4-2012

# Assurance of Energy Efficiency and Data Security for ECG Transmission in BASNs

Tao Ma
*University of Nebraska Lincoln*, tma@unlnotes.unl.edu

Pradhumna Shrestha
*University of Nebraska Lincoln*

Michael Hempel
*University of Nebraska-Lincoln*, mhempel2@unl.edu

Dongming Peng
*University of Nebraska-Lincoln*, dpeng2@unl.edu

Hamid Sharif
*University of Nebraska-Lincoln*, hsharif@unl.edu

*See next page for additional authors*

# Assurance of Energy Efficiency and Data Security for ECG Transmission in BASNs

Tao Ma, Pradhumna Lal Shrestha, Michael Hempel, Dongming Peng, Hamid Sharif, and Hsiao-Hwa Chen*, *Fellow, IEEE*

***Abstract*—With the technological advancement in body area sensor networks (BASNs), low cost high quality electrocardiographic (ECG) diagnosis systems have become important equipment for healthcare service providers. However, energy consumption and data security with ECG systems in BASNs are still two major challenges to tackle. In this study, we investigate the properties of compressed ECG data for energy saving as an effort to devise a selective encryption mechanism and a two-rate unequal error protection (UEP) scheme. The proposed selective encryption mechanism provides a simple and yet effective security solution for an ECG sensor-based communication platform, where only one percent of data is encrypted without compromising ECG data security. This part of the encrypted data is essential to ECG data quality due to its unequally important contribution to distortion reduction. The two-rate UEP scheme achieves a significant additional energy saving due to its unequal investment of communication energy to the outcomes of the selective encryption, and thus, it maintains a high ECG data transmission quality. Our results show the improvements in communication energy saving of about 40%, and demonstrate a higher transmission quality and security measured in terms of wavelet-based weighted percent root-mean-squared difference.**

***Index Terms*—Body area sensor network (BASN), electrocardiographic (ECG), energy saving, security, selective encryption, two-rate unequal error protection (UEP), wavelet-based weighted percent root-mean-squared difference (WWPRD).**

## I. Introduction

ELECTROCARDIOGRAPHIC (ECG) information reveals essential heart condition for heart illness diagnosing such as heart attacks, arterial blockages, enlarged heart muscle, etc., and it has been widely used in healthcare. According to statistical data collected by the Centers for Disease Control and Prevention (CDC), heart illnesses have been identified as the leading cause of death at least since 1980 in the United States [1]. The fast increase in the number of heart illness patients, most of them are elder people, has generated a large demand for low-cost, high-quality, and easy-to-use ECG diagnosis systems. Recent technological progress in wireless sensing and wearable sensors has made body area sensor networks (BASNs) technology a promising solution to help us to meet this growing demand. For example, a miniature ECG monitoring device has been developed with a size as small as $55\times23$ mm [2]. This device adopts ultra-low power circuitry using efficient system level power management, promising a long battery life. In addition, many sophisticated architectures for wireless ECG transmission have also been developed. The MobiHealth project [3] was accomplished with a mobile phone based BASN, where a cell phone had been utilized as a network coordinator. A good review of state-of-the-art hardware, technologies, and standards for BASN was presented by Chen *et al*. [4]. According to their studies, the sensors are becoming increasingly smaller and more wearable. The new ECG sensor uses textile-structured electrodes, which are embedded inside clothes. Also, numerous communication protocols such as 8011.15.4, Bluetooth, and TDA5250 have been designed and implemented in BASNs to lower power consumption. It is seen from all those pilot research and development projects that BASN has become a realistic and promising tool for implementation of wireless ECG diagnosis systems.

Nevertheless, there still exists a significant gap between growing demands for medical applications and insufficient research on ECG in BASNs. In error-prone wireless communication channels, packets loss is commonplace. However, ECG data are so important that any content loss or distortion should be avoided in order to maintain a satisfactory rate of correct diagnosis. Moreover, in a continuous monitoring system, the volume of ECG data is necessarily large, as a long period of monitor time is required in order to gather enough information about a patient. As an example, with a sampling rate of 360 Hz and 11-bits/sample data resolution, a 24-hour recording requires about 43 MB data per channel [5]. These factors, i.e., large data volume, high transmission quality and reliability, and unpredictability of wireless communication channels, have made the design of a battery-powered BASN very challenging. Therefore, energy efficient and reliable transmission becomes extremely critical for ECG data communications in BASNs. In addition, ECG signals contain sensitive and private health information about patients, and it is required by law that this individual physiological data should be kept strictly confidential for all times [6]. According to the recent research on patient identification with ECG signals, a single ECG signal without any patient name can still be used to acquire both cardiovascular details and patient's identification [7], [8]. The authors in [4]

Manuscript received June 21, 2011; revised November 1, 2011; accepted November 27, 2011. Date of publication January 3, 2012; date of current version March 21, 2012. This work was supported in part by the Taiwan National Science Council research under Grant NSC99-2221-E-006-016-MY3. *Asterisk indicates corresponding author*

T. Ma, P. L. Shrestha, M. Hempel, D. Peng, and H. Sharif are with the Department of Computer and Electronics Engineering, University of Nebraska-Lincoln, Omaha, NE 68182 USA (e-mail: tma@unlnotes.unl.edu; plshrestha@unlnotes.unl.edu; mhempel@unlnotes.unl.edu; dpeng@unlnotes.unl.edu; hsharif@unlnotes.unl.edu).

*H.-H. Chen is with the Department of Engineering Science, National Cheng Kung University, Tainan 70101, Taiwan (e-mail: hshwchen@ieee.org).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TBME.2011.2182196

also pointed out that the distinguishable human body characteristics create the challenges for protecting the privacy of patients. Therefore, secure ECG data transmission in wireless channel is indispensable in order to protect individual privacy.

