Wireless Body Area Sensor Network Authentication using HMAC function

Yogita L. Kumbhare
G.H.Raisoni college of Engineering, Nagpur

Pankaj H. Rangaree
G.H.Raisoni college of Engineering, Nagpur

Dr.G.M.Asutkar
Priyadarshini college of Engineering, Nagpur

ABSTRACT

Recent advancements in wireless body area sensor networks (WBASNs) realize the evolution from a traditional desktop telemedicine platform to a wireless and mobile diagnosis system for delivering medical and healthcare services. In a WBASN, wearable or implanted medical sensors around the human body form a wirelessly interconnected network to collect an individual's medical information ubiquitously and to perform critical and complicated tasks collaboratively. Wireless Body Area Networks provide efficient communication solutions to the ubiquitous healthcare systems. Health monitoring, telemedicine, military, interactive entertainment, and portable audio/video systems are some of the applications where WBANs can be used. The miniaturized sensors together with advance micro-electro-mechanical systems technology create a WBAN that continuously monitors the health condition of a patient. For example, sensors have become smaller and more precise, and energy efficiency of radio circuits and microcontrollers has been improved considerably. Sensor networks that are composed of wearable or implanted sensors are also known as Body Area Networks (BAN) or Wireless Body Area Networks (WBAN) depending on how sensors are connected with each other.

Wireless body area sensor networks low-power integrated circuits, and wireless communications have enabled the design of low-cost, miniature, lightweight, and intelligent physiological sensor nodes. These nodes, capable of sensing, processing, and communicating one or more vital signs, can be seamlessly integrated into wireless personal or body networks (WPANs or WBANs) for health monitoring. These networks promise to revolutionize health care by allowing inexpensive, non-invasive, continuous, ambulatory health monitoring with almost realtime updates of medical records via the Internet.

Wearable health monitoring systems allow an individual to closely monitor changes in her or his vital signs and provide feedback to help maintain an optimal health status. If integrated into a telemedical system, these systems can even alert medical personnel when life-threatening changes occur. In addition, patients can benefit from continuous long-term monitoring as a part of a diagnostic procedure, can achieve optimal maintenance of a chronic condition, or can be supervised during recovery from an acute event or surgical procedure.

Message Authentication is defined as 'Provision of assurance that the message is not altered'. Former is provided by Message Authentication codes (MAC) and this paper is provided by Hash functions. When MAC uses Hash function to generate authentication code it is called Hash based MAC (HMAC).

Keywords: body area networks, BASN security, authentication

1. INTRODUCTION

The field of computer science is constantly evolving to process larger data sets and maintain higher levels of connectivity. At same time, advances in miniaturization allow for increased mobility and accessibility. Body Area Networks represent the natural union between connectivity and miniaturization. A Body Area Network (BAN) is defined formally as a system of devices in close proximity to a person's body that cooperate for the benefit of the user.

With the advances in embedded microcontrollers, inexpensive miniature sensors, and wireless networking technologies, there has been a growing interest in using wireless sensor networks in medical applications. For example, wireless sensor networks can replace expensive and cumbersome wired devices for pre-hospital and ambulatory emergency care when real-time and continuous monitoring of vital signs is needed. Moreover, body sensor networks can be formed by placing low-power wireless devices on or around the body, enabling long-term monitoring of physiological data. For elderly patients and people with chronic diseases, an in-house wireless sensor network allows convenient collection of medical data while they are staying at home, thus reducing the burden of hospital stay. The collected data can be passed onto the Internet through a PDA, a cell-phone, or a home computer. The caregivers thus have remote access to the patient's health status, facilitating long-term rehabilitation and early detection of certain physical diseases. If there are abnormal changes in the patient status, caregivers can be notified in a timely manner, and immediate treatment can be provided.

With a number of advantages over wired alternatives, including: ease of use, reduced risk of infection, reduced risk of failure, reduce patient discomfort, enhance mobility and low cost of care delivery, wireless applications bring forth exciting possibilities for new applications in medical market.

