Public Key Cryptosystem Based Security in Wireless Body Area Network

A.Siva Sangari
IT Dept, Sathyabama University,
Chennai, India.
siva_sangari2k1@yahoo.co.in

J. Martin Leo Manickam
ECE Dept., St Joseph College of Engineering
Chennai, India.
josephmartin_74@yahoo.co.in

Abstract— **The wireless technology of electronics is growing day by day. Using this technology, real time medical data about patients' medical data can be collected by using simple wearable sensors based on a wireless body sensor network . A portable biomedical system can be build based on the network types available, which can monitor the patient's health in real time. In this paper we developed light weight public key crypto system for security in wireless body sensor network and also the experimental results of proposed scheme on bio sensor nodes which shows the efficiency of our system in practice.**

Index Terms—Wireless Body Area Network, Electro cardiogram Signal

I. INTRODUCTION

The sensors and wireless communication involve and capturing new applications in healthcare applications. The sensors can be either worn or implantable on the human body and travels with patient collecting data. The sensors are continuously collecting the data and send it to the mobile or laptop. The continuous patient monitoring creates the additional security and privacy demands. The wearable sensors measure both mobile and immobile patients in real time. The mobile patients can form a dynamic environment due to their mobility. The wearable healthcare monitoring system enables early detection of abnormal condition and prevention of its early sequence. There are different types of attacks and also threats faced by wireless body area network. These attacks include interruption, interception ,and modification . The security requirements for the wireless body area network are defined as follows

- Data confidentiality : The confidentiality ensures that the patient medical information must be protected form eavesdropper.
- Data integrity : The transmission of medical information can not be altered or modified by unauthorized person.
- Data freshness : The sensor nodes periodically send data to medical professionals ,there must be a guarantee that the data must be fresh data. Because the attackers try to send replay the messages.
- Data availability : The patient medical data should be available to medical users at all times.
- Authentication : The authentication is used to verify the user access.
- Authorization: Before the sensor nodes can provide the information to the user, they must be authorized and also medical personnel need to be authorized before they gain access to medical data.

Ensuring security and privacy is essential for WBAN. Cryptography and authentication methods are used to provide the secure communication between the sensor nodes in WBAN. various key management and distribution scheme have been developed to provide the security in WBAN. The key distribution methods have been developed to distribute the keys in WBAN. But this method is not suitable for body sensors due to limited sensor resources. In this paper we present a new scheme which utilize the ECG signal for generating the cryptographic keys. Using the proposed scheme, the inter sensor communication can be performed. The proposed approach eliminates key communication overhead. we innovated a new bio metric cryptography approach to authenticate the data secure manner.

Here we monitored 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 Zigbee in the receiving end is interfaced with a mobile. The data received is decrypted and monitored in the mobile. The zigbee network can be support large number of devices and longer ranges between the devices and also designed to respond quickly. The zigbee devices have more life time than blue tooth and also transmission range and bandwidth more than the blue tooth devices. The zigbee technology allows devices to be communicate with each other with low power consumption. The zigbee coordinator is responsible for maintaining the devices with in the same network.

II. RELATED WORKS

The secure communication between the body area network is not a easy task .The energy consumption should be minimal. Because the sensor nodes are powered by small batteries. Key design criteria also important in bio sensor nodes. The author [14] proposed use HMAC-MD5 for patient data. But this

method also weak in security .The authors of [15] proposed use ECC for set up keys between sensor nodes ad base station. Traditional cryptography algorithms are not suitable for WBAN.

With the wireless communications coming to homes and offices, the need to have secure data transmission is of utmost importance. Today, it is important that information is sent confidentially over the network without fear of hackers or unauthorized access to it. This makes security implementation in networks a crucial demand. Symmetric Encryption Cores provide data protection via the use of secret key only known to the encryption and decryption ends of the communication path. The bio sensors collect the patient data at regular intervals. The bio sensors will transmit the data to personal wireless hub (eg., laptop ,tablet ,smart phone).Then the personal wireless hub transfer this data to remote healthcare center. The attackers can eavesdrop the messages ,modify the messages and inject forged messages.

