LIGHT WEIGHT SECURITY AND AUTHENTICATION IN WIRELESS BODY AREA NETWORK

A.Siva Sangari

IT Department, Sathyabama University , Jeppiar Nagar
Chennai, Tamil Nadu, India
siva.kumaresh08@gmail.com

J.Martin Leo Manickam

ECE Department, St Joseph College of Engg
Chennai, Tamil Nadu, India
josephmartin_74@yahoo.co.in

Abstract

In recent year, the increasing number of wearable sensors on human can serve for many purposes like emergency care, health care remote monitoring, personal entertainment and communication etc. The healthcare application is used for 24 hours constant monitoring without disturbing day to day activities. The WBAN enables the medical applications to be developed using electronic devices and sensors. The WBAN is created by wearing small sensors on the human body. In this paper we propose a low cost and high quality electro cardiography and diagnostic system for healthcare applications . A major issue is how to preserve security and privacy of patient's medical healthcare information over wireless communication. The energy consumption and data security are still major challenges in healthcare applications. This paper based on light weight security algorithm. Skipjack is the secret key encryption algorithm which provide the secure communication between sensor node and mobile node. The proposed algorithm protect the patient data against eavesdropping attack.

***Keywords*: Wireless Body area network ; Electro cardiogram signal**

1. Introduction

The wearable sensors can be placed on the patient's body for pervasive and health monitoring for healthcare applications. A BANs consist of set of bio sensors which are wearable or implanted in to the human body for monitoring patient parameters like heart rate, pulse, pressure, temperature and oxygen saturation. The sensors have limited energy, power, computational capabilities, There is a need for securing medical data over wireless communication. It is important to give the safe data and satisfy the requirements of confidentiality, integrity and data freshness. Cryptography and authentication methods are used for securing data over wireless communication. The creation, deletion, modification ,storage and access of data need strict regulations. The WBANSs resemble wireless sensor networks in many aspects especially resource constrained networks. The wireless nature of WBAN enables patient do their daily activities without much constraints. The smart phone collect the data from sensors and send the data periodically to the health care. The real time patient monitoring system need the following requirements like

- Quality and reliability
- Power management
- Context awareness
- Security and privacy

The wearable sensors monitor both mobile and immobile patients in real time. The emergency data have the highest priority during the data transfer operation. In this paper we study the issues of patient monitoring from the viewpoint of mobile healthcare, and show how current secure strategies are applied to achieve the security and privacy requirements. Cryptography and authentication service are designed to provide secure data service in BAN through wireless communication. The design of an efficient key management in BAN is still challenging problem. security issues in BAN are very important because sensitive medical information must be protected from unauthorized users. In symmetric encryption ,the same key is used for both sender and receiver

side. We need to generate the different keys for continuous patient monitoring. This makes key management process complicated since the receiver side may not know in advance about which key is used.RC5 and skipjack are more appropriate for resource constraint devices. But RC5 requires key schedule is pre computed. So we selected 64 bit block cipher skipjack algorithm .

The rest of the paper is structured as follows. In section II we presented the related work and then discussed their security weakness. The section III describes the system model as well as different types of sensors. Section IV described the proposed model. Section V provided theoretical analysis and performance evaluation of proposed algorithm. Finally section VI concluded the paper.

2. Related Works

Krishna K. Venkatasubramanian et al() [3] proposed physiological-signal-based key agreement (PSKA), a scheme for enabling secure inter sensor communication within a BAN in a usable (plug-n-play, transparent) manner. PSKA allows neighboring nodes in a BAN to agree to a symmetric (shared) cryptographic key, in an authenticated manner, using physiological signals obtained from the subject. No initialization or pre deployment was required; simply deploying sensors in a BAN is enough to make them communicate securely.

Wei Wang, et al proposed the inter-pulse interval (IPI) signal pattern at transmitter side was summarized as a biometric authentication key using Gaussian mixture model (GMM) [9]. At the receiver side, a light-weight signature verification scheme was adopted that used IPI signals gathered locally at the receiver. The proposed authentication scheme has the advantage of high sample misalignment tolerance. The major contribution of this GMM approach was to apply stochastic pattern recognition to ECG signal security, which was fundamentally different from the traditional approaches.

