SECURITY ARCHITECTURE FOR AT-HOME MEDICAL CARE USING BODY SENSOR NETWORK

S.S.Mohanavalli[1] and Sheila Anand[2]

[1]Department of Electronics and Communication Engineering, Tagore Engineering College, Chennai, India
ssmvalli@gmail.com
[2]Department of Computer Science, Rajalakshmi Engineering College, Chennai, India
sheila.anand@gmail.com

ABSTRACT

Body Sensor Networks have considerably facilitated the continuous measurement of physiological parameters of human body. The sensors used to measure the body parameters, have several limitations in terms of power, computation capability, memory and communication capability. In this paper a novel architecture has been proposed to ensure continuous, unobtrusive and remote patient monitoring, taking into account the inherent hardware constraints of the sensors. The proposed architecture would enable senior citizens, patients with chronic ailments and patients requiring post-operative care to be remotely monitored in the comfort of their homes. Security threats and challenges inherent to wireless communication of sensor data have been discussed and a security mechanism to ensure data confidentiality, integrity and authentication has been proposed.

KEYWORDS

data confidentiality, integrity, remote monitoring, authentication, fabrication

1. INTRODUCTION

Recent advances in electronics have seen the development of small biomedical sensors which can be either worn or implanted on a human body. A wireless network of such intelligent sensors is known as a Body Sensor Network (BSN). The sensors measure physiological parameters of the human body, like ECG, pulse rate and blood pressure. These sensor data are collected and transmitted to external medical server(s) for remote monitoring by medical professionals. [1]

Persons requiring critical care; patients who have undergone surgery or persons with chronic ailments require continuous health monitoring and real-time feedback for immediate action in emergency situations. The patients would be subjected to discomfort and inconvenience due to prolonged hospitalization. Frequent visits to the hospitals may also be required for follow up treatment and care. Use of BSN can provide an alternative solution for remote monitoring of patients residing in the comfort of the homes. Patients can move about and follow their daily routine without the necessity of being confined to their beds. Data obtained over a long period of time in the patient's natural environment would offer the doctors a better insight into the patient's health condition and such data can be analyzed to arrive at the correct diagnosis and provide the right care [2].

DOI : 10.5121/ijasuc.2011.2106

BSN can also be used for Geriatric care by providing assisted living to aged persons in the comfort of their homes. Such technology driven solutions can also greatly contribute in controlling the rising cost of health-care.

Communication of health related information between sensors in BSN and the remote medical server has to be strictly private and confidential to protect patient privacy [3]. The sensor data sent using Internet and wireless transmission, is prone to different types of attacks such as eavesdropping, sending false values or replay of previous data. Medical professionals have to be certain that the data is not tampered in transit or at the point of origin as proper diagnosis requires accurate data.

In this paper, we propose a novel architecture for continuous and unobtrusive monitoring of aged persons or patients requiring post-operative care [4]. Patients would be fitted with wearable sensors that measure physiological parameters at predefined intervals and the data would be transmitted to hospitals or health care centers for medical care and diagnosis. Sensors have limited power and transmission range and the computing power and memory availability would also be limited. Hence it would not be easy for each sensor to individually and directly send data to the remote server. In our solution, we have proposed the use of an At-Home Base Station for collecting and consolidating patient sensor data and also for handling communication with the remote server. This paper also addresses the security requirements of confidentiality, integrity and authentication for wireless communication within the confines of the house.

Section 2 discusses the work related to security of medical sensor data and body sensor networks. Section 3 details the proposed architecture for At-Home monitoring; Section 4 gives the features for securing the data transmission within the home premises, and simulation results. Section 5 presents conclusion and future work.

2. RELATED WORK

Communication and computing technologies are being increasingly applied in health care systems to improve the quality and to reduce the cost of health care. Ensuring individual privacy and confidentiality of medical data has become a major concern. This section discusses some of the work done on security for a wireless Body Sensor Network (BSN).

One of the earlier works on sensor security was the development of the SPINS [5] protocol suite. SPINS provides confidentiality and authentication using symmetric cryptography. It has two constituent protocols, SNEP provides confidentiality and authentication. μTESLA provides broadcast authentication. These schemes are however more generic in nature and the unique security requirements of medical applications were not addressed. Conventional public key cryptographic systems cannot be directly applied due to constraints in sensor power and memory.

