows signal to be analyzed at frequency domain [10]. In this case, time-frequency information of input ECG signal "$\varphi(t)$" can be decomposed to different frequency bands; in this work, we decomposed ECG signal by "DWT" through shifting and scaling, in totally 16 levels, to achieve required frequency bands (VLF, LF, HF) via a prototype function, which is expressed as the following:

$$\varphi(t) \overset{\mathrm{DWT}}{\rightarrow} \{f_i\}, i\in[1,16] \tag{1}$$

In Eq. (1), "DWT" is applied for 'i' level's ECG signal decomposition. By using "DWT," the original ECG signal is decomposed to detail coefficient (CD) by high frequency pass filter and approximation coefficient (CA) by low frequency pass filter. After the first level decomposition, the coefficient (CA) continues to decompose into the second level, then, with continuous decomposition, ECG signal will be decomposed into the 16th level. The frequency ranges (VLF, LF, HF) will be extracted, the very low frequency (VLF) bands signals are $\{f_{15},f_{16}\}$ (0 – 0.04) Hz; the low frequency (LF) bands signals are $\{f_{14}\}$(0.04-0.15) Hz; the high frequency (HF) signals are $\{f_{12},f_{13}\}$ (0.15-0.5) HZ [5]; since after each level's decomposition, the lower half of last level's frequency bands becomes the new level's frequency bands, which is also shown in Table 2.

For the mathematical equations, we set high-pass filter as "h(n)," low-pass filter as "l(n)," "i" is the scaling number, represent the, The "i" level CA is represented by "$ap^i(f_{i,a})$," and the CDs is represented by $de^i(f_{i,d})$ as shown below,

Table 1 Peer work review

Time	Researcher	Pros	Cons
Sep. 2009	Fen Miao, Lei Jiang, Ye Li, and Yuan-Ting Zhang [6]	The biometric information-based key sets have higher security than the regular key. The encryption method is computational-friendly, as well as energy efficient.	Additional frequency transform can be saved with our scheme.
Dec. 2003	Hero, A.O. [2]	Using MIMO in wireless communication network, with space coding to constraint low interpret and low detection probability, communication security is improved.	Lack of an encryption method for transmitted signal, in their work, only protection of communication channels was considered.
Dec. 2012	Kun Hua [1]	A cooperative cellular network module based on Alamouti for multimedia communication was built in their work, and the BER performance was improved.	Do not have an encryption method; this module was built based on multimedia communication, which is 2D signal such as images, not for biomedical signal.
Aug. 2012	Karthikeyan Palanisamy [3]	Using Stroop color test for inducing stress, using ST for identifying stress levels. Improved classification accuracy.	Not applicable for on-body real-time stress monitoring system.
Nov. 2011	P. Karthikeyan [5]	Using real-time stress prediction and identification system over WBSN, and improved classification accuracy.	Do not considered security performance during signal transmission.
Oct. 2012	P. Karthikeyan [7]	Using DWT for decomposition and feature extraction	Do not apply in an application for further test; the classification rate is not promised
July. 2012	Kun Zhao [12]	Physically analyzed the position and placement of antenna contribution to improvement of communication performance.	Only analyzed the physical antenna placement, lack of channel protection for improvement the performance.

$$ap^{i}\left(f_{i,a}\right)=\sum_{i=1}^{2n} l\left(2\left(f_{i,a}\right)-i\right)ap^{i-1}(i-1),\quad i\in[1,16] \tag{2}$$

$$de^{i}\left(f_{i,d}\right)=\sum_{i=1}^{2n} h\left(2\left(f_{i,d}\right)-i\right)de^{i-1}(i-1),\quad i\in[1,16] \tag{3}$$

After ECG signal is decomposed to 16 levels in approximation coefficients, six statistical features are extracted from those frequency bands and applied as the input of K-nearest neighbor (KNN) classification. The six features are respectively "mean" values, covariance "cov," standard deviation "std," "power," "entropy," and "energy," which can be shown as

$$\text{mean}=\frac{1}{n\sum_{x=1}^{n} f_{i}x}; \tag{4.a}$$

$$\text{cov}=E((f_{i}(x-1)-\text{mean})((f_{i}x-\text{mean})); \tag{4.b}$$

$$\text{std}=\sqrt{\frac{\sum_{x=1}^{n}(f_{i}x-\text{mean})}{n-1}}; \tag{4.c}$$

$$\text{entropy}=-\sum_{x=1}^{n} p(f_{i}x)log_{10}p(f_{i}x); \tag{4.d}$$

$$\text{energy}=\sum_{x=1}^{n}(f_{i}x)^{2}; \tag{4.e}$$

$$\text{power}=1/n\sum_{x=1}^{n}(f_{i}x)^{2} \tag{4.f}$$

In the above six features, '$f_i x$' is i level wavelet coefficients, "x" means statistic in that level's wavelet coefficients, for "entropy" equation. '$p(f_i x)$' is the probability of '$f_i x$'.

