Journal of Theoretical and Applied Information Technology
10th April 2015. Vol.74 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RC6 BASED SECURITY IN WIRELESS BODY AREA NETWORK

[1]A.SIVA SANGARI, [2] J.MARTIN LEO MANICKAM ,[3] R.M.GOMATHI

Assistant Professor ,Department of IT , Sathyabama University
Professor, Department of ECE, St Joseph College Of Engineering
[1]siva.kumaresh08@gmail.com, [2] josephmartin_74@yahoo.co.in,[3]gomssrm@gmail.com

ABSTRACT

Wireless body area networks have grown more attention in healthcare applications. The development of WBAN is essential for tele medicine and Mobile healthcare. It enable remote patient monitoring of users during their day to day activities without affecting their freedom. A WBAN is a network of sensors placed on the human body for monitoring healthcare information. The surveillance of the person can be performed through wearable sensors. The WBAN used for diverse applications including healthcare applications and athlete monitoring .In WBAN, the body sensors in and around the patient body that collect all patient information and transferred to remote server through wireless medium. The wearable sensors are able to monitor vital signs such as temperature, pulse, glucose information and ECG. However there are lots of research challenges in WBAN when deployed in the network. The sensors have limited resources in terms of memory, size, memory and computational capacity. In this paper,we proposed secure communication between the sensor nodes using selective encryption.The RC6 algorithm is appled for that selective encryption.

Keywords : *Wireless Body Area Network, Electro Cardiogram Signal,Rivest Cipher*

1. INTRODUCTION

The elder people mainly suffered from chronic disease. The continuous patient monitoring is needed for caring elder peoples. The WBAN operation is closely related to patient's sensitive medical information. Because the unsecured information will lead to wrong diagnosis and treatment. The security is important thing in wireless medium. In WBAN, the unauthorized people can easily access the patient's data and data can be modified by the attackers. The creation, deletion, modification of medical information needs a strict security mechanism. In order to provide freeness and flexibility to patients, the sensors transmit their information to sensor head and head transfer all information to mobile through wireless medium. The communication between the sensors and between the sensor head to mobile is done by using either bluetooth or zigbee wireless communication. The communication link between the mobile to remote server is based on WiFi or WIMAX. When transmitting the medical information

The following issues are raised in communication.

- Quality and reliability
- Security and privacy
- Power management

A WBAN system which allows the different types of sensor connected to either base station or mobile that is connected to external networks. The WBAN is based on zigbee technology. The zigbee is the technology used for devices to communicate with each other with low power consumption. The zigbee coordinator is responsible for creating and monitoring devices in the network. The common security threats in WBAN are described as follows:

Eavesdropping: The attacker can be able to read the data maliciously when it is transmitted to the wireless medium.

Modification of data: The unauthorized entity inserts and deletes the information transmitted between the sensor nodes. The modified information will lead to wrong diagnosis for the patients.

Unauthorized access: When an attacker gains access to the patient information by acting as a real user.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Replaying: the attacker can eavesdropping the piece of information and replays that information frequently to destination for disturbs the communication.

The following security requirements are applicable to all elements in WBAN.

Confidentiality: It protects the data from an unauthorized user

Integrity: It guarantees the integrity of data against data modification, insertion and deletion.

Authentication: It is the process of giving authorized rights to users.

Availability: The information can be available at any time even in the node failure.

The following section describes attacks to the physical layer, data link layer, network layer and network layer. The attacks affect the capacity and performance of WBAN.

Physical layer: The most common attacks on the physical layer are jamming and tampering. The hacker can use few nodes to block the entire network. The attacker may damage the sensor nodes to acquire medical information.

Data link layer: The adversary corrupts the frame header information. So receiver is not to get correct checksum values. So, mismatch value occurs at the receiver side. It will degrade the network performance.

Network Layer: The hacker complicates the network by data packets continuously routed through the same router.

Transport layer: Flooding can be categorized to two types as follows: First, if the sensor receives more number of packets, then it cannot provide the requested service. In second, if the sensor transmits more number of packets, then the energy level is reduced.

2. RELATED WORK

Several key management scheme and distribution scheme have developed to provide security in WBAN. But still security in WBAN. The designing on key management and distribution is complex in WBAN. Conventional security and privacy mechanisms are not suitable for WBAN. The key distribution method [1] and asymmetric crypto systems are not suitable WBAN due to limited sensor resources.

In symmetric encryption, the same key is used for both encryption and decryption. The patient wearing body sensors will monitor data at all time and need to encrypt the data at all times. The number of keys also increased. It will complicate the key management process.