The focus of current research on sensor network for medical applications is on the specific requirements of health care systems. The various threats in the network like interception, communication jamming and modification have already been discussed along with BSN [6]. In this a technical architecture that provides patient privacy and data security using encryption and Access Control Lists have been given. The downside of this work is the non-monitoring of architecture performance against the attacks. CodeBlue, a Harvard University project is one of the pioneers in medical monitoring [7]. The focus of the project is on the development of wearable sensors and related equipment. The need and importance of security for such systems had been acknowledged but the concerned issues were least addressed.

ALARM-NET is an Assisted-Living network for pervasive and adaptive healthcare in an assisted-living community [8]. It uses AES for encryption of data transmitted over the network. The paper discusses query management, context aware privacy, power management and IP network security. The security for the sensor data is provided by SecureComm, a link layer suite in TinyOS. The paper does not discuss issues related to key management or the attacks against which the architecture is secure. I-LIVING is an Open System Architecture for Assisted Living [9]. It proposes a three - tier architecture, to provide data confidentiality and link level authentication using context information like authentication certificates and encryption keys stored in USB sticks. This requires pre-configuration of devices in the network to recognize the USB. Wireless Sensor Network for Wearable Physiological Monitoring [10], discusses a wearable jacket embedded with sensors that monitor the physiological parameters. The sensed values are sent to wearable data acquisition hardware to continuously monitor the physiological parameters and transmit by wireless communication to a remote monitoring station. Security aspects for the wireless transmission between the sensor network and data acquisition hardware and between the data acquisition hardware and the remote station have not been mentioned. SNAP [11], Sensor Network for Assessment of Patients specifically addresses security issues such as data confidentiality, authentication and key exchange. The key exchange is based on ECC; the sensor data is encrypted using RC5 algorithm and HMAC is used for authentication. This work also discusses the query mechanism used for accessing the sensor data. The proposed architecture appears more relevant for continuous patient monitoring in hospitals or large health care centres with many patients. The wireless sensor mote fitted on the patient collects the sensor data and transmits them directly to the nearest base station. Several such base stations have to be provided to pick up signals from the patients.

Cherkuri et.al. discuss the use of biometrics for securing the communication between the sensors implanted in the body [12]. They propose a system model in which the biosensors form a network among them and communicate wireless through single or multi hops to a control node. The control node sends data to a base station using wireless transmission. They suggest using asymmetric encryption between the control node and the base station. The paper mainly concentrates on key generation and exchange between the biosensors. This work does not take up any other security features. The architecture used by the IM3 project consists of Wireless Body Area Network [WBAN] on each patient, an external network and a back-end server [13]. Each WBAN communicates its data to a unique gateway, which forwards the same through the external network to the back-end medical server. The focus of this paper is on secure routing of medical data and a secure version of the CICADA protocol is discussed. Sensor data is encrypted using AES in the authenticated encryption mode like CCM or GCM, to provide both confidentiality and authentication. The authors suggest that it would be a better practice to use a low cost encryption and integrity procedure, probably because the method suggested would be computationally heavy on the sensors. In their paper, Balasubramanyan et al have focused on the security features related to data freshness and message integrity [14]. Hashed MAC is used to provide message authentication and periodic calculation of round trip time (RTT) guarantees data freshness. This work does not discuss other security issues.

3. PROPOSED ARCHITECTURE FOR AT-HOME MEDICAL CARE

This paper proposes an architecture to monitor one or more persons or family members, living in the same house both remotely and continuously. The members may be aged persons, persons requiring post-operative care or those suffering from few chronic illnesses that require continuous monitoring. The persons could be confined to their beds or could be mobile, carrying out their daily routine unattended.

The members would be equipped with one or more wearable sensors to measure their physiological parameters for continuous monitoring. The sensors used and data measured may vary from patient to patient depending on their health condition.

The proposed architecture is represented in Figure 1. The members or patients would be fitted with a Wearable Data Acquisition Unit (WDAU) to collect and aggregate the sensor data of an individual. The aggregated data would be transmitted to the At-Home Base Station (AHBS) using wireless communication. AHBS would then consolidate all the patient data and transmit the same to the Hospital Monitoring Station (HMS) for processing and follow-up by the medical care-givers.

