Vol 4 Issue 8 Sep 2014

ISSN No : 2230-7850

International Multidisciplinary Research Journal

Indian Streams Research Journal

Welcome to ISRJ

RNI MAHMUL/2011/38595 **ISSN No.2230-7850**

Indian Streams Research Journal is a multidisciplinary research journal, published monthly in English, Hindi & Marathi Language. All research papers submitted to the journal will be double - blind peer reviewed referred by members of the editorial board.Readers will include investigator in universities, research institutes government and industry with research interest in the general subjects.

International Advisory Board

Editorial Board

Address:-Ashok Yakkaldevi 258/34, Raviwar Peth, Solapur - 413 005 Maharashtra, India
Cell : 9595 359 435, Ph No: 02172372010 Email: ayisrj@yahoo.in Website: www.isrj.org

Indian Streams Research Journal
ISSN 2230-7850
Impact Factor : 2.1506(UIF)
Volume-4 | Issue-8 | Sept-2014
Available online at www.isrj.net

SECURITY AND PRIVACY IN WIRELESS BODY AREA NETWORK

Siva Sangari[1] and Martin Leo Manickam[2]

[1]Faculty of IT Department, Sathyabama University, Jeppiar Nagar, Chennai, India.
[2]Faculty of ECE Department, St Joseph College of Engg., Chennai, Tamil Nadu, India.

Abstract:-Wireless body area networks are a key component to the healthcare applications. The real time patient's medical data can be collected by using simple wearable sensors on the human body. The body sensors on patients gather all critical health information and report it to remote healthcare services immediately for monitoring real time conditions. We present the main characteristic and challenges associated with Wireless Body Area Network (WBAN) and present Elliptic Curve Digital Signature Algorithm (ECDSA) based authentication scheme. The proposed scheme authenticates the security between the aggregation node and base station. Security analysis shows our scheme can guarantee for data confidentiality integrity and authentication.

Keywords: Wireless Body Area Network, ECDSA, Elliptic Curve Cryptography, Electro Cardiogram Signal.

I.INTRODUCTION

The use of wireless sensors provides the improvement in quality of healthcare and also reduced storage costs, improved data availability and sharing. The sensors can be placed on a human's body for real time healthcare monitoring. The WBAN provides great convenience to patients and also medical users. Real time monitoring enables patients to retain their daily life. Each WBAN that connects all sensor nodes that are placed on the human body. Each sensor is connected to a microprocessor, transceiver and battery and also integrating with outside network via wireless technologies. The star topology is always preferred for WBAN because the master node aggregates all information from the sensor nodes and also acts as gateway to the outside the networks. The transmission of medical data over wireless link is very critical. The hackers not only affect the patient's privacy also compromise the security by modifying the medical data. Without security guarantees, the medical information may be leaked causes incorrect diagnosis and treatment .The adequate security features ensures the WBAN by data confidentiality, integrity and availability. To address the security issues in WBAN, we proposed the ECDSA based security and authentication scheme that provide the secure transmission between the aggregation node of patient with base station.

The remainder of this paper is organized as follows .In section II we discuss the related works in WBAN. In section III, we show the security architecture of WBAN and also security services. In section IV, we analyze the proposed scheme problem and also two tired authentication scheme. In section V, we discuss our experimental results and analyze the proposed scheme. Finally conclusions and future work described in section VI.

II.RELATED WORK

With the advance in wireless and networking technologies, WBAN is important key component in healthcare applications. Several security solutions are proposed to secure WBAN. In order to secure the inter sensor communications, the idea of employing physiological sensors was introduced in [1]. The purpose of OPFKAV is to provide the secure inter sensor communications by enabling the two sensors to agree on a symmetric key based on

common physiological signal collected by the senor nodes. It does not require any key pre distribution.

The wearable health monitoring system[2] has star topology for each patient which is connected via mobile network to healthcare provider. Physician can access the data via internet. The authors in [3] proposed a new solution to access the patient data in real time and provide the emergency services. Medical data can be prioritized based on emergency condition. Based on the emergency condition based service aims at improve the quality of service.