III. SECURITY ARCHITECTURE

The main design of security architecture of wireless body area network is shown in fig1.The patient data can be accessed in variety of locations .Each sensor collect the medical data and transferred to the aggregation node. The aggregation node transferred the data to mobile or laptop. If the patient is an outside the location, then the mobile send the data to remote server through internet. If the patient is in a hospital, then the mobile send the data using local area network. The secure communication between the sensor node and aggregation node is performed by using public key crypto system.

When two sensors in a WBAN want to securely communicate with each other by using ECG signal measured separately from the human body. The ECG signals are downloaded from MIT-BIH database. The ECG-based key agreement scheme employs electrocardiogram (ECG) signals to generate cryptographic keys, and avoids traditional predefined key establishment phases. Specifically, the keys from physiological value are distinct for different patients, so these keys are unique after they are generated. When two sensors are available, BSN want to securely communicate using ECG, these two sensors will simultaneously sample ECG signals following the same procedure. Then the collected ECG signals are transformed into a binary stream and thereby used to form a common key agreed on by the communicating sensors.

The ECG signal which is acquired from the individuals is preprocessed for quality check. It makes the necessary correction of the signal from noise. ECG delineation includes detection of P, Q, R, S and T waves from each heartbeat. Feature extraction includes determination of time intervals, amplitudes and angle features from its wave-forms. The heartbeats from the ECG trace are detected using QRS complex delineator, which is implemented using the technique proposed in some improvements. It works at analysis of digital slope, amplitude and width information of ECG waveforms. Once the heartbeat is detected, before and after QRS complex fiducially to seek for P and T wave delineations in each beat of the ECG, the temporal time windows are defined. The schematic diagram of ECG signal shown in Fig 2.

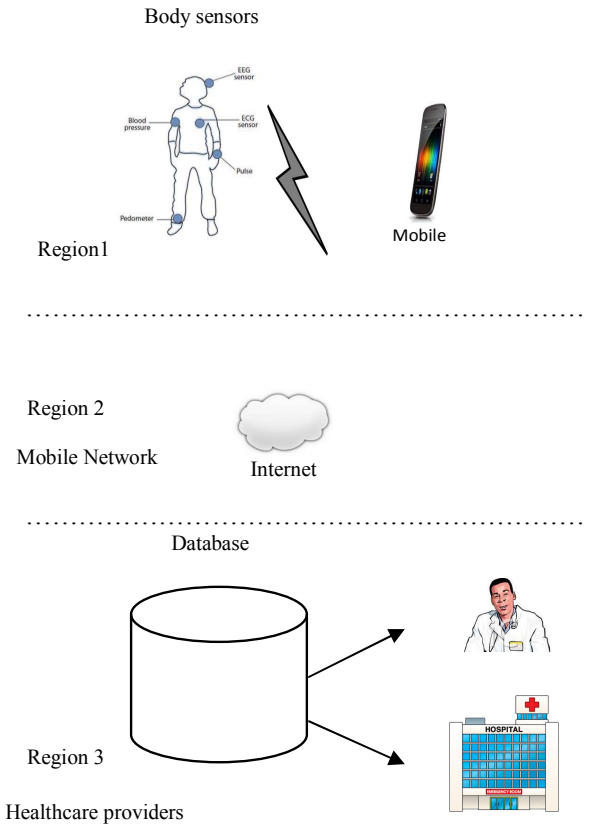

Fig 1 Wireless Body Area Arhitecture

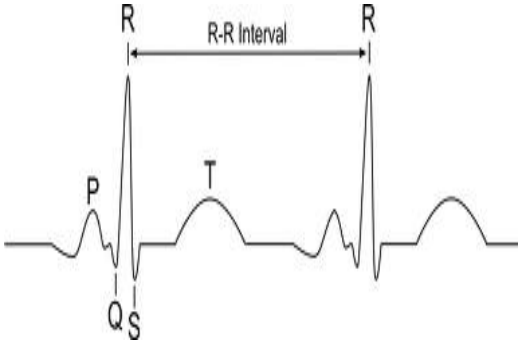

Fig 2. Schematic Diagram of ECG signal

A.Public Key Cryptography

The public key crypto system based on the chebyshev polynomial. The proposed approach is used for secure communication between the sensor nodes. The inter sensor communication between the element sensor node and

aggregation node is performed. The polynomial is defined by recurrent relation as follows [2].