Portable devices such as heart rate monitors, pulse oximeters, spirometers and blood pressure monitors are essential instruments in intensive care. Traditionally, the sensors for these instruments are attached to the patient by wires; and the patient sequentially becomes bed-bound. In addition, whenever patient needs to be moved, all monitoring device has to be disconnected and then reconnected later. Nowadays, all of these time-consuming jobs could be terminated and patients could be liberated from instrumentation and bed by wireless technology. Integrated wireless technology, these wireless devices could communicate with a gateway that connects to the medical center's network and transmits data to health data stores for monitoring, control, or evaluating in real time or offline after storage.

Continuous and pervasive medical monitoring is now available with the present of wireless healthcare systems and telemedicine services. In emergency situations, real-time health parameter is crucial. With wireless continuous medical monitoring systems, patients' information such as blood pressure, heart rate, and electrocardiogram can be sent instantly to specialized medical centers to store and process properly. As observed, such medical data present unique traffic patterns and result in distinct rate variations. Based on the collected data from body sensors, if any suspicious sign is detected and may lead to severe consequences, a real-time alert can be forwarded to a hospital, clinic or family doctor by using the best available transmission connection. Medical emergencies can be detected sooner and proper treatment can be applied timely. Health care effectiveness in several situations is improved significantly with the present of wireless communication technologies.

Wireless technology could be the best solution for mass emergency situations like natural or human-included disasters and military conflict where patients' records such as previous medication history, identification and other vital information are necessary. With the assistant of hand held devices in which wireless network integrated, the amount of time the doctors need to identify the problem, trace back the medication history of the patient and consult fellow doctors will be reduced significantly. Moreover, databases of patients that can be built up by continuous medical monitoring will be accessed and updated easily.

Generally speaking, two types of devices can be distinguished: sensors and actuators. The sensors are used to measure certain parameters of the human body, either externally or internally. Examples include measuring the heartbeat, body temperature or recording a prolonged electrocardiogram (ECG). The actuators (or actors) on the other hand take some specific actions according to the data they receive from the sensors or through interaction with the user. E.g., an actuator equipped with a built-in reservoir and pump administers the correct dose of insulin to give to diabetics based on the glucose level measurements. Interaction with the user or other persons is usually handled by a personal device, e.g. a PDA or a smart phone which acts as a sink for data of the wireless devices.

These sensors need to send their data to an external medical server where it can be analyzed and stored. Using a wired connection for this purpose turns out to be too cumbersome and involves a high cost for deployment and maintenance. However, the use of a wireless interface enables an easier application and is more cost efficient. The patient experiences a greater physical mobility and is no longer compelled to stay in a hospital. This process can enhancing the personal health care and in coping with the costs of the health care system. It defined as the health care practice supported by electronic processes and communication, the health care is now going a step further by becoming mobile.

A WBAN will consist of number of tiny sensor nodes and gateway ode used to connect to the external database server.The gateway node could connect the sensor node to range of telecommunication networks. These communication network could be either a standard telephone network,mobile phone network, a dedicated medical center/ hospital network or using WLAN(Wireless Lan Area Network) hotspots also known as WiFi.

WBAN is normally used to monitor heart patients either they are in mobile or in rest. Hence most of the Wireless Body Area Network consists of ECG sensors. ECG has the property of liveness. It varies from the person to person. ECG based biometric system can be easily combined with other biometric systems to enhance the reliability and security of the system. Hence in this work the features of ECG are used for biometric authentication in WBAN environment. The ECG data obtained from ECG sensors at the same time are plotted in the form of an ECG wave using Dot Net tool and the fiducially features are extracted from the ECG signal obtained from the biomedical sensors and is used as a biometric characteristic to authenticate ECG sensor nodes to the base station. An important requirement is to have accurate time synchronization, so that sensors take their measurements at the same time and produce the same value.

All wireless networks are inherently insecure as the only wireless medium through which they communicate is public to all so any one tune to same frequency as sensors are tuned to can breach the security. Even by purchasing and deploying the sensor of same company/type can enable the attacker to break the security.