The authors in[4] proposed a new secure and privacy technique, called SPOC. With SPOC, the efficient user centric control which is based on attribute based encryption. The proposed frame work can help the medical users with reliability and also proposed scheme reduced the communication overhead. Recently, the resource aware secure ECG based real time monitoring [5] was proposed. The cross layer frame work was introduced for remote monitoring. The important medical information was identified and protected by using selective encryption and compression. The proposed scheme balance the energy efficiency and transmission quality and performed unequal resource allocation and emergency signal detection with low delay.

The security challenges in WBAN are eavesdropping, interception of medical data and unauthorized access. The hacker is able to read the transmitted data and also inserts ,changes and deletes the medical information transmitted between the nodes. If health information of a patient can be modified, it will lead to wrong diagnosis treatment. The unauthorized user gain access to WBAN by masquerading as real users.

III.SECURITY THREATS AND WBAN ARCHITECTURE

Security in wireless body area network is very important. Because, the medical information must be protected from hackers that could be dangerous to the life of user. The security solutions proposed for wireless sensor networks are not suitable for WBAN. WBAN require some specific solutions. The following constraints are

1.Low Power: The sensors use the power to perform their task including signal detection and communication. During the charging, the temperature also increased. The human body can tolerate only limited amount of heat.
2.Memory: The memory capacity of bio sensor is very limited. So implementation of algorithm and key management only take minimum amount of memory.
3.Low Computation: The bio sensors have low computation power. Because sensors have very limited memory capacity. It cannot do the big calculations.

The security attacks affect the capacity and performance of the WBAN. The attacks can be categorized based on OSI layer model [6].

1.Physical Layer: The attacks on physical layer is jamming and tampering. Jamming refers to the interference with radio frequencies of WBAN .The adversaries use few nodes to block the entire network .Tampering refers to node is physically damaged by hackers.
2. Data Link Layer: The hackers are able to corrupt the data during the transmission. The receiver side is not able to receiver is not able to receive the entire data. Data authentication and integrity are needed for secure data transmission.
3.Network layer: The hacker complicates the data transmission by routing loops and selective forwarding. The other attacks are sinkhole and wormhole attack.
4.Transport layer: The main threats to transport layer are flooding and resynchronization attacks .The authentication is needed for secure data transmission.

For the above security risks in WBAN, security has been important concern in WBAN. The security structure of WBAN is to provide the following services for secure medical data transmissions.

1. Data Encryption: The data is encrypted before the data transmission .The data encryption provides confidentiality against the attacks.
2. Data Integrity: The receiver can make sure that the data is not modified by someone and verify the data coming from originated sender.
3. Data Freshness: The user always able to access the fresh data.

IV. WBAN ARCHITECTURE FOR HEALTHCARE MONITORING

The WBAN architecture presented in this paper includes the several components as shown in fig1.The different types of sensors used for patient body parameters. The different types of sensors deployed on human body such as ECG, pulse oximetry, respiration, blood pressure, blood sugar, temperature and humidity sensors. The following Fig.1 shows the general architecture of WBAN. The sensors placed on the human body are considered as

one cluster. The aggregation node is act as cluster head. The cluster head collects all information from sensor nodes and aggregates all information and forward the information to base station. The base station collects all information from all cluster heads and transfer data to remote users through internet.