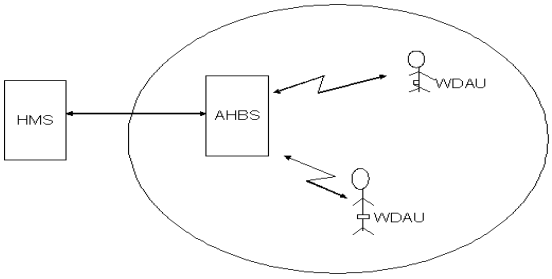

Figure 1. At-Home Architecture

Each patient has been identified by a unique ID termed Patient ID (PID). The PID has been associated with the patient data to identify the origin of the data. Each WDAU then transmits patient data to AHBS for consolidation and for further transmission to HMS. In the proposed architecture, the sensors do not need to transmit directly to the remote medical server. The energy, resource requirements and wireless range of the used sensors, only needs to be sufficient for transmission within the confines of the home. In most instances, single hop transmission would be sufficient to transmit from WDAU to AHBS and this consumes comparatively less power for wireless transmission.

The function of WDAU includes individual patient data aggregation and wireless transmission to AHBS. The computational requirements are limited and hence power consumption is less, thereby extending the battery life. The WDAU would be homogenous and would require similar resources in terms of data rate, power consumption and reliability. This provides a distinct advantage over operating in the public domain where the devices would be heterogeneous with different network and energy demands. Depending on the communication and security requirements AHBS ranges from a simple wireless router to a conventional computer system, with no constraints in power or computational capabilities. This paper also addresses the requirements for secured transmission of data between WDAU and AHBS. As this transmission is confined within the house, the security attacks would be considerably less than the internal/external attacks possible during direct transmission in the public domain.

The transmission of patient medical data between AHBS and the HMS can be carried out using regular communication channels like Internet, Virtual Private Network or dedicated line. Public key and other conventional security systems can be used to provide a high level of security and privacy for patient data.

The patients have the psychological advantage of being at home and carrying on their normal routine. There would be tremendous cost savings in terms of hospitalization charges, use of nurses or trained aides etc. It may also be possible to train paramedics to monitor such patient

data and alert the medical experts in emergency situations. In cases of anomalies in vital parameters, medical professionals can also direct AHBS via HMS to increase the sampling frequency of the sensors to collect the data at more frequent intervals. AHBS can also monitor the values of the vital parameters and alert the care givers via HMS.

4. SECURING TRANSMISSION BETWEEN WDAU AND AHBS

Security for a BSN must take into consideration the various features specific to the architecture. Wireless transmission is inherently insecure and prone to data loss. In this section, the security of the wireless transmission between WDAU and AHBS has been discussed. The security threats that need to be addressed includes, (a) eavesdropping on patient data (b) unauthorized modification of the patient data, (c) Injection or Fabrication of false values in the data, (d) Capture of data packets to be replayed later, so that the medical data appears to be genuine. Security exposure may give a wrong picture of the medical data leading to wrong diagnosis. The care-giver may wrongly conclude that the patient is normal and stable in condition. In addition to considering the above, the proposed security solution also takes into account the following important aspects; (a) the patients are mobile (b) more than one patient could be monitored in the same premise (c) sensors can get lost either inadvertently or (d) be physically forced away from the patient by the attacker to prevent monitoring.

The wireless communication of health related information between WDAU and AHBS must provide data confidentiality, authenticity, integrity and replay protection. These security requirements are provided using cryptographic primitives. There may be more than one member monitored at home and AHBS receives all the packets from the members and consolidates them. Therefore it is necessary for AHBS to correctly relate the measured physiological parameters to the right patient. To ensure that the set of sensor readings are appropriately identified, each patient is assigned a Patient ID (PID). The PID has been generated by HMS and stored in the WDAU. AHBS encrypts the same and stores the list of valid PID and verifies the PID received in all communications from WDAU.

Four physiological parameters namely: Blood Pressure, Pulse Rate, Oxygen Saturation (SaO2) and Temperature of the patients have been considered. The normal values of the parameters have been given in Table 1 [5]

TABLE 1
SPECIFICATION OF VITAL PARAMETERS MONITORED

Vital Parameters	Specification
Blood Pressure	Systolic: 60 - 200mmHg Diastolic: 50 – 110mmHg
Pulse Rate	72-90 beats per minute
Oxygen Saturation (SaO_2)	0-100%
Temperature	32°C-40°C

It is assumed that WDAU transmits sensor data every 10 seconds. The four sensor parameters have been randomly generated for continuous monitoring of five patients and the encryption / decryption and authentication process were simulated using TinyOS.

Wireless communication between WDAU and AHBS is secured using cryptographic methods like encryption / decryption and MAC. The patient data can be encrypted using symmetric key method or the more robust asymmetric key techniques. Considering the resource constraints in WDAU, symmetric key encryption algorithm is used here. Both the algorithm and the choice of the key length assure the confidentiality of the data. In addition the method of key exchange between WDAU and AHBS is crucial in maintaining the secrecy of the key used for encrypting the data. The key exchange, encryption and authentication procedure is discussed below.