In symmetric encryption, the same key is used for both encryption and decryption. For continuous remote patient monitoring we need to generate more number of keys for data security. The key management also complicated. In public key encryption two keys are used for encryption and decryption. The encryption key is used in WBAN and the decryption key is placed in random location.

IBE is the form of asymmetric cryptography[5]. The public key can be generated from arbitrary input string. The public key generation process was independent of secret key generation. The light weight IBE was suitable for wireless body area network. It was suitable for resource constraints devices. Each secret key was computed from linear combination of master secret key. If more than n number of secret keys was delivered ,then adversaries were able to capture the master secret key.

Triple-DES was too slow for software implementation in embedded medical PDAs or sensors. We found that the RC5 and skipjack to be most appropriate for embedded microcontrollers. Although RC5 is slightly faster. Also, for good performance, RC5 requires the key schedule to be pre-computed, which used 104 extra bytes of RAM per key. Because of these drawbacks, we selected Skipjack.

3. A Body Area Network Implementation for Healthcare

BANs is a network of wearable or implantable sensing nodes. The sensing nodes collect all health information and forward it to the sink node. The sink node forward the data to healthcare persons through internet. The sensing element consist of sensing node, analog to digital convertor, processor, memory. The threats faced by BAN are adversaries eavesdropping the wireless communication and also inject messages ,replay old messages. The medical data collected from different sensors can be centralized before passing on to the external network. The wireless technologies like Bluetooth and zigbee can be used for inter BAN communication. But communicating with external networks GPRS(general packet radio service) can be used. The security issues of BAN is very important. Because the sensitive information must be protected from unauthorized users.

Due to the sensitive and broadcast nature of WBAN face the lots of threats. Outside attackers can eavesdrop all messages ,modify messages, replay old messages. It was not usually to fix the fixed keys for data transmission between the BAN nodes and also BAN nodes and Mobile .Because the single encryption key will provide a large amount of cipher text for hackers to crack the data. Compared to the wireless sensor networks, it is easier to launch attacks in WBAN .To address above challenges this paper makes the following contribution. We are developing the WBAN with wireless communication facility. We have built the following wearable sensors.

1. ECG Sensor

ECG works mostly by detecting and amplifying the tiny electrical changes on the skin that are caused when the heart muscle "depolarizes" during each heartbeat. At rest, each heart muscle cell has a charge across its outer

wall. Reducing this charge towards zero is called de-polarization, which activates the mechanisms in the cell that cause it to contract.

2. Pulse Oximeter

Pulse oximetry is a non-invasive method allowing the monitoring of the saturation of a patient's hemoglobin. A sensor is placed on a thin part of the patient's body, usually a fingertip or earlobe, or in the case of an infant, across a foot. Light of two wavelengths is passed through of the absorbance due to the pulsing arterial blood alone, excluding venous blood, skin, bone, muscle, fat.

3. Temperature Sensor

The temperature sensor in which some physical change occurs with temperature, plus some means of converting this physical change into a numerical value (e.g. the visible scale that is marked on a mercury-in-glass thermometer. We have made the low cost RF board which has the following features. The heart of the RF board is micro controller and radio transceiver. The following fig 1 describes the general WBAN architecture.