Some more research works have been reported in the literature to address those issues. Yoo and coworkers [9] designed a quadratic level compression algorithm with which the encoding delay and hardware cost could be reduced. The main idea of this algorithm is to assign different compression ratios to different importance levels of data blocks so that an overall high compression ratio can be guaranteed while the reconstructed signal quality is maintained. However, this approach, which was applied directly to ECG data, may not offer needed energy saving. An efficient approach for ECG transmission was proposed in [10], where a predictive coding model was developed to reduce the amount of transmission data. However, this approach works based on a strict lossless compression scheme and offered a very low compression ratio (about 3:1), and thus, communication energy saving was also severely reduced. In [11], a similar approach as that in [9] was presented, where important and nonimportant portions of ECG data were protected separately using different amount of communication resources to reduce energy consumption without compromising transmission quality. However, the energy saving improvement was not significant, and we believe it is due to the fact that this unequal error protection (UEP) approach was applied directly to raw ECG data rather than the ECG codec output data. F. Sufi *et al*. [12] proposed an ECG encryption algorithm, in which about 25% of ECG data were selected to be encrypted.

It is seen that although the aforementioned research works can be utilized to solve the energy problem in BASNs to some extent, the improvement is still quite limited. In this paper, we are motivated to investigate the properties of the compressed ECG data, based on which we will show that a big room is still left for us to save more energy. In particular, we will propose a selective encryption algorithm and a two-rate UEP scheme, as an effort to further improve energy saving, transmission quality, and security. The major contributions of this study can be summarized as follows.

1) An efficient and yet secure ECG transmission scheme is proposed. In this scheme, a small amount of data (about 1%) is to be encrypted, thereby significantly reducing the encryption burden. At the same time, the encrypted parts are the coefficients in the first bit-plane, which is more robust to the brute-force attacks than state-of-the-art encryption standards. Therefore, the determining factor for the achievable level of security in our scheme depends entirely on the level of security of the employed encryption algorithm itself, such as Advanced Encryption Standard (AES). Furthermore, our security scheme is independent and it works compatible to almost all existing encryption algorithms.
2) The ECG feature distribution in the wavelet domain is studied in this study. Also, the unequal importance in set partitioning in hierarchical trees (SPIHT) coded bits is investigated. Based on these studies, a two-rate UEP scheme is proposed. Using this proposed scheme, we can save additional 40% energy without compromising ECG transmission quality on top of the compression energy saving (using 20:1 compression rate with about 6.3% PRD).

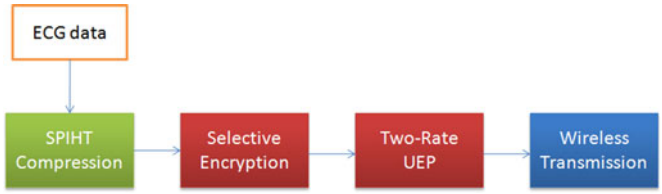



Fig. 1. Secure and energy efficient ECG transmission scheme.

The rest of this paper can be outlined as follows. Section II introduces the proposed scheme for ECG transmission. In particular, we will discuss its two major components, i.e., the selective encryption algorithm and the two-rate UEP algorithm in Sections III and IV, respectively. Section V will provide our simulation results as well as the discussions on the results, followed by the conclusions given in Section IV.

## II. ECG Transmission in BASN

A secure and energy efficient ECG transmission scheme is illustrated in Fig. 1. Raw ECG data are first compressed using a standard ECG encoding algorithm, and then selective encryption algorithm and two-rate UEP are performed in a serial way.

Based on the state-of-the-art technology reported in the literature, the core of ECG compression algorithm we used is SPIHT [13]–[19]. In the SPIHT compression algorithm, raw ECG data are first wavelet transformed. Then, the resulting wavelet coefficients are processed through set partition sorting and refining stages one by one with its threshold decreased by half at each stage until the coding budget is fulfilled. The idea behind this algorithm is bit-plane coding and position recording using a wavelet-tree-structure. In bit-plane coding, all wavelet coefficients are bit partitioned into nonoverlapping subsets, or

$$\left\{T_1, T_2, T_3, \ldots, T_n\right\}. \tag{1}$$

Subset $T_i$ consists of wavelet coefficients that are considered to be significant in bit depth $i$ ($|c|\, 2^{n-i}$) but insignificant in bit depth $i-1$ ($|c| > 2^{n-i+1}$), where $c$ is the value of wavelet coefficient. In this way, all wavelet coefficients are classified into these nonoverlapping subsets. In one subset, two types of information are recorded, including the values of coefficients in this subset, and the positions of coefficients in this subset. The values of a coefficient consist of two elements, i.e., sign bit and absolute values, which are recorded in partition sorting segment and refinement sorting segment in SPIHT, respectively. The positions of coefficients are recorded in the remaining output portion of the partition sorting stage. Let $P_i$ denote the position information of wavelet coefficients of subset $T_i$, and $V_i$ denote the value information of wavelet coefficients of subset $T_i$. These subsets are structured into a set of output bits of SPIHT coding as illustrated in Fig. 2.

Take subset $T_1$ as an example. All positions of wavelet coefficients are recorded in the first bit-plane. Its sign bits are recorded

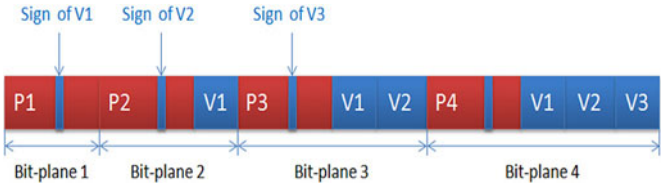



Fig. 2. Output bits from SPIHT codec.