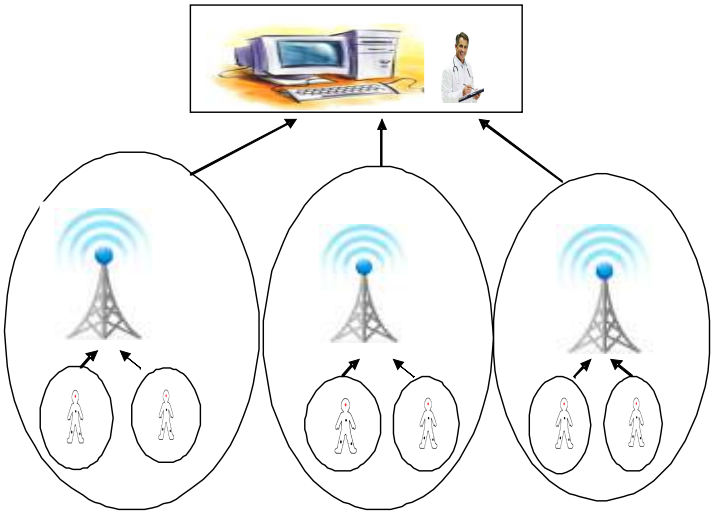

Fig.1 WBAN Architecture

IV.PROPOSED SCHEME

The idea behind the security of our proposed scheme is based on [8] elliptic curve cryptography. In our architecture, the sensor nodes and the data aggregation node are deployed on the human subject, while the base station is located away from the subject. The proposed method is based on elliptic curve based authentication. All the nodes in the network have public key and private key pair. Every calculate their public node key value Q by multiplying private key value d with generator point. The key pair will be Q=d*P. The mathematical equation of ECC satisfies the form: y2=x3+ax+b.The ECC parameters are (q ,a ,b ,P ,n ,h) where q is prime number defining elliptic curve ,a ,b are coefficients of elliptic curve ,P is generator point of elliptic curve , n is number that defines the order of P. The secure communication between the sensor nodes and base station achieved by using physiological signal based key generation and ECDSA scheme.

The secure communication is done by using the following steps The generated key must exhibit the randomness and distinctiveness properties. The ECG signal has been used for master key generation. The key value is generated from ECG signal. This key value km j extracted from ECG signal . The time is divided into fixed number of seconds and sensor collects the single item per second[7].

1.ECDSA key pair generation

1)Select the random integer d which is in the interval[0,n-1]
2)Compute Q=D*P where D is private key and Q is public key

2.Signature generation

1)The element node want to sign the message m ,it follows these steps
2)Calculate e=hash(m)
3)Z be the ln leftmost bits of e
4)Select a random integer k from [1,n-1]
5)Calculate the curve point (x1,y1)=k*G
6)Calculate r=x1 mod n. If r=0, go back to step 3.
7)Calculate s=k-1(z+rdA) mod n. If s=0, go back to step 3.
8)The signature is the pair (r,s).

3.Signature verification

1)Verify that r and s are integers in [1 , n-1]. If not, the signature is invalid.

2)Calculate e=HASH(m), where HASH is the same function used in the signature generation
3)Let z be the Ln leftmost bits of e.
4)Calculate w=s-1 mod n.
5)Calculate u1=zw mod n and u2=rw mod n.
6)Calculate the curve point (x1, y1) = u1 x G + u2 x QA
7)The signature is valid if r=x1 (mod n), invalid otherwise.

4.Before verifying the sensor node Sj signature's on the message, the base station need to calculate the domain parameters and public key Q. The sensor nodes send the message to the base station consisting of the following information : node ID, nonce value x1,message, key value km .A message authentication code value is calculated for the entire things and encrypted by base station's public key QB .The sensor node sends the encrypted information and signature value of message to the base station.
5. The base station verify the signature. If the signature is verified successfully it sends an acknowledgement to the sensor node Sj. informing that the signature is verified and message is received and nonce value x2. If signature verification fails ,the head node request to element node for another message and its signature. This process continues until an acknowledgement received.
6.After the signature verification ,the base station decrypt the data using its private key and recalculate the MAC value. The sensors send the reply to the base station containing x1 and x2.Then the key value k is combined with x1 and x2 generate the shared secret key ks which is used for encryption and decryption process. The following Fig.2 shows the proposed authentication scheme for secure data transmission.

TABLE I
List Of Notations Used In This Paper

Symbol	Definition
D_s , Q_s	Private key and public key of sensor node
D_b, Q_b	Private key and public key of base station
G	Elliptic curve base point
k_m	Master key
x1,x2	Nonce values
k_s	Shared secret key
Sign(m)	Signature value of message
MAC	Message authentication code
(r, s)	Signature