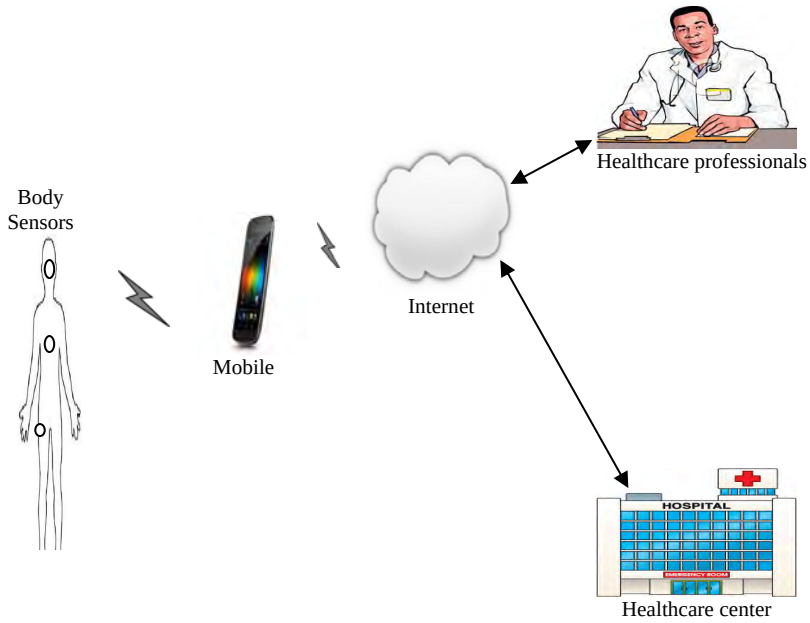

Fig 1 WBAN Architecture

Our sensor applications hardware consist of temperature sensor, ECG sensor, pulse oximeter. The heart of our RF board is micro controller. The RF board is attached to the sensors and we uses CC2430 as Texas instrument as RF and MCU. The CC2430 is small and low power consumption ships for zigbee communication. The sensor nodes are collect the signals from human body. The filtering process is used to increase the signal strength and also reduce the noise from the signal. Then an analog to digital conversion is applied to the signal for conversion of analog to digital signal. The digital signal is stored in micro controller. The micro controller will transmit the data via radio transceiver. Three sensor nodes are built on the common PCB board.