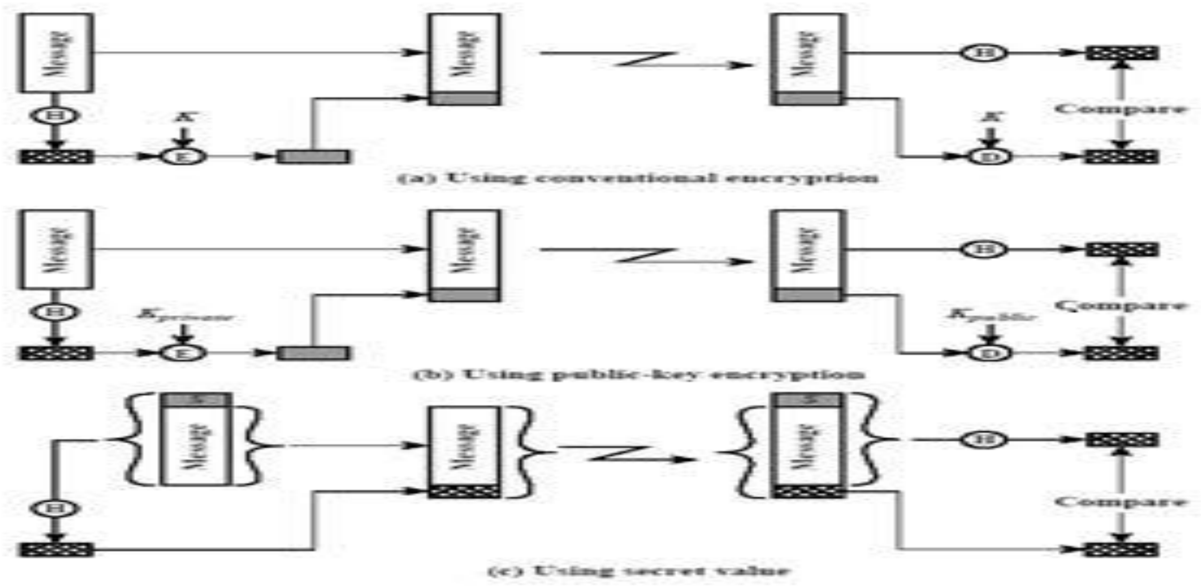
Body area sensor networks work on ISM band which is public and known to everyone so breaking the security of BAN is more attractive to adversary. If some adversary modify the message it can be very harmful as not only patient's privacy is compromised but also adversary can generate false messages to health monitoring department/doctor at very late hours which results discomfort for both patient and doctor/ health care staff etc. so an architecture for securing the contents of body area sensor network messages is required

In the field of data communication through computer networks, problem arises with the security of data. In the context of communications across a network, the following attacks can be identified: Disclosure, Traffic analysis, Masquerade, Content modification, Sequence modification, Timing modification, Repudiation.

Three ways to implement HMAC as shown in Fig. 1

1. Encrypt plaintext using CBC mode. Use the final block as the HMAC
2. Use a different key for HMAC and encryption if a confidential message is sent
3. Hash the message and encrypt the digest. Hash the message along with a shared key HMAC generated using hashing is known as an HMAC.

Implementation of this work is done in the wearable WBAN available.. For clinical analysis ECG must be taken from 4 to 13 places of the human body. In the first module the system is examined by taking ECG using four sensors placed in four different parts of the body of an individual and provides the security using HMAC function.



(a) Using conventional encryption

(b) Using public-key encryption

(c) Using secret value

Fig 1: Types of Implementing HMAC

2. SYSTEM ARCHITECTURE

The proposed wireless body area sensor network for health monitoring integrated into a broader telemedicine system is illustrated in Figure 2. The telemedical system spans a network comprised of individual health monitoring systems that connect through the Internet to a medical server that resides at the top of this hierarchy. Centered on a medical server, is optimized to service hundreds or thousands of individual users, and encompasses a complex network of interconnected services, medical personnel, and healthcare professionals. Each user wears a number of sensor nodes that are strategically placed on her body. The primary functions of these sensor nodes are to unobtrusively sample vital signs and transfer the relevant data to a personal server through wireless personal network implemented using Bluetooth. The personal server, implemented on a personal digital assistant (PDA), cell phone, or home personal computer, sets up and controls the WBAN, provides graphical or audio interface to the user, and transfers the information about health status to the medical server through the Internet or mobile telephone networks (e.g., GPRS, 3G).

