International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 14, No.1 (Sep-2023)

http://dx.doi.org/10.12785/ijcds/140153

A Survey of IEEE 802.15.6:
Body Area Networks

Sinan Ameen Noman[1], Haitham Ameen Noman[2], Qusay Al-Maatouk[3] and Travis Atkison[1]

[1]*Department of Computer Science,The University of Alabama, Alabama, United States of America*
[2]*King Abdullah II School of Engineering, Princess Sumaya University for Technology, Amman, Jordan*
[3]*School of Digital, Technologies and Art, Staffordshire University, Stoke on Trent, United Kingdom*

Received 04 Jun. 2022, Revised 13 Jul. 2023, Accepted 31 Jul. 2023, Published 01 Sep. 2023

Abstract: Recent advancements in wireless communication and integrated circuits have facilitated the deployment of Body Area Network (BAN) devices around the human body. These devices, known as Wireless Body Area Network (WBAN) devices, play a crucial role in ubiquitous health systems by monitoring and identifying diseases within the human body. This research paper provides a comprehensive overview of WBANs, including an examination of attack types, communication architecture, design considerations, and security protocols. By understanding these key aspects, researchers and practitioners can gain valuable insights into the development and deployment of WBAN systems, thereby enhancing healthcare monitoring and disease identification capabilities. The paper emphasizes the significance of security measures, such as encryption, authentication, access control, and secure key management, in safeguarding sensitive medical data. Moreover, it delves into the design aspects of WBAN devices, focusing on factors like power consumption, size, comfort, and wearability. Additionally, the paper explores communication protocols and architectures used in WBANs, addressing concerns related to data transmission efficiency, energy consumption, and quality of service (QoS). By optimizing these aspects, WBANs can ensure reliable and timely data transfer, improving overall network performance. Through a comprehensive analysis of WBANs, this research paper contributes to the advancement of knowledge in the field, offering valuable insights for the design, development, and secure implementation of WBAN systems in healthcare settings.

Keywords: Body Area Network, IEEE 802.15.6, Wireless Communication.

1. INTRODUCTION

WBAN stands for Wireless Body Area Network (IEEE 802.15.6) is a wireless sensor used to collect essential statistics about patients where the sensors are placed inside or over the patient body. In the past, the method of collecting information required the patient to be in a clinic or hospital with several wires connected to pads across the body. This raised health costs and limited the movement of the patient. Due to cost and time constraints, insufficient information could be obtained. Now things are quite different. When the WBAN showed up, everything changed. The body area network can now be created with fewer sensors, the positions of which rely on the type of information requested by the doctor to gather from the patient. With WBAN, the wires can be removed; it plays an essential part in improving the patient's comfort. The patient's data can now be sent in real-time rather than weeks later, providing potential treatment shortly and accelerating the diagnosis. There are several points to consider when designing a WBAN. Consider the implications of such a system; it would be able to sate small, networked devices' needs for high-performance processing power, allowing individual devices to tackle problems far larger than they are currently capable of. The rate of iterative processor upgrades would greatly slowed, as the expansion of device capability would no longer be conflated with corresponding logical processor updates. In effect, it would allow the burgeoning Internet of Things (IoT) to grow at a much faster rate, with a lower barrier to market entry [1].

The first point is what information we need to gather and which sensors we use to collect the data. The second point is storing data. The data can be stored on an application on a portable device like a smartphone, a computer application, or a cloud database. Features of the technological enhancements can include transferring data wirelessly from the WBAN sensors to the medical team, extending the collection time by optimizing the device power consumption, and an intuitive user interface to simplify the whole process. A Holter Monitor is an example of WBAN devices that are available nowadays in the health market. This device can gather and display the heart's performance and permits a doctor to determine if the patient's heart or if the patient

E-mail address: sanoman@crimson.ua.edu, h.ani@psut.edu.jo, qusay.almaatouk@staffs.ac.uk, atkison@cs.ua.edu

has a heart condition. It can be worn for 24 hours, transmits the data to a smartphone using Bluetooth, synced to the cloud, and provides an alert message to the medical staff when a flaw occurs. The device will reduce the diagnosis time, thereby allowing medical staff to reach the patient if abnormalities are detected instantly.

Apart from medical advantages, these WBAN devices can generate information when used in any physical activity, including fitness. This will help athletes and amateurs to track and understand their physical progress and extend their efforts to burn more calories. Efficiency and effectiveness, flexibility, and cost-effective are the main advantages of using WBANs. Moreover, WBANs may interface with other wireless technologies, such as Zigbee [2], Radio Frequency Identification (RFID) [3], WiBree [4], WPAN [5], WLAN [6], Video Surveillance Systems, and Cellular Networks. According to the World Health Organization (WHO), the aging population is becoming a significant dilemma at the same time that a sedentary way of life is causing plenty of people to have chronic diseases or suffer from obesity. Thus, it is fair to assume that this situation will contribute to an ongoing deterioration in the quality provided by healthcare system [7]. Figure 1 illustrates the statistics of aging population in developed countries. Briefly, several applications will benefit from the integration of emerging wireless technologies and WBANs such as fitness/health and monitoring, motion games, and assisted living applications that can improve the quality life of people.

The main purpose of this paper is to illustrate a survey on WBAN and its several application with the healthcare and non-healthcare industries. Section 2 presents different research studies related to WBAN. Section 3 presents the WBAN challenges. Section 4 presents WBAN applications. Section 5 presents the design aspects of WBAN. Section 6 presents the communication standards in WBAN . Section 7 examines the security protocols and technologies in WBAN. Section 8 illustrates the traffic types in WBAN. Section 9 presents the most common type of attacks in WBAN.

2. RELATED WORK

The following papers presents different research studies that illustrates techniques, algorithms, evaluations, and surveys that will help in improving the performance, security, and privacy in Body Area network devices.

Emil Jovanov, et al designed a wireless WBAN device that featured a standard radio Zigbee and a set of kinetic, environmental, and kinetic sensors [8]. They described how they rearranged their prototype WBAN communication for ambulatory monitoring and physical rehab applications. The system provides a real time analysis for data that being captured by sensors providing feedback and guidance to the patient. It also has the capability to generate warning messages on the user level of activity, state, and environmental conditions.

A research study from Kansas State University (KSU) , and University of Alabama in Huntsville (UAH) presents a survey of hardware and system level of WBAN infrastructure [9]. KSU efforts have focused on the development of a specific service called COBRA. This service is dedicated for medical information analysis and retrieval and HL7-compliant messaging tools. UAH efforts have targeted the development of activity and health monitors that use ZigBee wireless connection and hardware encryption in WBAN. Finally, their future efforts will include interoperability standards that will permit systems to be integrated with complex BAN infrastructures, negotiation of interface , and nomenclature.

A research paper proposed a solar energy node with a wearable sensor that allows the implementation of an autonomous wireless body area network for IoT applications[10]. The sensor can be placed on different body areas to diagnose and monitor physical signals such as heartbeat and body temperature. Moreover, the proposed sensor can identify falls using an accelerometer located on the node for emergency notification.

A research paper studied the functional, technical requirements, and core set of applications of the WBAN [11]. The researchers also talked about the main research challenges in WBAN, such as antenna design, QoS, reliability, scalability, privacy, security, scalability, and energy efficiency. Also, the researchers evaluated various technologies intended to address the emerging WBAN market. Finally, they present standardization activities in WBAN.

Researchers from China evaluated the WBAN in three different schemes' performance by using several metrics [12]. They also studied the mutual influences of contention-free period traffic (CFP) and contention access period traffic (CAP). Their outcomes exhibit that the non-slotted mode has more reliable performance than the slotted one in latency and throughput, but the power consumption cost is high. Finally, They gave suggestions for designing a novel Medium access control (MAC) for WBAN.

A research paper introduced a case study of security risk analysis of wireless body area network devices for health real-time remote monitoring and diagnoses as an after measure for deploying privacy and security features [13].They also evaluate privacy and security threats from the patient's point of view.

Researchers from National University of Singapore proposed a selective gateway method based on the residual energy of the sensor nodes [14]. This paper shows that the sensor node of a WBAN can be powered by the thermal energy collected from human temperature. The sensor node is provided with fall detection ability to support older adults' safety in a home environment and guarantees patients with disabilities in hospitals to be monitored by doctors and nurses timely.