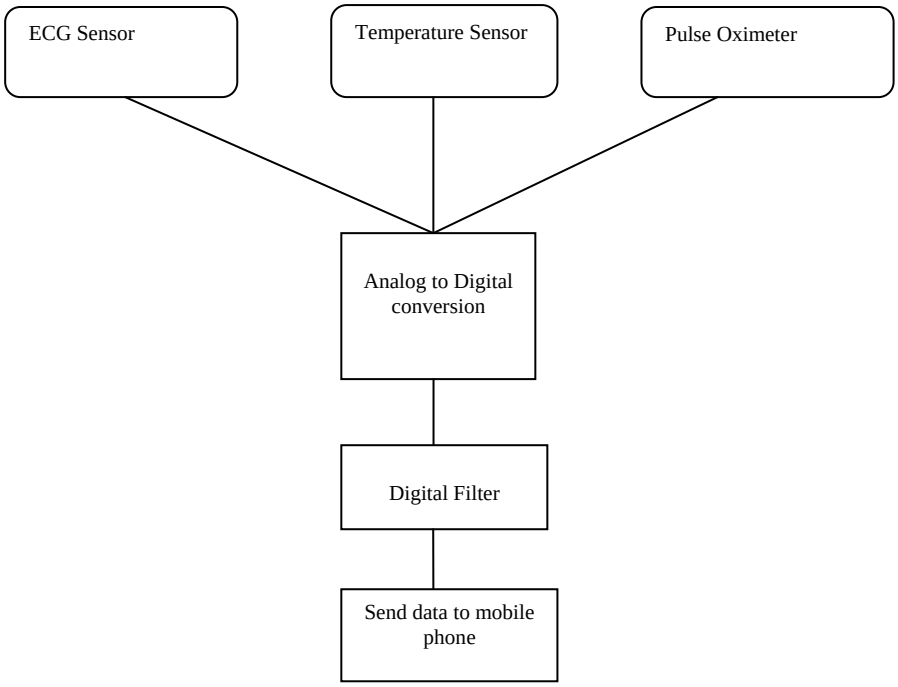

Fig 2 Flow diagram of a sensor hardware

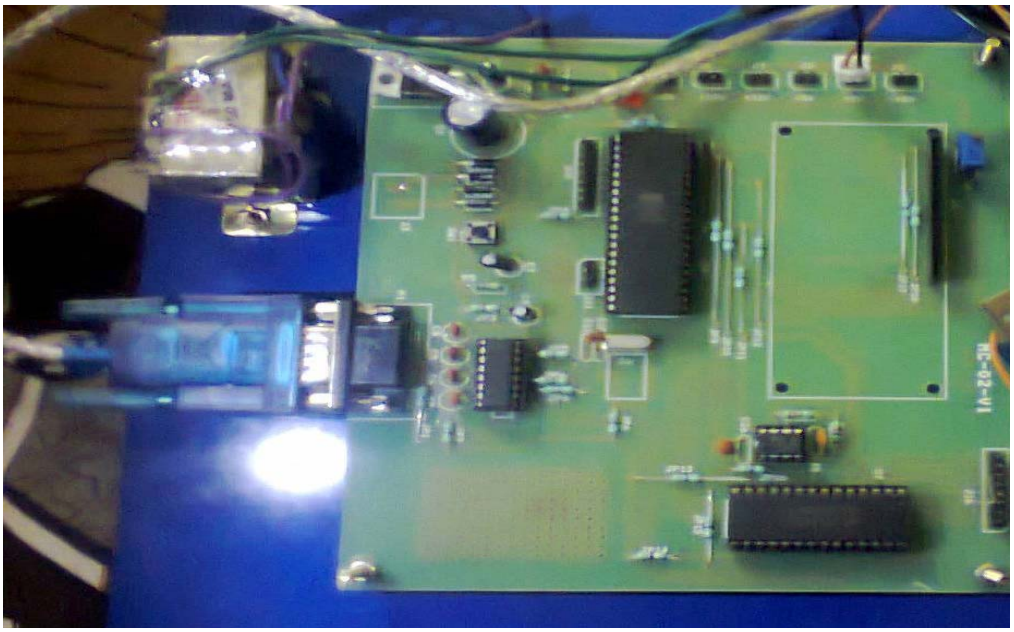

Fig 3 Sensor Hardware

4. Data Security

The wireless communication and sensor technologies have provided lot of benefits still there are many problems about the security and privacy in WBAN. Security issues in WBAN are very important. Because we need to protect the very sensitive medical information from unauthorized users. We have developed the low cost and low energy, low overhead method for securing the data. The existing conventional security methods are not suitable for resource constrained sensor networks. The skipjack algorithm most appropriate for sensor network. Skipjack is a block cipher that supports a 64 bit block size and a 80 bit key. The block is divided into 16 bit words and each round perform the permutation to one word from the block. It performs two different types of round functions ,A rounds and B rounds .Each encryption consist of totally 32 rounds. The rounds to be

performed in the order of 8 A rounds and then 8 B rounds, then another 8 A rounds ,finally finish with 8 B rounds. The Skipjack algorithm takes an 80 bit key which is broken up into 10 bytes, four of which are used per round. Skipjack iterates through 32 rounds in all, 8rounds of round A , 8 rounds of round B , and then repeats once more[2].

The A rounds and B rounds are described here:

$A(a ,b ,c ,d) = (d +G_k(a)+counter ,G_k(a),b , c)$,

$B(a ,b ,c ,d) = (d ,G_k(a), a +b + counter , c)$

The G_k box takes 16 bit input and 4 byte sub key. For each round 32 bit sub key is derived from 80 bit key. The 80 bit key is split into 10 bytes like k_0 to k_9. Each round uses 32 bit key as sub key. The first round uses k0,…,k3,the second round uses k4,…,k7 and the third round uses k8,k9,k0,k1.