The aforementioned six features are used as inputs of the KNN classification, which are dynamically chosen from 1 to 16 extracted frequency levels. Even the HF and LF gives the best performance of classification accuracy [7], which is approximately 88.33 and 79.27 %, respectively, but this classification accuracy is still not good enough to achieve better classification accuracy rate over 90 % [11]. We can dynamically add previous levels to the frequency signal with "HF" level for feature extraction.

$$\arg\min_{i\in(1,16)}\{f_{i}k\}=\{\{f_{i}k\}\Leftrightarrow\{P_{a}\},P_{a}\geq 90\%\}$$

$$P_{a}:\ \text{KNN successful classification rate} \tag{5}$$

Table 2 Frequency bands after each level's decomposition

Frequency domain $\{f_i\}, i \in [1, 16]$	f_1	f_2	……	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
Frequency bands (Hz)	1024–512	512–256	……	0.5–0.25	0.25–0.125	0.125–0.0625	0.0625–0.03125	0.03125–0.01562

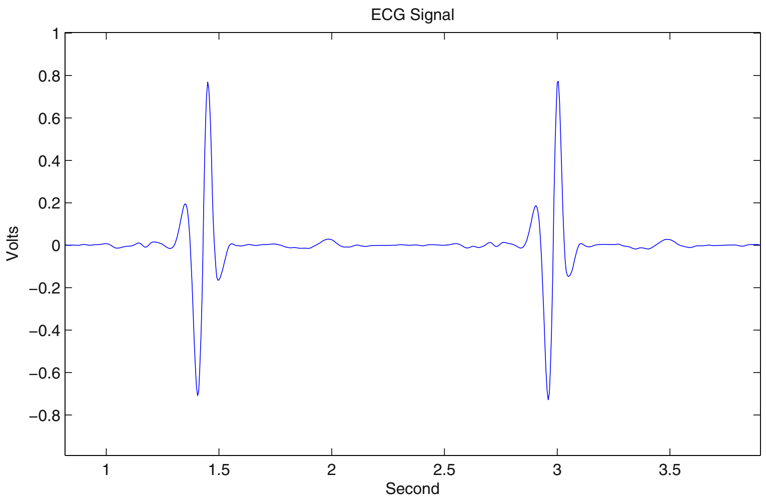
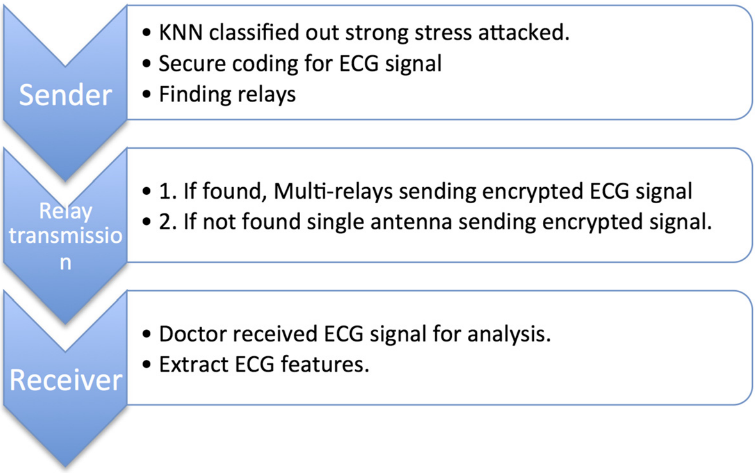


Fig. 2 Basic ECG signal

$$\begin{pmatrix} \operatorname{cov}(f_i,x) \\ \operatorname{std}(f_i,x) \\ \operatorname{entropy}(f_i,x) \\ \operatorname{energy}(f_i,x) \\ \operatorname{power}(f_i,x) \\ \operatorname{mean}(f_i,x) \end{pmatrix} \xrightarrow{\mathrm{KNN}:\,(P_a \geq 90\%)} \begin{pmatrix} '\mathrm{mode1}' \\ '\mathrm{mode2}' \\ '\mathrm{mode3}' \end{pmatrix} \qquad (6)$$

$$\Big\Uparrow \qquad \{\mathrm{LF}, \mathrm{HF}, \mathrm{LF\&HF}, \mathrm{LF\&HF\&Others}\} \rightarrow (f_i,x)$$

In Fig. 4, the LF bands signal alone on the rightmost can contribute 79.27 % accuracy rate for classification; similarly, HF can get 88.33 % accuracy rate alone. And the combined HF and LF bands signal can contribute classification accuracy over 90 %. In additional, HF and LF and Others can definitely make classification accuracy over 90 %; the features were extracted from dynamically added frequency bands, such as, "level 11" if needed. Then, under this dynamic feature extraction and classification, classification outputs are three stress level modes. For "mode1" = "relax," as we mentioned at previous page, is the "relax" condition, means there is no need for ECG signal transmission. If the KNN classification output is in category of "mode2," it means the patient may be experiencing emotional stress and needs to transmit classifier data (HF, LF, VLF) for further classification and analysis at the receiver side. If the output is "mode3" = "emergency," that means the patient needs emergent care; on-body devices have to transmit corresponding ECG signals to doctors as soon as possible and correctly regardless of the energy cost.



- KNN classified out strong stress attacked.
- Secure coding for ECG signal
- Finding relays

- 1. If found, Multi-relays sending encrypted ECG signal
- 2. If not found single antenna sending encrypted signal.

- Doctor received ECG signal for analysis.
- Extract ECG features.

