International Journal for Modern Trends in Science and Technology
Volume: 03, Issue No: 05, May 2017
ISSN: 2455-3778
http://www.ijmtst.com

Innovative Method to Secure ECG Signal using ECC in Wireless Communication

G.Purushothaman[1] | Dr. R.Ilango[2] | N.Karthika[3] | N.Ajith[4]

[1,2,3,4] Assistant Professor, Department of EEE, M.A.M.S.E, Tamilnadu, India.

To Cite this Article
G.Purushothaman, Dr. R.Ilango, N.Karthika and N.Ajith, "Innovative Method to Secure ECG Signal using ECC in Wireless Communication", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Issue 05, May 2017, pp. 99-103.

ABSTRACT

Mobile based healthcare is one of the fastest growing area of health care computing. One of the important social problems we are facing now is the increasing percentage of the aged in the population and also modern people face much more financial and society pressure than before, living and working in a rapid rhythm, the health status can't get often monitoring, sudden death occurs without any medical symptom. To deal with these challenges, it is necessary to research the automated health care (ECG) service with maximum data security in order to lay the foundation for its successful application on Mobile Cloud. In a mobile care system setting, wearable electrocardiogram ECG sensors can give a continuously monitoring over days or weeks anywhere anytime over the Bluetooth to mobile. The proposed system using SPIHT for compression the ECG data and the best encryption mechanism provides a simple and yet effective security solution for an ECG sensor-based communication platform, where end-to-end encryption of entire ECG data encrypting using ECC algorithm which is based on public key cryptography as a lightweight algorithm in Mobile Cloud. This part of the encrypted data is essential to ECG data quality and it saves significant additional energy saving due to its unequal investment of communication energy to the outcomes of the lightweight encryption, and thus, it maintains a high ECG data transmission quality.

KEYWORDS: *ECG, BASNs, CDC.*

I. INTRODUCTION

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 selective encryption mechanism provides a simple and yet effective security solution for man 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. Their 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.

A. ECG In Existing System

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 Centres 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. The fast increase in the number of heart illness patients, most of them 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 ×23 mm .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. 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. In addition, numerous communication protocols such as 8011.15.4, Bluetooth, and TDA5250have 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. 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.

B. 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 in-formation is useless if the position information is not reliable. Among different subsets, position information is not independent either. In fact, two lists, i.e., the list of insignificant points (LIP) and the list of insignificant sets (LIS), record the position information. The current-partition-sorting step per-forms the searches in both LIP and LIS of the previous bitplane. Therefore, the position information in the current bit-plane is de pendent on the previous position information.

C. Two-Rate UEP Scheme

In ECG signals, several important features for cardiac disease diagnosis are well defined. It is worth noting how these features are allocated in the wavelet domain, where we apply 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 cantered around 17 Hz. 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. ST segments often occupying a lower frequency range.

II. EXSISTING ALGORITHAM SPIHT-AES

i. 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 their scheme depends entirely on the level of security of the employed encryption algorithm itself, such as Advanced Encryption Standard (AES). Furthermore, their security scheme is independent and it works compatible to almost all existing encryption algorithms.

ii. The ECG feature distribution in the wavelet domain is studied in this study. In addition, 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 (using20:1 compression rate with about 6.3% PRD).

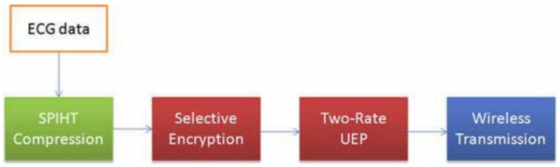

Figure 1: Existing ECG Transmission

III. DISADVANTAGES OF EXISTING SYSTEM

Recent technological progress in wireless sensing and wearable sensors has made BASNs technology a promising solution to help us to meet this growing demand.

i. 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.

ii. Existing schemes uses only AES algorithm to encrypt ECG signal but there is no assurance of ECG signal security.

iii. Key distribution is problem in existing scheme because of this Symmetric algorithm.