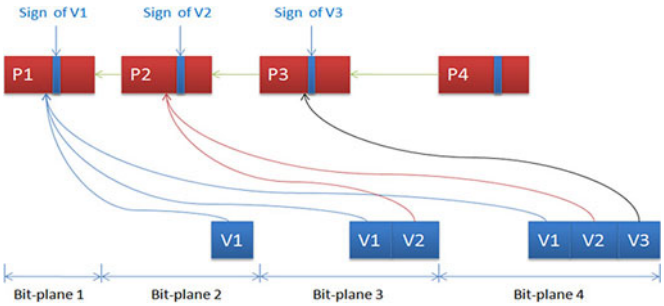



Fig. 3. Dependence relation between position information and value information.

in the first bit-plane and its absolute values are recorded in the consecutive bit-plane in an order arranged from significant bit to insignificant bit.

After SPIHT compression, our selective encryption algorithm is applied such that only important bits (about 1% of the data) are encrypted. Without revealing this small portion, the remainder of the bits, although transmitted unencrypted, becomes useless for decoding purposes and thus this results in severe signal distortions such that the data are indecipherable and unusable for identification purposes and therefore the security requirements are fulfilled. After that step, the encrypted bits are channel coded using our proposed two-rate UEP scheme, which will significantly improve ECG quality without compromising transmission energy consumption. The following two sections will be dedicated to discuss these two important components in detail.

## III. Selective ECG Encryption

Based on the previous discussions on the SPIHT compression algorithm, both the values and positions are recorded in the output from a compression codec. In a particular subset, value information is dependent on position information, i.e., value information is useless if the position information is not reliable. Among different subsets, position information is not independent either. In fact, the position information is recorded by two lists, i.e., the list of insignificant points (LIP) and the list of insignificant sets (LIS). The current-partition-sorting step performs the searches in both LIP and LIS of the previous bit-plane. Therefore, the position information in the current bit-plane is dependent on the previous position information. This dependence relation is demonstrated in Fig. 3.

The highest importance segment P1 is the basis for all the other segments. If P1 contains some errors, an avalanche effect will cause all the other segments to be incomprehensible to the decoder. Thus, the entire message becomes undecipherable.

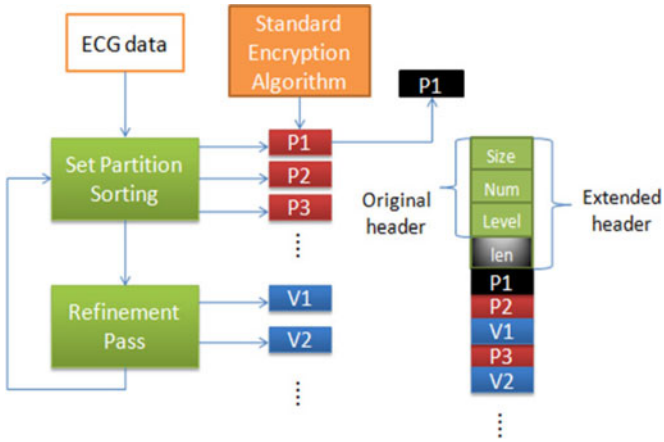



Fig. 4. Proposed encryption algorithm.

Based on this observation, we propose our ECG encryption scheme in Fig. 4. Position information and value information in each bit-plane are generated by set partition sorting and refinement passes. Only the position information in the first bit-plane is encrypted by using a standard encryption algorithm. The standard encryption algorithm can be carried out using either symmetric encryption (i.e., RC4) or public key encryption (i.e., RSA). The length of this position information is presented by an eight bit subheader, which is placed at the end of the original header. This original header consists of the size of ECG data, the bit-plane number, and the level of wavelet decomposition. When a receiver collects the bit-stream of encrypted ECG data, it also evaluates the length of the encrypted position information in the first bit-plane. This position information will be decrypted using the same cryptographic algorithm and the corresponding key. With P1 decrypted, next we can perform the decompression process.

The advantages for using this proposed algorithm can be summarized as follows. First, this algorithm can greatly reduce the encryption burden by significantly decreasing the number of bits to be encrypted. The encrypted size only occupies approximately 1% of the total compressed data when using 11 bit-planes. This is far less than the existing ECG encryption algorithms, which require that 25% to 50% of ECG data should be encrypted [12].

The second advantage of this algorithm is that it is very secure. Let us consider SPIHT encoded data of 2048 bits for example. Given a wavelet decomposition level of six, which is a typical value, and a sample rate of 360 samples/s, a brute-force attack needs to search $2^{2016}$ combinations before it can find the correct position information to crack the key. This number is considered to be safer than the state of the art encryption standards. For example, AES-128, having the key of 128 bits, needs $2^{128}$ times brute-force attack before crack the key, which is far less than the times of our scheme.

## IV. Two-Rate UEP Scheme

In ECG signals, several important features for cardiac disease diagnosis are well defined. It is worthy noting how these features are allocated in the wavelet domain, where we apply

TABLE I
WAVELET COEFFICIENTS DISTRIBUTION

| Frequency bands | Scale of frequency | Heuristic significances distribution |
|---|---|---|
| A5 | 0∼5.625 Hz | 6/27 |
| D5 | 5.625∼11.25 Hz | 9/27 |
| D4 | 11.25∼22.25 Hz | 7/27 |
| D3 | 22.5∼45 Hz | 3/27 |
| D2 | 45∼90 Hz | 1/27 |
| D1 | 90∼180 Hz | 1/27 |

the SPIHT compression algorithm. The QRS complex is a significant feature in the ECG signal, which is characterized by sharp slopes. Most of its frequency spectrum is located between 1 to 40 Hz and centered around 17 Hz [20]. The T wave always appears after the QRS complex, and it can appear in various shapes. Its frequency distribution is typically less than 6 Hz. The P wave normally appears before the QRS complex, and its frequency is usually below 10 Hz [21]. ST segments often occupy a lower frequency range [22]. Heuristically, the required wavelet decomposition level can be determined as

$$L = \left\lfloor \log_2(f_s) - 2.96 \right\rfloor \tag{2}$$

where $f_s$ is the sample rate. Hence, five decomposition levels are sufficient for a sample rate of 330 Hz. In this case, the wavelet coefficients heuristic distribution in terms of frequency partitions is demonstrated in Table I. [23]