Fig. 3 Process of collected ECG signal

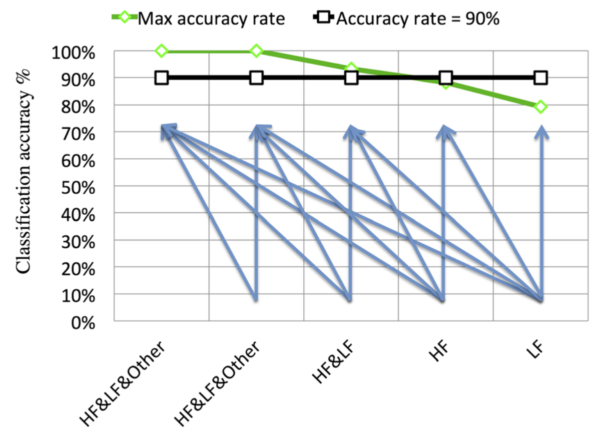


Fig. 4 Classification accuracy rate by processing different frequency levels

3.2 ECG signal encryption "dynamic AES"

Once the stress level is classified, such as "strong stress," it is highly possible to cause emergency accident. In both secure and privacy concerns, it appears extra important to protect the ECG signal from eavesdroppers and unauthorized receiver. Meanwhile, transmitting the corresponding ECG signal with minimum computational process (minimum delay) and the highest security protection is necessary for smartphone based ECG signal transmission.

In this section ECG signal, 'f_ik', stands for totally k levels of frequency signals that satisfies the classification rate from equation (4.e) and (4.f). To encrypt 'f_ik',, we applied Advanced Encryption Standard (AES) algorithm, also called as "AES algorithm." Generally, AES scheme is based on block cipher encryption and has been widely spread as a standard encryption application. It sufficiently satisfies the requirements of encryption strength and computational process.

The following is an integration design of compression and encryption for biomedical signals:

Input: cipher sets '$P(n)$', plaintext 'f_ik'
Output: ciphertext 'F_ik'

1. Dynamic key generation
   '$P(n)$' is a 128 bits cipher for ECG signal 'f_ik' based on Table 3.

Table 3 Keys sets according to transmitted signal

Frequency bands (Hz)	Key sets P
LF (0.04–0.15)	$P_1(n)$
LF (0.04–0.15), HF (0.15–0.5)	$P_2(n)$
LF (0.04–0.15), HF (0.15–0.5), f_{11} (0.5–1)	$P_3(n)$
⋮	⋮
LF	$P_k(n)$
⋮	
f_1	

2. Key expansion
   One hundred twenty-eight bits key are expand to 4 × 11 words from four words and can be calculated by:

$$\begin{aligned}w_{i+4} &= w_i \otimes g(w_{i+3})\\ w_{i+5} &= w_{i+4} \otimes w_{i+1}\\ w_{i+6} &= w_{i+5} \otimes w_{i+2}\\ w_{i+7} &= w_{i+6} \otimes w_{i+3}\end{aligned}$$

   Where 'g' function is known as round constant '$R\text{con}[j]$'.
3. ECG encryption
   (a) Byte substitution operation
   Plaintext 'f_ik' was input as 4 × 4 matrix in byte in their hex value. Then, one hex value as row input and the other hex value as column input were substituted through the S-box, where the S-box are constructed by arithmetic operations of finite field of form $GF(2^8)$.
   (b) Shift rows
   To diffuse the cipher, each row in the state array shift to left with according order, such as the following: no shift in first row, shift by one byte in second row, shift by two bytes in third row, and shift by three bytes in third row.
   (c) Mix columns
   A linear transformation, which performs each column with multiplication and addition, is shown as follows:

$$\begin{bmatrix} f'(0,j)\\ f'(1,j)\\ f'(2,j)\\ f'(3,j)\end{bmatrix} = \begin{bmatrix} 2f(0,0)+3f(0,1)+f(0,2)+f(0,3)\\ f(1,0)+2f(1,1)+3f(1,2)+f(1,3)\\ f(2,0)+f(2,1)+2f(2,2)+3f(2,3)\\ 3f(3,0)+f(3,1)+f(3,2)+2f(3,3)\end{bmatrix}$$

   The addition is meant as XOR.
   (d) Add round key
   The four sub-key words from previous key expansion are applied for each round literation (10 rounds for 128 bits key). Each byte in state array is XOR-ed with according sub-keys.
4. Encrypted ciphertext 'F_ik'
   The last round of encryption does not include "mix columns" step. After totally 10 rounds, followed with (a), (b), (c), and (d) four steps, the output is 128 bits ciphertext 'F_ik'.
5. Decryption components

Decryption follows the process order as inverse shift rows, followed with inverse substitution and inverse add round key, where the process is inverse corresponding transformation, note that no "inverse mix columns" at last round as well.

Additionally, as abovementioned, the AES encryption algorithm is improved by providing the dynamic key from time-varying ECG signal, as "dynamic AES," the dynamic key sets (cipher key), for current use, are generated from a function of the frequency domain of a short period of last transmitted ECG signal (plaintext), which offers time-varying candidates for biometrics-information-based cryptographic system.

