A Survey on Wireless Body Area Network Sensors and Security Issues

Sandeep K S, Hari Krishnan, Soumya K N, C R Manjunath

Department of Information Science and Engineering
School of Engineering and Technology, Jain University
Bengaluru, Karnataka, India

ABSTRACT

Healthcare has been the oldest and the most prominent industries in the history of humankind. Healthcare industry began with Ayurveda, Homeopathy, and now the Allopathy. Adding strength to these domains, e-healthcare and tele-medicine industries have started booming with the advent of technology. This has reduced the burden on small hospitals with limited infrastructures. With the growth of IOT and e-healthcare came Wireless body Area Network. Wireless Body area network with it brought implantable sensors, surface mounted sensors and held sensors. This has revolutionized the health care industry and made the lives of elderly and wheel-chair bound individuals' lives less cumbersome. Though in its youth stage, this technology still has many issues. One such issue is the security of the patient data being stored and transmitted. Here through this survey, we present various security issues with the Wireless Body Area Network. We also present the various kinds of sensors being used along with WBAN.

Keywords: Healthcare; Challenges; Security and privacy; sensors

I. INTRODUCTION

A wireless body area network (WBAN) is a wireless network of wearable devices. The aged and the diseased population in any country drives the technologists and physicians to come out with novel ideas. And the product of such an innovation was WBAN. The development of this technology started in around 1995 and this particular term " wireless body area network" was coined by Van Dam. Rapid advancements in wireless communication, semiconductors and Internet of Things has led to the improvement of this technology.

This technology consists of miniature and intelligent bio sensors installed inside the human body as implants or worn as a part of clothing as wearable technology or held by humans in pockets or hands. When the healthcare started booming its purpose was to deliver quality of life to individuals. For this to be achieved the patients have to visit their doctor with all their medical records. And further it is the responsibility of the hospital to arrange an appointment for the patient with the doctor. The doctor would have to analyze the previous prescriptions and suggest further medications to the patient.

This process is cumbersome as the patient will have to maintain the records as well as carry them along when he visits the doctors. But with the advent of e-health and IOT, the doctor can monitor the patient from at any place in the globe. This proves beneficial to aged and wheel chair bound patients as the doctor has access to all their real-time vitals like heart rate, brain liquid pressure, their calories burnt through physical activities, oxygen saturation, respiration rate etc.
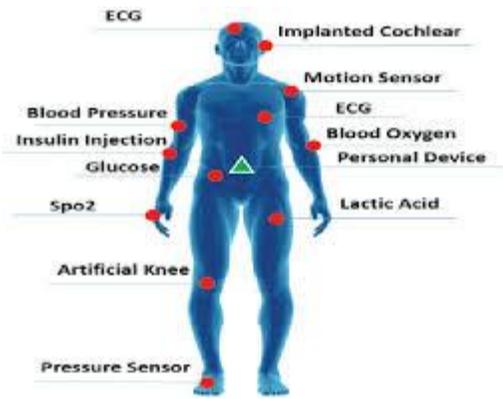
Fig 1. Vitals monitored by sensors

Using WBAN technology a lot of innovative applications are being developed. Some of them are ubiquitous health monitoring (UHM), Computer assisted rehabilitation emergency medical response systems (EMRS). The former frees people from visiting hospitals frequently and heavily depending on the hospital infrastructure and workforce. This is very beneficial for countries that do not have sufficient infrastructure for healthcare systems and enough trained workforce. While the latter is mainly used as temporary WBAN in disease struck areas to monitor the vitals of injured patients.

A. Challenges faced by WBAN in healthcare industry
1. Power supply issues: Most times the sensors are implanted inside the human body. In such cases, the batteries that power the senor are not replaceable. And hence, long lasting batteries or remote charging or charging through human body movements, body heat, body vibrations should be available.
2. Body movement: The patient is constantly in motion. So, the device should be robust and accommodate frequently changing network topology.
3. The electrically active circuits of sensors could cause electricity leakages and short circuits due to the inside of the body's warm, saline and electrolyte liquid rich nature. While the oxygen in the body can cause oxidation of the metal parts of the sensors. Hence, proper encapsulation from the surrounding environment is very necessary.
4. Heterogeneous device communication should be well established.
5. The data collected is very private medical data and hence strict confidentiality and security measures have to be taken to transmit data.
6. Miniature sensors consuming less power should be devised.
7. Quality of service(QoS): The data transmitted has to be error free.
8. Replacement of a sensor: Replacement of a sensor implanted inside a human body occurs usually through a surgery. And cutting open the human body every time is cumbersome as well as life threatening.
9. Compatibility with the human body: Sensors like smart tattoo and the ones implanted in the body should not cause any kind of harm (allergies or infections) to the human body. Hence biocompatibility is vital.