The resulting five decomposed frequency partitions are A5 (the lowest frequency band), D5, D4, D3, D2, and D1 (the highest frequency band). As a matter of fact, the frequencies of all features are located below 40 Hz, which are in the A5, D5, D4, and D3 bands. Moreover, the significance distribution from D5 to D1 is arranged in an monotonically decreasing order. This heuristic fact complies very well with the assumption of SPIHT compression algorithm and is the basis for the zero-tree concept. That is the reason why SPIHT compression works so well for ECG data.

### A. Unequal Importance of SPIHT Compressed ECG

The most widely used ECG quality metric over the past 40 years is percent root-mean-squared difference (PRD). However, more recently its popularity was surpassed by the wavelet-based weighted PRD measure (WWPRD) [23], which is claimed to be more accurate and to correlate very well with the subjective tests. In this paper, WWPRD is chosen as our quality measure.

WWPRD is the sum of different subband distortions weighed by a corresponding normalized coefficient, which is defined as follows [23]:

$$\text{WWPRD} = \sum_{j=1}^{N_L} w_j \times \text{WPRD}_j \tag{3}$$

where $w_j$ is the normalized sum of wavelet coefficients in the $j$th subband, and $\text{WPRD}_j$ is the normalized root-mean-square difference between the original wavelet coefficients and reconstructed wavelet coefficients.

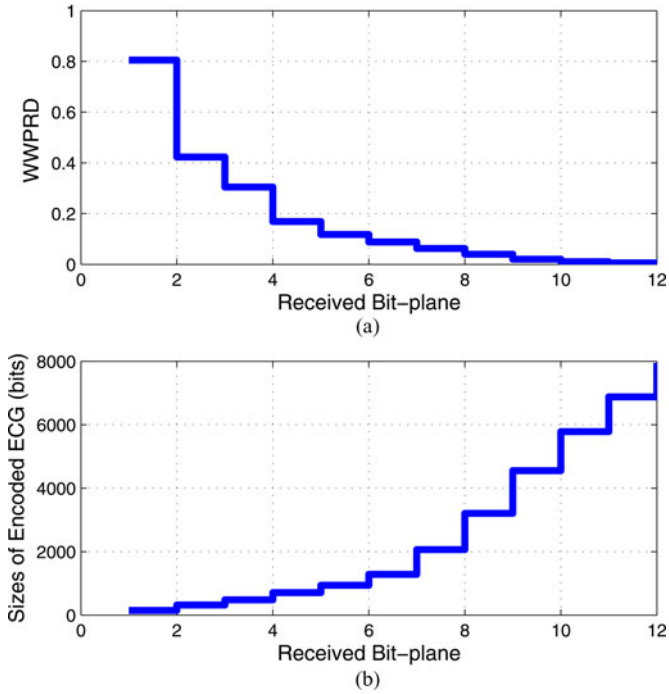



Fig. 5. WWPRD of ECG in different SPIHT encoding levels. (a) WWPRD of ECG in different coding level. (b) Sizes of encoded ECG for different encoding level.

The sample frequency is given as 330 Hz, decomposition level is 5, and wavelet basis is chosen as Daubechies 9, which is widely used and offers good compression results [15]. The quality assessment for different bit-planes is demonstrated in Fig. 5(a). The corresponding accumulated sizes of bit-planes are illustrated in Fig. 5(b). As more and more bit-planes are transmitted, the ECG as indicated by WWPRD is improved with a nonlinear slope. Segments in the first four bit-planes, with an increasing contribution for WWPRD of 0.2167 on the average, just occupy about 176 bits on the average. However, the rest of the bit-planes (5 to 12) consume as many as 905 bits on the average, and it contributes to ECG quality in terms of WWPRD only with 0.0207 increments per bit-plane. This property reveals a great unequality among the bits in compressed ECG data in terms of their contributions to ECG quality.

### B. Two-Rate Unequal Protection Scheme

Energy efficient transmission is very important in BASNs. According to the analysis in the previous section, different importance levels exist among different segments in terms of the contribution density that provides great opportunity to save energy without compromising the quality of ECG transmission by using unequal protection. In our approach, an unique communication protection method for transmitting ECG is proposed, in which transmission energy consumption is greatly reduced while at the same time it meets the quality requirements.

In our proposed scheme, the set of compressed bits of ECG data is divided into two portions. The first portion, which includes all segments in the first $k$ bit-planes, is channel encoded with a rate of $c_1$. The second portion, containing the remaining

$n-k$ bit-planes, is channel encoded with rate $c_2$. In [24], we have reported our previous work on the two-rate transmission scheme for ECG data in BASNs. In the following paragraphs of this section, we will further analyze the WWPRD qualities and procedural algorithm for SPIHT-compressed ECG data transmission in such a rate-switching scheme.