The medical server keeps electronic medical records of registered users and provides various services to the users, medical personnel, and informal caregivers. It is the responsibility of the medical server to accept health monitoring session uploads, format and insert this session data into corresponding medical records, analyze the data patterns, recognize serious health anomalies in order to contact emergency care givers, and forward new instructions to the users, such as physician prescribed exercises. The patient's physician can access the data from his/her office via the Internet and examine it to ensure the patient is within expected health metrics (heart rate, blood pressure, activity), ensure that the patient is responding to a given treatment or that a patient has been performing the given exercises. A server agent may inspect the uploaded data and create an alert . in the case of a potential medical condition. The large amount of data collected through these services can also be utilized for knowledge discovery through data mining. Integration of the collected data into research databases and quantitative analysis of conditions and patterns could prove invaluable to researchers trying to link symptoms and diagnoses with historical changes in health status, physiological data, or other parameters (e.g., gender, age, weight). In a similar way this infrastructure could significantly contribute to monitoring and studying of drug therapy effects.

The interfaces WBAN sensor nodes, provide the graphical user interface, and communicate with services. The personal server is typically implemented on a PDA or a cell phone, but alternatively can run on a home personal computer. This is particularly convenient for in-home monitoring of elderly patients. The personal server interfaces the WBAN nodes through a network coordinator (nc) that implements Bluetooth connectivity. To communicate to the medical server, the personal server employs mobile telephone networks (2G, GPRS, 3G) or WLANs to reach an Internet access point. The limited range of wireless communications partially addresses security within WBAN, the messages can be send using either software or hardware techniques.

The sensor node connected the CCU Box (Central Control Unit) collecting and monitoring data from individual wireless sensor node from single human body. The patient's data like heart rate, blood pressure, activity can access through the sensor node , sensor node transferred it to the CCU on which sensor is externally connected . The collected data from the control devices are then transferred to remote destinations in a The sensor node connected the CCU Box (Central Control Unit) collecting and monitoring data from individual wireless sensor node from single human body. The patient's data like heart rate, blood pressure, activity can access through the sensor node , sensor node transferred it to the CCU on

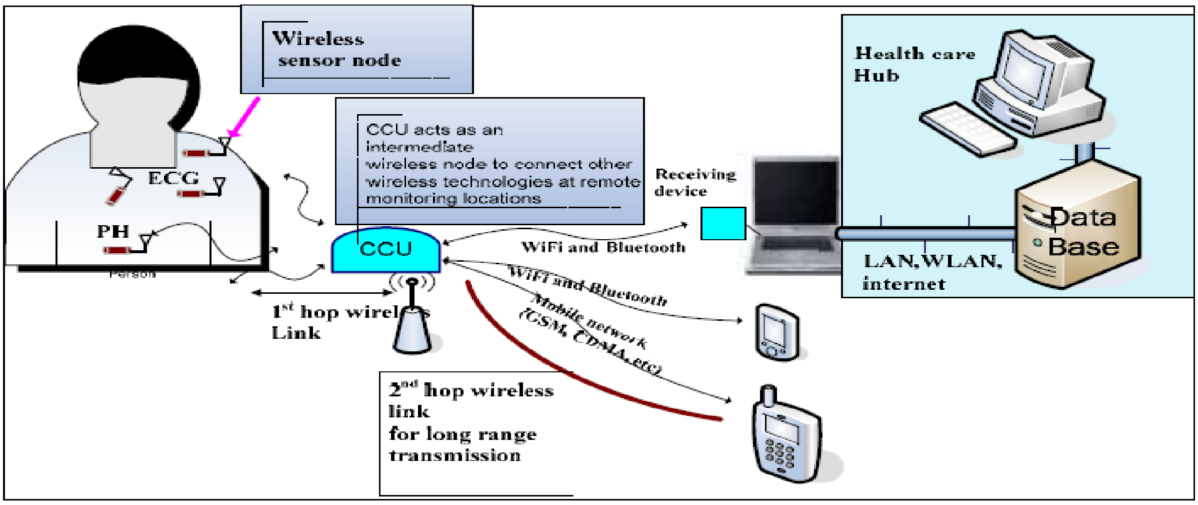

Wireless sensor node
CCU acts as an intermediate wireless node to connect other wireless technologies at remote monitoring locations
Receiving device
Health care Hub
Data Base
LAN,WLAN, internet
ECG
PH
Person
CCU
WiFi and Bluetooth
WiFi and Bluetooth
Mobile network (GSM, CDMA,etc)
1st hop wireless Link
2nd hop wireless link for long range transmission

Fig: 2 A Wireless Body Area Network

wireless body area network for diagnostic and therapeutic incorporating another wireless network for long range transmission which sensor is externally connected . The collected data from the control devices are then transferred to remote destinations in a wireless body area network for diagnostic and therapeutic incorporating another wireless network for long range transmission.