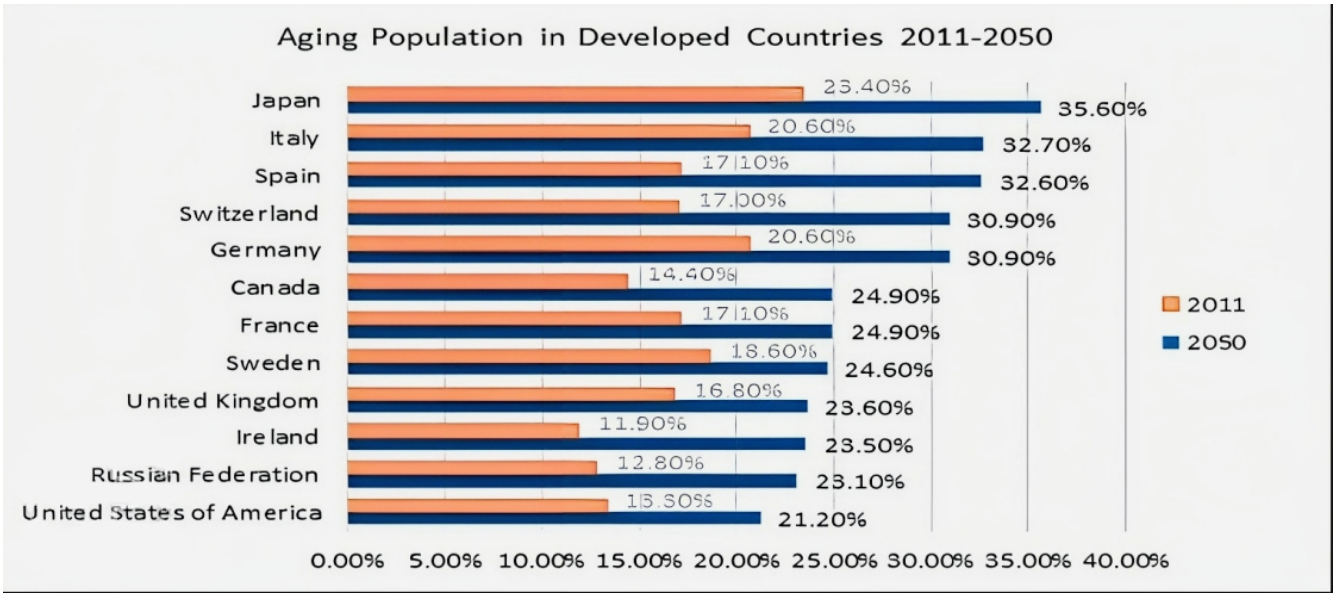


Figure 1. Aging Population in Developed Countries [7]

Researchers from the Harbin Institute of Technology presents a distributed WBAN for medical supervision. Their system contains three layers: remote monitoring network tier, mobile computing network tier, and sensor network tier [15]. Their system can collect, demonstrate, and store vital information such as Electrocardiography, blood oxygen, respiration rate, body temperature. Moreover, it also provides disease warning and medical service management. Furthermore, this paper sheds light on the system composition issues in design and implementation.

Chunqiang Hu et al. developed a security mechanism that makes a proper tradeoff between elasticity and security called FABSC [16]. FABSC stands for Fuzzy Attribute-Based Sign encryption that enabled data encryption, digital signature, and access control to patient's medical information in wireless body area networks. FABSC provides authenticity, confidentiality, unforgeability, and collision resistance. The researchers also were able to prove theoretically that their security mechanism is feasible and effective. Finally, they examined the security level of their proposed mechanism in practical WBAN.

Researchers from the Illinois Institute of Technology studied two crucial data security issues in WBAN [17]. Their research focuses on the security and reliability of shared data storage and patient medical data privacy. They reviewed several practical issues that need to be considered while fulfilling privacy and security requirements. Furthermore, Their lightweight scheme very efficient and has been validated through many experiments under different scenarios. They also make use of multi-hop on-body channel properties to improve the robust-ness of their authentication scheme. Finally, they surveyed and analyzed the applicability of relevant solutions in WBANs and sensor networks.

3. CHALLENGES OF WBAN

Although WBAN is helping significantly in healthcare ,medical systems, and other fields as well, there are still challenges to be tackled. These challenges are grouped into five main categories (Security, Privacy, Network, Energy Consumption, Mobility).

A. *Security*

Security is one of the primary challenges in WBAN. Many efforts have been made to achieve secure and accurate data transmissions in WBAN. The patient data should not be combined with data from other patients. The Data generated on the network should be secure; hence there is no unauthorized access to the data. Confidentiality, integrity, and authentication (CIA) are the primary security concerns of WBAN. In the case of a successful attack, such acts not only violate privacy but also lead to a disastrous scenario [18]. As reported in Healthcare IT news in February 2014, hackers breached a Texas healthcare system server, exposing the confidential health records of 405,000 people. This attack is considered as one of the highest HIPAA cyber-attacks. This attack also shows that implantable cardiac sensors can be compromised wirelessly [19]. We can see that from the previous case that security measures are mandatory to protect patient's data from possible threats. WBAN security architecture is more complicated and challenging than other networks. The performance requirements for WBAN architecture are (Usability, Scalability, Efficiency).

B. *Privacy*

Data confidentiality refers to the protection of data from being exposed by unauthorized access. It is considered as a crucial factor in WBAN. The WBAN devices used

in medical cases and are expected to transfer private and sensitive data about the patient's status. These data needed to be protected from unauthorized users and accessing these data might be dangerous to the life of the patient.

C. Network

As the network size grows, it primarily affects the performance and throughput of the network routing protocols. WBAN 's main limitations originate from resource limited devices and shared media. Bandwidth usage suffers from the sharing of links within each connected node.

• Multicast routing is an efficient technique for ad hoc networks due to frequent attachment and detachment with mobile nodes. It receives excellent attention in ad hoc networks due to its central broadcast capability and linking efficiency. There are various multicast routing challenges, include lack of quality of service (QoS), frequent updates, scalability, and multicasting delay.

• The self-organization of ad hoc mobile nodes is a challenging problem in many research studies with the effective routing protocol. Multi-hop routing is also a very effective approach if the source and destination are not connected directly. Dynamic topology, reconfiguration and management, free monitoring, no centralized control and scalability are the challenges posed by routing protocols. MAC layer is essential because it accesses the medium and communicates with the next hop. Hence, resource blockage, collisions could be managed in case of efficient MAC layer schemes. Hence, Carrier Sense Multiple Access (CSMA) and Back-off algorithm, handshaking, and contention windows need to be considered when designing and developing a MAC protocol for WBAN, mainly when there is ad-hoc connectivity.

D. Energy Consumption

As many WBAN devices are using wireless technology as their medium; hence, they are portable and wearable. WBAN devices' power is always limited; furthermore, these devices are small and carry a power source. There are many battery power management challenges, particularly in implanting small sensors in the patient body. The main issue is how we can make the battery inside the sensor to hold up for more than a month [20] . Removing the sensors and reimplant it will require even more management of the complications generated. The communication bandwidth and processing power are different parameters that play an essential part in the sensor's power consumption. Therefore, having better power management schemes and better scheduling algorithm is needed to be considered. Based on this method, energy harvesting can help eliminate the battery charging either partial or full. So solutions are more clean and green. Solar, thermo-electric, kinetic energy, and electromagnetic are examples for harvesting.

E. Mobility

Independence of location, and portable monitoring are the two main advantages in WBAN. However, the two advantages have limitations on mobility in some applications such as healthcare application. Mobility is defined as a seamless link between WBAN devices and users. Reach to sink is one of the biggest issues, and can be either single, or multi-hop.

4. WBAN APPLICATIONS

There are numerous valuable and innovative WBAN applications. When the WBAN is connected, it gathers the parameters of the body. The most popular applications are in the healthcare field. We categorize these applications into two main categories, i.e. Healthcare Applications and Non-Healthcare Applications. Figure 2 illustrates the medical and non-medical applications of WBAN.