In public key encryption, two keys are used for encryption and decryption. It requires computation overhead. The sensor devices have constraints processing speed, memory size and energy. The energy and memory efficient light weight cryptography algorithms are suitable for WBAN.

The PSKA scheme proposed in [3] .The fuzzy vault canbe used for lock the key values from sender side and receiver side recover the original key values using unlocking.But extra chaff points produce the unneccessary overhead.

The IBE lite is proposed in [4].The public key can be generated from an arbitrary string. If more than n secret keys are released ,the master secret key is vulnerable to hacker's attack

We proposed biometric crypto system which combines the features of bio metrics and light weight cryptography to enhance the security and privacy of the WBAN. The proposed system is primarily aimed at using bio metric data to generate key for the security. The traditional cryptography algorithms are not suitable resource constrained devices like wireless sensor nodes, smart cards and RFID. Sensor devices have critical resource constraints like energy, memory size and speed. The energy efficiency is important in sensor nodes. It is important to choose energy and memory efficient algorithm for sensor nodes. We have chosen light weight cryptography algorithm for WBAN. There is a need to develop the specifically cryptography algorithms for resource constrained devices.

3. PROPOSED MODEL

The health care applications become important agenda in many countries of world wide. The recent development in wireless sensor nodes will have important role in healthcare applications.Recent advances in sersor devices are capable of collecting signal information and processing ,forwards the information to the base sation.Each sensors are capable of collecting and sampling,processing the signal information where they are deployed. A WBAN is a network of bio sensors designed to deliver the data to remote users. Advances in communication and computing technologies have changed the

Journal of Theoretical and Applied Information Technology
10th April 2015. Vol.74 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

healthcare system from paper records to electronic data.

The E-healthcare provides great flexibility to patients and healthcare providers. The design of WBAN is very complex. Because, the highly confidential medical data are transferred to the remote users through internet. In this chapter we propose our research work towards on remote patient monitoringThe deployment of sensor nodes should satisfy security and privacy requirements.Without providing the security , the patient may get incorrect diagonosis and treatment.Some times it lead to death.The recent advances in wireless communication,the wearable or implantable sensors transfer information wirelessly to the base station without affecting their daily life activities. The following "fig 1" shows the general architecture of WBAN.

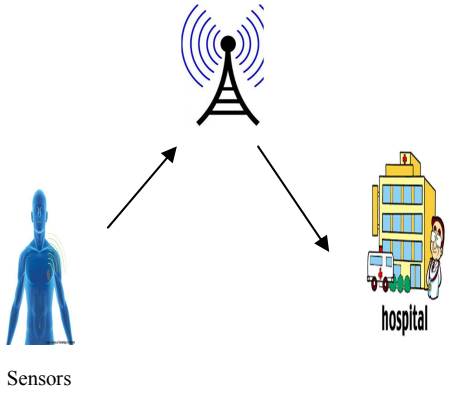

Fig 1 WBAN Architecture

The proposed approach can greatly reduce the encryption by reducing the number bits to be encrypted.The reaining number of bits are not encrypted.The accurate determination of QRS peak values are very important and the peak values are useful for analzing the ECG features.

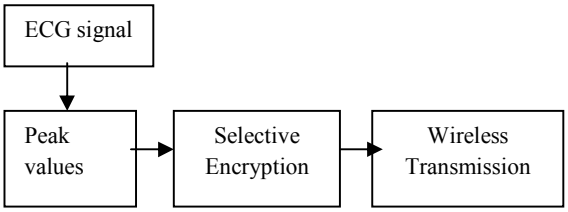

Fig 2 Selective Encryption

as follows :

$$X(t) = H(X(t))\,{}^{1}/_{\pi} \int_{-\infty}^{\infty} \frac{x(\tau)}{t-\tau}\, d\tau \quad \text{.....(1)}$$

The ECG data is filtered using filter and Hilbert transform is applied to this filtered signal The threshold value is uded for determination of peak values.The amplitude value of the signal is checked against the threshold value.The points above threshold will form a group. The highest amplitude points are identified as peak values.