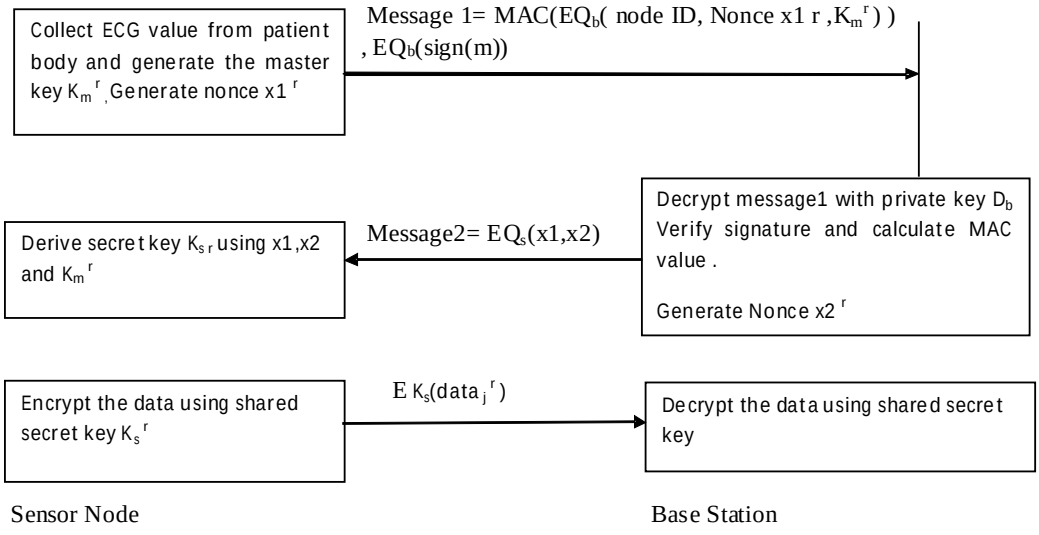

Fig 2 Mutual authentication between the sensor node and base station

V.PERFORMANCE ANALYSIS

In this section we have analyzed the key generation time and total number of messages exchanged and key storage. In our work, we combined physiological signal based key value generation and elliptic curve digital

signature algorithm. We used java programming for our implementation. The cluster head maintains the one private key and public key pair and m shared key and m signatures for each CH. All total CH stores 2m+4 keys . For cluster head key generation, the following number of messages are exchanged 1) Sensor node sends the signature of the message 2) Sensor node sends an encrypted message 3) Cluster head reply with request for another message or sends an acknowledgement to the sensor node .

Eavesdropping Attack: In this attack, the hacker eavesdrop the message transmitted from sensor node to base station. The proposed approach encrypts the master key value generated from physiological signal using public key. The hacker not able to eavesdropping the information.

Replay Attack: In replay attack, the medical information is repeated or delayed maliciously. To prevent this attack, the nonce values are generated from both sender and receiver side.

Confidentiality: The hacker is not able to obtain any cipher text information. Because physiological value is sent in the encrypted form. The hacker not able to find the key value.