IV. PROPOSED ALGORITHAM: SPIHT-ECC

A. SPIHT

The main purpose of compression is to represent an ECG image with the smallest possible number of bits. It can assist the transmission and processing of image. Among many medical signal sources, the compression of electrocardiogram (ECG) is in great demand. Many types of ECG recordings generate a vast amount of data. These include up to 48 hour. Halter recordings, telemetry recordings, continuous ECG performed in intensive care units and stress test ECG. With the growing use of these ECG signals to detect and diagnose heart disorders, ECG compression becomes mandatory to efficiently store and retrieve this data from medical database. Other practical importance includes transmitting real time ECG over the mobile communication network and storing patient data in a medical smart card. In this paper, we treated ECG signal as image recorded on an ECG paper. ECG paper is traditionally divided into 1mm squares. Vertically, ten blocks usually correspond to 1 mV, and on the horizontal axis, the paper speed is usually 25mm/s, which makes one block 0.04s (or 40ms). We also have "big blocks" which are 5mm on their side. Knowing the paper speed, it’s easy to work out heart rate. If the number of big block is1, the rate is 300, if it is 2, the rate is 150 and so on. Rates in between these numbers are easy to interpolate. In recent years, wavelet based embedded image coder is quite attractive in modern applications. Wavelet transform, bit plane coding and other techniques make embedded image coders practically, which not only provide efficient compression performance, distortion scalability, resolution scalability, but the efficiency of a wavelet based compression scheme relies on the efficiency of specifying to the decoder which coefficients to quantize before which others, and of the corresponding bit allocation. Said and Pearlman developed an algorithm, called set partitioning in hierarchical trees (SPIHT) based on the same basic concepts. It was more effective in transmission of significance information to the decoder. Both the schemes relied on partial magnitude ordering of the wavelet coefficients, followed by progressive refinement, and produced embedded bit streams. The transmission of ordering information is achieved by a subset partitioning approach that is duplicated at the decoder. The refinement is based on ordered bit plane transmission of the magnitudes of the coefficients previously ascertained as significant. In this work, a low bit rate image coder of modified SPIHT algorithm without arithmetic coder has been demonstrated for High speed ECG compression. The modifications of the SPIHT compressor have been presented combining the sorting and refinement phase. With the elimination of List of Significant Pixels (LSP) and List of insignificant pixels (LIP) lists, the memory requirement has been reduced tremendously.

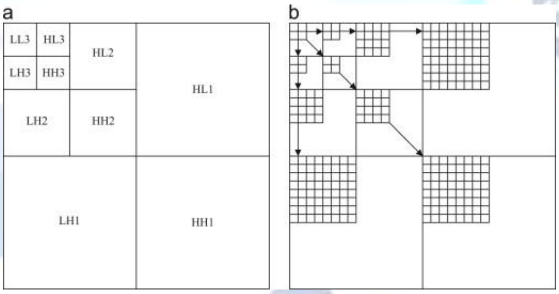

Figure 2: SPIHT structure (a, b)

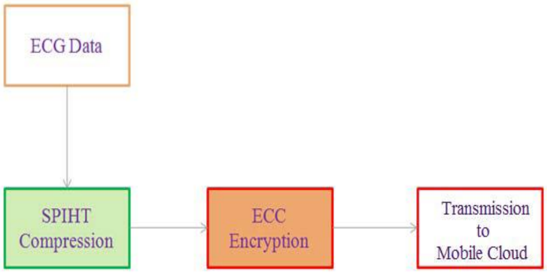

Figure 3: Proposed Security Enhanced ECG Transmission

B. Elliptic Curve Cryptography (ECC)

Elliptic curve cryptography [ECC] is a public-key cryptosystem just like RSA. Analysis of ECC with other Cryptosystems

i. RSA – Integer Factorization

ii. ECC - Elliptic Curve Discrete Logarithm problem

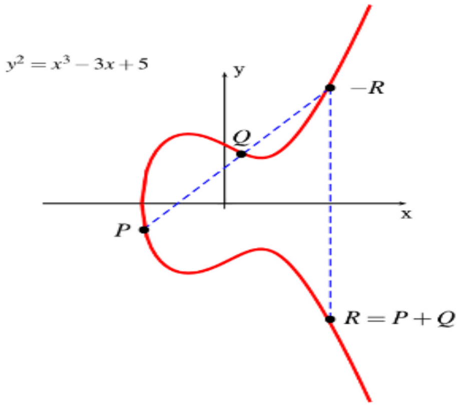

Figure 4: ECC Encryption

Elliptic curve cryptography (ECC) was proposed by Koblitz and Miller in 1985. Compared with other commonly used public key cryptosystems such as RSA and discrete logarithm, claims have been made that ECC offers a smaller key length, better security, and a smaller hardware realization than other methods. ECC is particularly suitable for embedded applications, the benefits being

i. ECC offers the highest security per bit of any known public key cryptosystem so a smaller memory can be used

ii. ECC hardware implementations use less transisters,as an example, a VLSI implementation of 155-bit ECC has been reported which uses only 11,000 transistors compared with an equivalent strength 512-bit RSA processor which used 50,000 transistors.

iii. ECC is probably more secure than RSA, the largest and RSA and ECC challenges solved being 512-bit and 97-bit respectively. In cracking the 97-bit ECG problem, approximately twice the computing power of the RSA problem was used.

V. ADVANTAGES OF PROPOSED SYSTEM

The proposed scheme going to use lightweight ECC (Ecliptic Curve Cryptography) to secure the ECG Signal.

i. ECC is best suited for energy efficient devices like wireless sensors, Mobile, etc.

ii. MD5 algorithm going to use ensuring the security of ECG signal.

iii. In addition, this scheme uses SPIHT for compressing the ECG signal to save energy.

iv. Simultaneous compression and encryption will save energy and secure the signal, Its equivalent to dual encryption like security.