A. Healthcare Applications

There are number of devices that can be attached to the patient's body, i.e. heart rate sensors, Electrocardiography, pulse Oximeter. Some of these devices are invasive while others are non-invasive devices. Figure 3 illustrates an example of WBAN healthcare applications.

• **Nitric Oxide Sensor:** This sensor can help in detecting Cancer cells. This sensor has the ability to detect Nitric Oxide when emitted from the cells in the affected area.

• **Movement Sensor:** WBAN helps the doctors to track and monitor the patient's movement which is required in home rehabilitation program.

• **Allergic Sensor:** This sensor can detect the allergic symptoms automatically in the environment and provide a report immediately to the doctor and the patient.

• **Insulin Sensor:** This sensor can monitor the glucose level inside the patient body when implanted, and able to inject the insulin automatically when needed.

• **Telemedicine:** Doctors can remotely diagnose and monitor patients using telecommunication technology. They can also give an online consultation to their patients.

• **Ambient Sensors:** These sensors are implanted in the patient's body and can help them stay at home and continuously monitored by the doctors without visiting the hospital. Furthermore, these sensors will give an urgent notification to the nearby healthcare in case of an emergency.

WBAN sensors can also track and monitor the health of uniformed workers as their purpose to maintain the security, safety, and peace of the public sector they serve, i.e., soldiers that require medical assistance during the war.

B. Non Healthcare Applications

• **Safeguard Applications:** Safeguard applications can monitor the toxic level in the air and notify the people in that area if there is a threat on their life when detected.

• **Sport Applications:** In the athletic field, there are several readings can be obtained from the athletes using

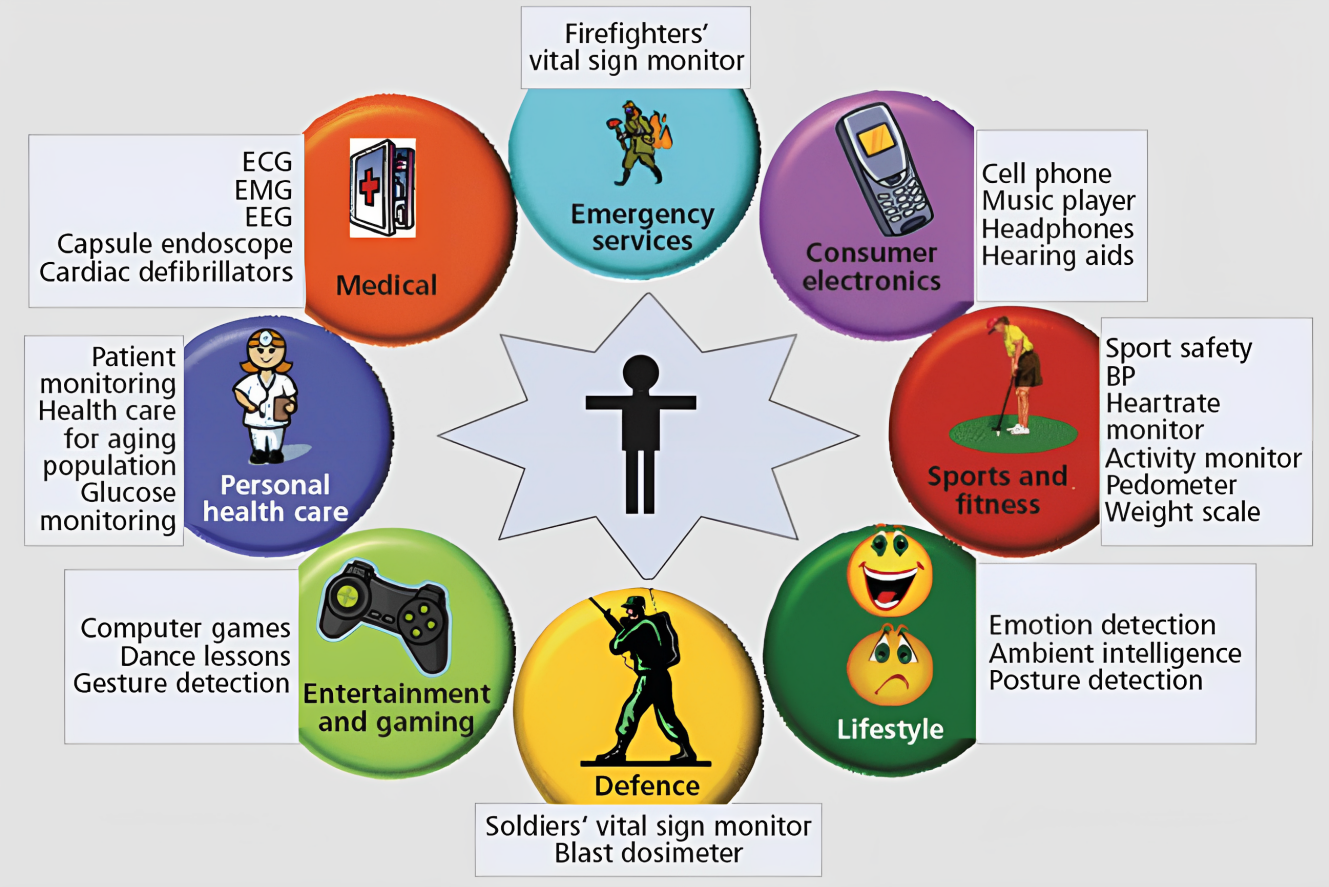


Figure 2. WBAN Applications

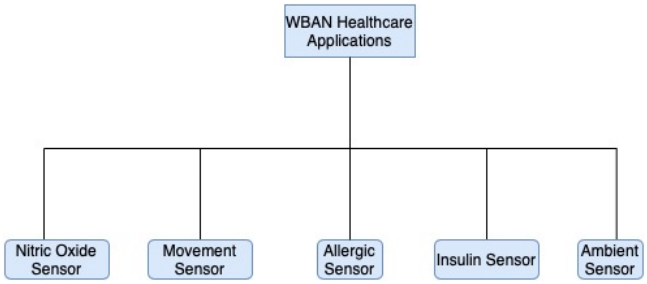


Figure 3. WBAN Health Applications

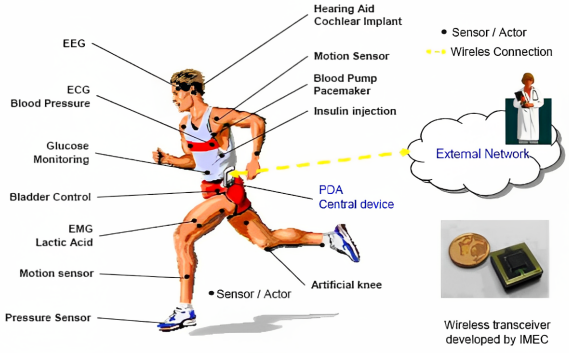


Figure 4. WBAN Sport Applications

WBAN devices without the need to ask them to be on a treadmill in a certain laboratory. These data can transform coach's decision-making and make the athletes improve their performance, and provide them with techniques to avoid injuries. Figure 4 illustrates the WBAN sports application.

There are several ways to use WBANs in the military. Some of these applications provides on different aspects such as location, health, temperature and levels of hydration. These readings can help in administering casualty care, such as morphine, enhance concentration, and strength improvement.

• **Military Applications:** There are several ways to use WBANs in the military. Some of these applications provides on different aspects such as location, health, temperature and levels of hydration. These readings can help in administering casualty care, such as morphine, enhance concentration, and strength improvement. A WBAN may become

Figure 5. WBAN Military Applications

Figure 6. Interactive Gaming Applications

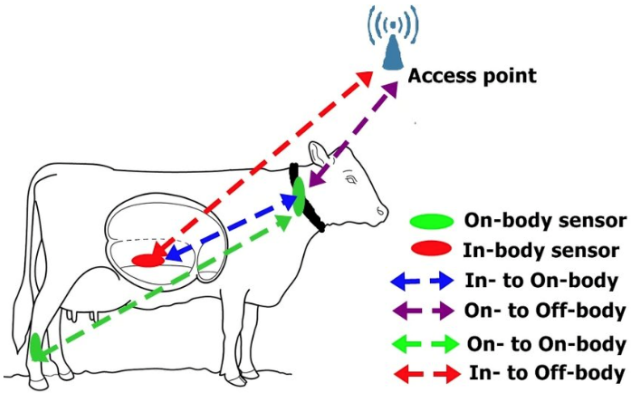


Figure 7. Types of WBAN sensors for animals

a wearable electronic network in a uniform battle dress that connects various types of devices such as cameras, health monitoring, PDAs, life support sensors, and sends data to and from the soldier's wearable device.