According to the dependence relationship of the segments in SPIHT coding algorithm, the mean of WWPRD quality of received ECG data $\triangle\varepsilon$ is the sum of all possible WWPRD qualities weighted with their corresponding success rates. Let $\varepsilon_p^i$ and $\varepsilon_v^i$ denote the resultant WWPDR quality when all segments in the first $i$ bit-planes are successfully received but an error is encountered in the $(i+1)$th bit-plane position segment or value segment, respectively. Also, let $\rho_p^i(c)$ and $\rho_v^i(c)$ denote the probabilities of channel-packet decoding failure when coding rate $c$ is used to protect the position segment and value segment information, respectively. The value segment information is essentially useless when its corresponding position segment is lost. The decoding process will stop as long as one bit-plane segment (either position or value) has errors. In our approach, the total encoded ECG is divided into two parts, the first $k$ bit-planes are transmitted with coding rate $c_1$, and the remaining $n-k$ bit-planes with coding rate $c_2$. Their average values of WWPRD quality are denoted as $\varepsilon_k(c_1)$ and $\varepsilon_{n-k}(c_2)$, which are expressed in (5) and (6), respectively.

$$\begin{aligned}\varepsilon_k(c_1) = &\sum_{i=1}^{k}\Bigg\{\varepsilon_p^i\prod_{j=1}^{i}\Big(1-\rho_v^j(c_1)\Big)\prod_{j=1}^{i}\Big(1-\rho_p^j(c_1)\Big)\\ &\times\Big(\rho_p^{i+1}(c_1)\Big)\Bigg\}+\sum_{i=1}^{k}\Bigg\{\varepsilon_v^i\prod_{j=1}^{i}\Big(1-\rho_v^j(c_1)\Big)\\ &\times\prod_{j=1}^{i}\Big(1-\rho_p^j(c_1)\Big)\Big(1-\rho_p^{i+1}(c_1)\Big)\rho_v^{i+1}(c_1)\Bigg\}\end{aligned} \tag{4}$$

$$\begin{aligned}\varepsilon_{n-k}(c_2) = &\prod_{j=1}^{k}\Big(1-\rho_v^j(c_1)\Big)\prod_{j=1}^{k}\Big(1-\rho_p^j(c_1)\Big)\\ &\times\sum_{i=k+1}^{n}\Bigg\{\varepsilon_p^i\prod_{j=k+1}^{i}\Big(1-\rho_v^j(c_1)\Big)\\ &\times\prod_{j=k+1}^{i}\Big(1-\rho_p^j(c_2)\Big)\Big(\rho_p^{i+1}(c_2)\Big)\Bigg\}\\ &+\sum_{i=k+1}^{N}\Bigg\{\varepsilon_v^i\prod_{j=k+1}^{i}\Big(1-\rho_v^j(c_2)\Big)\\ &\times\prod_{j=k+1}^{i}\Big(1-\rho_p^j(c_2)\Big)\\ &\times\Big(1-\rho_p^{i+1}(c_2)\Big)\rho_v^{i+1}(c_2)\Bigg\}.\end{aligned} \tag{5}$$

The total WWPRD quality of ECG data is

$$\triangle\varepsilon = \varepsilon_k(c_1)+\varepsilon_{n-k}(c_2). \tag{6}$$

Next, we formulate the energy consumption of transmitted ECG data as shown in (8) [25]. Let $L_p(i)$ and $L_v(i)$ denote the lengths of the position segment and value segment in the $i$th bit-plane, respectively. Also let $P_t$, $R_s$, and $b$ denote the transmitting power, symbol rate, and bits per symbol. We have

$$E = \frac{P_t}{R_s b}\Bigg\{\sum_{i=1}^{k}\frac{L_p(i)+L_v(i)}{c_1}+\sum_{i=k+1}^{N}\frac{L_p(i)+L_v(i)}{c_2}\Bigg\}. \tag{7}$$

Our goal is to maximize WWPRD quality of ECG data within the prescribed energy transmission budget. Both $\triangle\varepsilon$ and $E$ are functions of $k$, $c_1$, and $c_2$, and we expect to maximize $\triangle\varepsilon$ by adjusting parameters $k$, $c_1$, $c_2$, and to restrain the average energy consumption within the budget $E_{\max}$, or

$$\widetilde{\triangle\varepsilon} = \max_{\{k,c_1,c_2\}:E<E_{\max}}\{\triangle\varepsilon\}. \tag{8}$$

Before transmission, both position segments and value segments are divided further into the packets with a fixed length $L$. These packets are encoded and, thus, protected by our concatenated FEC scheme, which is composed of rate-compatibly punctured convolutional (RCPC) codes and cyclic redundancy check (CRC) codes. This scheme is preferable because of its simplicity of implementation and flexibility of adjusting protection levels for importance difference in the source data.

Theoretically, the bit-error rate of RCPC is bounded by [24].

$$P_b(c) \le \frac{1}{P}\sum_{d=d_{\text{free}}}^{\infty} c_d P_d \tag{9}$$

where $P$ is the puncture period and $c_d$ is the distance spectra, which is dependent on the specific code. $P_d$ is the probability that a wrong path at distance $d$ is selected. It is dependent on the channel model and SNR.

Assume that the packet size is $L$, the loss rate of position segment and value segment in the $i$th bit-plane with RCPC coding rate $c$, respectively, is

$$\rho_p^i(c) = 1-\Big\{\Big(1-P_b(c)\Big)^L\Big\}^{\lceil\frac{L_p^i}{L}\rceil} \approx 1-\Big(1-P_b(c)\Big)^{L_p^i} \tag{10}$$

$$\rho_v^i(c) = 1-\Big\{\Big(1-P_b(c)\Big)^L\Big\}^{\lceil\frac{L_v^i}{L}\rceil} \approx 1-\Big(1-P_b(c)\Big)^{L_v^i} \tag{11}$$

where $L_p^i$ and $L_v^i$ are the lengths of the position segment and value segment in the $i$th bit-plane, respectively.

Combining (7), (8), (11), and (12), we see that our two-rate UEP algorithm is then formulated as follows.

1) $I/Odefinition$: Input parameters include encoded ECG data $\{(p_0),(p_1,v_1),\ldots,(p_n,v_n)\}$. Output variables are optimal coding rate bituple $\{c_{n1}^k, c_{n2}^k\}$ and bit-plane partition mark $k$.
2) $Setup$: Apply each available coding rate in prescribed coding library into on-site test to get bit-error rate. By

using these test results, we can get the loss rate of position segments and value segments which are calculated according to (11) and (12).