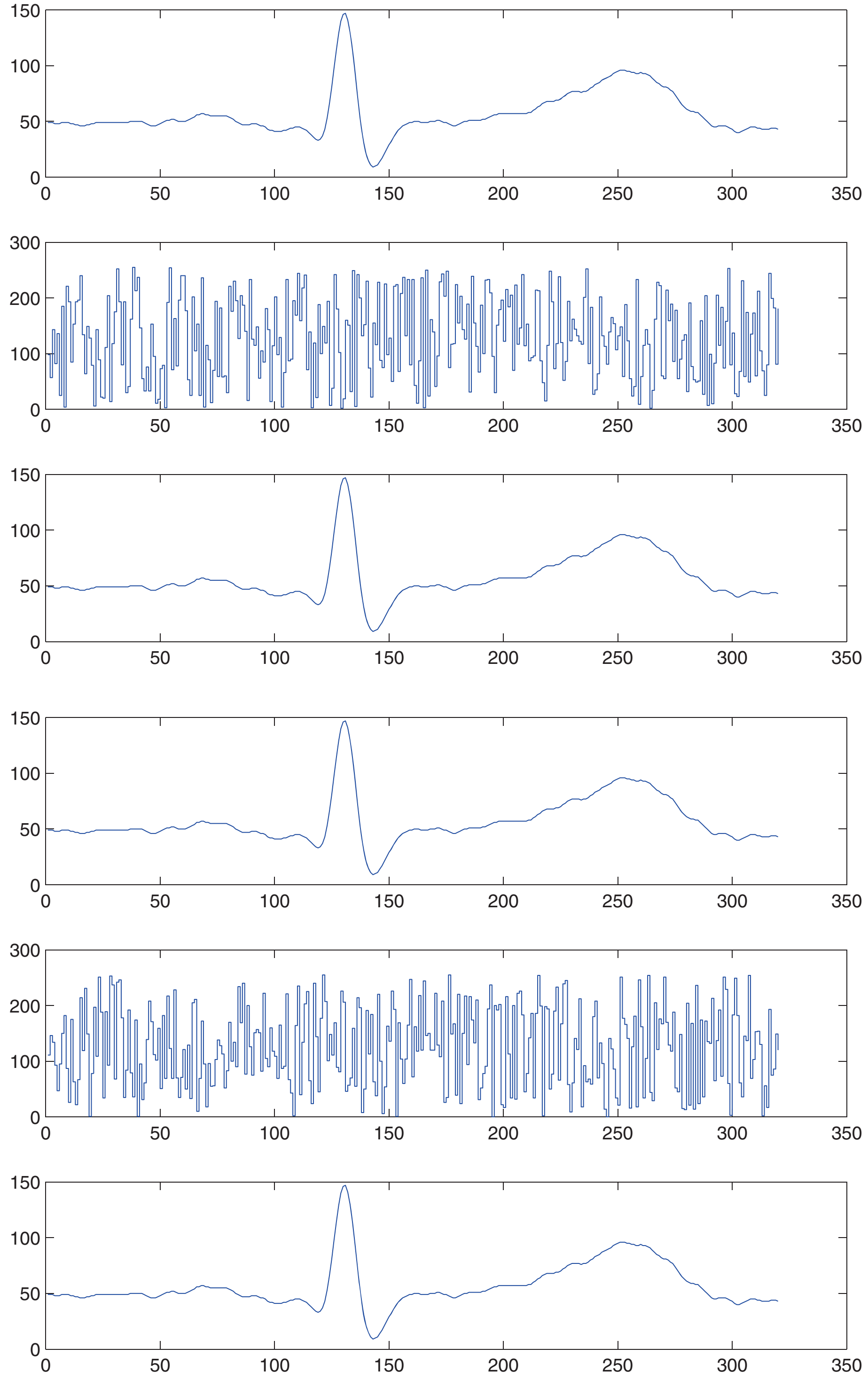


Fig. 5 "Dynamic AES" for ECG signal

Specifically, the frequency bands ECG signal is varying for each time transmission. Thus, for example, the LF and HF bands ECG signal were transmitted; meanwhile, the key sets were extracted from those two frequency bands followed with the following: (1) For each frequency levels, we extract 180 coefficient samples, totally 360 samples from two frequency bands. (2) Divided all coefficients into 20 blocks, 18 coefficients in, and then, quantized 18 coefficients individually into binary. (3) Quantization process provides 4 binary bits from each coefficient, totally 72 bits for each block. Finally, the key set ' $P(n)$ ' from transmitted LF and HF, and for next time encryption, is generated as 20 blocks *72 bits.

For each time encryption, the transmitter selects a 128-bits cipher from the generated cipher sets, where the encryption process followed with the proposed "AES algorithm." By this way, concerning about the energy constraint and resource limitation, our biometrics cryptosystem based on AES algorithm provides high secure strength as well as the minimum energy consumption.

Figure 5 shows two examples (in two columns) of our biometric cryptosystem, from top to end, respectively displayed as input ECG signal, encrypted signal, and decrypted signal in each column. It can be observed that the encrypted signal (in the second row) looks totally unrecognizable and randomly distributed, where the noise-like signal makes eavesdropper much more difficult to track and crack the patients' private information. The third row shows decrypted ECG signal which perfectly reproduced the original ECG at the receiver. The dynamically changed key, which gives totally different ciphertexts, makes our secure system even stronger.

3.3 Encrypted signal transmission Fig. 6

The major bottlenecks of Wireless Body Area Network (WBAN) are costly in power consumption and distance limitation. Due to the limitation of smart phone's power supply and the antenna capacity, on-body smart devices can greatly improve its transmission capability with the assistance of cooperative relays. In this work, we applied MIMO techniques to improve the quality of services (QOS), which then also improved the security of data transmission. Spatial coding is applied for the encrypted data set "$(F_ix)_n$" transmission through relays [9]. In such cooperative network, we use Alamouti code onto data "(F_ix)" for the spatial coding between transmitter (T) and destination (D, as shown in equation (9)). Here, Rayleigh-fading coefficient is set as "f1." For data frames ' F_0 ' *to* ' F_n ', each data information in their frames are actually transmitted two times, at both relays. The receiver side "D" can be shown as equation (9).