The network could perform different functions such as detector to prevent victims from friendly fire, monitoring the psychological condition of soldier, calling support by using the antenna that embedded in the uniform when something urgent happened, chemical recognition. As a result, WBANs demonstrate great opportunities for modern warfare survival and lethal. Figure 5 illustrates the WBAN military applications.

Interactive Gaming Applications: Body sensors allow gamers to perform real body movements, such as shooting, boxing, which can give a real-time feedback to the gamer on how many calories burned during the session. Furthermore, it will enhance their entertainment experience and give them a boost to improve their workouts. There are currently many companies that offer interactive gaming experience. For instance, in 2013, Microsoft offers a sensor called " Kinect", as with this sensor, it enables the user to track their calorie burn process across multiple games in real-time. Figure 6 illustrates three types of sensors that offered by Sony, Microsoft, and Nintendo. All of these devices are capable of tracking and monitoring the user activity.

- **Secure Authentication:** This application includes the use of biometrics, such as fingerprints, iris recognition, and facial expressions.

- **Animal Monitoring Applications:** There is a symbiotic relationship between animals and humans. WBANs can be used to improve and diagnoses various types of diseases in animals. The sensors can be either in-body , or on-body sensors. These animals can play an essential part in improving human health as they can feed humans with milk, eggs, and meat. Figure 7 illustrates the types of WBAN sensors that can be attached in animals.

- **Additional Sensors:** There are many other sensors that can be found nowadays in wearable devices such as Apple watch [21], which can provide information to the user like body temperature, speed, heart rate, oxygen level, location, and timer. The WBANs can provide interfaces for remote monitoring the physiological data of human body, drug administration in clinics/hospitals, and patients' rehabilitation. In the future, it will be possible to monitor patients continuously and provide them the medication they need, whether they are in home, hospital, or elsewhere. Table 1 illustrates various types of WBAN sensors with their measurements.

5. DESIGN ASPECTS

To ensure the functionality of medical monitoring WBAN devices, there are specific network and hardware requirements that needed to follow [22].

A. Network Requirements

1) Range

A range of 2-5 meters is enough, as WBAN enables the sensors to communicate with each other in or around the patient's body.

2) Number of Sensors

The standardization group of WBAN predicts a maximum of 256 appliances per network. WBAN standardiza-

TABLE I. Various types of WBAN sensors with their measurements

WBAN SENSOR	MEASUREMENT
Accelerometer	Movement
Gyroscope	Positioning/Orientation
Blood Pressure	Human body pressure
Blood Glucose	Blood sugar
Humidity	Room humidity
Temperature	Body temperature
Respiration	The rate of respiration
Electromyography (EMG)	Muscle functionality
Electrocardiography (ECG)	Heart functionality
Electroencephalogram (EEG)	Brain functionality

tion In order to monitor applications, a lot of actuators or sensors are needed on the same WBAN. A maximum of 256 per network are the number of sensors per network

3) Network Density

According to WBAN standard, the end-users should be able to have 2-4 sensors per m2.

4) Interference

In order to achieve reliable communication, interreference must be suppressed as much as possible.

5) Transmission Quick Time

A very fast transmission is very necessary, as the goal of it to monitor the patient's data in real time.

6) Encryption/Security

To achieve integrity from the transmitted data, The transferred data must be secured.

7) Reliability and Quality of Services (QoS)

Since reliability is one of the major requirements when it comes to design medical WBAN devices, the time delay should be less than 125 ms for medical applications and less than 250 ms for non-medical applications. On the other hand, the QoS will help in evaluating the delay in the proposed medical devices.

8) Compatibility

The proposed medical WBAN device should be able to communicate with other devices using personal area network (PAN), such as infrared, Bluetooth.

9) Different Data Rate Support

The data rate in applications have different requirements (between 10 kb/s to 10mb/s). The medical applications need lower data rate most of the time. On the other hand, the non-medical applications such as multimedia applications needs the most significant data rate.

10)Priority

The traffic messages of WBAN devices must be given priority over other network messages. There are three types of traffic have to be supported by WBAN: burst traffic, periodic traffic, and emergency traffic. The emergency traffic can send an alert to the medical staff in case of a heart attack or other severe problems.

B. Hardware Requirements

1) Low Power Consumption

This relies on the nature of the sensors whether invasive or non-invasive device and the type of application. It would be desirable to have an efficient power saving mode to avoid individuals to charge the application battery regularly.

2) Size of Sensors

Sensors should not affect the mobility of WBAN application. This can be achieved by making the sensors small, and the monitoring should be transparent as well.

3) Battery Lifetime

The need for increasing battery life in wireless sensor is growing. Hence, invasive sensors must have a long battery life. The product current draw must be kept to absolute minimum. This requires the company to use efficient techniques and low-power components to de-energize components when they are not in use.

4) Low cost

The low cost sensors is very important. To make a mass adaptation of WBAN devices, the monitoring application must be cheaper than the traditional monitoring system.

5) Low Complexity

The low-cost requirement is interconnected with complexity. The sensors have to be easily produced and have low-complexity to make them cheap. We can clearly state that when the sensors have low-complexity it will gain mass adoption. WBAN COMMUNICATION ARCHITECTURE Compared to current wireless communication technologies, such as Bluetooth, WBANs allow communication in or around the human body through sophisticated devices. Figure 8 shows the architecture of WBAN's health monitoring system. Blood pressure sensors and motion sensors such as (EEG, ECG, EMG) transfer data remotely to the personal server (PS) using Bluetooth/WLAN connection. The medical doctor's site will receive the data in order to do a real-time diagnoses.Furthermore, the data will be stored in a medical databases.

The WBAN architecture can be categorized into three Blood pressure sensors and motion sensors such as (EEG, ECG, EMG) transfer data remotely to the personal server (PS) using Bluetooth/WLAN connection. The medical doctor's site will receive the data in order to do a real-time diagnoses.Furthermore, the data will be stored in a medical databases.

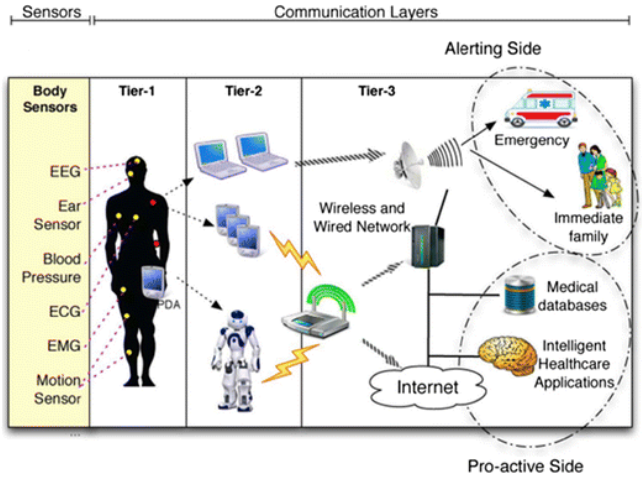


Figure 8. WBAN health monitoring system architecture [42]

Figure 9. The Ad-hoc based Inter-BAN Communication Architecture [23].

The WBAN architecture can be categorized into three categories: Intra-BAN communications, inter-BAN communication, and Beyond-BAN communication [23]. These components cover various aspects, ranging from high-level to low-level design issues. Furthermore, it facilitates the development of a component-based, and broad range of applications. Specific requirements can be obtained through market demand, and application's context by customizing each design component, such as coverage, reliability, QoS. The WBANs rarely works alone, unlike Wireless Sensor Network (WSN) that typically work as autonomous system. The inter-BAN communication can be defined as the communication between the access point and the personal server. The access point can be strategically placed in a dynamic environment to handle emergency situations. Furthermore, it can be implemented as part of the infrastructure. Likewise, tier-2 communication (as shown in figure 8) used to interface WBANs with several networks that can be easily accessed in daily life situation.