$T_o(x)=1$
$T_1(x)=x$
$T_{P+1}(x)=2xT_p(x)-T_{p-1}(x)$
$T_p(x)$ is a polynomial of degree s.
$T_r(Ts(x))=T_s(T_r(x))=T_{rs}(x)$……(1)
Using Equ 1 the secure communication between the sender and receiver is created. It is similar to the Diffie-Hellman protocol[1].The proposed algorithm is based on public key crypto system.

1) The element sensor node generate a random number x and generates the random integer s. The random number x can be derived from physiological signal like ECG signal. Then it computes $T_s(x)$ and send the pair$(x,T_s(x))$ to head node.
2) The head node generates random integer r and also generate the random number x from ECG signal and computes $T_r(x)$ and send it to the element sensor node.
3) Both element node and head node calculate $T_{rs}(x)$ according to equation 1.The patient data is represented by P. The encrypted message is calculated by
$P'=P*T_{rs}(x)$ ……(2)
4) The head node will decrypt the original message by
$P=P'/T_{rs}(x)$……..(3)

B. Hardware Implementation

Our system has been designed to measure physiological parameters of human body. The inputs from the sensors are processed and integrated. The results are sent through laptop or mobile through the zigbee module. The system consist of two sensors temperature sensor and heart rate sensor. The temperature sensor is in contact with skin and allowing it to measure temperature of the skin. Heart beat is sensed by using a high intensity type LED and LDR. Each sensor can be paired and integrated with transceiver. The sensors in a node are responsible for collecting the bio signals. The storage unit has 128 kb flash memory. The source code of control and signal processing codes are stored in storage unit.

The finger is placed between the LED and LDR. As sensors photo diode or a photo transistor can be used. The skin may be illuminated with visible (red) using transmitted or reflected light for detection. The very small changes in reflectivity or in transmittance caused by the varying blood content of human tissue are almost invisible. Various noise sources may produce disturbance signals with amplitudes equal or even higher than the amplitude of the pulse signal. Valid pulse measurement therefore requires extensive preprocessing of the raw signal. The new signal processing approach presented here combines analog and digital signal processing in a way that both parts can be kept simple but in combination are very effective in suppressing disturbance signals. The setup described here uses a red LED for transmitted light illumination and a LDR as detector.

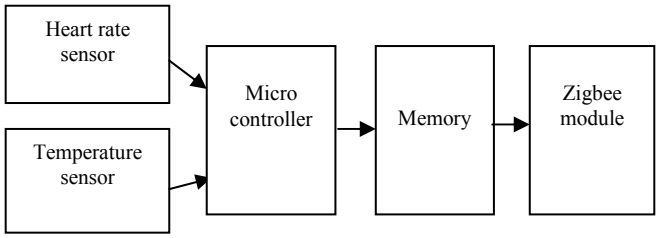

Fig 3 Block diagram of system hardware

IV. PERFORMANCE ANALYSIS

The ECG signals measured on different areas of the same human body have similar values within the time period. Then apply the fast fourier transform on both nodes and get the peak values and these peak values can be used as a random number for public key crypto system for secure communication between the sensor nodes. The encrypted and decrypted ECG signal is shown in fig 4. The random number can be generated from ECG peak values.

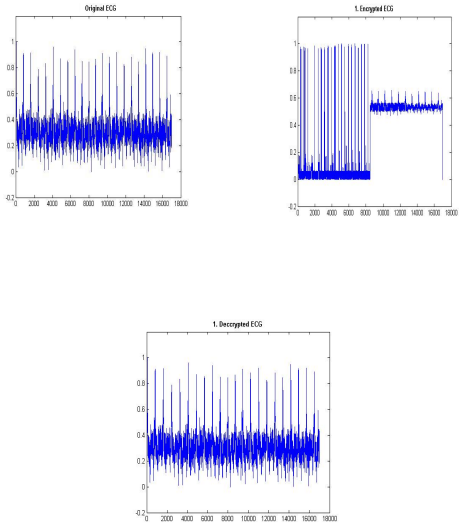

Fig 4 a)Original signal b) Encrypted signal
c) Decrypted signal

This paper provides a continuous and wireless data acquisition and transmission of data . In this section we conduct the security analysis of proposed approach. We focus on three aspects : data confidentiality analysis, data integrity analysis, and security analysis .