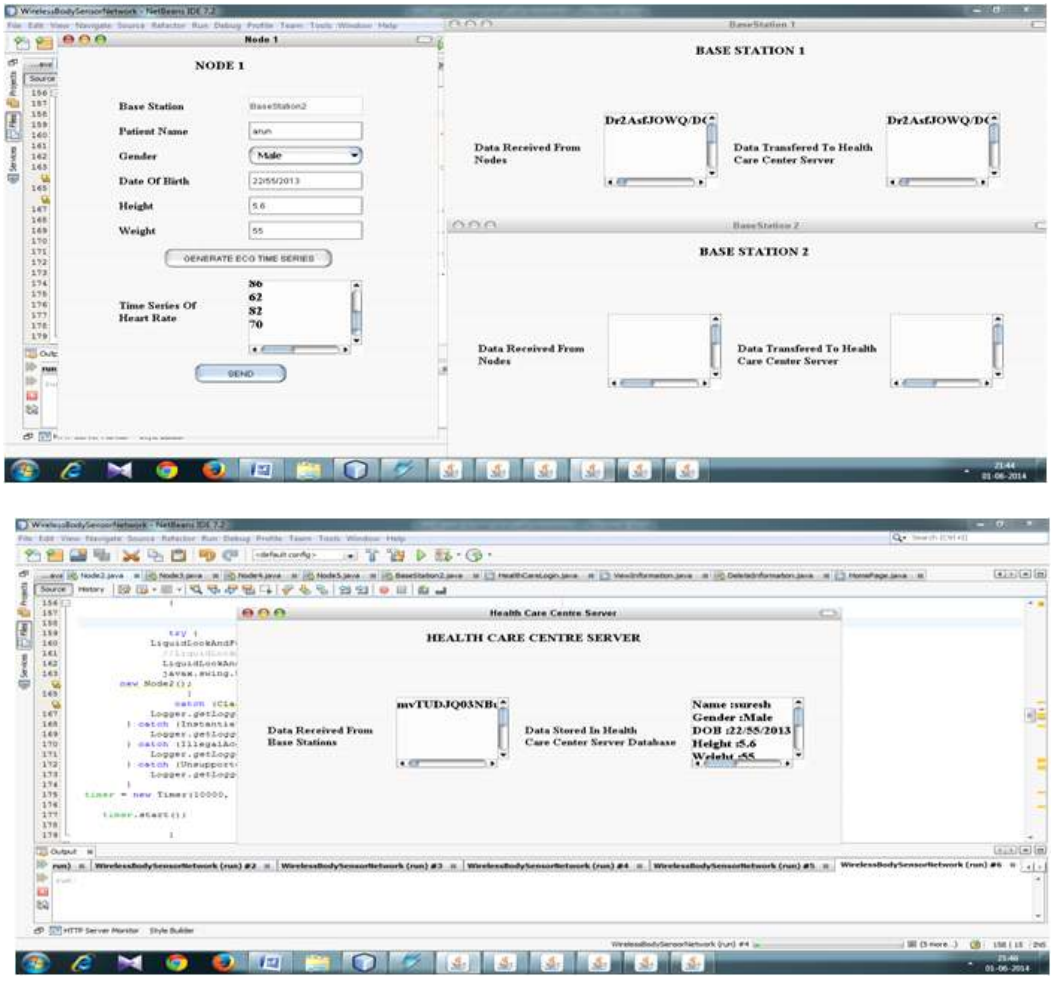

Fig 4 Data Transferred to Database

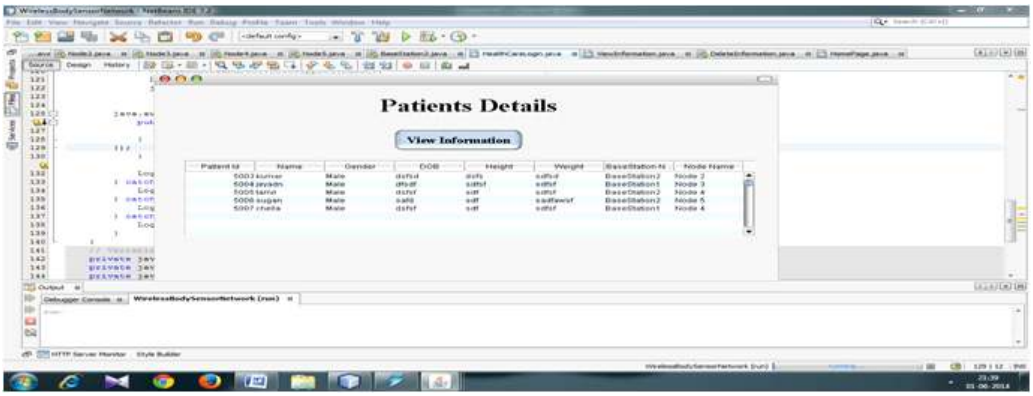

Fig 5 Data Stored In Database

VI.CONCLUSION

We have proposed a ECC based security scheme to achieve confidentiality, integrity and authentication in wireless body area network. The security analysis and experimental results shows that our scheme is suitable for real time applications. In our approach the ECG signals are used for generating the master key and using ECDSA algorithm for signature generation. The proposed scheme is light weight and energy efficient security solution for WBAN. The performance of proposed scheme can be further improved by extracting more features from WBAN and also implement the proposed scheme in hardware platform.