The inter-BAN communications model can be divided into two categories, ad hoc-based, and infrastructure based architecture [23]. While the ad-hoc based architecture is used to make fast deployment easier when it comes across a dynamic environment, such as disaster site, or on emergency response, the infrastructure-based architecture provide flexibility, centralized control, and larger bandwidth. Figure 9 illustrates the Ad-hoc based Inter-BAN communication architecture.

The Inter-BAN communication technology can be considered as mature, as it include: Bluetooth, Zigbee, cellular, etc. WBAN can be considered as a smart when the WBAN device can integrate easily with other applications. Bluetooth is a very popular wireless short-range protocol, but WBANs require protocols that supports low power consumption. Although Bluetooth has a very good short-range communication, it is not an optimal solution for WBANs. Most of WBAN applications prefer to use ZigBee protocol. As ZigBee has the ability to support mesh networks. Nowadays, ZigBee is used for communications between sensors in a network. ZigBee becomes very popular for five reasons, which can be addressed as follows: (1) provide longer battery life, (2) it generates low-power consumption, (3) supports 128-bit security, (4) provide low-latency communication, (5) it has the basic features for communication between the wireless nodes and sensors [23].

WLAN technology is used by most of the applications as it is much faster than the 3G/4G cellular networks. By contrast, many people carry their cellphones and uses the cellular network that offers a user-friendly interface and can be easily connected with peripheral devices.

Ultra-Wideband (UWB) refers to communication technology that uses a large bandwidth, which generally have a transmission bandwidth greater than 500MHz. The Federal Communications Commission (FCC) also facilitates license-free use of UWB in the 3.1 – 10.6 GHz band. This allows UWB application to be suited for indoor, short-range and RF-emission sensitive environments, such as hospitals. UWB is also an excellent technology for precise location, complementing the Global Positioning System (GPS) indoors for tracking WBAN devices.

At the same time, concerns about magnetic and electronic energy absorbed by humans from RF circuits placed in close proximity, which means that WBAN devices need to use low transmission, and low transmission power duty cycles. According to recent studies, WBAN standard will use UWB and exceeds conventional transmission in this respect. Therefore, it attracts a lot of attention. Within the IEEE 802.15.6 task group, an ongoing work aims to support various applications with various data rates, where QoS are essential in life-threatening circumstances.

When it comes to design of such networks, the user experience with video/audio streaming is also essential, although it is much less important. Some proposals are tuning the current IEEE 802.15.4 protocols to achieve

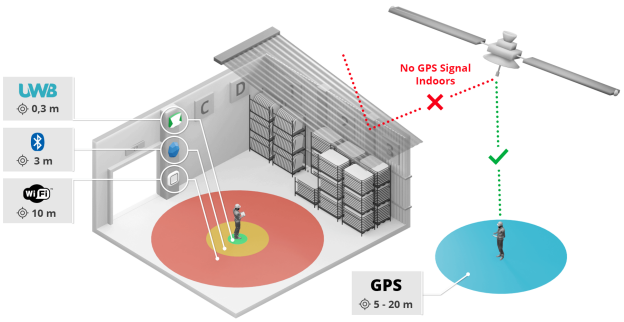


Figure 10. Indoor Positioning System & Global Positioning System [43].

better traffic from WBANs, while other are advancing a completely new strategy to use new radio technologies, such as UWB, to address new issues. Figure 10 illustrates the indoor positioning system (IPS) and (GPS).

6. WBAN COMMUNICATION STANDARDS

The motivation of wireless communities to standardize their technologies has several reasons behind it. Standardization enables wide use of the products through interoperability since manufacturers rely on fixed specifications to develop their products. Furthermore, customers do not need to rely on a specific vendor. Due to the nature of the body, the WBAN often follows a star topology. This section introduces the technologies that serve WBAN devices and focuses on MAC techniques to support WBAN.

A. IEEE 802.15.4 STANDARD

The Task Group 4 (TG4) introduced a communication standard called IEEE 802.15 provided toward Wireless Personal Area Network (WPAN). This technology has become the defacto standard that supports both WBAN and Wireless Sensor Network (WSN), called IEEE 802.15.4. Recently, many research studies have emerged on the design of WSN standards and power-aware algorithms. The IEEE 802.15.4 standard is taking into account both MAC and physical layers. Due to WBAN design challenges, designing these networks requires the need for new protocols. In this matter, the IEEE 802.15 community has introduced improvements to the MAC and physical layers of the IEEE 802.15.4 protocol stack to mitigate the drawbacks of IEEE 802.15.4.

B. IEEE 802.15.6 STANDARD

The current standards (e.g., IEEE 802.15.4) do not comply with medical communication regulations and standards, as they do not fulfill application needs in many aspects, such as power consumption, reliability, low power, and traffic issues. As a result, a new Task Group (TG6) proposed a new communication standard that focuses mainly on various applications, such as sports, medical, and military applications. This standard aims to achieve highly reliable, ultra-low power, and low-cost wireless communication. The new proposed standard (IEEE 802.15.6) offers three types of bandwidths established in three physical layers:

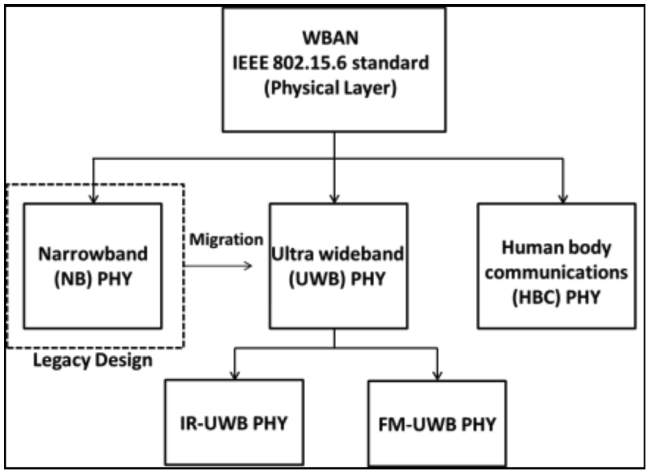


Figure 11. Classification of the physical layer in IEEE 802.15.6 [44]

1) Human Body Communication (HBC), 2) Narrow Band (NB), 3) Ultra-wideband (UWB) [23]. Figure 11 illustrates the classification of the physical layer in IEEE 802.15.6 The data range is limited to 3 meters for in-body communication and at least 3 meters for body-to-body communication. The transfer rate of data is between 15.6Mbps in HBC and 75.9Kbps in NB. To manage the channel access across the three physical layers, the IEEE TG6 proposes one shared mac only. It combines contention-less and contention access techniques to maintain various data flaws that might happen in WBAN, such as periodic traffic and burst, continuous. The administrator divides the channel or the time into a successive number of Super frames. In order to have access to the channel, the administrator chooses one of three access modes, which presented in the following:

1. Beacon Mode with Beacon Super frame Periods: In this access mode, the administrator sends successive beacon frames to define the beginning and the end of the SuperFrame, known as the beacon period.

2. Non-Beacon Mode with Super frames: This access mode do not have a beacon, and the SuperFrame might only consist of Type 1 phase or Type 2 phase [24].

3. Non-Beacon Mode without Super frames: The administrator in this mode follows an unscheduled allocation. Therefore, every node defines its schedule considering either Random Access Period1 (RAP1) or Exclusive Access Period1 (EAP1) as access phases, through which it competes for channel access following Carrier Sense Multiple Access (CSMA/CA).From this brief, we can see that these various channel access mechanisms offer the flexibility to support different types of WBAN applications. However, selecting the optimal solution and determining the parameter of SuperFrame and is not an easy task and needs more study.

7. SECURITY PROTOCOLS AND TECHNOLOGIES IN WBAN

The WBAN and IT infrastructure must perform security operations with confidentiality, availability, and data integrity of the patient's. It is necessary to ensure that the Health Insurance Portability and Accountability Act (HIPPA) is followed when addressing privacy issues in WBAN.