$$s = \begin{pmatrix} s_1 & s_2 \\ -s_2^* & s_1^* \end{pmatrix} \tag{8}$$

The fading channel was introduced at the receiver side, thereby, the received data can be described as

$$D = \begin{bmatrix} \begin{pmatrix} F_0(j) & -F_1(j)^* & F_0(j+1) & -F_1(j+1)_* & \cdots\cdots & F_0(j+n) & -F_1(j+1)^* \\ -F_1(j) & F_0(j)^* & -F_1(j+1) & F_0(j+1)^* & \cdots\cdots & -F_1(j+n) & F_0(j+1)^* \end{pmatrix} \\ \begin{pmatrix} F_2(j) & -F_3(j)^* & F_2(j+1) & -F_3(j+1)^* & \cdots\cdots & F_2(j+n) & -F_3(j+1)^* \\ -F_3(j) & F_2(j)^* & -F_3(j+1) & F_2(j+1)^* & \cdots\cdots & -F_3(j+n) & F_2(j+1)^* \end{pmatrix} \\ \begin{pmatrix} F_{n-1}(j) & -F_n(j)^* & F_{n-1}(j+1) & -F_n(j+1)^* & \cdots\cdots & F_n(j+n) & -F_{n-1}(j+1)^* \\ -F_n(j) & F_{n-1}(j)^* & -F_n(j+1) & F_{n-1}(j+1)^* & \cdots\cdots & -F_{n-1}(j+n) & F_n(j+1)^* \end{pmatrix} \end{bmatrix} \tag{9}$$

After Alamouti is applied for channel coding, encrypted signal is sent to the receiver. Such low probability of interception and low probability of detection features will greatly improve the transmission security. Regarding low probability of interception (LPI), we try to speed up the information data rate in multiple channels from sender to receiver and zero out the data rate in eavesdropper's channel by considering the research in [2].

At first, cut-off rate for sender and receiver ends is informed and is formed as,

$$D\left(F_i(x)_1 || F_i(x)_2\right) = \frac{\eta}{4} tr\left(H^\dagger \left(F_i(x)_1 - F_i(x)_2\right)^\dagger \left(F_i(x)_1 - F_i(x)_2\right) H\right) \tag{10}$$

Then, cut-off rate for only receiver end informed,

$$D\left(F_i(x)_1 || F_i(x)_2\right) = ln\left| I_M + \frac{\eta}{4} \left(F_i(x)_1 - F_i(x)_2\right)^\dagger \left(F_i(x)_1 - F_i(x)_2\right)\right| \tag{11}$$

Finally, if cut-off rate for neither transmitter nor receiver side informed

$$D\left(F_i(x)_1 || F_i(x)_2\right) = ln \frac{\left| I_T + \frac{\eta}{2}\left(F_i(x)_1 F_i(x)_1{}^\dagger + F_i(x)_2 F_i(x)_2{}^\dagger\right)\right|}{\sqrt{\left| I_T + \eta F_i(x)_1 F_i(x)_1{}^\dagger \right| \left| I_T + \eta F_i(x)_2 F_i(x)_2{}^\dagger \right|}} \tag{12}$$

$$\mathrm{cov}\left(F_i(x)_n\right) = \left(I_T + \eta F_i(x)_n F_i(x)_n{}^\dagger \right. \quad (13)$$

In above three equations, the first cut-off rate for both ends informed depends on the difference of the received signal pair: $F_i(x)_1H$ and $F_i(x)_2H$. For the cut-off rate, if only receiver informed, it depends on $F_i(x)_1$ and $F_i(x)_2$. For neither transmitter nor receiver is informed, it depends on:

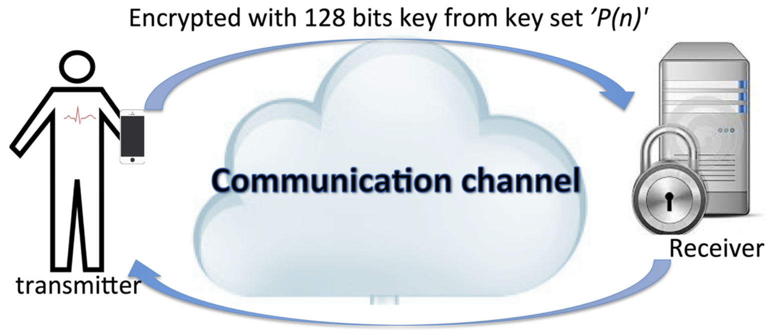


Fig. 6 Encrypted signal transmission

$$\begin{aligned}\mathrm{cov}\left(F_i(x)_1\right) &= \left(I_T + \eta F_i(x)_1 F_i(x)_1{}^{\dagger}\right)\\ \mathrm{cov}\left(F_i(x)_2\right) &= \left(I_T + \eta F_i(x)_2 F_i(x)_2{}^{\dagger}\right)\end{aligned} \tag{14}$$

In the last case, only temporal information could be applied to distinguish the signals, but its spatial information is totally unclear to uninformed receivers. The expected situation result is that channels between sender and receiver destination maintain high-data rate, while the eavesdropper catch up the information in a very limited given time.

$$\mathrm{LPI} = (F_i x)_n \frac{1}{\sum \lambda_i} \tag{15}$$

$$\mathrm{LPD} = \frac{1}{(F_i x)_n} \sum_{i=1}^{(F_i x)_n} \sigma_i^2 \le P_{\mathrm{LPD}} \tag{16}$$

Regarding the low probability of detection (LPD), we evaluate the data error rate for the performance improvement. The relation of error rate to low detection probability is mathematically mapped to the constraint of mean squared power, as explained in [2]. We set 'P_n' as maximum of tolerable error rate, then eigenvalues = $\mathrm{cov}(F_i(x)_n)$ of the matrix $D_n = \begin{pmatrix} F_i(x)_n & -F_i(x)_{n+1} \\ -F_i(x)_{n+1}{}^{*} & F_i(x)_n{}^{*} \end{pmatrix}$ represents by σ_i, the equation shows below:

$$\frac{1}{D_n} \sum_{n=1}^{D_n} \sigma_n^2 \le P \tag{17}$$

For both sender and receiver informed communication channel, 'H' conditioned denotes squared transmitter power.