B. Other Applications of WBAN
1. Training athletes:
   Sports industry constantly strives to get the best performance out of capable athletes and therefore monitoring sportspersons on field body stimulus under various stress conditions is very necessary. Hence such systems, should deliver results in real-time and should be reliable.
2. Public safety:
   Roughly 98'000 individuals die each year due to medical mishaps caused by human blunder. Sensor Network can keep up a log of past medical accidents, and can advise the event of the same mishap and therefore can diminish numerous such accidents.
3. In uniformed services:
   Firefighters, cops, and military personnel are constantly fighting danger. Monitoring their body in real time is very necessary. Also, monitoring the environment around them for increased levels of toxins around them is equally important.

II. ARCHITECTURE OF A TYPICAL WBAN

WBAN consists of miniature sensor nodes surface mounted on the body or implanted inside the body or hand held devices. These devices respond to physical stimuli and transmit the vital signs across the network. It consists of a power unit, transmitter or a transceiver, and a memory unit. The challenges in the power unit of a sensor are variety. The battery should be long lasting as well body heat scavenging methods should be used.
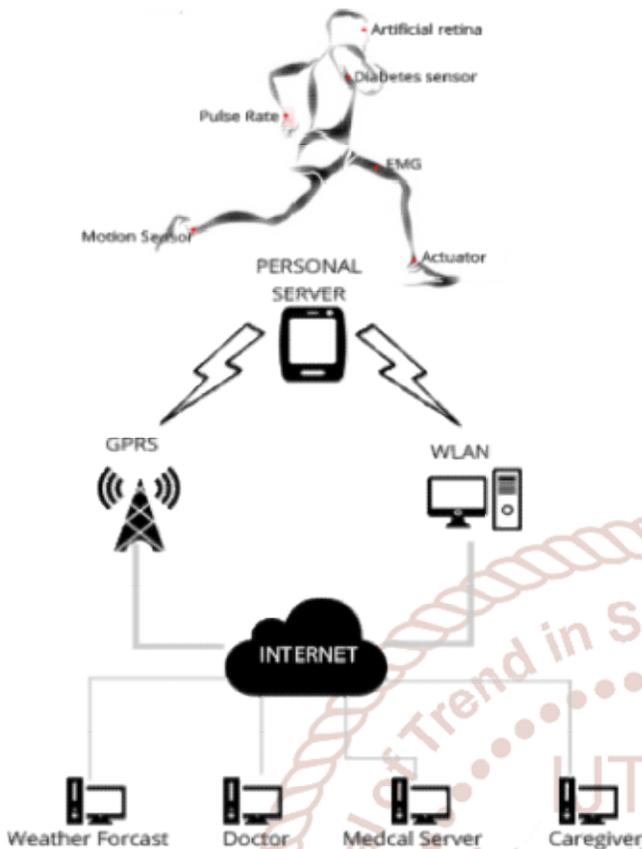
Fig 2. Architecture of WBAN

The information from the sensor node is routed to the Personal server or a Personal Device. This is also called the sink node or a Body Control Unit (BCU). This could be smart phone, a tablet or a smart monitor. . The main purpose of this is to communicate data sent by the sensors to external gateway.

Sometimes the sensor would be connected to an actuator. The actuators on WBAN usually act like drug delivery systems when triggered. The triggering happens either when the doctor notifies or directly when sensor given information falls below a set threshold.

The data passes through the gateway and goes to the medical server through the internet. This data stored in the server can be accessed by the doctor or a care taker.
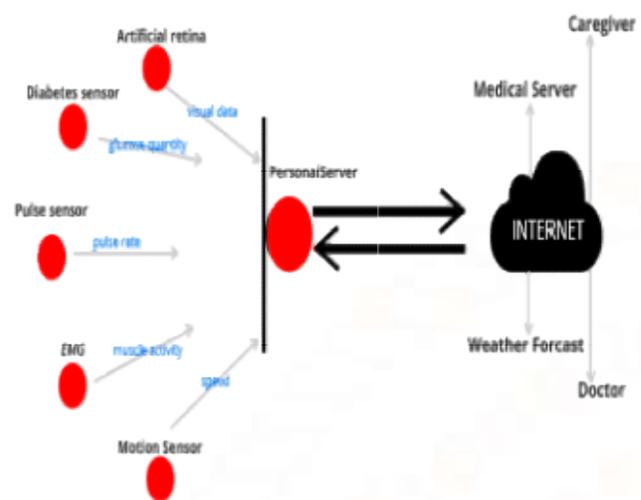

Fig 3. DataFlow diagram of a WBAN

III. SECURITY AND PRIVACY ISSUES

Security and privacy are the most important concerns in medical data transmission. If this data is not safeguarded then, privacy of the patients will be invaded due to the security breach. Several mechanisms for security have been devised yet 100% security has not been achieved. Data Security refers that data is stored in the database securely and transmitted among various nodes and tiers in the network securely. Data Privacy refers to inhibition of unauthorized access to critical patient information. A patient will always be concerned that his private health details will be stolen and misused. So security of such data will always be an important task.