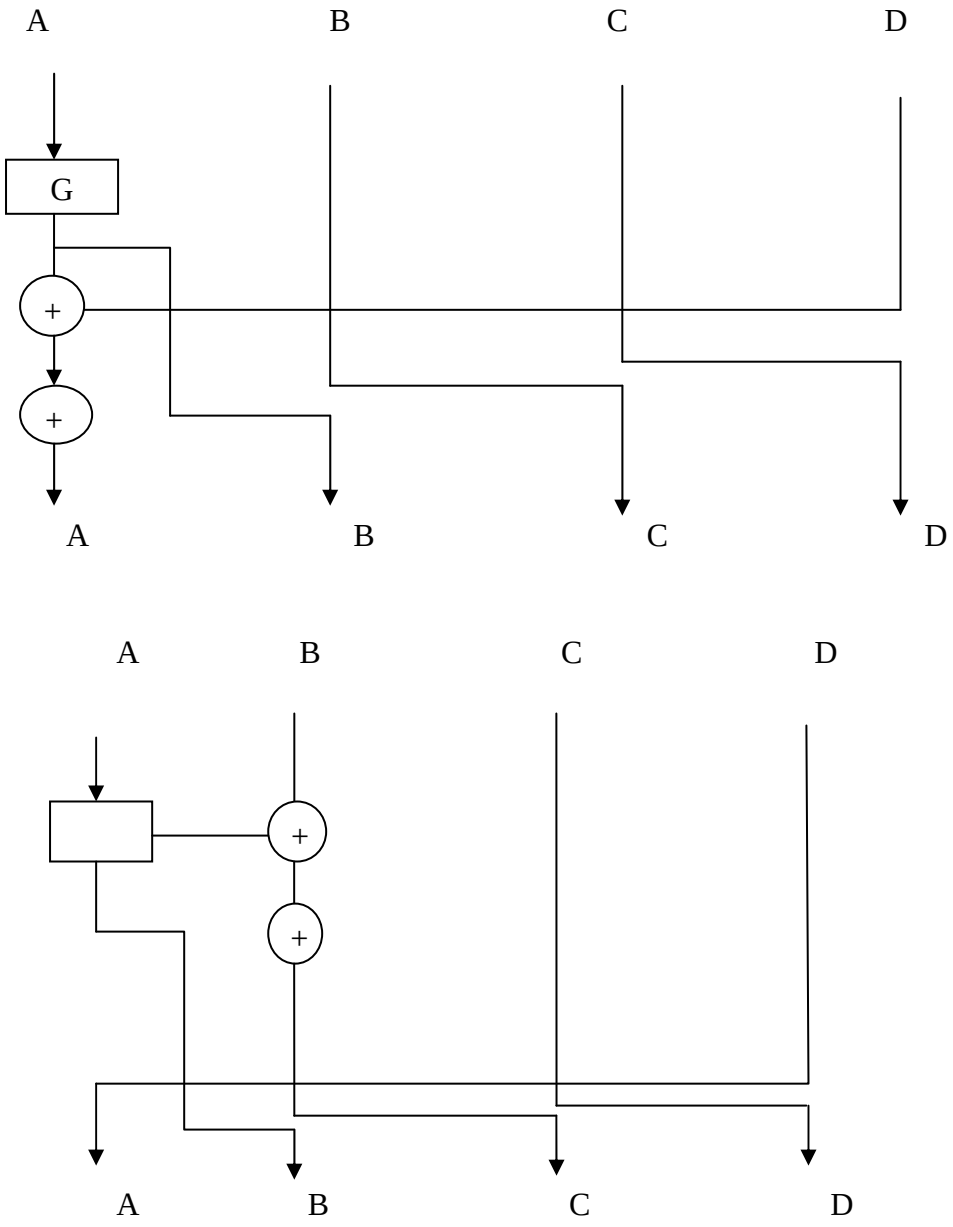

Fig 5 Round B function

In this paper '+' denote exclusive or operation and counter denotes the counter value and it start from 1 to 32 rounds. The G_k takes 16 bits input and 4 byte sub key .The 80bit key is split into 10 bytes like k_0 to k_9 . Each round takes 4 bytes use as its sub key. The skipjack A rounds and B rounds closely related to their internal structure. The structure of round B is inverse of round A. To decrypt a cipher text, it reverses the key schedule and the order of the rounds as well as all the arrows in the feistel structure. The following fig 6 shows the secure data transmission between the sensor nodes and mobile device or laptop. The sender information is encrypted by using skipjack algorithm and then calculate the hash value for key and sensor data. These results sent it to the receiver side. The receiver again calculates the hash value for encrypted message. If both values are equals, then only the authentication is successful. The secure one way hash function can be used for generating the keys. A one way hash function take arbitrary length input data and produce fixed key values. It is challenging to securely deliver the data from the sensor head to mobile nodes. In each WBAN ,exactly one sensor is chosen as cluster head. The cluster head collect all information and transfer it to mobile nodes. We have used the skipjack for securing data between cluster head and mobile nodes .

