ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Security Issues in Wireless Body Area Networks: In Bio-signal Input Fuzzy Security Model: A Survey.

M.V. Karthikeyan[1]*, and J Martin Leo Manickam[2].

[1]*Faculty of Electronics and Communication Engineering, St. Joseph's Institute of Technology ,Student, Anna University, Chennai - 600119 , Tamilnadu, India.
[2]Faculty of Electronics and Communication Engineering,St. Joseph's College Of Engineering, Tamilnadu, Chennai - 600119, India.

ABSTRACT

In this competitive world, development of science and technology is considered as most important for satisfying all the needs of the society both directly and indirectly. The existing general principle is that when technology develops, the challenges also develop parallel to it. In this current scenario, wireless communication is being concentrated for the development of the all the fields. Especially Wireless body area networking has gained more significance in medical fields like implanting pacemakers, retinal chip, etc. Simultaneously, the challenges relating to these implants have also increased. Security in implants is becoming a threat. We present a comprehensive survey consisting of various sections like: WBAN Architecture, Sensors and signal, Technical Requirements, channel modeling, network security and security. We concluded the paper with some security solutions and discussions.

Keywords: Wireless Body Area Sensor Networks, Body Area Nodes, Fuzzy vault, inter pulse interval (IPI), Bio-signals.

Corresponding author

ISSN: 0975-8585

INTRODUCTION

The new inventions in health care devices have led to the considerable increase in life span. The factors along with miniaturized bio-sensing elements and dedicated wireless communication band have led to the development of a new arena called wireless Body Area sensor Networks (WBANs) [1] to a practical level where WBAN was first introduces byT.G.Zimmerman [9] in 1996 which was initially known as wireless personal area networks or 3 meter distance communication. BAN plays a significant role in medical, non-medical, military and emergency services. According to the world health organization, cardiovascular disease cause An estimated 17.5 million people died from CVDs in 2012, representing 31% of all global deaths [2] in the world. All over the world 180 million people are currently affected by Diabetes and around year 2030 it is expected to be360 million [3]. The obese count of people is amount 2.3 billion by the end of 2015. A rapid rise in Neuro - degenerative diseases such as Alzheimer's and Parkinson's is threatening millions more. The raised of blood pressurevalues (defined as diastolic and/or systolic blood pressure ≥140/90 mmHg) in adults aged 18 years and over was around 22% in 2014 [4] globally .

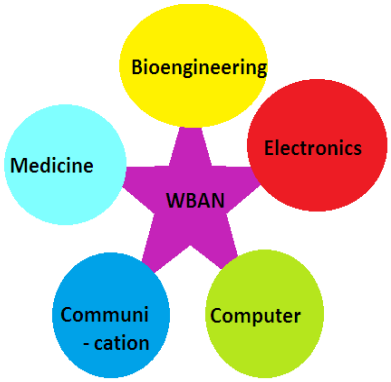

Figure. 1.Interdisciplinary research of WBAN

In India, the status is little different which needs more attention. While considering India where there is a significant growth in population of aged people and where the expenses spent for caretakers is high, need for an inexpensive pervasive monitoring [5] is essential, as they continue their daily routines role without any hindrances both on continuous basis and on emergency crisis. On the other hand, it also plays a vital in non-medical application for the intensified and rigorous sports training and monitoring [6] of persons' activities on their work is more useful in developing their skills. WBAN has also contributed in the military field, by continuous monitoring of vital signs of soldiers in war field. Where the Figure .1.shows that WBAN is a interdisciplinary work and needs its application in many applications. The development of this latest technology has made to sense and communicate various medical and non-medical signs that is clearly shown in figure .2.

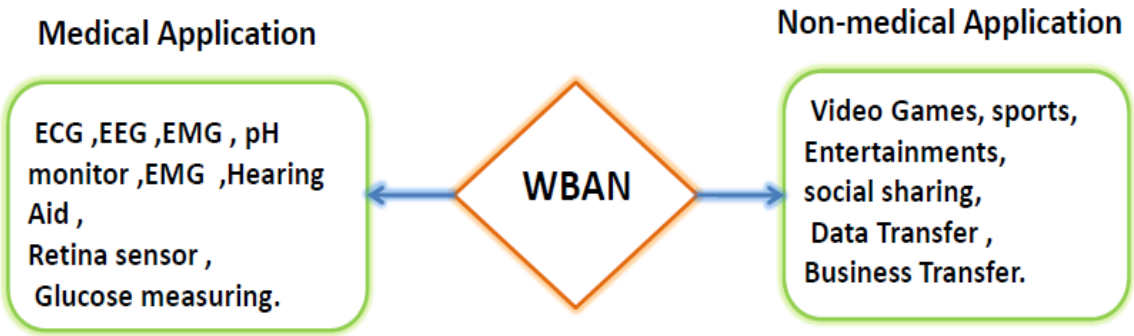

Figure. 2 .WBAN Applications

In this literature, we analyze various types of security threat, security attacks, bio-sensors, routing attack with special emphasis given for the security issues of date transmitted by the biosensor which is placed in the human body, either through invasive method or a non-invasive one and which is connected to another reliable node through a highly vulnerable and open access wireless channel.

Devices like Cardioverter Defibrillator (ICDs) ,wearable ECG,EMG,EEG ,BP,SPO2 and Temperature monitor can be implanted over the subject and the data can be monitored, collected and communicated through an open wireless channel to the doctor, daily monitoring unit,emergency care center and ambulatory service in emergency conditions, where the communication of these signal are made through a dedicated frequencies [7] like Wireless Medical Telemetry Services (WMTS), Unlicensed Industrial Scientific And Medical (ISM) Band, Ultra Wide Band and Medical Implanted Communication (MICS) band for bio-medical signal transmission. The WMTS is urged by federal communication commission (FCC) [8] which operates on 14Mhz band where only trained technicians and authorized persons are allowed to operate this medical frequency, as this frequency range is utilized only by limited people where very low interference sources are present,but the main disadvantage in this frequency is that it cannot support video and voice data transmission. A licensed MICS band used to communicate between sensors are developed for communicating with the implants specially which operates in frequency range of 402 – 405 MHz, the latest allotted spectrum is the ISM band (2.4Ghz) which is a dedicated open source frequency in Industry, Medical and Science field, where this had overcome the disadvantages like providing guard bands in it to avoid adjacent channel interference. Thus, a more collusion free radio network is provided, but still the data transmitted is kept open in the transmission medium. The existing low range, zigbee and Bluetooth technology cannot be used [10] as the power consumption is still high (100 mW) compared with a bio-sensor Node.

Many research works are surveyed in this literature work, but all the practical issues are not addressed with all conditions concerned in it in order to get a commercial product. Still many challenging issues are unanswered, for instance, high data processing /complex computation,secure transmission of sensed data, memory of sensor,number of biosensor and the increasing great demand of remote monitoring of patients .In this paper we are going to bring the various light weight security mechanism developed to protect data acquired from the biosensor and communicated through an open wireless channel to the nearby biosensor node or to a Body area sensor Coordinator (BNC) which act as a source and sink for the Body Area Sensor Node (BN). Various other works are presented here in LOS security [11] of the WBAN signal with simple hardware security mechanism inbuilt in it. The main reason to survey on security is based on the fact that a report points out it has already warned by the US Food and Drug Administration about 300 medical devices at risk of cyber attacks, including pacemakers, implantable insulin pumps, ventilators and defibrillators, No wonder former US Vice President Dick Cheney even underwent a surgery to turn off the wireless function on his pacemaker (to prevent it from being hacked).

Wireless Body Area Network Architecture

The WBAN architecture shown below in Figure .3 is the most suitable multihop communication path [12], ithas been calculated that the power consumed by each node to transmit the data is very less than a single hop communication. Each Body Area Sensor Node (BN) collects the data and forwards it to the Body Area Sensor Network Coordinator (BNC) for data aggregation.Thus, a more power saving communication scenario is discussed.