(1) Data Confidentiality : It prevent the data access from unauthorized users. The attacker is not able to find the key.
(2) Data integrity and authentication: It ensures that data is not modified by the attackers.
(3) Security analysis: The attackers can not measure the ECG signals. So the attackers are not able access the key.

V. CONCLUSION

In this paper we presented the secure public key crypto system using chebyshev polynomial for secure communication between the sensor nodes. A wireless sensor network with low power and low cost portable patient monitoring system is explored in this paper. The wireless data acquisition and transmission of data in a secured way implemented and also using public key cryptosystem for secure inter sensor communication in WBAN. The low power, low cost, flexible structure for accurate measurement and for long-distance monitoring of patients condition in real time is designed .The security analysis and experimental results shows that our proposed scheme is suitable for real time applications.

REFERENCES

[1] O.Elkeelany and S.Nimmagadda, "Effect of loop-unrolling in hardware reconfigurable implementations of RC5-192 encryption algorithm" IEEE Region 5 Conference, pp. 1-4 , Apr. 2008.

[2] [2] L.Hua, L.Jianzhou, and Y. Jing, "An efficient and reconfigurable architecture for RC5", Canadian Conference on Electrical and Computer Engineering, pp. 1648-1651, May 2005.

[3] [3] K.Hyejung, K.Yongsang, and Y.Hoi-Jun, "A low energy bio sensor node processor for continuous healthcare monitoring system" , IE EE Asian Solid-State Circuits Conference, pp. 317-320, Nov. 2008.

[4] [4] R.L.Rivest, "The RC5 encryption algorithm," in Proc. 1994 Leuven Workshop on Fast Software Encryption, vol. 1008, pp. 86-96, Springer- Verlag, 1995.

[5] N.Sklavos, C.Machs, and O.Koufopavlou, "Area optimized architecture and VLSI implementation of RC5 encryption algorithm," in Proc. 10th IEEE International Conference on Electronics, Circuits and Systems, vol. 1, pp. 172-175, Dec. 2003.

[6] Omar Elkeelany "Performance Comparisons, Design, and Implementation of RC5 Symmetric Encryption Core using Reconfigurable Hardware" IEEE 2009.

[7] H. Wang, B. Sheng, and Q. Li, "Elliptic curve cryptography based access control in sensor networks," *Int*. J. Security Netw., vol. 1, no. 3/4, pp. 127–137, 2006.

[8] H.Wang, B. Sheng, C. C. Tan, and Q. Li, "Comparing symmetric-key and public-key schemes in sensor networks," in Proc. IEEE ICDCS, 2008, pp. 11–18.

[9] M. Mont, P. Bramhall, and K. Harrison, "A flexible role-based secure messaging service: Exploiting IBE technology for privacy in health care,"in Proc. Int. Workshop Database Expert Syst. Appl., 2003, pp. 432–437.

[10] K. Malasri and L. Wang, "Addressing security in medical sensor networks,"in Proc. HealthNet, 2007, pp. 7–12.

[11] S.-D. Bao, Y.-T. Zhang, and L.-F. Shen, "A new symmetric cryptosystem of body area sensor networks for telemedicine," in Proc. Conf. Jpn. Soc. Med. Electron. Biol. *Eng.*, 2005, p. 654.

[12] S.-D. Bao, Y.-T. Zhang, and L.-F. Shen, "Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems," in Proc. IEEE Eng. Med. Biol., 2005, pp. 2455–2458.

[13] Kai Y. Cheong and Takeshi Koshiba*, Member, IEEE* " More on Security of Public-Key Cryptosystems Based on Polynomials" IEEE Transactions On Circuits And System Express Briefs, Vol. 54, No. 9, September 2007 .

[14] A. Ali, S. Irum, F. Kausar, and F. Khan, "A cluster-based key agreement scheme using keyed hashing for body area networks," Multimed. Tool Appl., 2011, DOI: 10.1007/s11042-011-0791-4.

[15] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "IBE-Lite: A lightweight identity-based cryptography for body sensor networks," IEEE Trans. Inf Technol. Biomed., vol. 13, no. 6, pp. 926–932, Nov. 2009.