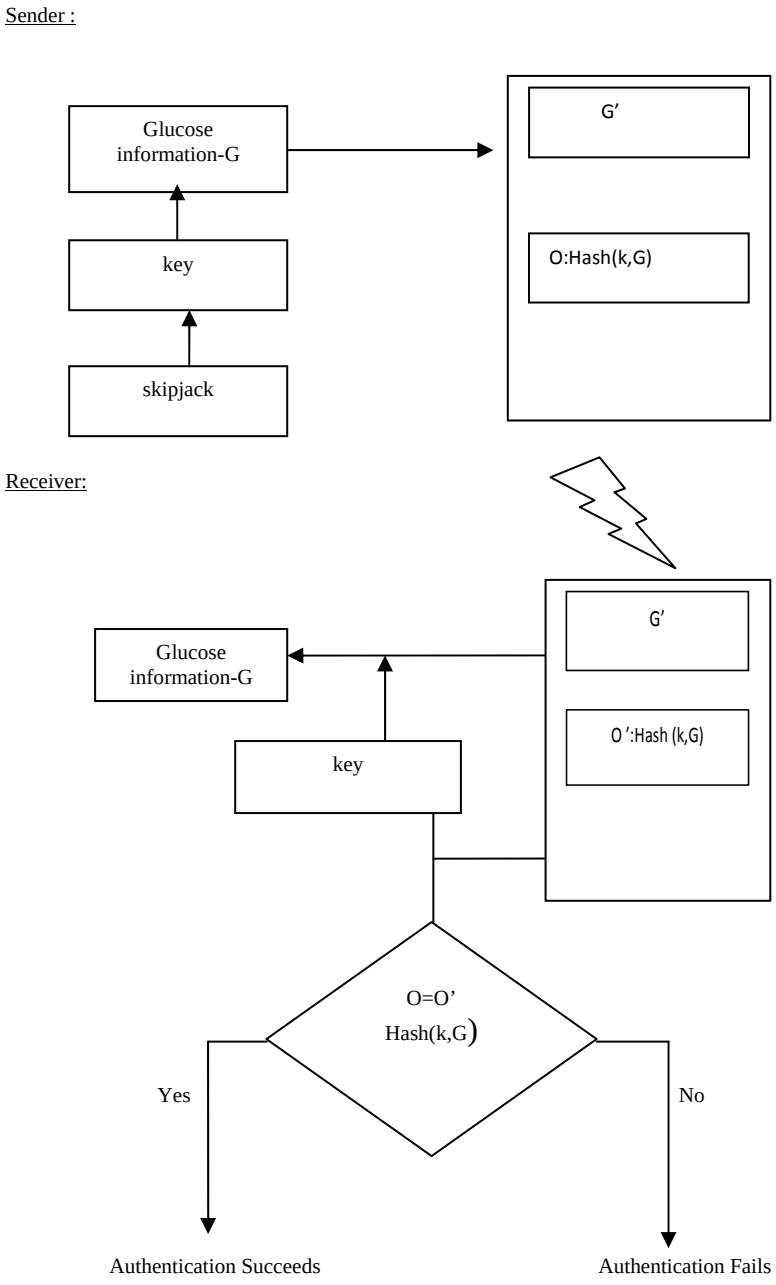

Fig 6 Skipjack authentication Scheme

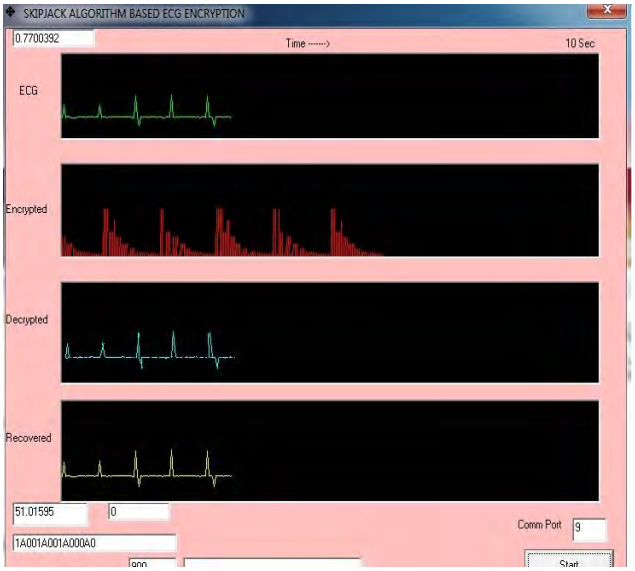

Fig 7 Recovered ECG signal

5. Performance Analysis And Evaluation

In this section ,we validate the proposed scheme. In this validation process ,the ECG signals are downloaded from MIT-BIH arrhythmia data base. This data base contain two ambulatory ECG signals. We can evaluate our algorithm using experiments conducted on commercial available products. The proposed security algorithm shows significant power savings over RSA algorithm. The skipjack is most optimal for sensor nodes ,since its operation and key schedule makes its suitable for sensor nodes and also building blocks are simple and the wireless technology of electronics is growing day by day. Using this technology, sensor-network arrangement such as distributed and self-organization can be constructed. A portable biomedical system can be build based on the network types available, which can monitor the patient's health in real time. This system applies Zigbee communication protocol, and uses the RF transceiver. It has the characteristics of low power consumption, low cost, flexible structure and accurate measurement, and it can achieve the long-distance monitoring of patients condition in real time .The ordering of A rounds and B rounds make harder to detect the cipher text. The permutation used in this algorithm which maximize the security and minimize the minimize the bad interaction between the two rounds.

In this paper, we have described the design procedure and results on tele-healthcare in nursing homes through wireless sensor networks. Our research in this field included medical sensor design, signal transmission, medical privacy and security and so on. Our results showed the feasibility of applying wireless sensor networking to medical monitoring anytime and anywhere. The adversaries able to eavesdrop all information within BAN. The proposed scheme is to keep data confidentiality and authenticity. Our future work is to build a larger-scale networking system with more lightweight security schemes.