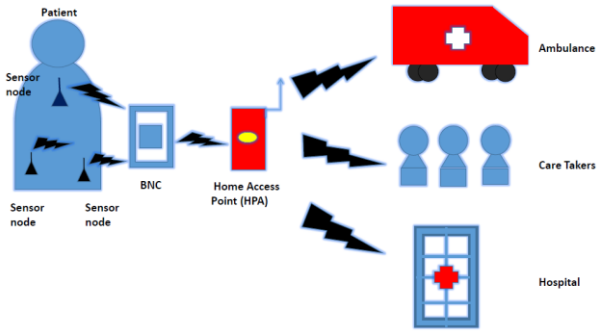

Figure. 3 Architecture of wireless body area sensor network

WBAN level security architecture [13]

- Level 1 – sensor notes that monitor (BAN nodes – BN).
- Level 2 – BNC link between DNC – base station.
- Level -3 – remote base station.

Tire 1 / Level 1: This forms the basic structure of the architecture called as Bio-sensor Node or Body Area Sensor Node (BN).The biosensor which is in direct contact with the human body, either invasive and non-invasive the lower level, will sense physiological changes occurring in the human subject .

Tire 2 / Level 2: All the nodes kept in close proximity to human body collect the vital signs from the subject, process it and forward it to the Body Area Sensor Network Coordinator (BNC). The main interest of the paper deals with the various security solutions in the transmission of the Bio-signal over the above said various frequency ranges, between BN and BNC. The BNC, which collect the data, does not have any constraint in computation complexity (high data rate), memory and energyconsumption. It is always kept outside the body, where tampering is possible in certain situations.

Tire 3/ Level 3: The data collected from the BNC is forwarded to an access point and from there it transmits over a secure channel for long distance to a Hospital, caretaker and to an ambulatory service during emergencies.

Sensors and signals:

The Bio-Sensors are going to measure the various vital body signals of the candidate and their ranges are given in Table. 1 [52].

Blood Pressure

The pressure exerted by blood circulating inside the body, on the walls of blood vessels, which is measured inside the body is read as Blood Pressure (BP). During the cardiac cycle, pressure changes between maximum (systolic) and minimum (diastolic).

In recent years a cuff less BP sensor watch had been developed by Poon et.al, in which the pulse transit time (PTT) based BP measuring device [14] is used to measure the systolic and diastolic count which is also an indirect method of measuring the heart rate.

Before this system AMON system [15] created a BP sensor that uses an inflatable cuff positioning around wrist and obtains systolic and diastolic measuring via the oscillometric scheme [16]. It cannot be used to measure the continuous BP variations and moreover the cuff based measurement causes pain to the patient or its user.

Table. 1. Biometrics range .[52]

Biometric	Range
Blood Glucose	64-140 mg/dL
Blood Pressure	120-160 mmHg (range is from hypotension to hypertension)
Temperature	97.0 – 105.0 F (varies across ages ,normal and abnormal condition)
Hemoglobin	1.1-17.2g/dL (varies between male and female)
Blood Flow	Greater than 0.9 ABI(normal), Less than 0.5 ABI (abnormal)

Photoplethysmography (PPG)

A pulse oximeter is a measuring device that indirectly reads the oxygen saturation level (SPO2) and the changes in blood volume, which coincide with the cardiac cycle. It can be fixed to a finger or to earlobe. The pulse oximeter (Spo2) consist of red and infrared light emitting diodes (LEDs) and photo detector. The photo detector measures the amount of light reflected by the body parts illuminated by the red and infrared light emitting diode (LEDs).Which indicate the amount of light absorbed by blood that flow in the body organs. The relative absorption of light by the blood is related to the ratio of oxygenated hemoglobin to deoxygenated hemoglobin and this principle is taken for spo2 measurement. The quantity of blood flow varies with time, gives an overall variation in the light absorption. This generates a quasi periodic signal represented as a photoplethysmography (PPG), which

directly measures the heart rate. Yang and Rhee et al., [17] designed a PPG wearable biosensor, in the form of a ring likely to be worn continuously, making suitable for continuous monitoring.

Figure .4.PPG Ring sensor [56]

Another re-defined ring sensor with more resistant to noise component created due to motion and changes in light level was designed by Asada et.al [18].This contributed to an idea with reduced power consumption by high frequency and with low duty cycle modulation, where an image of it is presented Figure .4.

Electrocardiogram (ECG)

The spreading of electric charge through the heart muscles, with respect to time. The spreading of these charge result in quasi –periodic contraction of the heart muscles this is represented in an ECG waveform.

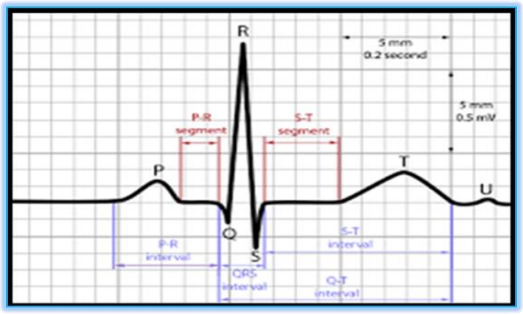

Figure .5. ECG Signal Features

Thus with a twelve lead configuration, a non-invasive means of studying the electrical activity of the heart can be made. Fulford-Jones et.al modeled [19] an Mica 2 mode [20] supporting a ECG sensor ,acting as a Hardware component ,coordinates with two electrodes and generate a single ECG signal. The AMON method includes an ECG sensor that generates a Single-Lead ECG signal. A simple ECG signal is shown in figure .5.

The sensor also utilizes an algorithm that calculates, RR distance, QT interval and QRS pulse width from the ECG waveform. Cao et.al. have developed a wireless three-pad ECG system [21,22] , A pad placed on the human body have two – three electrodes and sealed in a board and at the input placed a amplification circuitry. The benefit of this scheme over the others mentioned is that it enables the user to synthesize straight 12-lead ECG signals from the three leads being measured

Electroencephalography (EEG)

It represents the electrical activity of the brain. Recordings in mobile EEG (AEEG) have immense value in diagnosis of epilepsy and during continuous monitoring of a comma patient. During daily routine activities, Wireless EEG sensors makes the recording of EEG signal, less weight and less obtrusive. Jovanao et.al., have proposed using their Wireless Intelligent Sensor(WISE) for EEG signal acquisition applications [23]. This sensor is a microcontroller-based system capable of data acquisition, analog signal conditioning, low-level real time signal processing and wireless communication. The latest design proposed by FArshchi et.al. have created a wireless

neural interface, using Mica2 dot [24] systems as the wireless sensor platforms, which is modeled to acquiring two channels of EEG data [25].

Electromyography (EMG)

The study of function of muscle through monitoring the electrical signals emitted by the body muscles [26] is called EMG. When a superficial muscle contracts, it emits anelectrical signal that emanates from several muscle fibers combined and connected from different motor unit. These electrical signals can be received by placing a surface electrode above the skin and the spatrio-temporal summation of these electrical signals is called electromyogram (EMG). Thus, EMG signals are considered as the best means for monitoring muscle activity.

Implanted Sensors/ Actuator Systems

The above described electrical monitoring devices, ideas,implementation and prototype designs have given the proven and implemented ideas [27] in the application of WBAN systems consolidated and given by Garth V. Crosby et.al. The Sensor and Actuators made at their basic level is without a security structure in protecting the data collected by them when combined with a Wireless network.

Neural Stimulator Implant in human body

If the patient is suffering from either Parkinsons's disease, intractable epilepsy or some chronic pain, as a treatment measure, Implantable neural stimulators [28] are placed into the brain or spinal cord where it helps to send electrical impulses to actuate the nerve system.