3) *Search for the optimun*: For partition marker $i$ from 1 to $n$, do the following steps.
   a) Using (7) and (8), and the loss rate of each segment obtained during setup, we get all possible bituples in the prescribed coding library $\{c_1, c_2, c_3, \ldots, c_M\}$ obtained by finding the optimal tuple which maximizes the WWPRD quality $\triangle\varepsilon$ within the energy transmission budget $E_{\max}$. Then, this optimal tuple $\{c^i_{n1}, c^i_{n2}\}$ and its corresponding WWPRD quality value $\triangle\varepsilon(i)$ are recorded into an array $A$.
   b) Search for the maximal $\triangle\varepsilon(i)$ from array $A$, and output its corresponding bit-plane partition $k$ and coding rate $\{c^k_{n1}, c^k_{n2}\}$.

## V. Results And Discussions

In this section, theoretical simulations are conducted to evaluate the proposed two-rate UEP algorithm. In our experiments, the raw ECG data are first source encoded by SPIHT and then processed with the help of the two-rate UEP algorithm. The SPIHT encoded bit-stream is split into equal-sized packets that are first appended by a CRC, and then protected by using one of the available RCPC codes. Instead of obtaining bit-error-rate through testing, we theoretically calculated it using (10), which provides an independent and generic evaluation of our approach.

Two experiments were then conducted. In the first experiment, we evaluated the performance in terms of the average overall coding rate versus WWPRD quality. The configurations of this experiment are: AWGN channel, BPSK modulation, 8-bit CRC, 100-bits packet size. And RCPC generate code is [133 171 145], RCPC memory is 6 bits. The overall coding rate for one packet is calculated by

$$R = \frac{L_D}{K\left\lceil \frac{L_D + L_{\mathrm{CRC}} + L_M}{P} \right\rceil} \tag{12}$$

where $K$ is the puncture number, $P$ is the puncture period. $L_D$, $L_{\mathrm{CRC}}$, and $L_M$ are the lengths of the data, CRC, and the needed memory of RCPC, respectively.

RCPC codes offer very flexible coding rates and optimal coding performance. Thus, it is very suitable for our scheme. Let $R_{c1}$ and $R_{c2}$ denote the code rate $c_1$ and $c_2$. Also, let the number of packets encoded by $c_1$ and $c_2$ be $N_{c1}$ and $N_{c2}$. The average overall coding rate is then

$$R_a = R_{c1}\frac{N_{c1}}{N} + R_{c2}\frac{N_{c2}}{N}. \tag{13}$$

In this experiment, we compared the performance of two-rate UEP with that of single rate EEP. The results are shown in Fig. 6. Heuristically, the ECG quality requirement is satisfied when WWPRD is below 0.1. As shown in the results, our two-rate UEP algorithm can achieve a very good quality under an overall coding rate of 0.7 with SNR = 0 dB, while EEP can only offer an overall coding rate of approximately 0.4 without quality compromise.

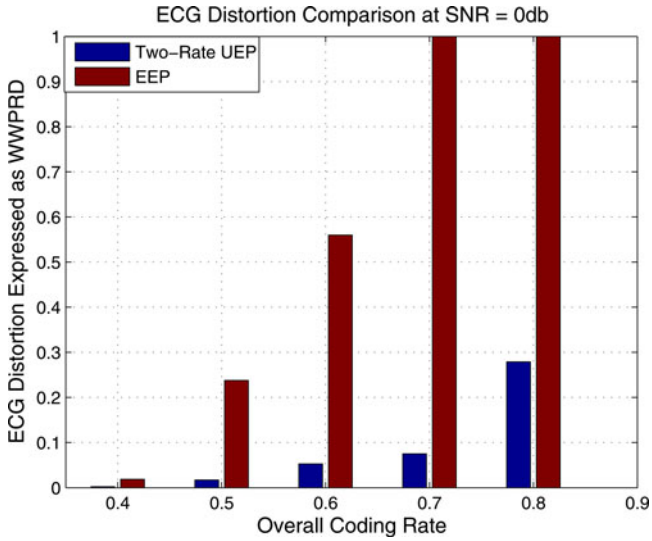



Fig. 6. ECG distortion comparison over the overall coding rate.

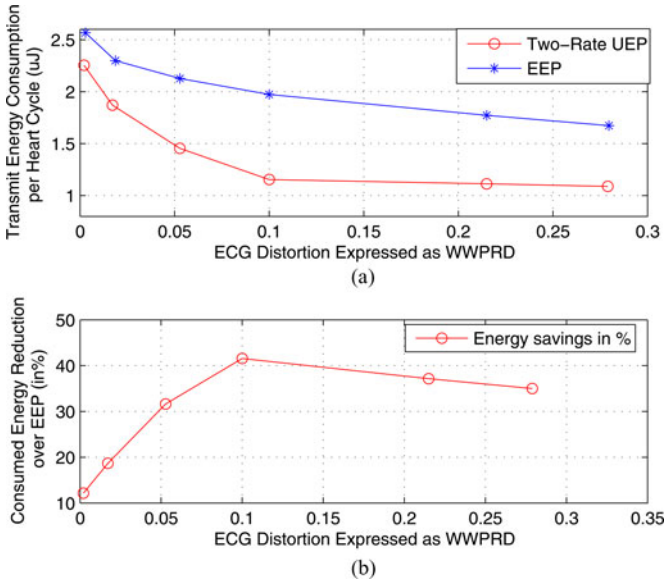



Fig. 7. Energy consumption comparison over WWPRD.

In the second experiment, we evaluated the ECG quality versus energy consumption. The configurations are: 0 db·m transmitting power, 2500 kb/s. Others are the same as the first experiment. The transmit energy consumption is calculated by (5).