4 Experiment result

In this paper, for wireless ECG signal preprocessing, we firstly applied LPF and HPF for artificial and machine noise removal; then, for on-body stress level classification, we used "DWT" for ECG signal decomposition, for better analysis in both frequency and time domain; third, six statistical features were extracted from dynamic frequency bands for stress level classification.

Especially, in this classification technology, the features are extracted from dynamic multiple frequency levels, which achieve the stable and outstanding classification accuracy, instead of from individual frequency level, such as "LF." Then, we applied time-varying biometric key sets based on "AES" to improve the security feature in the proposed system. In this work, the dynamic encryption method is achieved from different width of frequency spectrum, which is representing the biometric information of ECG signals. The encryption keys are individual for each time's transmission. After that, specifically for "Mode2 or 3," we need to transmit the corresponding ECG signal for further analysis.

Also, due to the limitation on power supply, we involved cooperative transmission for energy efficiency concern, which is also connected to the system security performance indirectly, as pointed out in [2].

Then, for the existence of information intercept and detection probabilities by eavesdroppers, we explored that increasing the signal power can achieve low probability of intercept (LPI), at the same time, increasing the communication rate leads to low probability of information detection (LPD). Finally, following simulations proves that communication security performance is largely improved.

In Fig. 7, for single transmitter and multi-receiver communication channel, it can be observed as expected that the more receiver antennas were involved, the better bit error rate (BER) performance will be, thereby, the transmission quality can be easily improved by increasing receiver antennas. Figure 8 shows the BER performance of two relays and two receivers, it can be observed that if more antennas involved in the sender side, an even better performance will be realized. Unfortunately, for ECG signal transmission in WBAN, multiple sender antennas solutions are impractical, thereby, it is necessary to adopt multiple smart phone relays to build up a