Glucose Monitoring

There is a risk of Hypoglycemia, if the blood glucose level gets lowered. Continuous monitoring can be enabled by placing implantable sensor inside the subcutaneous tissue of abdomen. The radio transmission of glucose data occurred in every 5 minutes and the glucose level can be monitored for every 30seconds [30].With a closed feedback loop [29] in the implanted sensor , a drug delivery system is placed in the feedback path which injects a variable amount of insulin in the blood stream for the control of blood glucose level .

Technical Requirements

The various vital signs when measured with Bio-sensors show the following technical requirements given in Table .2 [32] that must be considered for the design purpose of the Biosensors and for the on channel processing devices. The author Maulin Patel et al. , has framed all the technical requirement of the WBAN in his paper [32]. The wireless technology has improved in a drastic manner with the increased awareness of monitoring the vital signs of the patients. Due to this, the wireless body area sensor networks has got its reflection and improving.

The stringent requirement and wide range of application, has made WBAN as its own technical specification [31] which is listed in Table 3

Channel Modeling

Channel modeling is a crucial task as it involves human subject, where the sensors to be placed and the regulations doesn't permit it. Also the mobility/movement of sensors makes the empirical calculation more complicated.

Physical Layer Design

In the PHY LAYER design technology of WBAN the channel model plays a crucial role. As the WBAN can be placed on various parts in and around human body, it needs a health care facility to complete the network. It makes difficult to set up an experimental channel modeling to sense, aggregate and transmit these signals. Also the motion of these sensors, running, rapid changing environment, mobility and multipath, makes the channel model more complicated, where very limited information and models are present [33].

ISSN: 0975-8585

Antenna Design

The design of antenna in an hostile environment is really a challenging issue. The placing of antenna in and around the patient's body makes it difficult due the size, shape, material and by the position [34].

In Communication, usually antennas made of copper will be placed for good transmission and for receiving good signals. But, in case of implantable sensor, only a biocompatible and non-corrosive metals can be used. In that case, only platinum and titanium are suitable. Unfortunately, both are proved as week in communicating signals. The position of antenna also depends on the patient's aging, location and posture which limits the implementation [35].

Table. 2.Technical Requirement of BAN. [32]

APPLICATION	TARGET DATA RATE	NO OF NODE	TOPOLOGY	SETUP TIME	P2P LATENCY	BER	DUTY CYCLE	BATTERY LIFE TIME
DEEP BRAIN STIMULATION	1 Mb/s	2	P2P	< 3 s	< 250 ms	10^{-3}	< 50%	>3 years
HEARING AID	200 kb/s	3	Star	< 3 s	< 250 ms	$< 10^{-10}$	< 10%	>40 hours
CAPSULE ENDOSCOPE	1 Mb/s	2	P2P	< 3 s	< 250 ms	$< 10^{-10}$	< 50%	>24 hours
ECG	72 kb/s (500 Hz sample, 12-bit ADC, 12 channels)	< 6	Star	< 3 s	< 250 ms	$< 10^{-10}$	< 10%	>1 week
EEG	86.4 kb/s (300 Hz sample, 12-bit ADC, 24 channels)	< 6	Star	< 3 s	< 250 ms	$< 10^{-10}$	< 10%	>1 week
DRUG DOSAGE	< 1 kb/s	2	P2P	< 3 s	< 250 ms	$< 10^{-10}$	< 1%	>24 hours
EMG	1.536 Mb/s (8 kHz sample, 16-bit ADC, 12 channels)	< 6	Star	< 3 s	< 250 ms	$< 10^{-10}$	< 10%	>1 week
O2/CO2/BP/TEMP/RESPIRATION/ GLUCOSE MONITORING,ACCELEROMETER	< 10 kb/s	< 12	Star	< 3 s	< 250 ms	$< 10^{-10}$	< 1%	>1 week
VIDEO/MED IMAGING	< 10 Mb/s	2	P2P	< 3 s	< 100 ms	$< 10^{-3}$	< 50%	>12 hours
AUDIO	1 Mb/s	3	Star	< 3 s	< 100 ms	$< 10^{-5}$	< 50%	>24 hours

ISSN: 0975-8585

Table. 3.Stringent Requirement of WBAN. [31]

CHARACTERISTIC	REQUIREMENT	DESIRE RANGE
OPERATING SPACE	In, on or around the body	Typically 0–3 m and extendable up to 5 m
NETWORK SIZE	Modest	< 64 Devices per BAN
DATA RATE	Scalable	From sub kb/s up to 10 Mb/s
TARGET LIFETIME	Ultra-long for implants Long for wearable	Up to 5 year for implants Up to 1 week for wearable
TARGET FREQUENCY BANDS	Global Unlicensed and Medical bands	MedRadio, ISM, WMTS, UWB
PEAK POWER CONSUMPTION	Scalable	e.g., Between 0.001–0.1mW in stand-by mode up to 30mW in fully active mode
MAC	Scalable, reliable, versatile, self-forming	Low power listening, wake up, turn-around and synchronization
TOPOLOGY	Star, Mesh or Tree	Self-forming, distributed with multi-hop support
DEVICE DUTY CYCLE	Adaptive, Scalable	From 0.001% up to 100%
COEXISTENCE	Coexistence with legacy devices and self-coexistence	Simultaneous co-located operation of up to 10 independent BANs
QOS SUPPORT AND DIFFERENTIATION	Real-time waveform data, periodic parametric data, episodic data and emergency alarms	• BER: from 10–10 to 10–3 • P2P latency: from 10ms – 250ms • Reservation and prioritization
FAULT TOLERANCE	No single point of failure	Ability to isolate and recover from failures. Self-healing capability
DYNAMIC ENVIRONMENT	Body shadowing (twisting, turning, running),attenuation	Seamless operation of multiple nodes moving in and out of range of each other
SECURITY	Many levels, long term, short term, light weight	Authentication, Authorization, Privacy, Confidentiality, Encryption, Message integrity
SAFETY/BIOCOMPATIBILITY	No harmful effects of long term continuous use	Meet regulatory requirements. e.g., FDA, SAR and HIPPA
SETUP TIME AND PROCEDURE	Not to be perceived as a slow or tedious	Up to 3 sec
ERGONOMIC CONSIDERATION	Size, shape, weight and form factor restricted by location and organ Non-invasive, unobtrusive, small size, weight and form-factor	unobtrusive, weight , form-factor ,Non-invasive,small size,
REPROGRAMMING, CALIBRATION,CUSTOMIZATION	Configurable, Personalized, integrated and context aware services	configure devices wirelessly ,Ability to reprogram, recalibrate and tune

WBAN Network Security Requirements.

The WBAN requires more security. While discussing of its security, this feature is enabled in all the communication systems, even in an emergency situation like Nuclear Leakage [36] To communicate between the Transceivers, with open radio frequencies, a simple Binary code is enabled. Below mentioned are the security requirements which must be attained, according to the Accountability Act of 1996 [37]

Data confidentiality

The Bio-sensors (BS) acquire vital data from the place it had been placed on patients, which also consist of actuators with it. Vital information transmitted from the Body Area Sensor Node (BN) on an open frequency can be directly exposed to an Adversary/Hacker who can eavesdrop(who copies the information) on the communication frequency and can overhear the critical/vital information. This overhearing of patient's date can cause serious ill effects like mistreatment which may at times lead to death and can also used for many illegal purposes. The confidentiality of patient's vital information over communication link can be achieved through a light weight cryptographic algorithm usually a symmetric key encryption [38] is the most reliable since public key cryptosystems [39] is too rich for an energy constraint sensor node.