• Confidentiality: Exchanging data between the nodes in the network should be secured and protected from being accessed by unauthorized users.

• Integrity: The patient's data should be protected from alteration when transferring data between the nodes and protect the data from various types of integrity attacks, such as replay attack.

• Availability: The network should be available all the time since it carries a very high sensitive life-saving information. We can clearly say that the CIA triad is very essential and should be take into consideration when it comes to design a WBAN device. The following list illustrates different security approaches in WBANs.

A. Tiny Sec

In the wireless sensor community, Tiny Sec is very popular and has been implemented on different hardware devices. Tiny Sec is a software based security architecture which implements link-layer encryption. Tiny Sec encrypts the packet with keys and compute the entire packet, including the header with a message authentication code (MAC).

B. Elliptic Curve Cryptography

The Elliptic Curve Cryptography (ECC) can be considered as a viable option for public key cryptography in WBANs. The ECC has a compact signature, a small key size, and provide a fast computation. Although ECC has been implemented successfully in many types of WBAN devices, it is still not the best choice when we want to design a WBAN device. This is primarily because of its power consumption requirements which are higher than symmetric systems.As a result, many have suggested that ECC can be implemented for security-sensitive operations, and infrequent operations only, such as key establishment throughout the code update or the early network setup of the network.

C. Hardware Encryption

Hardware encryption implemented in WBAN devices with Zigbee wireless sensor. However, not all the node sensors have encryption support in hardware. The hardware encryption can be implemented by using ChipCon2420 Zigbee compliant RF transceiver [25]. This RF transceiver use AES encryption for security operations with 128-bit keys. Furthermore, these security operations consist of CBC-MAC authentication, and Counter Mode (CTR) as well [26].

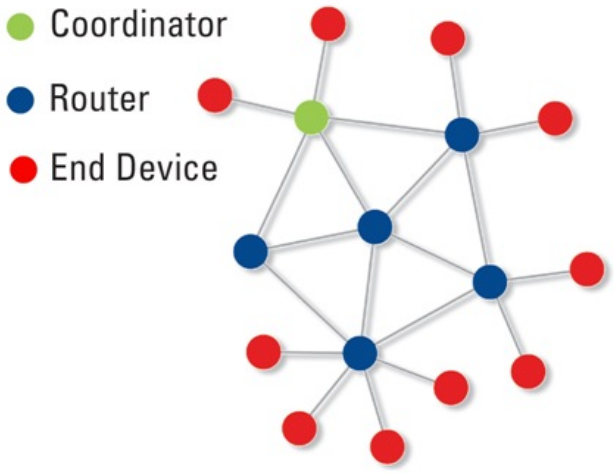


Figure 12. The Zigbee Network.

D. ZigBee

A new standard for low-power consumption introduced by ZigBee. The network layer of ZigBee is designed to operate on top of the IEEE 802.15.4 defined MAC and PHY layers. Additional security services defines by ZigBee, including authentication processes, and key exchange. In order to perform various functions, the ZigBee coordinator specifies a trust center that is responsible for key distribution and joining the network. Zigbee network has three types of nodes (Routers, Coordinator, and End device).

• Routers: The routers help in carrying data across multi ZigBee networks. In some scenarios, ZigBee network topology can be created without routers, and this can be achieved when the network is a (point-to-point) or (point-to-multipoint).

• Coordinator: This type of node exists in every ZigBee network. It initiates and manages the network functions and routing functions as well.

• End Devices: Sensors can be configured as end devices. Most of the time, these devices are in standby mode and become active at a particular time to collect and transfer data. These end devices are connected to the network through the routers. Figure 12 illustrates a typical ZigBee network topology. ZigBee is targeted at RF applications that need a significant battery lifespan, low data rate, and secure networking. During the standby mode, ZigBee can make devices operational for several years [27]. ZigBee can operate in three specific frequencies: 868 MHz, 915 MHz, and 2.4GHz. Hence, the interference with the (WLAN) transmission, particularly at 2.4 GHz, is the major disadvantage of using the ZigBee in WBAN applications. As ZigBee devices operate at a low data rate, it can be inappropriate for real-time and large-scale WBAN applications. However, it can still be very suitable for personal use, such as health monitoring, sports, etc. The

range that the ZigBee can cover is between 50 - 70 meters.

E. Biometrics

Biometrics is a useful mechanism that can be used in authentication and key establishments of WBAN sensors. It uses the physiological characteristics of the body itself as a factor in the key management system. The required characteristics for a useful biometric physiological value are introduced below:

- Invulnerable: hard to compromise.
- Acceptable: public acceptance.
- Time variance: changes over time.
- Universal: possessed by the majority of patients.
- Random: hard to guess.
- Distinctive: significantly different in any two patients.
- Collective: easily collected and measured.
- Effective: implement a relatively secure system within the constraints of computing, processing, and power of the WBAN sensors.

F. Bluetooth

Bluetooth is an IEEE 802.15.1 short-range communication standard, which is generally known as Wireless Personal Area Network (WPAN) [28]. With Bluetooth, it expects to create a network with low power consumption and provide security. A common Bluetooth network creates a Piconet where a Bluetooth device acts as a master, and the other seven Bluetooth devices act as slaves, which enables each device in the network to communicate simultaneously with each other. Another type of Bluetooth network can be created with more than one Piconet identified as Scatternet. In Scatternet, a Piconet node (can be either slave or a master) joins as a slave in a different Piconet. Figure 13 illustrates how a Piconet and Scatternet can be created using a Bluetooth connection. Bluetooth contains multiple protocols, such as Logical Link Control and Adaptation (L2CAP), Link Manager Protocol(LMP), and Baseband. The Baseband exchanges the data in the form of packets and enables the link between Bluetooth devices. The LMP held security issues, such as authentication, encryption, exchanging encryption keys. The L2CAP sends packets to either a hostless system or host controller interface. Furthermore, it can multiplex data between higher-level protocols and provide quality service (QOS) communication

G. IEEE 802.15.4 Security Suites

Various security suites can be implemented as a part of the IEEE 802.15.4. The security suites are mainly divided into two modes: the unsecured mode, and secured mode. In the unsecured mode, there is no selection of any type of security. The secure mode has eight distinct security suites, which are defined by the standard. The first suite is called " the null suite", which provides no security service at all. The other security suites can be much further categorized based on multiple security properties. Table 2 illustrates the security suites of IEEE 802.15.4.

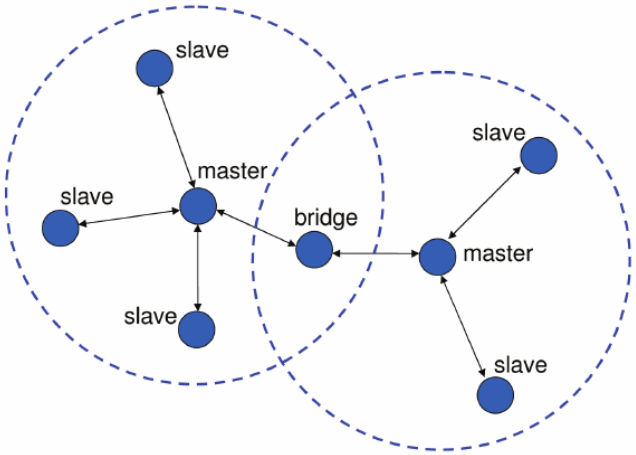


Figure 13. The Bluetooth Network [45].

TABLE II. The Security Suites of IEEE 802.15.4

Security Suite	Description
AES-CTR	This suite provides data encryption, and access control.
AES MAC-32, AES BC MAC-64, AES-CBC MAC-128	These types of suites provides authentication only.
AES-CCM-32, AES-CCM-64, AES-CCM-128	These types of suites provides encryption and authentication as well.
Null	This type of suite does not provide security service at all.

8. WBAN TRAFFIC TYPES

Normal traffic is the data traffic which is used to monitor the normal condition of a person without any criticality and on demand events. Emergency traffic is initiated by nodes when they exceed a predefined threshold or in any emergency situation. Such type of traffic is totally unpredictable. On-demand traffic is initiated by the authorized personnel like doctor or consultant to acquire certain information for diagnostic purpose In WBAN, traffic can be categorized into three types:

- Normal traffic: This type of traffic is used to monitor the normal condition of the patient without any criticality and on demand events.