A. SECURITY THREATS

Network security break is a situation where an unauthorized person gets to access stored or transmitting data. WBAN operates in an open access environment and hence it is very easy to accommodate attackers. And hence stored and data being transmitted will always be vulnerable to attacks. Some kind of attacks include eavesdropping, injection attacks and modification of critical data. Providing protection against these kind of attacks becomes even more difficult due to restricted power consumption. The malicious activities on a network occur due to incidental failure, where some node might leave the network and some may enter the network often, so that an attacker's false information may be inserted in the legitimate node, thus breaking patient information's security. The threats we just discussed can be categorized into two:

1. Threats occurring due to compromised device capabilities.
2. Threats occurring due to dynamically changing networks.

After analyzing all that threats posed to the security we have realized how important security is to our systems. To devise a stringent security protocol, resource constraints are usually a barrier. Some factors to be considered to devise an efficient security protocol are: data integrity, authenticity and confidentiality.

The following describe the goals or the necessities of a wireless body area network.

1. Data Confidentiality
Protection of data from eavesdropping and non - disclosure to other networks is an important issue. Data confidentiality can be achieved by using shared key, digital signature, hash function, two way authentication to encrypt the data over a network channel.
2. Data Authenticity
Identity of the nodes in the network refers to data authenticity. Both the member nodes and coordinator nodes need an assurance that the data is being arrived from a trusted sender (sensor). For this purpose, all the member nodes and the coordinator nodes will compute Message Authentication Code(MAC) for all the data being received by sharing a private key. If the MAC has been calculated correctly, then the member nodes and the coordinator nodes will come to a realization that the data is from a trusted source.
3. Data Integrity
The healthcare records are collected from many different patients and hence, it has to be consistent (a single source of truth). Any wrong information stored about the patient could be life threatening as the patient's medication is dependent on the information gathered from the sensor nodes. Data Integrity can be achieved by Data Authentication protocols, by assuring that the data is being arrived from a trusted source. Data signature techniques can be also be used to achieve data integrity.
4. Secure Management
Large amounts of data is generated by the WBAN network. And hence, managing the datasets generated securely is of paramount importance. For this purpose, encryption and decryption has to be carried out. Asymmetric key management,

Symmetric key management etc are some of the other technologies to provide for secure management.

5. Availability:
Data should be highly available at all times. Data availability at all times is very important in any medical application as it is very necessary to carry out the operation required, else it may lead to the loss of a valuable life. Backing up data in secured servers is an important step to achieve this goal.
6. Encryption:
This is an important method to achieve security of data. To decrypt an encrypted file there should be a secret code. Some of the encryption algorithms are RSA algorithm, DES algorithm(Data Encryption Standard) Advanced Data Encryption Standard etc.
7. Data Security:
Data Security refers to maintaining the overall confidentiality of the data in the databases from adversaries or unauthorized persons. The IEEE 802.15.6 standard helps to achieve this. A brief of this standard is given as follows:
    1) Level 0 - Unsecured communication:
    Lowest level of security. Data is transmitted in unsecured frames. It doesn't provide protection against replay defense, confidentiality, authenticity validation, privacy protection.
    2) Level 1 - Authentication but no Encryption:
    Unencrypted but authenticated frames are used to transmit data. It provides protection against replay defense, authenticity, integrity and reliability. But it doesn't provide for privacy protection and confidentiality.
    3) Level 2 - Authentication but no Encryption:
    Considering the well being of data, unauthorized access to data is prohibited. As the data contained in databases of WBAN have sensitive information about the person's health it can't be disclosed to unauthorized persons. Non-cryptographic methods are used to achieve this.
8. Data Privacy:
Considering the well being of data, unauthorized access to data is prohibited. As the data contained in databases of WBAN have sensitive information

about the person's health it can't be disclosed to unauthorized persons. Non- cryptographic methods are used to achieve this.

9. Interference:
   Interference between different networks belonging to the same domain can lead to data corruption. It can cause system failure due to signal degradation.

10. Data Freshness:
    To guarantee Integrity of data and confidentiality data freshness has to be guaranteed. Data Freshness refers to not reusing data and the frames being in correct order. There are two kinds: Strong Freshness and weak freshness. Strong freshness guarantees delay with ordered frames and weak freshness doesn't guarantee delay.

11. Packet Alterations:
    Packets while in transmission can be subject to modifications and security breaches.

IV. SENSORS

In today's fast paced world, there are numerous sensors being developed every other day. Medical applications of such sensors is mostly limited to huge medical machines operated by humans. With the development of WBAN its other uses in the medical field is being discovered.