Data Authentication

The data packets sent between BN and BNC must be authentic, that it must be verified that the data are sent from that trusted sensor and received by the BNC only and no fabricated packets or modified packets generated by the adversary are being communicated. A symmetric cryptograph technique is utilized for data authentication in WBAN and the cost of computation is very less. A search shared key is placed in BN and BNC, that computes message authentication code [40] of all data. (If the arrived data is from adversary, the Message Authentication Code (MAC) does not match with the BNC, then it knows, it was not sent from the trusted sensor).When a data packet arrives with a correct MAC, The BNC identify with its MAC and confirms as it is sent by a trusted BNs (Sensor) and receives and the decrypts the data.

Data Integrity

It is a security threat when a patient's vital body signs are transmitted / communicated over an insecure channel from BN to BNC.Due to lack of data integrity, the adversary can add some fragments or modify the data within the packet being communicated to the BNC. Deficiency in data integrity may lead to very dangerous ordering and does not provide guarantee database in life – critical situations. These data integrity can be achieved by implanting a data authentication protocol. This ensures that the received data is not modified by the adversary.

7.4. Data Freshness

The adversary may capture patient's vital signal in a transmission and reply them later in order to confuse the BNC. At the receiver end the delivered data frames must be in proper sequence and unused .there are two types of freshness i) providing partial message sequence ,without information delay is weak freshness. which is applicable in sensor measurement jobs and ii) providing full information sequence ,allows for delay estimation is strong freshness is useful for time synchronization within the network.

Secure Management

The BNC in secured manner associates and disassociates the sensing data sensor into the network. It also performs the secure management of the key pre-distribution to the nodes for encryption and decryption operation of data. [41]

Secure Localization

In many WBAN application areas, the accurate location of patient position is more important. But the tracking mechanism for patient, is low in technology and allows an attacker to send inappropriate locations of the patient either by presenting false signal strength or by replying signals. Thus, an exact location of patient can't be obtained for a particular application.

Availability

In WBAN, the main objective is to make patient related data available to the doctor, all the time. But the adversary may target the availability of the information by capturing or disabling (E.g. Capturing a retinal sensor node may result in loss of life). During this kind of critical situations, the BN must switch operation to another BN in case of loss of availability.

WBAN Security Threats and Attacks

The following presents the denial of service affecting the capacity and performance of the physical, data link, network layer of a WBAN protocol stack.

Physical Layer Attack

The major attacks that are challenging are physical attack, privacy violation and denial of service (DOS) attacks. As the sensor is closer in proximity of patient body so tampering of sensor is not that much easy. Privacy is considered as a fundamental right all over the world. Any inconvenience or interruption into any person's private life is contrary to law. So occurrence of any infringement on the part of any person's privacy is vehemently condemnable. But Denial of Service is a challenging issue. As the BN sensor nodes are stringent in battery power, protection against this is very difficult. When an adversary places a powerful sensor, it can easily jam a sensor node and prevent the BNC from collecting patient's vital information on regular basis. The Denial of Service (DOS) attack or attack on network availability affects the capacity and reduces the network performance of WBAN.In the following we briefly present the DOS attack to the physical, data link, network and transport layer of the open system Interconnection (OSI) protocol stack.

Data Link Layer Attack

The data link layer performs frame detection, reliability, and multiplexing and channel access. The attacks on this layer are collusion, unfairness and exhaustion. When jamming occurs at link level, it refers to collusion. When an adversary intentionally transmits extra packet/traffic with other nodes on the same channel, collusion occurs. Exhaustion of battery resource may occur when a self-sacrificing node always keeps the channel busy.

Network Layer Attack

Routing is not a necessary action in WBAN. It is not required to forward a data packet of a patient to other patient which misleads to life threatening situations usually the BNs are connected in star topology to the BNC whereas routing is possible when multiple WBAN's communicate with BNCs.

Table. 4. Various attack. [41]

OSI LAYER	DENIAL OF SERVICE ATTACK	DEFENSE MECHANISM
PHYSICAL LAYER	Jamming	Detect and sleep, route around jammed areas
	Node Tampering	Temper-proof boxing
LINK LAYER/MEDIUM ACCESS CONTROL	Collusion , Unfairness and Exhaustion	Authentication , anti-replay protection and Rate limitation
	Denial of Sleep	Authentication and anti-replay, detect and sleep, broadcast attack protection
NETWORK AND ROUTING LAYER	Homing	Encryption
	Misdirection	Authorization, monitoring

	Black hole	Authorization, monitoring, redundancy
	Neglect and greed	Redundancy, probing
TRANSPORT LAYER	Flood	SYN cookies
	De-Synchronization	Packet authentication
APPLICATION LAYER	Overwhelming sensors	Sensor tuning, data aggregation
	Reprogramming attack Authentication and anti-replay protection Authentication streams	Reprogramming attack Authentication and anti-replay protection Authentication streams
	Path-based DOS Authentication and anti-replay protection	Path-based DOS Authentication and anti-replay protection

Selective forwarding: When an adversary intentionally drops a BW in the routing path, it receives the packet and selectively forwards it just for a particular distinction or drops it completely (all packets).Where first level communication of WBANS architecture does not support selective forwarding attack [42](intra Ban),

Spoofing attack: When information are exchanged between nodes, the adversary try to alter, spoof or replay the information thereby making the network routing more complicated [43].

WBAN involve in Routing. The following attack's are considered.

Sybil Attack: The adversary claims multiple false identities or impersonating the existing ones. In WBAN at intra-BAN level of transmission, this attack can use feigned identities to send false information to the BNCs [44].
Hello flood attack: When the BNC is made to have a large number of connection request by an adversary, low memory space of the device suffer to satisfy the supply request ,so this kind of flood attacks are more vulnerable in WBAN[44].

Transport Layer Attack.

The transport layer has two security threats, flooding and de-synchronization. In flooding attack, the adversary send continuous connection request until a maximum limit or exhaust of memory is achieved. In de-synchronization attack the adversary forges the data packet between BNs, causing them for an infinite cycle within the WBAN.

Regulatory Laws

Issues regarding medical security and privacy regarding medical records, is gaining significance all over the world, which has ultimately led to various regulatory laws in order to prevent its misuse. Each and every country differs in their own regulatory laws relating to this current issue. Health Information Technology for Economic and Clinical Health Act (HITECH) [45] has contributed to the regulations that are to be followed by doctors, hospitals, health care organizations, other professional or people related to medical or health professionals. The said Act concentrates more on security measures for data administration policies, data safeguards and supporting systems. According to this Act, persons or health care providers who disclose the patient health information for any kind of money-making activities or for any harm, will be subject to strict civil and criminal proceedings leading to either fine of $250,000 or imprisonment for 10 years. Further, the Act also ensures

- Security and confidentiality of the patient health report.
- Protection against violation of security, confidentiality and integrity.
- Protection against unauthorized access or use of patient medical records or information.

The HITECH Act also encourages the act of enlarging the use of Information Technology to store, transmit, capture, share and use data regarding health care. It further introduces the new provision stating that when there is any breach on the security or privacy and if the patient health information [45] has been leaked/disclosed, person or the respective organization who manages the said record is bound to notify it to the aggrieved patient.

Even though there exists various regulatory laws pertaining to the medical security and privacy, certain situations fall as exceptions where the information's has to be let out to other persons or rescuers in case of emergency which cannot be prevented.

Proposed Security Mechanism with Physiological Signals

The Body Area Sensor detected signals are very safely exchanged between nodes and with BNC by the following mentioned methods with computation, memory and battery life time in constrain which are very limited in WBAN, but not losing the trade off in security of the subject physiological data. Mostly the papers utilize physiological signals [46,47] (Either a ECG or a PPG) for the generation of common key in nodes and the light weight identity based- cryptography. Many other biometric based cryptosystems have been published like face recognition, finger print and iris scanner images. But they developed it as a fixed template for an individual. When this bio-template is compromised at any point of communication, the entire network and data gets exposed to the attacker.