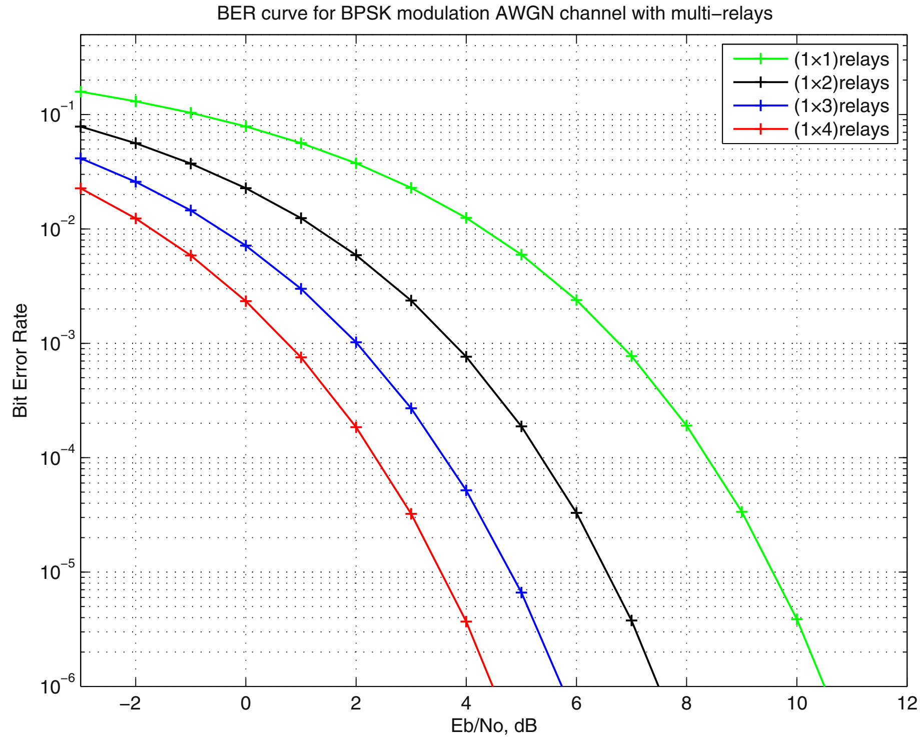


Fig. 7 BER performance for single transmitter and multi-receiver

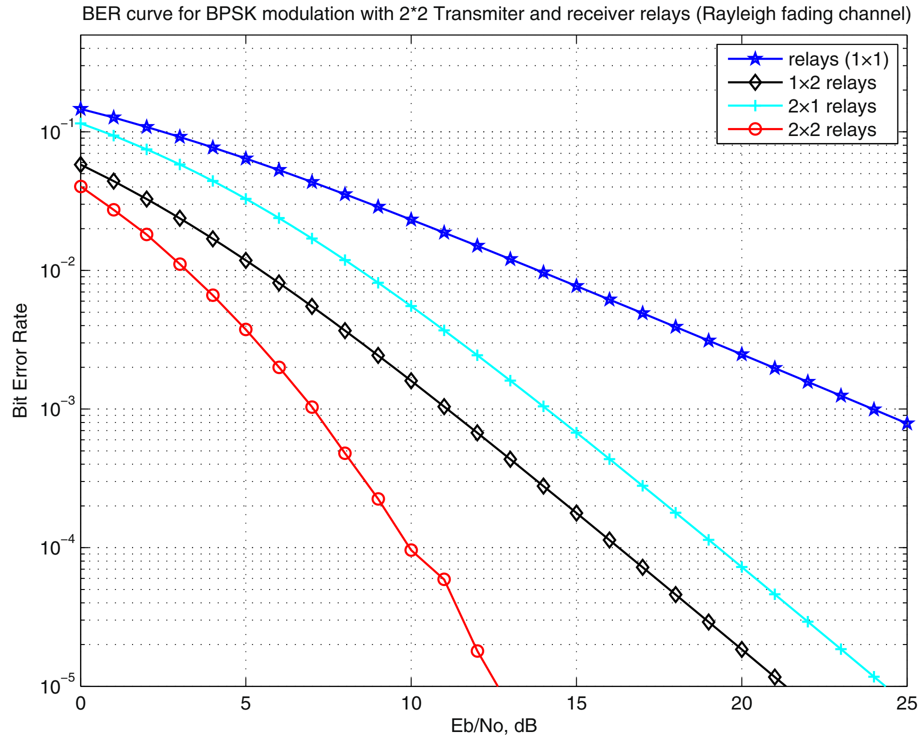


Fig. 8 BER performance for 1 × 1, 1 × 2, 2 × 1, 2 × 2 relays

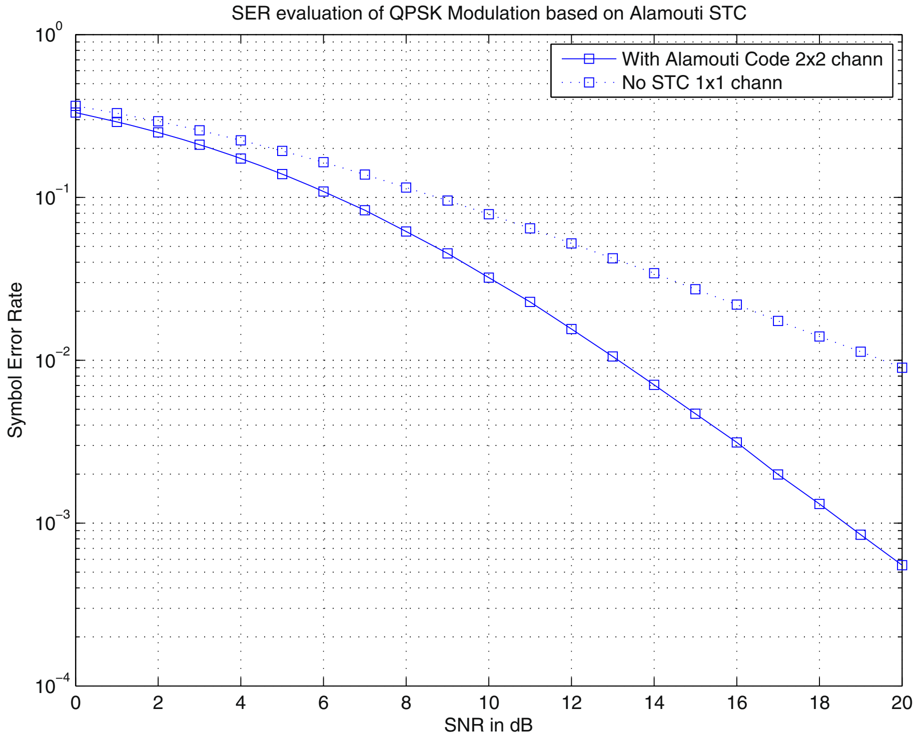


Fig. 9 SER performance for 2 × 2 channel

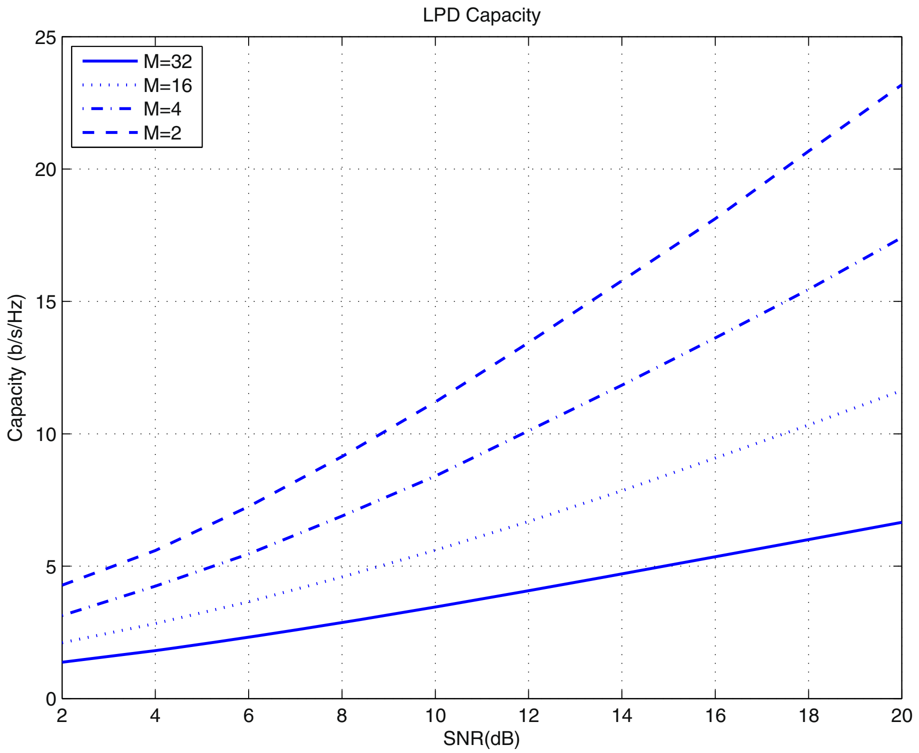


Fig. 10 Capacity of low probability of detection

virtual MIMO network, which can improve the security as well the data transmission quality.