REFERENCES

1.OPFKA: Secure and Efficient Ordered-Physiological-Feature-based Key Agreement for Wireless Body Area Networks Chunqiang Hu_y, Xiuzhen Cheng_, Fan Zhang_, Dengyuan Wu_, Xiaofeng Liaoy, Dechang Chen z©2013 IEEE

2.Enabling Technologies for Wireless Body Area Networks: A Survey and Outlook Huasong Cao and Victor Leung, University of British Columbia Cupid Chow and Henry Chan, The Hong Kong Polytechnic University,2009 IEEE

3.Patient Vital Signs Monitoring using Wireless Body Area Networks Baozhi Chen, John Paul Varkey, Dario Pompili, John K-J Li, and Ivan Marsic Departments of Electrical and Computer Engineering and Biomedical Engineering Rutgers University, Piscataway, New Jersey 2010 IEEE.

4.Analysis of Using Interpulse Intervals to Generate 128-Bit Biometric Random Binary Sequences for Securing Wireless Body Sensor Networks Guang-He Zhang, Carmen C. Y. Poon, Member, IEEE, and Yuan-Ting Zhang, Fellow, IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE, VOL. 16, NO. 1, JANUARY 2012

5.SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency Rongxing Lu, Member, IEEE, Xiaodong Lin, Senior Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 3, MARCH 2013.

6.Resource-Aware Secure Ecg Healthcare Monitoring Through Body Sensor Networks Honggang Wang, University Of Massachusetts, Dartmouth Dongming Peng, Wei Wang, And Hamid Sharif, University Of Nebraska-Lincoln Hsiao-Hwa Chen, National Cheng Kung University Ali Khoynezhad, University Of Nebraska Medical Center IEEE Wireless Communications , February 2010.

7.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

8.Kriangsiri Malasri and Lan Wang, Computer Science Dept., University of Memphis" SNAP: An Architecture for Secure Medical Sensor Networks " IEEE 2007.

9.Huasong Cao and Victor Leung, University of British Columbia Cupid Chow and Henry Chan, The Hong Kong Polytechnic University "Enabling Technologies for Wireless Body Area Networks: A Survey and Outlook "IEEE Communications Magazine • December 2009

10.Wei Wang, Member, IEEE, Honggang Wang, Member, IEEE, Michael Hempel Member, IEEE,Dongming Peng, Member, IEEE, Hamid Sharif, Senior Member, IEEE, and Hsiao-Hwa Chen, Fellow, IEEESecure Stochastic ECG Signals Based on Gaussian Mixture Model for e-Healthcare Systems "IEEE SYSTEMS JOURNAL, VOL. 5, NO. 4, DECEMBER 2011

11.Jian Ren, Senior Member, IEEE, and Lein Harn "An Efficient Threshold Anonymous Authentication Scheme for

Privacy-Preserving Communications "IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 3, MARCH 2013
12.Hairong Yan, Hongwei Huo, Member, IEEE Youzhi Xu, and Mikael Gidlund, Member, IEEE "Wireless Sensor Network Based E-Health System –Implementation and Experimental Results "IEEE Transactions on Consumer Electronics, Vol. 56, No. 4, November 2010

Siva Sangari
Faculty of IT Department, Sathyabama University, Jeppiar Nagar, Chennai, India.

Publish Research Article
International Level Multidisciplinary Research Journal
For All Subjects

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication,you will be pleased to know that our journals are

Associated and Indexed,India

- International Scientific Journal Consortium
- OPEN J-GATE

Associated and Indexed,USA

- Google Scholar
- EBSCO
- DOAJ
- Index Copernicus
- Publication Index
- Academic Journal Database
- Contemporary Research Index
- Academic Paper Databse
- Digital Journals Database
- Current Index to Scholarly Journals
- Elite Scientific Journal Archive
- Directory Of Academic Resources
- Scholar Journal Index
- Recent Science Index
- Scientific Resources Database
- Directory Of Research Journal Indexing

Indian Streams Research Journal
258/34 Raviwar Peth Solapur-413005,Maharashtra
Contact-9595359435
E-Mail-ayisrj@yahoo.in/ayisrj2011@gmail.com
Website : www.isrj.org