We have focused only on wearable and implantable Bio-sensors. Electric data from human body is used to generate session/common key inside node as they are random, unique and can't be recreated by another individual. The key generated from such a Bio-signal must satisfy the goals of the secret key like (i) *length* of the key (128 bits long), (ii) *Random*, (iii) *time variant,* where knowing the physiological signal at any time will not provide any significant advantage in predicting the future generating key, (iv) Distinctiveness, it clearly states that physiological signal of one individual cannot be used for another patient and (v) the physiological signal must be an universally measurable quantity. The below discussed methods utilize the schemes like fuzzy commitment [48], fuzzy vault scheme [49], its latest fuzzy extractors [50] and Biometric symmetric keys [62] based for maximum security.

The paper Biosecure presented by Krishna et.al [51] in 2003 proposed a completely novel method of key generation and distribution in centralized manner shown in Figure. 5 which does not utilize the cryptosystems scheme which is being utilized by other authors at the time of light weight cryptography. A novel approach is designed in which the secure intra body communication is achieved with Rivest Cipher 5(RC5) [52] and Message Digest 5 (MD5) algorithm [53] that existed previously and modified for the resource constraint system for encryption of subject data. The author used fuzzy commitment scheme for data communication. The entire process is that the data is encrypted with a key, generated with an ECG signal generated by the patient, at that instant mentioned as session key where the idea of key pre sharing or the extra communication over head is pulled off from the system the commit and encrypt key are combined and encrypted with commit key and the encrypted data with session key are added by MAC (Message Authentication Code) [54] and all the three values are combined and then transmitted to the receiver who also generates its session key from the ECG signal. If the session key and MAC of the sender and receiver matches, the data is decrypted and used, else rejected. Still the data is secure to communicate with nodes and not with control node which needs an additional node deployment. This fuzzy commitment scheme doesn't address much about node sensing error. Implementation details are not being presented in this paper, but this technique has reduced the computation and complexity when compared with the primitive Asymmetric technique.

To secure WBAN poon et al., [55,56] used the time information of heart beat as an excellent biometric characteristics. To secure the WBAN, a biometric value is generated from a sequence of ECG signal where the Inter-Pulse Interval (IPI) which is the timing information of the source signal from human being is taken and this IPI is generated which is used as the security key. The IPI is used for two basic purpose; one is to secure the transmission of secure key between the two nodes and another is that it is also used as an identity for mutual authentication between sensors. But the experiment shows that the average hamming distance between the key generated from

ECG signal sources for the same subject is 65 or 60, even though the key are long and random. As this randomness test passed standards imposed by the National Institute of Standard and Technology (NIST) [57], this kind of key generation is accepted. However an R-wave detection process is required before IPI measurement, which not only increases the computational complexity, the accuracy of R wave detection also affects the performance of IPI – based security mechanism. In addition we are required to measure 30 seconds of the ECG/PPG signal to generate a 128 bit unique key that is extracted only from the last 4-bits of each IPIs, that is approximately 32 IPI's, which needs a 33 consecutive heart beat signal to be measured, which increases the Bio-signal measuring time difficult for a Real –time system and computation length, which is again a resource constrain system.

In [58], the author venkatakrishna et al., 2008 described the implementation of a WBAN key sharing, with PPG based physiological signal. This implementation used the fuzzy vault [47] method of securely exchanging the Secret/Session key (S). The architecture support solely in inter-sensor communication. This paper mainly focuses on generating a set of common points from the PPG signal captured from a single patient. This set is used to construct a V^{th} order polynomial, where the secret key (S) is Hidden in the coefficient of the polynomial. To unlock the fuzzy vault, the receiver will also generate a similar set of points with the same PPG signal but detected at some different part of the human body (finger tip or ear). When a minimum number of values from transmitter set matches with the receiver set, then the vault can be unlocked and the secret random key is extracted, which conforms the sender node is the authentic node kept in same subject and this is secure for further data exchange.

The disadvantage in this idea of using fuzzy vault is, adding some amount of chaff points at the sender end to the set points makes extra over head for communication and in the receiver end removing this chaff points put additional effort in computation, both of this communication and computation over head are made in extra cost of energy consumption of the sensor.

In [59] this, the author venkatakrishna et al.,2008 designed an ECG based key agreement scheme (EKG), He had designed a secret key generation method, in which the key is generated by sampling the ECG signal, with that a FFT is performed, out of it 320 coefficient is selected and grouped. This method uses the SHA-256 hash [60] value of the 320 coefficient (Secured Hash Algorithm-256).The random key is generated and it is hashed with the EKG coefficient data, time and Node ID. When both the sender and receiver EKG common blocks match the hash value at the receiver end, it decrypts the random key. The idea proposed is a novel one, where two different keys are used and Message Authentication Code (MAC) is applied. It becomes less complex and low communication architecture for a resource constrain WBAN network.shown in below Figure 6.

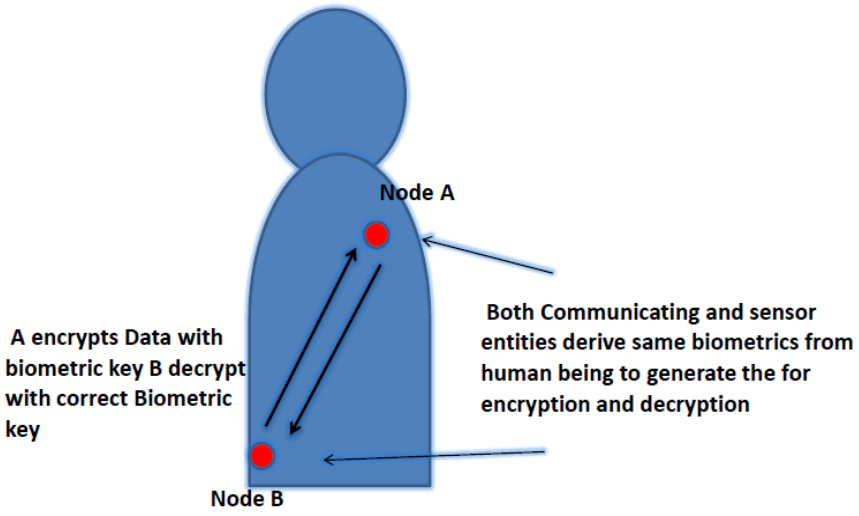

Figure 6. Biosensor Communication Scenario.

The author venkatakrishna et al.,2010 proposed PSKA [61] paper has very efficiently utilized the physiological signal of the subject, as these signal are unique, random and re-generation is highly difficult. He had

extracted the peak points in an ECG or in the PPG signal where the Fast Fourier Transform (FFT) is applied to the physiological signal. Here communication is between two sensors within a single subject. The coefficients generated are used by fuzzy vault scheme. The randomly generated key is securely locked in the vault with chaff points and exchanged between the nodes where the unlocking is possible with the same coefficient. With addition of chaff points, the security has increased. But the communication overhead has increased to a greater extent, thereby making it as a design not perfectly suitable for WBAN.

The author Fen miao et al .,[62] has taken the weakness of Biosignal dynamic random nature and modified the fuzzy vault .the paper had varied the parameter like the polynomial degree from 6 to 20 and reduced the half tolerance error rate (HTER) drastically by 10 times, also shown a good change in FAR and FRR .The basic aim is reduction in recognition error pattern of the Bio signal which is random, a linear block codes error correction scheme is utilized. An enveloping process is also additionally done to prevent real points from being revealed. The redundancy bits are generated from the Error correction codes which is additional confusion points when chaff points are already present in the scheme. Also the chaff points are generated using random number generation method which is complex and the overall computation is increased both in transmitter and in receiver, which is not suitable for WBAN.