Here we analyze the security of our proposed algorithm. Encryption and decryption are performed in sender and receiver side. The adversary eavesdrop on information from sensor nodes. The proposed algorithm encrypt all data before the data transmission .So, the adversary not able to capture the information. The skipjack was able to provide an encryption time of 25 µs per byte. The AES was also provide an encryption time of 50 µs per byte. The RC5 had an average encryption time of 33 µs per byte. The skipjack was also best algorithm in terms of memory .Because it needed only average 2600 bytes of RAM. The other algorithms needed 8000 bytes. The following fig 8 shows the average encryption time of various algorithms. We see that AES require more encryption time than skipjack. The fig 9 shows the amount of storage needed for different algorithms.

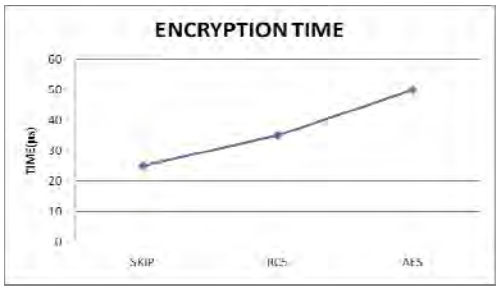

Fig 8 Encryption time per byte

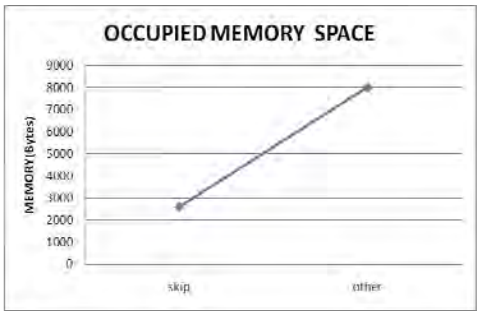

Fig 9 Amount of storage needed for encryption

6.Conclusion

The secure communication within the BAN is required to keep the patient's privacy and security. In this paper, we present skipjack algorithm in which security and privacy is to be maintained in authenticated manner. Our major contributions in this paper include 1) Hash based authentication approach in both sender and receiver side 2) Skipjack algorithm for secure data transmission. Our studies show that the proposed scheme is a light weight and energy efficient scheme. We provided the detailed discussion on privacy and security in health care applications. We have implemented the wireless healthcare monitoring system and demonstrated the proposed model is more practical. Our results showed the feasibility of applying wireless sensor networking to medical monitoring anytime and anywhere. Our future work is to build a larger-scale networking system with more lightweight security schemes

References

[1] Zhaoyang Zhang .;Honggang Wang .; Athanasios 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 .

[2] Lars Knudsena; , David Wagnerb,; On the structure of Skipjack,; ElseveirDiscrete Applied Mathematics 111 (2001) 103–116.