As shown in the architectural diagram of a typical WBAN, sensors are the data collection units. The data collected from such sensors is relayed over to the personal server(your smart phone or monitor or smart tablet). From there, the data is sent to the person monitoring the patient(doctor or a caretaker) via a gprs or a wlan.

In the following table we discuss the various sensors being widely used in WBAN along with their uses. These are only a few of the widely used sensors.

Table 1. Sensors in WBAN and their applications

SENSOR	APPLICATION / DISEASE	REMARKS
ECG Sensors **Heart rate sensor** **Insertable cardiac monitor** **Pulse oxi-meter** **Holter monitor**	To track sudden heart related issues in long time cardiac outpatients	Insert able cardiac monitor is placed right under the skin to monitor heart for a long duration.
ICD (pacemaker)	arrhythmias	When irregular heartbeats are recorded it gives low energy electric pulses to bring it back to normal rhythm.
Accelerometers **Gyroscope**	Paraplegia	Some other kinds of sensors are used to stimulate movement.
Smart tooth	Oral sensory implant	Eating and talking habits of people can be detected.
	Alzheimer, depression	WBAN can help homebound and aged patients by detecting their mental behavior and alerting caretakers of any unwanted mishaps.

Pulse generator	Parkinson's disease	Implanted in the brain through a surgery. It provides electrical impulses to control body movements.
Artificial Retina	Visual Impairment (Retinal degeneration)	When light hits the eye it is converted into electrical signals that stimulate retinal neurons in the brain to restore vision.
Allergy sensor	Asthma	Detects allergens in the surroundings and alarms the patient if his body might react to the allergens.
EMG (electromyography)	Mobility impairment due to muscle problems.	Monitors muscle activity.
Electroencephalogram (EEG)	Sleeplessness, headaches, tumors in the brain, brain death	Monitors the brain's electrical activity.
Continuous glucose monitor(CGM) Insulin Actuator	Diabetes	CGMs are implanted under the skin usually near the right upper arm. It signals the doctor or the caretaker in case of drop in glucose levels.
Neural dust	Nervous system monitoring.	Monitors the nervous system using the ultrasound waves projected inside the body.

CONCLUSION

Wireless body area network is a rising and promising innovation that will change an individuals' health services encounters revolutionarily. In this survey, we tried to showcase how WBAN has been changing the world of medicine. We also tried to survey the various sensors used in WBAN and also the various security issues faced by this technology. We have also discussed the various other domains in which this technology is being used. The challenges presented in the paper can serve as future research domains to improvise the existing technology to make world a more better place to live in.

REFERENCES

1) Lawrence Yu, Brian J. Kim, and Ellis Meng. "Chronically Implanted Pressure Sensors: Challenges and State of the Field". Sensors (Basel) 2014 Nov; 14(11): 20620–20644. Published online 2014 Oct 31.

2) Hatice Ceylan Koydemir and Aydogan Ozcan. "Wearable and Implantable Sensors for Biomedical Applications".

3) Sofia Najwa Ramli, Rabiah Ahmad." Surveying the Wireless Body Area Network in the realm of Wireless Communication". 2011 IEEE

4) Deena M. Barakah, Muhammad Ammad-uddin. "A Survey of Challenges and Applications of Wireless Body Area Network (WBAN) and Role of A Virtual Doctor Server in Existing Architecture", 2012 Third International Conference on Intelligent Systems Modelling and Simulation

5) Duygu Karao ̆glan and Albert Lev ̇i. "A Survey on the Development of Security Mechanisms for Body Area Networks". The Computer Journal Advance Access published August 1, 2013.

6) Peter Van Daele, Ingrid Moerman, and Piet Demeester. "Wireless body area networks: status and opportunities".2014 IEEE

7) Shashi Kant Shankar, Anurag Singh Tom, "A Survey on Wireless Body Area Network and electronic-Healthcare",IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016, India.

8) Vikash Mainanwal, Mansi Gupta , Shravan Kumar Upadhayay. "A Survey on Wireless Body Area Network: Security Technology and its Design Methodology issue". IEEE Sponsored 2nd International Conference on Innovations in Information,Embedded and Communication systems (ICIIECS)2015

9) Smita Sharma, M M Tripathi, V M Mishra. "Survey Paper on Sensors for Body Area Network in Health Care".

10) M Raj Kumar Naik, P.Samundiswary. "Wireless Body Area Network Security issues- Survey". 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)

11) Samaneh Movassaghi, Mehran Abolhasan, Justin Lipman, David Smith, Abbas Jamalipour. "Wireless Body Area Networks: A Survey". IEEE communications surveys & tutorials, vol. 16, no. 3, third quarter 2014

12) Ibrahim Abdulai Sawaneh , Ibrahim Sankoh, David Kanume Koroma, "A survey on security issues and wearable sensors in wireless body area network for healthcare system