The Author Lin Yao et al., has used the SVO logic [63] to formally verify the correctness of the algorithm proposed by him in this paper 2011 [64]. An image of the ECG signal is taken as the Biometric value from the sensor which is combined with random pre-deployed key given by the Control Unit (CU) with it a Bios crypt is generated at the bio-sensor and transmitted to the CU. There is a similar algorithm executed by the CU placed on the patient. Only this CU has the Biometric image captured at that instance. When both receive Bioscrypt and the Bioimage in XOR the resulting is the Key deployed by the CU. If resulting key match with the Key with CU the sensor is Authentic and legal, where data from this sensor can be accepted and can be processed. Further the old random number is incremented by some fixed value and encrypted with the Key which is matched successful. If the key is not matched, the author has not mentioned any steps in algorithm as of how to proceed further. This algorithm has the disadvantage like using an idea of the primitive algorithm like symmetric cryptography of deploying a pre-shared key in both sensor and CU. In this, an image of the Bio-signal is used, which is a new way of approach in WBAN which can also be considered as a demerit.

The improved juel's algorithm proposed by y.Dodis et.al. , [50] is an improved version of the fuzzy vault algorithm which uses a unique Monic polynomial to send the coefficients, also otherwise called as fuzzy Extractors, is applied in ECG-IJS for secure key exchange. In this author [65] zhaoyang zhang et al. , on 2012 constructed a more efficient algorithm that does not have a fuzzy vault in it, being completely removed, this is more energy saving when compared with PSKA of about 70% during transmission power, as it does not require to transmit any chaff points which makes an excess computation and additional bandwidth. This also includes a Hash based authentication of data between nodes. The only disadvantage is that the communication takes place between the nodes and not with the external interface.

The author Guanglou zheng, et al ., [66] has proposed a cryptographic security mechanism 2015 that utilizes the primitive idea known as One Time Pads (OTPs) and an Error Correction Codes (ECC). Combinedly the algorithm has stated that using the ECG signal, an OTP is generated as keys and Encryption is done with it. He referred as ECG Data Encryption (EDE). The idea proposed here has a major advantage as it does not require a cryptographic structure for key pre-deployment, refreshment, revocation and storage. This algorithm padded with OTPs, can resist against brutal force attack.

The author has specified the implanted sensor as Implanted Medical Sensor (IMD) which he has discussed as it does not initiate a session on its own to the programmer/Doctor. It is discussed that the OTP is a key, it is just a Binary string of the ECG signal from the patient extracted from the IPIs, where the long term signal are eliminated and only the Residual ECG signal are used to generate the OTP key. In this, secret S is used to generate the key and the author has not discussed in this paper. Then a hash (SHA-1) algorithm is computed on the cryptographic string combined with the ID details. Then the most distinct feature is that, all hashed details are transmitted in a public channel. At the receiver end, the key is generated with ECG signal, picked at different points of the human /patient

by placing the sensor externally by the programmer. On decryption, the cipher text and the secret S is evolved. At the receiver end the same hash algorithm is performed with the cipher text, ID of both devices and the secret S. If hash and the secret S of the transmitter and the receiver matches, then an acknowledgment stating "Success" is sent to the IMD else an acknowledgment statement "Failure" is sent to the IMD and asking for another key Agreement session.

The poon et al. , [55,56] proposed the IPI model, where the Binary Sequence (BS) extracted from the RR-interval of the ECG signal is used as the secret/session key of length 128 bits. But, from a single RR-interval only four bits are random. Thus, in order to generate a 128 bit BS, it requires to measure 32 IPI of ECG signal. For a normal human being having a 60-100 beats per minute (bpm) when considered, to generate a 128 bit BS, it requires to measure for time duration of 20-30 seconds. This time duration is more to measure and not suitable for real time systems. Thus, keeping his demerit in note the author Guanglou et al. , [67] proposed 2016, his model of measuring five distinct points from a single ECG pulse is used to generate the BS. In this algorithm, from a single ECG signal five features are traced and extracted (RR,RQ,RS,RP&RT).The author has come with a different solution of measuring the time interval between peaks with two number of CG signal and extracting the feature values. Where the interval are denoted as RR,RQ,RS,RP and RT ,with low latency computation, the time consumed in generating the random key is reduced significantly and he had achieved the goal of low latency for WBAN. It has shown these advantages also over the Pseudo Random Number Generation (PRNG) and complex computation schemes. A comparison table of all the Fuzzy vault system with Bio-signal as input is given with its various parameters in Table 5.

Other than these fuzzy security solutions various non-fuzzy vault methods has been proposed and effectively implemented. This methodology had given a good result and has also been compared. BARI+ [68] it is compared with LEAP+ [69] and shown that the Average Energy consumed is comparatively less. In OPFKA [70] the energy consumption is (0.2195mJ) and proved to be less compared to the PSKA . IBE – Lite [39] has been compared with Symmetric key and RSA algorithm, where the storage capacity and the data overhead is higher when compared to those two, Lightweight and Confidential Data Discover and Dissemination for Wireless Body Area Networks [12] which utilizes the concept of multiple one way Hop-in sensor nodes. The algorithm is based on Hash logic and an evaluation result is generated with the parameters like execution time, memory overhead, propagation overhead, energy overhead and proved to be higher in all data ranges .most of the above algorithms use the multi –hop or a sink model as shown in the Figure7.

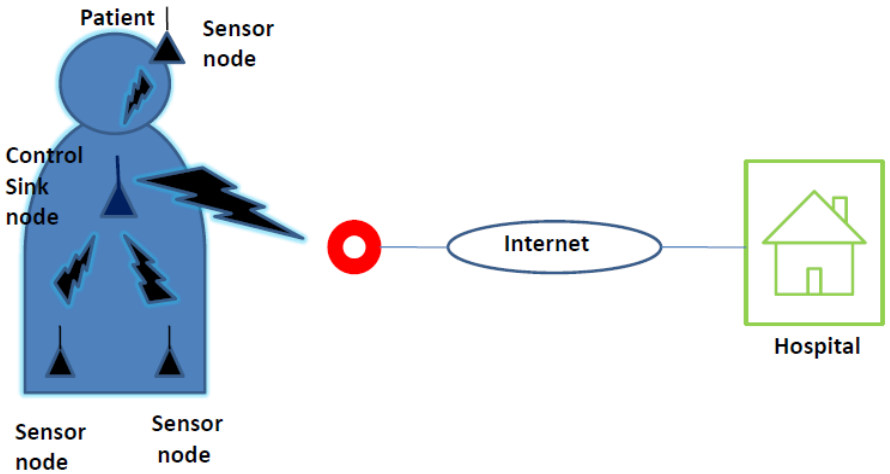

Figure 7. System model with Central Sink Node.