4.1. Key Exchange

On initialization, both WDAU and AHBS individually generate a 160 bit public/private key pair using Elliptic Curve Cryptography (ECC) algorithm [15].

The well known protocol Diffie-Hellman is used for key exchange between WDAU and AHBS. The secret key K_S is generated at WDAU, as a function of its private key (K_{RM}) and the public key received from AHBS (K_{UB}). Similarly, AHBS generates the secret key K_S using its private key (K_{RB}) and WDAU public key (K_{UM}). The secret keys generated at both places are identical and has been verified to be the same at both AHBS and WDAU. Further, AHBS generates a session number (SN) for use in subsequent transmissions of data.

The processing steps are detailed below:

Step 1: AHBS generates a nonce n1 and a random session number SN

Step 2: SN and nonce are encrypted at AHBS using the secret key and sent to WDAU

Step 3: WDAU decrypts and obtains the nonce n1 and session number SN.

Step 4: WDAU encrypts the nonce n1 with the secret key and sends it to AHBS.

Step 5: AHBS decrypts and verifies that the secret key generated is the same.

This procedure also ensures the secure transmission of the session number. The random generation of SN prevents replay attack. The sequence of steps is summarized in Table 2.

TABLE 2
SECRET KEY GENERATION AND VERIFICATION

AHBS:K_{UB},K_{RB}
AHBS→WDAU:K_{UB}
WDAU : K_{UM},K_{RM}
WDAU →AHBS :K_{UM}
WDAU:K_S= f(K_{UB},K_{RM})
AHBS:K_S=f(K_{UM},K_{RB})
AHBS→WDAU:E_K=(n1,SN)
WDAU:D_K(n1,SN)
WDAU→AHBS:E_K(n1)

4.2. Data Encryption and Authentication

The sensor data sent from WDAU to AHBS is encrypted using AES algorithm and the secret key used is the generated key K_S. Sensors measure the values at the intended time intervals and are sent to WDAU. This has to be worn by the patient. The block diagram of the encryption and authentication at WDAU is given in Figure 2

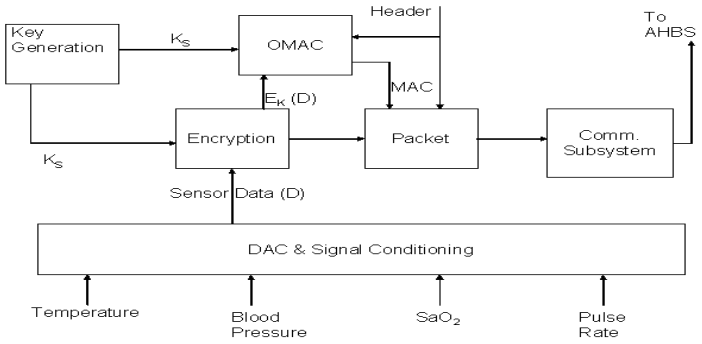

Figure 2. Encryption/Authentication at WDAU

The WDAU collects the data from the various sensors, consolidates them and encrypts the data using a secret key. The patient ID (PID) is also encrypted along with the sensor measurements. The Message Authentication Code (MAC) is generated by WDAU on the encrypted information and header. The same key K_S is used to generate the MAC. The header, encrypted data and MAC are all combined into a data packet and transmitted to AHBS.

On receiving the packet, AHBS generates MAC using its secret key. The generated MAC is then compared and verified with the received MAC. This ensures the authenticity of the received data packet. AHBS then decrypts the packet. The block diagram of the decryption and authentication at AHBS is given in Figure 3.

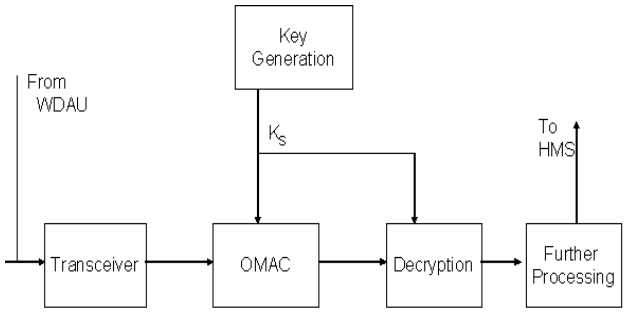

Figure 3. Decryption/Authentication at AHBS

AHBS also verifies the PID transmitted with the sensor data. It compares the received PID with the list of valid PID. If the PID is not valid the packet is discarded.