- Emergency traffic: This type of traffic is completely unpredictable. With Emergency traffic, the traffic is initiated by nodes when they run over the threshold or in any other emergency circumstances.

9. TYPES OF ATTACKS IN WBAN

The current WBAN devices might be accessed via wireless and even controlled or upgraded by external devices. This means that these WBAN devices are vulnerable to

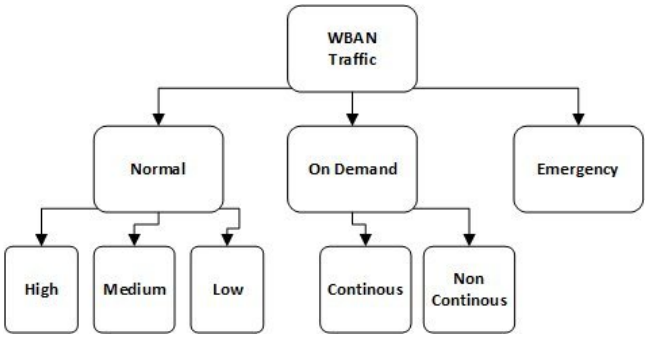


Figure 14. WBAN Traffic Types [46].

privacy and security attacks, and could threat the lives of the patients. Thus, security and privacy vulnerabilities in WBAN are a critical issue. The following is a list of the widespread security attacks conducted in WBANs.

• Eavesdropping Attack: Also known as snooping attack or sniffing attack. This type of attack enables the hacker to listen to the network and read the confidential information that transmitted from the WBAN device [29].

• Tampering Attack: The attacker can physically change the sensors, which may lead to replace the entire sensor, damage the sensor, or change a part of the sensor [30]. This type of attack enables the attacker to obtain patient's information or the shared cryptographic keys [31].

• Jamming Attack: This type of attack is very critical, as the attacker is capable of jamming the entire network [31]. This attack can put the life of the patient under threat as the WBAN sensor will not be able to send patient's data to the healthcare or to the doctor that monitor the patient's health in real-time.

• Exhaustion Attack: This type of attack are a form of denial of service attack (DOS) whereby the attacker sends a huge amount of data to the sensor and this will lead to make the battery sensor of the WBAN device to drain faster than it would be drained in normal condition [32][33]. This attack is dedicated to invasive WBAN sensors.

• Blackhole Attack: Also known as Sinkhole attack. This type of attack enables the attacker to make a malicious node that attracts all the network traffic in the WBAN sensors [33] [34].

• Denial of Service Attack (DOS): The attacker prevent the patient and the doctor to control and monitor the WBAN device [35] [36] [37].

• Flooding Attack: This type of attack is very close to the exhaustion attack as it capable of sending a huge amount of data to exhaust the WBAN resources [30].

• Selective Forwarding Attack: This type of attack enables the attacker to prevent some messages from being forwarded to the healthcare provider or doctor [39] [40].

• Collision Attack: This type of attack enable the adversary to send dummy packets in the WBAN [35].

• Spoofing Attack: This type of attack is capable of disrupt the network as it enables the adversary to target the routing information and modify it [39] [40].

• Sybil Attack: The name of this attack is derived from a book called "Sybil" ,which talks about a woman that has a multiple identity disorder. With Sybil attack, the adversary creates illegitimate multiple identities with stealing or creating identities of illegitimate nodes on the WBAN [34] [41].

• Data Modification Attack: The attacker is capable of alter the patient's data partly or fully and send it back to the healthcare or doctor [42].

• Impersonation Attack: The adversary eavesdrop the legal BAN nodes private data or WBAN controller (BNC). The adversary uses the identity information of the node or BNC.

• De-Synchronization Attack: This attack is a form of transport layer attack. In this attack, the adversary forges messages between nodes causing them to ask for data transmission of the missing frames [31].

10. Conclusions

In conclusion, this literature review provides an overview of the current state of research on Wireless Body Area Networks (WBANs). The review identified key challenges and opportunities in the field, and highlighted the potential of WBANs to revolutionize healthcare and improve quality of life.

The literature suggests that WBANs can improve the accuracy and efficiency of medical diagnosis and treatment, enable remote patient monitoring and telemedicine, and facilitate personalized healthcare. However, there are several challenges that need to be addressed to realize the full potential of WBANs, including issues related to reliability, security, privacy, interoperability, and power consumption.

The review also revealed several areas of active research in the field, including the development of novel communication protocols, algorithms for signal processing and analysis, wearable sensors, and energy harvesting techniques. These research areas have the potential to overcome the challenges of WBANs and enable their widespread adoption in healthcare.

Overall, the literature review suggests that WBANs are a promising technology that can significantly impact the healthcare industry. Future research should focus on addressing the challenges of WBANs and developing innovative solutions to enable their adoption in clinical settings. With continued research and development, WBANs have

the potential to transform the way healthcare is delivered and improve patient outcomes.

References

[1] Noman, S.A., Noman, H.A., Al-Maatouk, Q. and Atkison, T., 2023. Internet of Things Communication, Networking, and Security: A Survey. International Journal of Computing and Digital Systems.

[2] Poole, I., 2004. What exactly is ZigBee?. Communications Engineer, 2(4), pp.44-45.

[3] Want, R., 2006. An introduction to RFID technology. IEEE pervasive computing, 5(1), pp.25-33.

[4] Agarwal, K. and Sharma, D., 2017. Wireless communication wibree (bluetooth low energy technology). International Journal of Electrical, Electronics and Computers, 2(2), pp.1-4.

[5] Etutorials.org. 2022. Chapter 3: Wireless Networks: Part One: Introduction to the Mobile and Wireless Landscape: Mobile and wireless design essentials: Mobile devices: eTutorials.org. [online] Available at: http://etutorials.org/Mobile devices/mobile wireless design/Part One Introduction to the Mobile and Wireless Landscape/Chapter 3 Wireless Networks/ [Accessed 4 June 2022].

[6] IEEE 802 LAN/MAN Standards Committee, 2019. IEEE 802.11, The Working Group Setting the Standards for Wireless LANs.

[7] Rutherford, T., 2012. Population Ageing Statistics. House of Commons Library [Internet].[cited 2015 Nov 8].

[8] Jovanov, E., Milenkovic, A., Otto, C. and De Groen, P.C., 2005. A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. Journal of NeuroEngineering and rehabilitation, 2(1), pp.1-10.

[9] Warren, S., Lebak, J., Yao, J., Creekmore, J., Milenkovic, A. and Jovanov, E., 2006, January. Interoperability and security in wireless body area network infrastructures. In 2005 IEEE engineering in medicine and biology 27th annual conference (pp. 3837-3840). IEEE.

[10] Wu, T., Wu, F., Redoute, J.M. and Yuce, M.R., 2017. An autonomous wireless body area network implementation towards IoT connected healthcare applications. IEEE access, 5, pp.11413-11422.

[11] Patel, M. and Wang, J., 2010. Applications, challenges, and prospective in emerging body area networking technologies. IEEE Wireless communications, 17(1), pp.80-88.

[12] Li, C., Li, H.B. and Kohno, R., 2009, June. Performance evaluation of IEEE 802.15. 4 for wireless body area network (WBAN). In 2009 IEEE International conference on communications workshops (pp. 1-5). IEEE.

[13] Lim, S., Oh, T.H., Choi, Y.B. and Lakshman, T., 2010, June. Security issues on wireless body area network for remote healthcare monitoring. In 2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (pp. 327-332). IEEE.

[14] Hoang, D.C., Tan, Y.K., Chng, H.B. and Panda, S.K., 2009, November. Thermal energy harvesting from human warmth for wireless body area network in medical healthcare system. In 2009 International conference on power electronics and drive systems (PEDS) (pp. 1277-1282). IEEE.

[15] Wang, C., Wang, Q. and Shi, S., 2012, May. A distributed wireless body area network for medical supervision. In 2012 IEEE international instrumentation and measurement technology conference Proceedings (pp. 2612-2616). IEEE.