2.1 Requirements for Wireless Medical Sensors

Wireless medical sensors should satisfy the main requirements such as *wearability*, *reliability*, *security*, and *interoperability*.

Wearability. To achieve non-invasive and unobtrusive continuous health monitoring, wireless medical sensors should be lightweight and small. The size and weight of sensors is predominantly determined by the size and weight of batteries. But then, a battery's capacity is directly proportional to its size. We can expect that further technology advances in miniaturization of integrated circuits and batteries will help designers to improve medical sensor wearability and the user's level of comfort. Section 5 further discusses energy efficiency in WWBAN.

Reliable communication. Reliable communication in WWBANs is of utmost importance for medical applications that rely on WWBANs. The communication requirements of different medical sensors vary with required sampling rates, from less than 1 Hz to 1000 Hz. One approach to improve reliability is to move beyond telemetry by performing on-sensor signal processing. For example, instead of transferring raw data from an ECG sensor, we can perform feature extraction on the sensor, and transfer only information about an event. In addition to reducing heavy demands for the communication channel, the reduced communication requirements save on total energy expenditures, and consequently increase battery life. A careful trade-off between communication and computation is crucial for optimal system design.

Security. Another important issue is overall system security. The problem of security arises at all three tiers of a WWBAN-based telemedical system. At the lowest level, wireless medical sensors must meet privacy requirements mandated by the law for all medical devices and must guarantee data integrity. Though key establishment, authentication, and data integrity are challenging tasks in resource constrained medical sensors, a relatively small number of nodes in a typical WWBAN and short communication ranges make these tasks achievable.

Interoperability. Wireless medical sensors should allow users to easily assemble a robust WWBAN depending on the user's state of health. Standards that specify interoperability of wireless medical sensors will promote vendor competition and eventually result in more affordable systems.

3. PROPOSED PLAN

HMAC (Hash-based Message Authentication Code) is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret key as shown in Figure 3 . As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message. Any cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1 accordingly. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output length in bits, and on the size and quality of the cryptographic key.

An iterative hash function breaks up a message into blocks of a fixed size and iterates over them with a compression function. For example, MD5 and SHA-1 operate on 512-bit blocks. The size of the output of HMAC is the same as that of the underlying hash function (128 or 160 bits in the case of MD5 or SHA-1, respectively), although it can be truncated if desired. The design of the HMAC specification was motivated by the existence of attacks on more trivial mechanisms for combining a key with a hash function. For example, one might assume the same security that HMAC provides could be achieved with MAC = H(key ∥ message). However, this method suffers from a serious flaw with most hash functions, it is easy to append data to the message without knowing the key and obtain another valid MAC.

