

Secure and Energy Efficient Transmission of ECG Signals in Wearable Sensor Networks – A Survey

Sumi Thomas

Research Scholar, Department of ECE, SNGCE Kadayiruppu, India.

Soniya Peter

Asst. Professor, Department of ECE, SNGCE Kadayiruppu, India.

Abstract – Security and energy efficient transmission are two important issues in wearable sensors. Health conditions of VIPs, soldiers etc. are of very important and high security has to be maintained. The transmission of the ECG signal using sensors to distant monitoring centers increases the power consumption due to the Bluetooth transceivers. Wearable sensors uses electrodes attached to the body of patients to collect ECG data and it is processed and transmitted to monitoring center or hospitals at a distant locations using WAN or CDMA. This paper presents a study of different secure and energy efficient ECG signal transmission methods.

Index Terms – Electrocardiogram (ECG), Wearable Sensors, Compressed Sensing (CS), Digital Signature.

1. INTRODUCTION

A traditional Holter monitor can record up to 24 hours of ECG signals, and the recorded data is subsequently retrieved and analyzed by a clinician. Due to the short duration involved and the unknown context within which the ECG signal is captured, reliable interpretation of the recorded data is always a challenge. To address these drawbacks, some more advanced ECG monitoring systems are emerging. They can also detect and signal a warning in real-time if any adverse event is captured. Recent research has also focused on the development of wireless sensor networks (WSN) and pervasive monitoring systems for cardiac patients. For example, a number of wearable systems have been proposed with integrated wireless transmission, GPS (Global Positioning System) sensor, and local processing. Commercial systems are also becoming available. For example, CardioNet provides a remote heart monitoring system where ECG signals are transmitted to a PDA (Personal Digital Assistant) and then routed to the central server by using the cellular network. Pentland recently presented the wearable MITHril system where ECG data, GPS position, skin temperature and galvanic skin response can be captured by a PDA.

Whilst WSN technology continues to evolve for a broad range of applications and settings, it does not specifically tackle the challenges associated with human body monitoring. The human body consist of complicated internal environment that responds to and interacts to the external environment, but is in a way separate and self-contained.

Human body monitoring using a network of wireless sensors may be achieved by attaching these sensors into the body surface as well as implanting them to the tissues. Human body environment is not only on a smaller scale, but also requires different type and frequency of monitoring with different challenges than those faced by WSN. The realization that the proprietary designed WSN are not ideally suited for monitoring human body and its internal environment has led to the development of a wireless body sensor network (BSN) platform. BSN architecture aims to set a standard of development of a common approach towards pervasive monitoring.

The figure 1[1] represents a subject with a number of sensors attached to their body, each sensor is also connected to a small processor, wireless transmitter, and a battery, and all together forming a BSN node complex capable of seamlessly integrating at home, office and hospital environments. The BSN node ensures the accurate capturing of data from sensor to which it is connected, carries out low level processing of data and wirelessly transmit this information to a local processing unit (LPU). The data in this way from all the sensors are collected, processed and transmitted to a central monitoring server through a wireless LAN, Bluetooth or mobile phone. The ECG signal is collected through electrodes connected to the body of the patients. The signal obtained will be of low amplitude and it has to be processed. It is first send to any nearby devices like mobile phone or personal computers and using the internet in the phone or PC, it is transmitted to a distant diagnostic center.

A wearable ECG sensor, as shown in figure 2 can be used to acquire, process, and wirelessly transmit ECG signal to a monitoring center. The main challenge involved in the development of the sensor is to make the device low profile, secure, unobtrusive, and easy to use with long battery life for continuous usage. A high level of integration with inbuilt signal acquisition and data conversion is required to minimize the size, cost, and power consumption of such a sensor. The major source of power consumption in such a system is the wireless transceiver, and hence, it is desirable to carry out preliminary ECG analysis tasks like QRS detection and RR interval

estimation locally. This allows the transmission to be triggered only when it is deemed necessary based on cardiac rhythm analysis [2].