Comparison results between the two-rate UEP and EEP are shown in Fig. 7. As can be seen, the WWPRD quality is significantly improved. The WWPRD quality of the two-rate UEP is much higher than that of EEP at the same transmit energy consumption level. Therefore, our scheme achieves a significant energy saving of between 10% and 42%. Since for a typical application a WWPRD range between 0.05 and 0.2 is desirable, our scheme can achieve a minimum of 32.7% energy saving per transmitted heart cycle. Also, please note that a lower WWPRD represents a reduction in error of the received ECG waveform and, thus, a higher quality.

Some more related results from our studies under different SNR configurations have been presented in [26], where we focused on the cross-layer implementation techniques for general E-Healthcare technologies and the ECG signal transmissions.

## VI. Conclusion

Energy saving and security are the two most critical issues for ECG transmission in BASNs. In this work, an energy-efficient and secure scheme for ECG transmissions in BASNs is presented. Characteristics of compressed ECG are extensively explored and the unequal ECG quality distribution among the output bits of the compression codec is studied. In this study, we proposed a simple and yet effective encryption scheme in which only 1% of the compressed ECG data needs to be encrypted and the remainder is intrinsically secured due to the dependence of the codec on the protected data portion for successful decompression of the entire bit stream. This algorithm greatly reduces the burden of ECG encryption, while also providing a significant energy saving. After encryption, the ECG data are protected by our proposed two-rate UEP scheme, which achieves further substantial energy saving without compromising ECG signal quality. Our simulation results showed that this scheme is able to provide more than 40% additional energy saving at a WWPRD of 0.099 after compression that maintains a high quality of the ECG data, while providing desired security in medical applications.

## References


[1] Data from centers for disease control and prevention (CDC). 2006. [Online]. Available: http://www.cdc.gov/nchs/hus.html.

[2] M. Munshi, X. Xu, X. Zou, E. Soetiono, C. S. Teo, and Y. Lian, "Wireless ECG plaster for body sensor network," in *Proc. Int. Summer School Symp. Med. Devices Biosens.*, 2008, pp. 310–313.

[3] L. Zhong, M. Sinclair, and R. Bittner, "A phone-centered body sensor network platform cost, energy efficiency and user interface," in *Proc. Int. Workshop Wearable Implantable Body Sens. Netw.*, 2006, pp. 179–182.

[4] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and L. Victor, "Body area networks: A survey," *J. Mobile Netw. Appl.*, vol. 16, pp. 171–193, 2011.

[5] G. Nave and A. Cohen, "ECG compression using long-term prediction," *IEEE Trans. Biomed. Eng.*, vol. 40, no. 9, pp. 877–885, Sep. 1993.

[6] Health Insurance Portability Accountability Act (HIPAA). [Online]. Available: http://www.hhs.gov/ocr/privacy/

[7] L. Biel, O. Pettersson, L. Philipson, and P. Wide, "ECG analysis: A new approach in human identification," *IEEE Trans. Instrum. Meas.*, vol. 50, no. 3, pp. 808–812, Jun. 2001.

[8] A. Chan, M. Hamdy, A. Badre, and V. Badee, "Wavelet distance measure for person identification using electrocardiograms," *IEEE Trans. Instrum. Meas.*, vol. 57, no. 2, pp. 248–253, Feb. 2008.

[9] H. Kim, Y. Kim, and H. J. Yoo, "A low cost quadratic level ECG compression algorithm and its hardware optimization for body sensor network system," in *Proc. Int. Conf. Eng. Med. Biol. Soc.*, 2008, pp. 5490–5493.

[10] A. Boskovic and M. Despotovic, "An efficient approach to ECG signal transmission via GPRS," in *Proc. Int. Conf. Comput. Tool (EUROCON)*, 2005, vol. 1, pp. 76–79.

[11] H. Wang, D. Peng, W. Wang, H. Sharif, H. H. Chen, and A. Khoynezhad, "Resource-aware secure ECG healthcare monitoring through body sensor networks," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 12–19, Feb. 2010.

[12] F. Sufi, S. Mahmoud, and I. Khalil, "A wavelet based secured ECG distribution technique for patient centric approach," in *Proc. Int. Summer School Symp. Med. Devices Biosens.*, 2008, pp. 301–304.

[13] S. Jalaleddine, C. Hutchens, R. Strattan, and W. Coberly, "ECG data compression techniques-a unified approach," *IEEE Trans. Biomed. Eng.*, vol. 37, no. 4, pp. 329–343, Apr. 1990.

[14] Q. Ruan and Y. Zhang, "An improved algorithm based on EZW for ECG signal," in *Proc. Int. Conf. Signal Process.*, 2000, pp. 922–925.

[15] Z. Lu, D. Y. Kim, and W. Pearlman, "Wavelet compression of ECG signals by the set partitioning in hierarchical trees algorithm," *IEEE Trans. Biomed. Eng.*, vol. 47, no. 7, pp. 849–856, Jul. 2000.

[16] G.-H. Jeong and I.-S. Lee, "Wavelet-based ECG compression using dynamic multi-stage vector quantization," in *Proc. IEEE Conf. Ind. Electron. Appl.*, May, 2009, pp. 2100–2105.

[17] S.-G. Miaou, H.-L. Yen, and C.-L. Lin, "Wavelet-based ECG compression using dynamic vector quantization with tree codevectors in single codebook," *IEEE Trans. Biomed. Eng.*, vol. 49, no. 7, pp. 671–680, Jul. 2002.

[18] M. Blanco-Velasco, F. Cruz-Roldan, J. Godino-Llorente, and K. Barner, "ECG compression with retrieved quality guaranteed," *Electron. Lett.*, vol. 40, no. 23, pp. 1466–1467, Nov. 2004.