5. SECURITY PROVIDED BY THE PROPOSED CRYPTOGRAPHY SOLUTION

Based on Shannon's work in Information theory, in order to achieve perfect security it is necessary that the key should be as long as the message to be transmitted and should be a one-time pad. But it is practically infeasible to manage such long keys. Moreover in constrained situations such as that in a sensor network where nearly all resources are to be used very cautiously, the idea of a one-time pad is not a feasible solution. Instead, the focus is on increasing the computational security, by achieving semantic security, that is, the same message would generate a different cipher for every encryption

AES with 128 bit symmetric key is used as encryption algorithm. The key length is sufficiently long to provide a reasonable amount of security for the at-home scenario. The block size used in encryption is 128 bit, which is the standard fixed size for AES, with 10 rounds. So far, no known successful attack has been reported on 10 round AES for 128 bit key.

CCFB block cipher mode is used to achieve semantic security and it has been specifically developed for low-end devices and small embedded systems like sensor motes and RFID tags. There are several other fast single-pass schemes but their use is deterred by patents. CCFB is a two-pass Authenticated Encryption with Associated Data (AEAD) scheme not covered by any known patents [6].

Protection from Known Attacks

Our present work concerns preventive measures which involve the use of cryptographic algorithms to provide confidentiality, integrity and authentication of the medical data being transmitted between WDAU and AHBS.

In the proposed solution, it is difficult to compromise the 128 bit secret key. The secret key is not transmitted either using a secure channel or a trusted third party so it cannot be comprised in transit. WDAU and AHBS generate the secret key independently and also verify that they have generated the same key prior to the actual data transmission. To further ensure that the secret key is secure, the security solution has the provision of being able to refresh the key every 12 hours, or as and when requested by AHBS.

We discuss some of the common attacks and the protection provided by our security solution.

(i) **Eavesdropping**: This is a passive attack, where the attacker only listens to the transmission with the intention of trying to obtain the type of information being transmitted. Listening to the traffic of the At-Home architecture will not reveal much information as all packets are encrypted and knowledge of secret key is required to decrypt the data.

(ii) **Modification**: An attacker gains access to the contents of the packet and changes the values of the measured parameters. This is an active attack on the integrity of the data. This attack requires the knowledge of the secret key K_S. Additionally, data integrity is verified using OMAC.

(iii) **Fabrication**: This is an active attack in which the attacker fabricates false readings and inserts them into the packet. This is an attack on the authenticity of the data. This would require the attacker to know both the secret key and the PID. The PID cannot be falsified since it is verified by ABHS for every data packet received from WDAU.

(iii) **Replay**: An attacker copies the entire packet and replays it at a later time. This active attack would mislead the physician into understanding that the patient is normal. This attack could become life threatening. The attacker should know the session number (SN), which is a random number generated by AHBS and exchanged during key verification. The session number is changed every 12 hours. Since this is a random number it is not feasible for an attacker to correctly guess the session number.

(iv)**Interruption**: An asset of the system is destroyed or temporarily disabled so that the service becomes unavailable. This is an attack on the availability of data. If the attacker tampers with the WDAU hardware, it would be sensed by AHBS which can raise an alarm at HMS for appropriate action. If AHBS is tampered and the transmission of patient data is interrupted the HMS would be able to monitor such disruption of data and initiate suitable action. HMS can also be configured to send a message to any close relative or authorized person of the patient for quick remedial action.

6. CONCLUSION AND FUTURE WORK

We have presented a novel architecture for continuous unobtrusive monitoring of patients at home using BSN. Sensors are used to measure physiological parameters of persons at home and the sensed data is sent to hospitals / healthcare centers for remote monitoring. Security solution has been proposed to provide for data confidentiality, integrity and authentication for transmission of patient data within the home. Protection offered against common attacks is also discussed.

As future work, we intend to address the end-to-end security between WDAU and HMS in the proposed architecture. We also plan to develop more robust techniques for authentication of patients.

REFERENCES

[1] B.Latre', et al., "A Survey on Wireless Body Area Network ", Wireless Networks Journal, Springer,vol.16, Nov.2010.