VI. RESULT AND COMPARATION

In this section, MATLAB simulations are conducted to evaluate the proposed ECC based encryption. In our experiments, the raw ECG data are first source encoded by SPIHT and then processed with the help of the ECC security algorithm. The SPIHT encoded bit-stream is split into equal-sized packets that are first encrypted by ECC algorithm and then signed by private key of sender, and then send to receiver. Once received by the receiver decrypted by ECC with using private key of receiver and then verified by senders public key. Instead of obtaining bit-error-rate through testing, we have done public key cryptography technique with using digital signature concepts (Figure 4,5& 6).

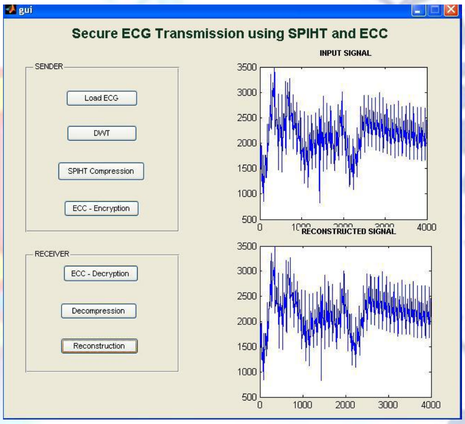

Figure 4: Proposed Mat Lab Implementation

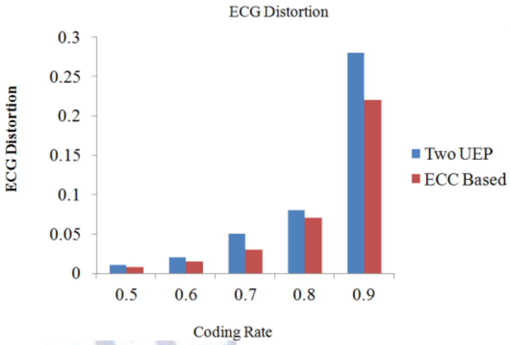

Figure 5: ECG Distortion Comparison

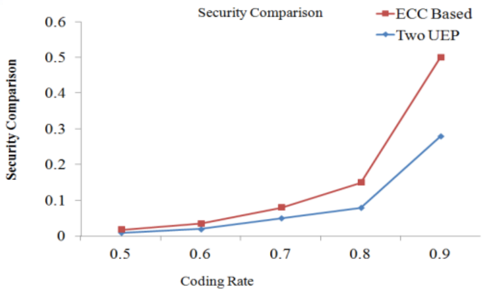

Figure 6: Security Comparison

VII. CONCLUSION

Energy saving and security are the two most critical issues for ECG transmission in BASNs. In this project, an energy efficient and lightweight secure scheme for ECG transmissions in BASNs would be 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, I proposed a simple and yet effective encryption scheme in which only 1% of the compressed ECG data needs to be encrypted using ECC. This ECC algorithm greatly reduces the burden of ECG encryption, while also providing a significant energy saving. This proposed simulation results showed that this scheme would be able to provide more than 40% additional energy saving at 0.099 after compression that maintains a high quality of the ECG data, while providing desired security in medical applications.

REFERENCES

[1] 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.

[2] Adrian D. C. Chan, Mohyeldin M. Hamdy, Armin Badre and VesalBadee, "Wavelet Distance Measure for Person Identification

[3] C. P. Wu, and C. C. J. Kuo, "Design of Integrated Multimedia Compression and Encryption Systems", IEEE Transactions on Multimedia, VOL. 7, No. 5, Oct. 2005, pp. 829-839

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

[5] DR Stinson, Cryptography, Theory and Practice, 2nd edition, Chapman & Hall, CRC Press, Boca Raton (2002).

[6] G.H Jeong and I.S Lee, "Wavelet-based ECG compression using dynamic multi-stage vector quantization," 4th IEEE Conference on Industrial Electronics and Applications, pp.2100-2105, 2009

[7] G.Nave and A. Cohen, "ECG compression using long-term prediction," IEEE Trans. Biomed. Eng., vol. 40, no.9, pp. 877- 885, Sep. 1993. Health Insurance Portability Accountability Act (HIPAA).

[8] 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, vol. 17, no. 1, pp. 12–19, Feb. 2010.

[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] Health Insurance Portability Accountability Act of 1996 (HIPAA), Centers for Medicare and Medicaid Services (1996)

[11] Health Insurance Portability and Accountability Act of 1996, 104th Congress, Public Law 104-191, 1996

[12] M. Blount et al, "Remote health-care monitoring using Personal Care Connect", IBM Systems Journal, Vol. 46, No. 1, 2007, pp. 95-113