ISSN: 0975-8585

Table .5. comparison of various security methods

AUTHOR	INPUT BIOMETRIC SIGNAL / KEY LENGTH	TIME /FREQUENCY /WAVELET DOMAIN	FUZZY VAULT / CHAFF POINT	OTHER CRYPTO CODES USED
Krishna et al, [51],2003	Combination of Bio-Metric values / 128 bit key length	No signal processing	Fuzzy commitment Scheme / No chaff Points	RC5
poon et al, [55 ,56]	Electrocardiogram (ECG) / Plethysmogram (PPG BioMetric key length generated is 128 Bits	Inter – pulse – interval is taken/ Time domain analysis	Fuzzy commitment Scheme / No chaff Points	
Krishna et al, [58],2008	Plethysmogram (PPG)/ BioMetric key length generated is 128 Bits	Fast Fourier Transform (FFT)	Fuzzy vault scheme /chaff points 1000 combined with 30 legitimate signal	MAC-Not mentioned
Krishna et al, [59],2008	Electrocardiogram (EKG) / Bio metric key length generated is 128 Bits	Fast Fourier Transform (FFT)	Fuzzy commitment Scheme/ No chaff Points	
Krishna et al, [61], 2010	Plethysmogram (PPG) / Electrocardiogram (EKG)/ Bio metric key length generated is 128 Bits	Fast Fourier Transform (FFT)	Fuzzy vault scheme /chaff points	MD5 or SHA 1
Fen maio et al,[62], 2010	Electrocardiogram (ECG) / Plethysmogram (PPG BioMetric key length generated is 128 Bits	Inter – pulse – interval is taken/ Time domain analysis	Modified Fuzzy vault scheme /chaff points	
Yao et al, [64], 2011	Pre stored data /peak values of ECG signal	Wavelet Transform	Biometric Templates	Discrete hash and XOR
zhaoyang zhang et al,[65] 2012	Electrocardiogram (ECG)/ BioMetric key length generated is 128 Bits	Fast Fourier Transform (FFT)	Improved Fuzzy vault scheme /No chaff points	SHA -1(or) SHA-2
Guanglou zheng et al ,[66], 2015	Electrocardiogram (ECG) key and Bio metric key length generated 128 Bits RR – Time Interval	Time Domain analysis	One Time Padding (OTP)	Secure Hash Algorithm -1(SHA-1) And XOR

DISCUSSION

Security

Due to various technological advancements, fields like communication and sensing has come closer to the human perception. Data protection has become more significant than that of Data Acquisition as the Data may be hacked by either illegal social elements or any other interested parties. Its really a difficult task to protect the privacy thereby providing it a security solution. In this paper, various proven security approached to WBANs has been discussed. With all these novel ideas proposed, low resource constraint system, must be still explored. The IEEE 802.15 Task Group 6 [71] has been formed to provide standardization in security operations of WBAN and this will help to provide a security suitable for the near future.

Challenges in Preventive Healthcare

With the advanced developments in computer application, the WBAN is combining the cognitive interfaces and dynamic programming environment. It is possible to make multiple measurement in the human body and collect it to aid in preventing diseases /symptoms and diagnose them in a quick way.Power Consumption Of all the stages in WBAN network the BN performs sensing the data, computing and communicating. Of all these, the communication part is more expensive when considered with energy of the device. Hence in the above mentioned, all the security algorithm the number of communication path is reduced by one way hash function and Bio key, which avoids the phase of key deployment and in key authentication, thus connection expenses is eliminated. The use of Ultra wide Band Transceivers (UWB) [72] possibly reduces the communication based power consumption [73]. The data level duty cycle [74] combined with signal duty reduces the power consumption in WBAN. Thus by providing all these power reducing mechanisms, the life time of the sensor is extended and further avoids the replacement of battery, prevents from uncomfort and pain for the patient.

CONCLUSION

The recent development in the personal computing devices in the market goes hand-in-hand with the social network application, with it the WBAN can be boosted to a more active state. Although initially, WBAN was specially developed to provide a support for a particular application, on later days it got easily altered to combine with agriculture, education, business, entertainment and helping in constructing a smart environment. WBAN should be explored in a more interoperability nature for sending the data over other networks like internet and mobile, making it easily accessible and acceptable through the existing technology. For all these to happen unconstructively, the underlying major advancement should be made with regard to the privacy and data security of the patient related information and the applications running on them. To protect the patient data and the sensor node the above said fuzzy systems provide the un crack system .we have mainly concentrated on the Bio-signal based key generation method ,signal is processed in frequency or time domain which is advantages, need to combine a chaff points and also compared it with the other cryptosystems is greatly analyzed in this paper. When connected passively with other network, probability of changing the settings of the sensor is more when it is made available in social system which may result in vulnerable data privacy violation and any other attack. Thus, of all these systems discussed, the security is the primary concern in WBAN and it has been discussed here only with respect to Bio-signal with fuzzy systems.

REFERENCES

[1] Latré Benoît, Bart Braem, Ingrid Moerman, Chris Blondia, and Piet Demeester,M A . Wireless Networks2010; vol. 17: 1-18.
[2] http://www.who.int/mediacentre/factsheets/fs317/en/
[3] http://www.who.int/diabetes/facts/world_figures/en/index.html
[4] WHO Health Database. http://www.who.int/
[5] Abderrahim Bourouis ,Mohamed Feham and Abdelhamid Bouchachia.International Journal of Computer Science & Information Technology (IJCSIT) 2011;Vol 3(3):74-82.
[6] http://www.ieee802.org/15/pub/TG6.html, Date Visited, 16 December 2008.
[7] Sana Ullah, Pervez Khan, NiamatUllah, Shahnaz Saleem, Henry Higgins, Kyung Sup Kwak . Int. J. Communications, Network and System Sciences 2009; 797-803.
[8] https://www.fcc.gov/document/fcc dedicates spectrum enabling medical body area networks.
[9] Zimmerman, T.G. IBM systems J 1999;vol .38(4):566-574.
[10] Guang He zhang, Carmen Chung Yan Poon, Yuan Ting Zhang. ISNR Communication and Networking 2011.
[11] Karthikeyan, M.V., Martin Leo Manickam, J.International Journal on Recent and Innovation Trends in Computing and Communication 2015; Volume: 3(6): 3520 -3525.
[12] Daojing He, Sammy Chan, Yan Zhang, Haomiao Yang. IEEE Journal Of Biomedical And Health Informatics 2014; Vol. 18(2) : 440 – 448.
[13] Mohanavalli,S.S. and Sheila Anand.2011. International Journal of Ad hoc ,Sensor & Ubiquitous Computing(IJASUC) 2011; Vol.2(1):pp. 60 – 69.
[14] Poon , C.C., Wong, M.Y., Zhang, T.Y. Proceedings of IEEE/NLM Life Science Systems and Applications Workshop 2011;1-2.