[2] S.Park and S.Jayaraman, "Enhancing Quality of life through Wearable Technology", IEEE Engineering and Biology Magazine, May-June 2003, vol.22 pp 41-48

[3] A.Bhargava and M.Zoltowski, "Sensors and Wireless Communication for medical care, Database and Expert Systems Applications", Proc. 14th Intl. Workshop Sep 2003.

[4] S.S.Mohanavalli, Sheila Anand, Security Architecture for At-Home medical care using sensor networks, Proceedings of International Conference on Sensor Networks, Uniquitous and Information Computing, 2010.

[5] A. Perrig, R. Szewczyk, J.D Tygar, V.Wen, and V.Culler, "SPINS: Security Protocols for Sensor Networks", Wireless Networks, 8 (2002), pp. 521- 534.

[6] Chol-soon Jang, Deok-Gyu Lee, Jong-wook Han, A Proposal of Security Framework for Wireless Body Area Network, International Conference on Security Technology, 2008.

[7] V. Shnayder, B.R. Chen, K. Lorincz, T.R.F .Fulford-Jones and M. Welsh," Sensor networks for medical care", Technical Report TR-08-05, Harvard University, Apr.2005.

[8] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin and J. Stankovic," ALARM-NET: Wireless sensor network for assisted-living and health monitoring", Technical Report CS -2006-01, University of Virginia, 2006.

[9] Q. Wang, W. Shin, X. Liu, Z. Zeng, C. Oh, B. Al-Shebli, M. Caccamo, C. Gunter, E. Gunter, J. Hou, K. Karahalios and L. Sha," I-LIVING: An open system architecture for assisted living", IEEE SMC, 2006.

[10] P.S. Pandian, K.P. Safeer, P. Gupta, D.T. Sankunthala, B.S. Sundersheshu and V.C. Padaki," Wireless sensor network for wearable physiological monitoring", Journal of Networks, vol 3, May 2008.

[11] K. Malasri, L. Wang," Addressing security in medical sensor networks", HealthNet, June 2007.

[12] S.Cherkuri, K.K.Venkatasubramanian, S.K.S.Gupta, "BioSec: Abiometric based approach for securing communication in wireless networks of biosensors implanted in the human body", Parallel Processing Workshops,Oct 2003.

[13] D.Singlee, B.Latre, B.Braem, M. De Soete, , P.De. Cleyn, B.Preneel, I. Moerman, C.Blondia, " A secure cross layer protocol for multi hop wireless body area networks", In 7th International Conference on Ad Hoc Networks & Wireless, vol LNCS 5198, Sep 2008.

[14] V.B.Balasubramanyan, G.Thamilarasu, R.Sridhar, "Security solution for data integrity in wireless biosensor networks ," 27th International Conference on Distributed Computing Systems, Jun 2007.

[15] Stefan Lucks," Two-pass authenticated encryption faster than generic composition", Fast Software Encryption, 2005.

[16] Chiu C. Tan, H. Wang, S. Zhong and Q. Li," IBE-Lite: A lightweight identity based cryptography for body sensor networks", IEEE Transactions on Information Technology in Biomedicine, Vol 13, Nov, 2009.

[17] H. Li and J .Tan," Heartbeat- driven medium access control for body sensor networks. IEEE Transactions on Information Technology in Biomedicine, vol 14, Jan, 2010.

[18] V. Venkatasubramanian, A. Banarjee and S.K.S. Gupta," PSKA: Usable and secure key agreement scheme for Body Area Networks", IEEE Transactions on Information Technology in Biomedicine, Vol 14, Jan 2010.

[19] Certicom Research. Standards for Efficient Cryptography (SEC) 1: Elliptic Curve Cryptography. Sept 2000

[20] Certicom Research. Standards for Efficient Cryptography (SEC) 2: Recommended Elliptic Curve Domain Parameters. Sept 2000.

[21] Crossbow Solutions Newsletter. Motes for Mobile Communication and Tele-Medicine, 2005.

[22] C.Karlof, N. Sastry, D. Wagner, "TinySec : A Link Layer Security Architecture for Wireless Sensor Networks", Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, November 2004, ACM Press, pp. 162-175.

[23] A. Liu, P. Kampanakis, and P. Ning, "TinyECC: Elliptic Curve Cryptography for Sensor Networks", http://discovery.csc.ncsu.edu/software/TinyECC

[24] M.Healy,T.Newe, E.Lewis, Security for Sensor Networks :A review., IEEE Sensors Applications Symposium, 2009.

[25] A.K.Jain, A.Ross,S.Pankanti, Biometrics : A Tool for Information Security, IEEE Transactions on Information Forensics and Security,2006.