[19] M. Blanco-Velasco, F. Cruz-Roldan, J. Godino-Llorente, and K. Barner, "Wavelet packets feasibility study for the design of an ECG compressor," *IEEE Trans. Biomed. Eng.*, vol. 54, no. 4, pp. 766–769, Apr. 2007.

[20] A. Al-Fahoum and I. Howitt, "Combined wavelet transformation and radial basis neural networks for classifying life-threatening cardiac arrhythmias," *J. Med. Biol. Eng. Comput.*, vol. 37, pp. 566–573, 1999.

[21] L. Khadra, A. Al-Fahoum, and H. Al-Nashash, "Detection of life-threatening cardiac arrhythmias using the wavelet transformation," *J. Med. Biol. Eng. Comput.*, vol. 35, pp. 626–632, 1997.

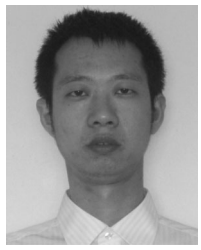
[22] J. Pan and W. J. Tompkins, "A real-time QRS detection algorithm," *IEEE Trans. Biomed. Eng.*, vol. BME-32, no. 3, pp. 230–236, Mar. 1985.

[23] A. Al-Fahoum, "Quality assessment of ECG compression techniques using a wavelet-based diagnostic measure," *IEEE Trans. Inf. Technol. Biomed.*, vol. 10, no. 1, pp. 182–191, Jan. 2006.

[24] T. Ma, M. Hempel, D. Peng, and H. Sharif, "Rate-switching unequal error protection for wireless electrocardiogram (ECG) transmission," in *Proc. Military Commun. Conf.*, 2010, pp. 1181–1186.

[25] J. Hagenauer, "Rate-compatible punctured convolutional codes (RCPC codes) and their applications," *IEEE Trans. Commun.*, vol. 36, no. 4, pp. 389–400, Apr. 1988.

[26] T. Ma, M. Hempel, D. Peng, H. Sharif, F. Rezaei, P. Shrestha, and H. H. Chen, "Using cross-layer techniques for communication systems: Techniques and applications, using cross-layer techniques for ECG Transmissions in Body Area Sensor Networks," in *Using Cross-Layer Techniques for Communication Systems,* H. F. Rashvand and Y. S. Kavian Eds., IGI Global, Hershey, PA, Apr. 2012, doi:10.4018/978-1-4666-0960-0.

**Tao Ma** received the B.Sc. and M.Sc. degrees from Xian Jiaotong University, Xi'an, China, in 2005 and 2008 respectively, both in electrical engineering. He is currently working toward the Ph.D. degree in the Department of Computer and Electronics Engineering, University of Nebraska-Lincoln, Lincoln.

His research interests include cross-layer design for QoS provisioning in wireless data networks, multimedia distribution, and ultralow power sensor network.

**Pradhumna Lal Shrestha** received the B.E. in electronics and communication from Tribhuvan University, Kathmandu, Nepal, in 2007, and the M.S. degree in telecommunications engineering from the University of Nebraska-Lincoln, Lincoln, in 2011, where he is currently working toward the Ph.D. degree in the Department of Computer and Electronics Engineering, University of Nebraska-Lincoln, Lincoln.

His research interests include theoretical and mathematical modeling, wireless communications, signal processing, high-speed networks, among others.

**Michael Hempel** received the Ph.D. degree in computer engineering from the University of Nebraska-Lincoln, Lincoln, in 2007.

He is currently a Research Assistant Professor in the Department of Computer and Electronics Engineering, University of Nebraska-Lincoln. His research interests include wireless communications networks and multimedia communications.

**Dongming Peng** received the B.A. and M.A. degrees in electrical engineering from the Beijing University of Aeronautics and Astronautics, Beijing, China, in 1993 and 1996, respectively, and the Ph.D. degree in computer engineering from Texas A&M University, College Station, in 2003.

From 1996 to 1997, he was a Faculty Member at Beijing University. In 2002, he joined the University of Nebraska-Lincoln, where he is currently an Associate Professor. His research interests include digital image processing, computer architectures, parallel and distributed computing, and sensor network.

Dr. Peng is one of the recipients of the Best Paper Award in the IEEE Wireless Communications and Networking Conference 2008. He has also served as a Referee and Program Committee Member for several conferences and journals.

**Hamid Sharif** received the B.S.E.E. degree from the University of Iowa, the M.S.E.E. degree from the University of Missouri-Columbia, and the Ph.D. degree from the University of Nebraska-Lincoln.

He is the Charles J. Vranek Professor in the College of Engineering, University of Nebraska-Lincoln, Lincoln, where he is also the Director of the Advanced Telecommunications Engineering Laboratory. He has published a large number of research articles in international journals and conferences. Dr. Sharif has been the recipient of a number of best papers awards. He has been serving on many IEEE and other international journal editorial boards and currently is the Co-Editor-In-Chief for the Wiley Journal of *Security and Communication Networks*. He has contributed to the IEEE in many roles including the elected Chair of the Nebraska Section, elected Chair of the Nebraska Computer Chapter, elected Chair of the Nebraska Communication Chapter, and the Chapter Coordinator for the IEEE Region 4 in USA.

**Hsiao-Hwa Chen** (S'90–M'92–SM'01–F'10) received the B.Sc. and M.Sc. degrees from Zhejiang University, Zhejiang, China, and the Ph.D. degree from the University of Oulu, Oulu, Finland, in 1982, 1985, and 1991, respectively.

He is currently a Distinguished Professor in the Department of Engineering Science, National Cheng Kung University, Tainan, Taiwan.

Dr. Chen is the Founding Editor-In-Chief of Wileys *Security and Communication Networks Journal*. He is a Fellow of IET and a Fellow of BCS.