[15] Anliker, U., Award,P.Lukowicz, J, Troster, G, Dolveck, F, Baer, M, Keita, F, Schenker, B.E., Catarsi, F, Coluccini, L, Belardinelli, A, Shklarski,D, Alon, M, Hirt, E, R. Schmid R, M. Vuskovic M.IEEE Transactions on Information Technology in Biomedicine 2004; vol. 8, :415-427.
[16] Carr, J.J, Brown M.J. Introduction to Biomedical Equipment Technology 2011.
[17] Yang, B.H, Rhee S.Robotics and Autonomus Systems 2000; vol. 30: 273-281.
[18] Asada, H.H., Shaltis, P, Reisner, A, Sokwoo Rhee. IEEE Engineering in Medicine and Biology Magazine 2003; 28 – 40.
[19] Fulford-Jones,T.R.F., Wei, Y.G., Welsh, M . 26th Annual International Conference of the IEEE EMBS San Francisco, CA, USA 2004 :2141-2144.
[20] Crossbow Technology, Inc. Mica2: Wireless Measurement System. http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/MICA2_Datasheet.pdf.
[21] Huasong Cao, Haoming Li, Leo Stocco and Victor C. M. Leung, M.C. 5th Annual International ICST Conference on Body Area Networks2010.
[22] Huasong Cao, Haoming Li, Leo Stocco and Victor, C., Leung M. 5th Annual International ICST Conference on Body Area Networks 2010.
[23] Emil Jovanov, Dejan Raskovic, Johnprice, john chapman , Antony moore, Abhishek Krishnamurthy. Biomed sci Instruments 2001;vol.37;373-378.
[24] http://www.xbow.com/products/Product_pdf_files/Wireless_pdf/MICA2DOT_Datasheet.pdf.Crossbow Technology, Inc. Mica2dot: Wireless Microsensor Mote.
[25] Farshchi, S., Mody, I., Judy W.J. Proceedings of the 26th Annual International Conference of the IEEE EMBS 2004.
[26] Basmajian, J.V., and Deluca, C., Muscles Alive.Baltimore: Williams & Wilkins , 5th edition 1985.
[27] Garth V. Crosby, Tirthankar Ghosh, Renita Murimi , Craig A Chin A . International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) 2012;Vol.3(3).
[28] Ghovanloo, M., Beach , K., Wise,D.K., Najafi, K. Proceedings of IEEE-EMBS Special Topic Conference on Microtechnologies in Medicine and Biology 2002;277–282.
[29] Garg,S.K., Schwartz, S, Edelman, V.S. Diabetes Care 2004; vol. 27: 734-738.
[30] Maloney, J.M, and Santini, T.J.J. Proceedings of the 26th Annual International Conference of the IEEE EMBS 2004; USA:2668-2669.
[31] Kiran Bynam, Noh-Gyoung Kang, Chihong Cho, Seung-Hoon Park, Sridhar Rajagopal, Eun Tae Won, Giriraj Goyal, ArunNaniyat, Mi-Kyung Oh, Hyung Soo Lee, Chul-Hyo Lee, Jae-Young Kim.TG6 Technical Requirements Document, IEEE P802.15-08-0644-09-0006.https://mentor. ieee.org/802.15/.
[32] Maulin Patel, JianfengWang.IEEE Wireless Communications 2010;80-88.
[33] Yazdandoost, M.K. IEEE 2009;802.15-08-0780-06-0006.
[34] Higgins, H, Yang, G.Z. In Body Sensor Networks, Ed. ,Londen ,UK, Springer 2006; 117–143.
[35] Zaric, A., Costa, .R.J., Fernandas, A.C.IEEE Transactions on Antennas and Propagation 2014 ;Vol.62 (12).
[36] Karthikeyan, M.V., Manasa R. Recent Advances In Space Technology Services And Climate Change (RSTSCC) 2010;25-28.
[37] The Health Insurance Portability and Accountability Act of 1996 (HIPAA),Centers for Medicare and Medicaid Services.
[38] Feldhofer, M., Dominikus, S, and Wolkerstorfer, J. Proceedings of CHES Springer Verlag 2004; vol. 3156:357 -370.
[39] Chiu C. Tan , HaodongWang, sheng Zhong, QunLi. IEEE Transactions On Information Technology In Biomedicine 2009; Vol. 13(6).
[40] Strong User Authentication and HIPAA: Cost-Effective Compliance with Federal Security Mandates. Available online: http://www.techrepublic.com/whitepapers/strong-user-authenticationand-hipaa-cost-effective-compliance-with-federal-security-mandates/2345053.
[41] Shahnaz Saleem , Sana Ullah , Kyung Sup Kwak. Sensor 2011; 1383-1395.
[42] Raazi, U.R, SungyoungLee, JCSE4 2010;23-52.
[43] Karlof,C, David Wagner. Ad Hoc Network 2003 ; 293-315.
[44] Douceur, J. Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02) 2002.
[45] Health Information Technology for Economic and Clinical Health Act (HITECH). http://waysandmeans.house.gov/media/pdf/110/hit2.pdf

[46] Available(online)http://physionet.org/physiobank/database/mitdb/ MIT-BIH,MIT-BIH arrhythmia database, Jul.10, 2012.
[47] Goldberger, A.L., Amaral ,N.A.L., Glass , L., Hausdorff ,M.J., Ivanov ,C.P., Mark ,G.R., Mietus ,E.J., Moody ,B.G., Peng, K.C.,and Stanley,E.H. Components of a new research resource for complex physiologic signals,Circulation 2000; vol. 101(23):215-220.
[48] Juels, A., and Wattenberg,M. Proc. 6th ACM Conf. Computer. Communication. Sec 1999; 28–36.
[49] Juels, A., and Sudan, M.Proc. IEEE Int. Symp. Inf. Theory 2002;408-415.
[50] Dodis,Y., Reyzin, L., and Smith, A. Advances in Cryptology—EUROCRYPT (Lecture Notes in Computer Science Series), C. Cachin and J. Camenisch, Eds. New York: Springer, vol. 3027; 523–540.
[51] Cherukuri, S., Venkatasubramanian, K.K., and Gupta, S.K.S. Proc. IEEE Int. Conf. Parallel Process. Workshops 2003; 432–439.
[52] Ronald.R.rivest.The RC5EncryptionAlgorithm 1997.
[53] www.saylor.org/site/wp-content/upload/2012/07/MD51.pdf
[54] www.saylor.org/site/wp-content/uploads/2012/07/Message-authentication-code1.pdf
[55] Zhang, Y.T., and Bao, D.S. IEEE Communication. Magazine 2006; vol. 44(4) :73–81.
[56] Shu-Di Bao, Poon, C., Yuan-Ting Zhang, Lian-FengShen. IEEE Transactions On Information Technology In Biomedicine2008; Vol. 12(6):772-779.
[57] http://www.nist.gov/
[58] Venkatasubramanian, K.K., Banerjee, A., and S. K. S. Gupta, S.K.S. Procedings of IEEE Military Communications Conference 2008; 1–7.
[59] Venkatasubramanian, k., Banerjee, A., and S. Gupta, S. INFOCOM Workshops 2008; 1-6.
[60] http://www-ma2.upc.es/~cripto/Q2-06-07/SHA256english.pdf.
[61] Venkatasubramanian, K.K, Banerjee, A., and Gupta, S.K.S. Trans. Info. Tech. Biomed 2010, vol. 14: 60-68.
[62] Fen miao, Shu-Di Bao.Global Telecommunications Conference (Globecom 2010) IEEE 2010;1-5.
[63] Lin Yao, Lei wang , Xiangwei Kong , Guoweiwu, Feng Xia.computers and mathematics with Applications 2010; Vol.60(2):234-244.
[64] Yao, L., Liu, B., Wu, G., Yao, K., and Wang, International Journal of Distributed Sensor Networks 2011.
[65] Zhaoyang Zhang, Honggang Wang, Athanasios V. Vasilakos, and Hua Fang.IEEE Transactions On Information Technology In Biomedicine 2012; vol. 16(6).
[66] Guanglouzheng, Gengfa fang , RajanShankaran and Mehmet A.orgun. IEEE Access 2015;Vol 3: 825 – 836 .
[67] Guanglouzheng,Gengfa fang ,RajanShankaran and Mehmet A.orgun .et al. IEEE Journal of Biomedical and Health Informatics 2016.
[68] Khaliq-ur-Rahman, Raazi Syed Muhammad, Heejo Lee , Sungyoung Lee and Young-Koo Lee. Sensors 2010; 10 : 3911 – 3933.
[69] Zhu .S, Setia, S., and Jajodia, S. ACM Trans. on Sensor Networks (TOSN) 2006:500–528.
[70] Chunqiang Hu, Xiuzhen Cheng, Fan Zhang_, Dengyuan Wu, Xiaofeng Liao, Dechang Chen. IEEE INFOCOM proceedings 2013: 2274 -2282.
[71] IEEE SA IEEE 802.15 WPANTM TaskGroup6(TG6) Body Area Networks http://www.ieee802.org/15/pub/TG6.html.
[72] Staderini, E.M. IEEE Aerospace and Electronic Systems Magazine 2002; 17(1) :13–18.
[73] Herwaarden, W.V., and Sarro M.P.Sensors and Actuators 1986;10: 321-346.
[74] Penders, A. J., Bert Gyselinckx, Ruud Vullers, Michael De Nil, Venkatarama S.R., Nimmala, Jef van de Molengraft, Firat Yazicioglu, Tom Torfs, Vladimir Leonov, Patrick Merken, Chris Van Hoo. International Workshop on Wearable and Implantable Body Sensor Networks 2008;94-98.