Energy efficient transmission is very important in WBAN. In our approach only important information of ECG values only transmitted.So,the energy consumption is grately reduced.We insert chaotic mapping in to RC6 algorithm This paper presents a RC6 block cipher which is derived from RC5 for transmission security of biomedical systems.The RC6 has a block size of 128 bits and supports 32 bit integer multiplications .The RC6 is able to run to provide improved security and throughput.It is characterized by three parameters (w,r,b).It encrypt 4w bit blocks by four processors and r rounds ,b byte secret key.The RC6 works with four w bit registers A,B,C,D which contains initial plain text input and final output of the encryption.The plain text is stored in four w bit registers with r number of rounds.The RC6 operation consist of independent rotations and modular additions and exclusive OR operations.The RC6 operation is interleaving of two RC5 operations and make dependent rotation on each bit in a word. Here we monitor the patient's heart beat and body temperature using sensors. The microcontroller uses the algorithm to encrypt the measured data and then it is transmitted using Zigbee.The sensor head aggregates all information from the sensor nodes and encrypt it using RC6 algorithm and tranfer encrypted data to the base station.

Wireless sensors and evaluated the system performance.In our experiment the raw ECG data are first filtered and peak point are identified using Hilbert ransform and then the peak values rae encrypted by using RC6 algorithm.the The doctors and patients can access the details either through mobile or laptop.Our work on remote monitoring grew from necessity of a complete and generic wireless health platform.

4. PERFORMANCE EVALUATION

We implemented our solution on wireless sensors and evaluated the system performance. We conduct the security analysis of our proposed

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

approach.The attacker is not able to capture the information.The adversaries can not measure the ECG signal.The proposed scheme significantly reduce the communication and storage overhead.Our major contribution of this paper is to apply RC6 for data authentication in WBAN. We proposed simple and energy efficient scheme for WBAN. This proposed method greatly reduces the burden of ECG encryption.

5. CONCLUSION

Secure communication in WBAN are strongly need to preserve the security and privacy of WBAN.In this paper we present RC6 algorithm for security and privacy concern. Our proposed scheme is light weight and provides energy efficient solution in WBAN.The performance of proposed scheme can be further improved by using extracting features from WBAN and keys can be generated from ECG signals that can be used for further data communication.

REFERENCES

[1] Shinyoung Lim,Tae Hwan Oh Young B. ChoiTamil Lakshman," *Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring* "978-0-7695-4049-8/10 , 2010 IEEE.

[2] Zhaoyang Zhang, Honggang Wang, V. Vasilakos, and Hua Fang" ECG-Cryptography and Authentication in Body Area Networks " IEEE Transactions On Information Technology In Biomedicine, Vol. 16, No. 6, November 2012

[3] Krishna K. Venkatasubramanian, Ayan Banerjee, and Sandeep Kumar S. Gupta, *"PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks "* IEEE Transactions On Information Technology In Biomedicine, Vol. 14, No. 1, January 2010

[4] Jinyuan Sun, University Of Florida Yuguang Fang, *"Privacy And Emergency Response In E-Healthcare Leveraging Wireless Body Sensor Networks "*Xiaoyan Zhu 2010 IEEE IEEE Wireless Communications • February 2010

[5] Daojing He, Chun Chen, Sammy Chan, Jiajun Bu, and Athanasios V. Vasilakos" *ReTrust: Attack-Resistant and Lightweight Trust Management for Medical Sensor Networks "* IEEE Transactions On Information Technology In BiomedicINE, VOL. 16, NO. 4, JULY 2012 .

[6] Chiu C. Tan, Haodong Wang, Sheng Zhong *"IBE-Lite: A Lightweight Identity-Based Cryptography for Body Sensor Networks "* IEEE Transactions On Information Technology In Biomedicine, Vol. 13, No. 6, November 2009

[7] Honggang Wang, , Dartmouth Dongming Peng, Wei Wang, And Hamid Sharif, Hsiao-Hwa Chen, Ali Khoynezhad, *"Resource-Aware Secure ECG Healthcare Monitoring Through Body Sensor Networks "*1536-1284/10, IEEE Wireless Communications ,February 2010 .

[8] Juan A. Fraile, Javier Bajo, Juan M. Corchado, and Ajith Abraham*," Applying Wearable Solutions in Dependent Environments "*IEEE Transactions On Information Technology In Biomedicine, Vol. 14, No. 6, November 2010

[9] De Capua, C. ,Meduri, A., Morello, R, *"A Smart ECG Measurement System Based on Web-Service- Oriented Architecture for Telemedicine Applications*," Instrumentation and Measurement, IEEE Transactions,vol. 59, no. 10, pp.2530-2538, 2010.

[10] Daojing He, Chun Chen, Sammy Chan, Jiajun Bu, and Pingxin Zhang" *Secure and Lightweight Network Admission and Transmission Protocol for Body Sensor Networks* "IEEE Journal Of Biomedical And Health Informatics, Vol. 17, No. 3, May 2013.