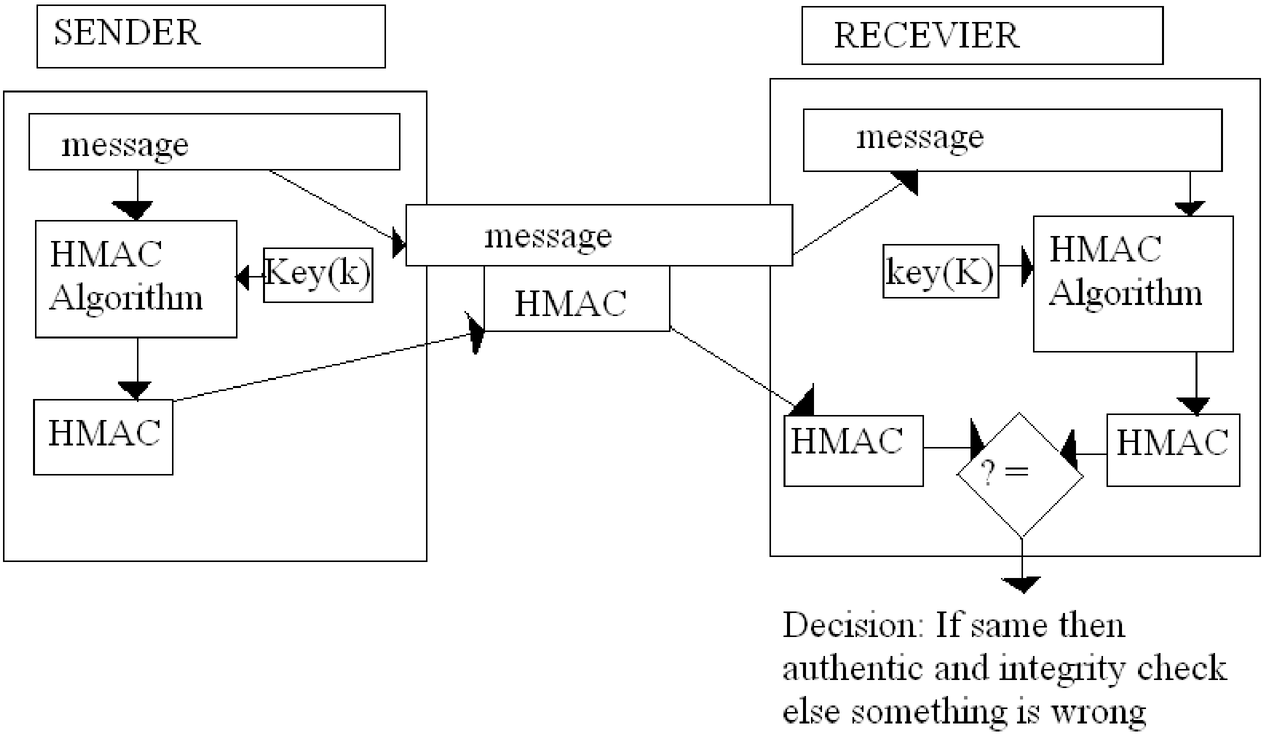


Figure 3: HMAC Generate

Using MAC = H(key ǁ message ǁ key) is better, however various security papers have suggested vulnerabilities with this approach, even when two different keys are used.

No known extensions attacks have been found against the current HMAC specification which is defined as H(key1 ǁ H(key2 ǁ message)) because the outer application of the hash function masks the intermediate result of the internal hash. The values of ipad and opad are not critical to the security of the algorithm, but were defined in such a way to have a large Hamming distance from each other and so the inner and outer keys will have fewer bits in common.

The cryptographic strength of the HMAC depends upon the size of the secret key that is used. The most common attack against HMACs is brute force to uncover the secret key. HMACs are substantially less affected by collisions than their underlying hashing algorithms alone. Therefore, HMAC-MD5 does not suffer from the same weaknesses that have been found in MD5.

The sender of a message runs it through a HMAC algorithm to produce a HMAC data tag. The message and the HMAC tag are then sent to receiver . The receiver in turn runs the message portion of the transmission through the same HMAC algorithm using the same key, producing a second HMAC data tag. The receiver then compare the first HMAC tag received in the transmission to the second generated HMAC tag. If they are identical ,the receiver can safely the integrity of the message was not compromised, and the message was not altered or tampered with during transmission.

In this way the safe data of the person is send to the doctor. Doctor can operate to the patient according that data without interacting the patient physically.

4. CONCLUSION & FUTURE WORK

We have proposed architecture for providing data and sender authentication in wireless body area sensor networks. The architecture is power efficient as there are no acknowledgements and the communication of base station is solely with some cluster head so every in-body node do not communicate with base station we also provided freshness in our proposed architecture which ensures no man in middle attack, its implementation is kept for future work.

5. REFERENCES

[1] Raju Singh(March 2011) "Confidentiality & Authentication Mechanism for Biometric Information Transmitted over Low Bandwidth & Unreliable channel" School of Computer Engineering and IT, Shobhit University, Meerut, India Vol.3, No.2,

[2] Honggang Wang, Hua Fang, Liudong Xing, Min Chen,(2011) " An Integrated Biometric-based Security Framework Using Wavelet-Domain HMM in Wireless Body Area Networks (WBAN)" IEEE Communications Society subject matter experts for publication in the IEEE ICC proceedings.