[3] Krishna K. Venkatasubramanian.; Member, IEEE, 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] A. Fort, J. Ryckaert.; C. Desset.; P. De Doncker.; P. Wambacq,.; and L. Van Biesen.; Ultra wideband channel model for communication around the human body *IEEE J. Selected Areas Commun.*, vol. 24, no. 4, pp. 927– 933, Apr. 2006

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

[6] Shnayder et al; Simulating the Power Consumption of Large-Scale Sensor Network Applications, *SenSys'04,* November 3–5, 2004.

[7] C. C. Y. Poon.;Y.-T. Zhang.; and S.-D. Bao.; A novel biometrics method to secure wireless body area sensor networks for telemedicine and M-health, *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 73–81, Apr.2006.

[8] J. Elson.; L. Girod, .; D. Estrin, ;Fine-grained network time synchronization using reference broadcasts, in *Proc. 5th Symp. Oper. Syst. Des.Implementation*, 2002, pp. 147–163.

[9] Wei Wang,; Honggang Wang,; Dongming Peng,; Hamid Sharif,; Secure Stochastic ECG Signals Based on Gaussian Mixture Model for e-Healthcare Systems, IEEE Systems Journal, Vol. 5, No. 4, December 2011

[10] D. J. Malan.; M. Welsh.; and M. D. Smith; A public-keyinfrastructure for key distribution in TinyOS based on ellipticcurve cryptography, in *Proc. IEEE 2nd Int. Conf. Sens.AdHocCommun. Netw.*, Oct. 2004, pp.71–80.

[11] A. Banerjee.; K. Venkatasubramanian.; S. K. S. Gupta ; Challenges of implementing cyber-physical security solutions in body area networks, presented at the 4th Int. Conf. Body Area Netw., Los Angeles, CA, Apr.2009.
[12] A. J. Menezes.; P. C. van Oorschot, .; S. A. Vanstone.; Handbook of Applied Cryptography. Boca Raton, FL: CRC Press, Oct. 1996.
[13] F. M. Bui .; D. Hatzinakos; Biometric methods for secure communications in body sensor networks: Resource-efficient key management and signal-level data scrambling,, in Proc. EURASIP J. Adv. Signal Process., 2008, pp. 1–16.
[14] E. S. Reddy.; I. R. Babu ; Authentication using fuzzy vault based on iris textures, in Proc. 2nd Asia Int. Conf. Model. Simul., 2008, pp. 361–368.
[15] W. J. Scheirer .; T. E. Boult, Cracking fuzzy vaults and biometric encryption, in Proc. Biometrics Symp., Sep. 2007, pp. 1–6.
[16] A. Kholmatov.; B. Yanikoglu; Realization of correlation attack against the fuzzy vault scheme, *SPIE Security, Forensics*, Steganography,and Watermarking of Multimedia Contents X, vol. 6819, pp. 1–7, Jan. 2008.
[17] P. Mihailescu. (2007, Aug.). The fuzzy vault for fingerprints is vulnerable to brute force attack. The Computing Research Repository. [Online]. Available:http://www.citebase.org/abstract?id=oai:arXiv.org:0708.2974
[18] K. Venkatasubramanian.;A. Banerjee, .; S. K. S. Gupta; Green and sustainable cyber-physical security solutions for body area networks, in Proc. 6th Int. Workshop Wearable Implantable Sens. Netw. (BSN 2009), Washington, DC,pp240–245.
[19] Fei hu.;Sunil kumar.;Yang xiao.;Towards a secure RFID/Sensor based Tele cardiology system,2007 IEEE.
[20] Marina Sukor.;Sharifah Ariffin .; Norsheila Fisal and S.K. Syed Yusof.; Adel Abdallah.; performance study of wireless body area work in medical environment,second asia international conference on modeling and simulation,2008 IEEE.
[21] Dr. Shinyoung Lim.; Dr. Tae Hwan Oh.; Dr. Young B. Choi.; Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring, 2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing .
[22] Kathy Dang Nguyen.; Ioana Cutcutache.; Saravanan Sinnadurai .; Shanshan Liu.; Fast and Accurate Simulation of Biomonitoring Applications on a Wireless Body Area Network ; 2008 IEEE.