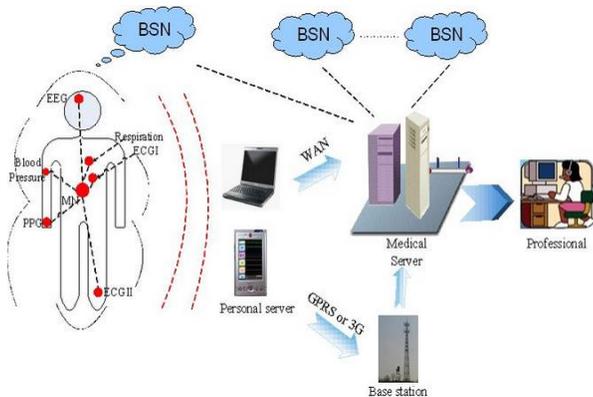


Figure 1 Diagrammatic representation of wearable BSN

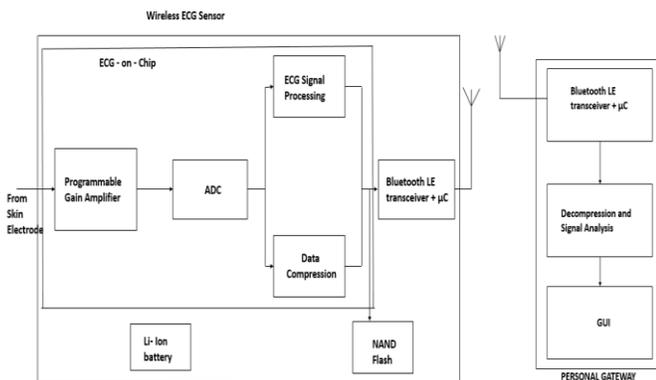


Figure 2 Wearable ECG monitoring system

Electrodes are attached to the body of patients and ECG data is collected. It is given to a programmable gain amplifier, in which gain can be controlled by external signal, and it is amplified to required level. Analog signal is digitized using ADC. ECG signal is then processed and transmitted through Bluetooth transceiver. There is a NAND flash, which is a non-volatile storage technology that does not require power to retain data and there is a Li-ion battery. Graphical User Interface (GUI) allows user to interact with electronic device.

2. SECURE AND ENERGY EFFICIENT ECG SIGNAL TRANSMISSION METHODS

Secure transmission of ECG signal can be accomplished by using XML Digital Signature technology. For this proposed system; here we have to use a medical toolkit, which is capable of measuring daily health conditions of electrocardiogram (ECG), and this digital signal is transferred to a receiving device (ECG Circuit) for signal processing and we use EKG shield for converting them as usable for 3G/2G network [3]. Then this digital signal or data will be used for laptop/ Android

Phone by parsing (SAX parser) into XML document. The XML document will be signed with a digital Signature and will be stored in a Sedna XML database. Then it will be sent to another laptop/Android Phone using Internet. At the receiver end the data is retrieved and verified. And when the receiver will receive this verified secure and authenticated signal with showing the result, the doctors can diagnosis the disease.

In the present system, the patients ECG signal are parsed into XML document and are digitally signed with a private key and saved in the XML data base. Then the signed XML doc is sent to an appropriate doctor. Health workers carry ECG circuit device for measuring ECG. These ECG circuit devices are connected with a Smartphone/ Laptop/Notebook, which uploads the data into the local medical center database server. The medical center sends the request through internet connection to the nearest available doctor. The signature is verified at the receiver end. The receivers have the public key to decrypt the data. After decrypting the signature a hashed value will be found. Now the provided data will be again hashed with the same algorithm and match with the previously found hashed value. If these two hash values are same then the doctor is confirmed that the data sent from medical center is not modified by any third party. The doctor then makes an evaluation of the measured data and provides consultations by telephone/Internet. Fig.3 shows this new and advanced ECG System with XML Digital Signature [4]. To sign the document the sender will sign the document with the private key retrieved from the certificate. After signing the document the document will be saved into database for distribution. The certificate has to attach so that the receiving end can get the public key for verification.

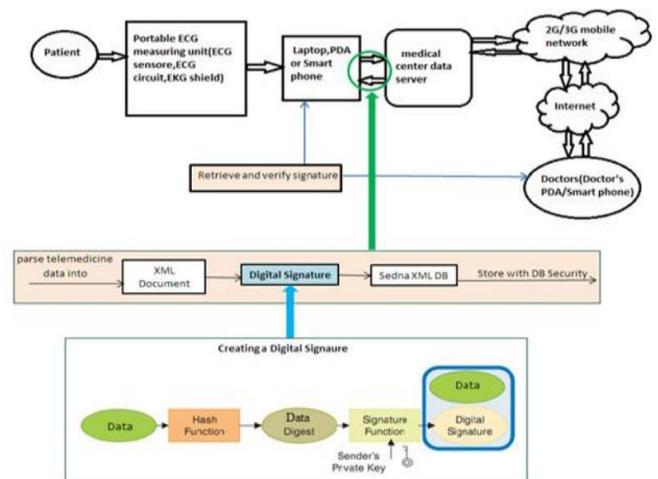


Figure 3 ECG System with XML Digital Signature

Another secure method of transmission of ECG data is by using SPHIT compression as shown in Fig. 4. 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. 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. 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 [5].



Figure 4 Secure and energy efficient ECG transmission scheme

Based 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. 5.