[3] Cory Cornelius(August 2010) "On Usable Authentication for Wireless Body Area Networks" Department of Computer Science Dartmouth College, Presented at HealthSec,

[4] Mikael Soini, Jussi Nummela, Petri Oksa, Leena Ukkonen and Lauri Sydänheimo (2009)." Wireless Body Area Network for Hip rehabilitation" Tampere University of Technology, Department of Electronics, Rauma Research Unit pp. 202-206 .

[5] Jamil Y. Khan, Mehmet R. Yuce, and Farbood Karami "Performance Evaluation of a Wireless Body Area Sensor Network for Remote Patient Monitoring"

[6] A. Soomro, D. Cavalcanti, "Opportunities & Challenges using WPAN and WLAN Technologies in Medical Environments", IEEE Communications Magazine, vol:45, no:2, Feb 2007, page 114-122.

[7] Mohammed Mana1, Mohammed Feham1, and Boucif Amar Bensaber2 (Mar. 2011)"Trust Key Management Scheme for Wireless Body Area Networks", International Journal of Network Security, Vol. 12, No. 2, PP. 71-79.

[8] M. R. Doomun and K. M. S. Soyjaudah, \Analytical comparison of cryptographic techniques for resource-constrained wireless security," International Journal of Network Security, vol. 9, no. 1, pp. 82-94, July 2009.

[9] Adnan Saeed, Miad Faezipour (2009)" Plug and Play Sensor Node for Body Area Network", IEEE

[10] Lin Yao1, Bing Liu1, Guowei Wu1, Kai Yao2, Jia Wang1(2010) " A Biometric Key Establishment Protocol for Body Area Networks ", 1School of Software, Dalian University of Technology, Dalian, China,IEEE

[11] Jamil Y. Khan (09,07, 2009)"Wireless Body Area Network for Medical Applications", ,school of computer science,Australia,IEEE

[12] Mohammed Mana1, Mohammed Feham2, and Boucif Amar Bensaber3, (November, 2009) "SEKEBAN (Secure and Efficient Key Exchange for wireless Body Area Network)", International Journal of Advanced Science and Technology Vol. 12.

[13] Sensors"Emil Jovanov, Dejan Raskovic, John Price,John Chapman, Anthony Moore, Abhishek Krishnamurthy,(2008)" Patient Monitoring Using Personal Area Networks of Wireless Intelligent"IEEE.

[14] CHRIS OTTO, ALEKSANDAR MILENKOVIĆ, COREY SANDERS, EMIL JOVANOV, (2006)" SYSTEM ARCHITECTURE OF A WIRELESS BODY AREA SENSOR NETWORK FOR UBIQUITOUS HEALTH MONITORING", Journal of Mobile Multimedia, Vol. 1, No.4 ,307-326.

[15] Chao Chen and Carlos Pomalaza-Ráez, June 2010"Implimenting and EvaluatingA wireless body Sensor System for Automated Physiological Data Acquisition At Home", International Journal of Computer Science and Information Technology, Volume 2, Number 3.

[16] Frank Agyei-Ntim, Member IEEE, Kimberly Newman, Senior Member IEEE September 2-6, 2009 "Lifetime Estimation of Wireless Body Area Sensor Network for Patient Health Monitoring", 31st Annual International Conference of the IEEE EMBS Minneapolis, Minnesota, USA.

[17] Adnan Saeed, Mehrdad Nourani, Gil Lee, Gopal Gupta and Lakshman Tamil,(2007)" A Scalable Wireless Body Area Sensor Network for Health-Care Monitoring "The University of Texas at Dallas, Richardson, Texas,IEEE.

[18] Adnan Saeed*, Miad Faezipour*, Mehrdad Nourani*, Subhash Banerjee,(June 2009)" A Scalable Wireless Body Area Network for Bio-Telemetry" Journal of Information Processing Systems, Vol.5, No.2,

[19] Aleksandar Milenković, Chris Otto, Emil Jovanov(July 2005) "Wireless Sensor Networks for Personal Health Monitoring:Issues and an Implementation".

[20] Mehmet R. Yuce & Steven W. P. Ng & Naung L. Myo &Jamil Y. Khan &Wentai Liu, (25 July 2007)"Wireless Body Sensor Network Using Medical Implant Band" .