Alamouti capacity improves the transmission quality largely by transmitting data in multiple space channels. As the transmission quality is improved, the security also is accordingly improved. Shown in Fig. 9, the symbol error rate with Alamouti encoded is much lower than the non-Alamouti scheme.

At the same time, simulation results in Fig. 10 reflected the LPD capacity, in which "M" means the number of transmitter antennas, and within a severe the channel condition, the more number of "M," the higher LPD capacity. Which means, a secure communication can be promised by its LPD property.

Based upon experimental results, the classification accuracy gains are 90 % higher, in which the classification features are extracted from the combined LF&HF signal. As expected, it gains better accuracy rate when more frequency levels are added. Then, comparing to the traditional AES, our encryption experiment results achieved an improved energy efficiency and security by the biometric information-based key sets generation scheme and the time-varying random-like encrypted data. Finally, as shown in the experimental results, Figs 7, 8, 9, and 10, data transmission quality (bit error rate) is improved by the cooperative relay and Alamouti encoding techniques. For instance, cooperative relay transmission reduces the energy consuming at sender side, and by increasing sender relays, an even better transmission quality can be achieved.

5 Conclusions

In this paper, we try to classify heart disease patients' emotional stress levels to prevent further dangerous situation by proposing a secure and energy efficient ECG signal transmission solution in WBAN. We especially designed a dynamic keying method for signal encryption through biometric information among ECG signals, which can guarantee both high classification rate (>90 %) and energy efficiency. At the same time, cooperative relays were applied during data transmission for an additional security transmission purpose. Through this way, the improvement of transmission rate and signal power capacity are able to lower the probability of data intercept and data detection (LPI and LPD) by taking the advantages of both temporal and spatial diversities.

Competing interests

The authors declare that they have no competing interests.

Authors' contributions

KH participated in the general studies and the sequence alignment. HX drafted the manuscript and performed the statistical analysis. Both authors read and revised the final manuscript.

Received: 1 March 2015 Accepted: 25 November 2015
Published online: 15 January 2016

References

1. K. Hua, W. Wang, H. Wang, A. Alghamdi, A, Multiplexing-diversity balanced cooperative wireless cellular network based on Alamouti space time code for multimedia transmission. Global Communications Conference (GLOBECOM), 2012 IEEE, pp.1896 - 1900. Anaheim, CA; 2012
2. AO Hero, Secure space time communication, information theory. IEEE Transactions on **49**(12), 3235–3249 (2003)
3. P KarthiKeyan, murugaPPan murugaPPan, sazali yaacob, "Descriptive analysis of skin temperature variability of sympathetic nervous system activity in stress". J. Phys. Ther. Sci **24**, 1341–1344 (2012)
4. JH Tulen, P Moleman, HG van Steenis, F Boomsma, Characterization of stress reaction to the stroop color word test. Pharmacology, biochemistry, and behavior **32**(1), 9–15 (1989)
5. P. Karthikeyan, M. Murugappan, S. Yaacob, ECG signals based mental stress assessment using wavelet transform, Control System, Computing and Engineering (ICCSCE), 2011 IEEE International Conference on, pp. 258 – 262. code for multimedia transmission. Global Communications Conference (GLOBECOM), 2012 IEEE, pp.1896 - 1900. Penang; 2011
6. M Fen, J Lei, L Ye, Z Yuan-Ting, *Biometrics based novel key distribution solution for body sensor networks* (31st Annual International Conference of the IEEE EMBS, Minneapolis, Minnesota, USA, 2009)
7. P. Karthikeyan, M. Murugappan, S. Yaacob, "a study on mental arithmetic task based human stress level classification using the discrete wavelet transform". Sustainable Utilization and Development in Engineering and Technology (STUDENT), 2012 IEEE Conference on, pp.77 – 81.Kuala Lumpur; 2012
8. JH Tulen, P Moleman, HG van Steenis, F Boomsma, Characterization of stress reaction to the stroop color test. Pharmacol Biochem Behav **32**(1), 9–15 (1989)
9. R. Luijcks, H. J. Hermens, L. Bodar, C. J. Vossen, J. van. Os, R. Lousberg Psychophysiological stress and emg activity if the trapezius muscle, international journal of behavioral medichine. Published online 2014 Apr,doi: 10.1371/journal.pone.0095215.
10. A. Josko, Discrete wavelet transform in automatic ECG signal analysis, Instrumentation and Measurement Technology Conference Proceedings, 2007. IMTC 2007. IEEE, pp.1 – 3, 1–3.Warsaw; 2007
11. Feng-Tso Sun, Cynthia Kuo, Heng-Tze Cheng, Senaka Buthpitiya, Patricia Collins, Martin Griss, Activity-aware mental stress detection using physiological sensors. Second International ICST Conference, MobiCASE 2010, Santa Clara, CA, USA, pp 211–230,October 25–28, 2010
12. Z Kun, Z Shuai, Y Zhinong, T Bolin, H Sailing, SAR study of different MIMO antenna designs for LTE application in smart mobile phone. Antennas and Propagation, IEEE Transactions on **61**(6), 3270–3279 (2013)