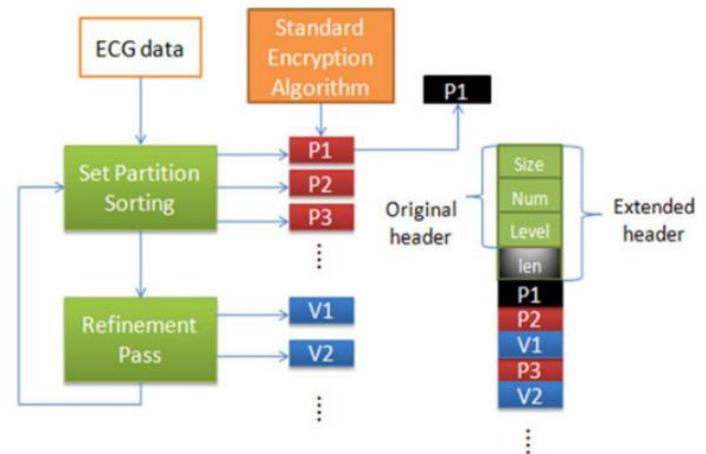


Figure 5 Encryption Algorithm

Compressed Sensing (CS) based compression algorithm is used for energy efficient transmission of ECG data. Sensing and processing information have traditionally relied on the Shannon sampling theorem, one of the central tenets of digital signal processing. This theorem states that, given a signal of bandwidth Ω , it is sufficient to sample it at 2Ω samples per second to ensure faithful representation and reconstruction. However, this traditional ADC paradigm has been challenged lately. First, there are many situations where Ω is so large that constraints put on sampling architectures are simply unbearable. Second, even for relatively low signal bandwidths such as our target wearable ECG application, given the established sparsity of the ECG signal, Nyquist-rate sampling produces a large amount of redundant digital samples, which are costly to wirelessly transmit, and severely limit the sensor nodes lifetime. If one sets course to design energy efficient embedded ECG sensors, it is desirable to reduce the number of acquired ECG samples by taking advantage of the sparsity, or, the reduced “information rate” of the ECG signal. Compressed sensing is a methodology that has been recently proposed to address this problem. But it is also particularly well suited for low-power implementations because it reduces the need for resource-intensive digital signal processing operations [6].

3. CONCLUSION

The survey includes the works and findings done by various researchers on ECG signal compression techniques. Security is an important issue while transmitting ECG data to distant monitoring centers, especially in case of VIPs. This survey presents different encryption methods to enhance the security of the data during transmission. Compressed Sensing based method is also discussed which can be used for energy efficient transmission.

REFERENCES

- [1] www.google.com
- [2] C. J. Deepu, Y.Lian, "A Joint QRS Detection and Data Compression Scheme for Wearable Sensors" IEEE Trans. Biomed. Eng., VOL. 62, NO. 1, pp. 165-175, Jan. 2015.
- [3] UmmeSaymaBusra, Mohammad ZahidurRahman, —Mobile Phone Based Telemedicine Service for RuralBangladesh: ECGI, in Proc. of IEEE Intl. Conf. on Computer and InformationTechnology (ICCIT), p.203-208, March 8-10, 2014, khulna, Bangladesh.
- [4] Md. Momin Reja, Sonia Corraya, UmmeSaymaBusra, - "A New Technique for ECG Telemedicine Data Security and Privacy Using Digital Signature and XML Database" IJARCCCE, Vol.4, Issue.4, April 2015, pp-400-404.
- [5] Tao Ma, Pradhumna Lal Shrestha, Michael Hempel, Dongming Peng, Hamid Sharif, and Hsiao-Hwa Chen, "Assurance of Energy Efficiency and Data Security for ECG Transmission in BASNs", IEEE TRANSACTIONS ON BIOMEDICAL ENGINEERING, VOL. 59, NO. 4, APRIL 2012, pp- 1041-1048.
- [6] Hossein Mamaghanian, Nadia Khaled, David Atienza and Pierre Vandergheynst, "Compressed Sensing for Real-Time Energy-Efficient ECG Compression on Wireless Body Sensor Nodes", IEEE TRANSACTIONS ON BIOMEDICAL ENGINEERING, VOL. 58, NO. 9, SEPTEMBER 2011, pp- 2456-2466.

Authors



Ms Sumi Thomas received B. Tech degree in Electronics and Communication Engineering from Mahatma Gandhi University, Kerala, India in 2012. Currently pursuing M.Tech in Communication Engineering from Mahatma Gandhi University, Kottayam, Kerala, India. Her area of interests includes Biomedical Engineering and Signal Processing.



Ms Soniya Peter, Assistant Professor in the Department of Electronics and Communication Engineering, SNGCE. Secured M.Tech in Signal Processing from Rajagiri School of Engineering and Technology, Mahatma Gandhi University and B.Tech in ECE from Mahatma Gandhi University, Kottayam. Working areas includes Signal Processing and Array Processing.