[16] Hu, C., Zhang, N., Li, H., Cheng, X. and Liao, X., 2013. Body area network security: a fuzzy attribute-based signcryption scheme. IEEE journal on selected areas in communications, 31(9), pp.37-46.

[17] Li, M., Lou, W. and Ren, K., 2010. Data security and privacy in wireless body area networks, IEEE Wireless Communications.

[18] Barua, M., Liang, X., Lu, R. and Shen, X., 2011, April. PEACE: An efficient and secure patient-centric access control scheme for eHealth care system. In 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 970-975). IEEE.

[19] "Texas Healthcare System suffers 405K-patient HIPAA Security Breach," HIPAA Journal, 04-Feb-2014. [Online]. Available: https://www.hipaajournal.com/texas-healthcare-system-suffers-405k-patient-hipaa-security-breach/. [Accessed: 04-Jun-2022].

[20] Arney, D., Venkatasubramanian, K.K., Sokolsky, O. and Lee, I., 2011, January. Biomedical devices and systems security. In 2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society (pp. 2376-2379). IEEE.

[21] Apple Watch Series 6. Apple. Retrieved June 4, 2022, from https://www.apple.com/watch/.

[22] Zhen, B., Patel, M., Lee, S., Won, E. and Astrin, A., 2008. TG6 technical requirements document (TRD). IEEE P802, 15.

[23] Chen, M., Gonzalez, S., Vasilakos, A., Cao, H. and Leung, V., 2011. Body area networks: A survey. Mobile networks and applications, 16(2), pp.171-193.

[24] Salayma, M., Al-Dubai, A., Romdhani, I. and Nasser, Y., 2017. Wireless body area network (WBAN) a survey on reliability, fault tolerance, and technologies coexistence. ACM Computing Surveys (CSUR), 50(1), pp.1-38.

[25] Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D. and Jamalipour, A., 2014. Wireless body area networks: A survey. IEEE Communications surveys & tutorials, 16(3), pp.1658-1686.

[26] "CC2420." CC2420 Data Sheet, Product Information and Support TI.com, www.ti.com/product/CC2420.

[27] Block Ciphers Modes of Operation — Cryptography — Crypto-IT. Retrieved from http://www.crypto-it.net/eng/theory/modes-of-block-ciphers.html Adibi, S., Ed. (2015) Mobile Health: A Technology Road Map. Vol. 5, Springer, Berlin.

[28] Acampora, G., Cook, D.J., Rashidi, P. and Vasilakos, A.V., 2013. A survey on ambient intelligence in healthcare. Proceedings of the IEEE, 101(12), pp.2470-2494.

[29] Adibi, S. ed., 2015. Mobile health: a technology road map (Vol. 5). Springer.

[30] Sharma, N. and Bansal, E.M., 2011. Preventing impersonate attacks using digital certificates in WBAN. International Journal of Advanced Engineering Sciences and Technologies, 9, pp.31-35.

[31] Javadi, S.S. and Razzaque, M.A., 2013. Security and privacy in

wireless body area networks for health care applications. In Wireless networks and security (pp. 165-187). Springer, Berlin, Heidelberg.

[32] Al-Ani, H. and Al-Zubidy, A., 2017, April. Introducing IJam Wireless De-authentication Attack Tool. In Proceedings of the SouthEast Conference (pp. 199-202).

[33] Saleem, S., Ullah, S. and Kwak, K.S., 2011. A study of IEEE 802.15. 4 security framework for wireless body area networks. Sensors, 11(2), pp.1383-1395.

[34] Saleem, S., Ullah, S. and Yoo, H.S., 2009. On the security issues in wireless body area networks. International Journal of Digital Content Technology and its Applications, 3(3), pp.178-184.

[35] Noman, H.A., Abdullah, S.M. and Mohammed, H.I., 2015. An automated approach to detect deauthentication and disassociation dos attacks on wireless 802.11 networks. International Journal of Computer Science Issues (IJCSI), 12(4), p.107.

[36] Wang, Y., Attebury, G. and Ramamurthy, B., 2006. A survey of security issues in wireless sensor networks.

[37] Pandey, A. and Tripathi, R.C., 2010. A survey on wireless sensor networks security. International Journal of Computer Applications, 3(2), pp.43-49.

[38] Bradai, N., Chaari, L. and Kamoun, L., 2011. A comprehensive overview of wireless body area networks (WBAn). International Journal of E-Health and Medical Communications (IJEHMC), 2(3), pp.1-30.

[39] Hughes, L., Wang, X. and Chen, T., 2012. A review of protocol implementations and energy efficient cross-layer design for wireless body area networks. Sensors, 12(11), pp.14730-14773.

[40] I. Shaqiri and A. Tentov, "Some aspects of Routing Protocols at Wireless Sensor Networks", IJCT, vol. 15, no. 4, pp. 6654–6658, Feb. 2016.

[41] Raazi, S.M.K.U.R., Lee, H., Lee, S. and Lee, Y.K., 2010. BARI+: a biometric based distributed key management approach for wireless body area networks. Sensors, 10(4), pp.3911-3933.

[42] Talwar, M. and Mallikarjun, C.S., 2014. Security threads and quality of service challenges for wireless sensor networks: A Survey. History, 10(21), pp.15-23.

[43] Xing, K., Srinivasan, S.S.R., Rivera, M.J., Li, J. and Cheng, X., 2010. Attacks and countermeasures in sensor networks: a survey. In Network security (pp. 251-272). Springer, Boston, MA.

[44] Zia, T. and Zomaya, A., 2006, October. Security issues in wireless sensor networks. In 2006 International Conference on Systems and Networks Communications (ICSNC'06) (pp. 40-40). IEEE.

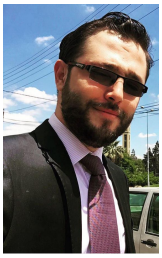
[45] Albahri, O.S., Albahri, A.S., Mohammed, K.I., Zaidan, A.A., Zaidan, B.B., Hashim, M. and Salman, O.H., 2018. Systematic review of real-time remote health monitoring system in triage and priority-based sensor technology: Taxonomy, open challenges, motivation and recommendations. Journal of medical systems, 42, pp.1-27.

[46] Indoor GPS tracking (2021) Sewio RTLS. Available at: https://www.sewio.net/indoor-gps-tracking/ (Accessed: April 30, 2023).

[47] Meacham, S., Gioulekas, F. and Phalp, K.T., 2016. Sysml based design for variability enabling the reusability of legacy systems towards the support of diverse standard compliant implementations or standard updates: the case of ieee-802.15. 6 standard for e-health applications. EAI Endorsed Transactions on Pervasive Health and Technology, 2(5), p.e1

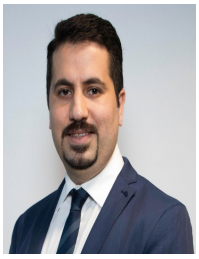
[48] Donegan, B.J., Doolan, D.C. and Tabirca, S., 2008. Mobile message passing using a scatternet framework. International Journal of Computers Communications Control, 3(1), pp.51-59.

[49] Henna, S., Sajeel, M., Bashir, F., Asfand-e-Yar, M. and Tauqir, M., 2017. A fair contention access scheme for low-priority traffic in wireless body area networks. Sensors, 17(9), p.1931.



Sinan Ameen Noman is a PhD Candidate at the department of computer science. University of Alabama, United states of America.

Haitham Ameen Noman received the B.Sc. degree in Software Engineering from Al-Ahliyya Amman University, Amman, in 2009. He went on to obtain his M.Sc. from New York Institute of Technology (NYIT) in Information, Computer and Network Security in 2012. He obtained his PhD degree from University Technology Malaysia, Kuala Lumpur, in 2017, in Computer Science. He joined the Department of Computer Engineering at Princess Sumaya University for Technology, Amman, Jordan in September, 2018. He served as Assistant Professor from 2018. He is a certified ethical hacker, certified network defender and Certified academic instructor from EC-Council. He has participated in organizing and delivering different information security courses to members of Jordanian army. His current research interests include Penetration Testing, Reverse Engineering, Network Forensics, Wireless Security and Cyber Criminology. Dr. Haitham has taught many courses of the curriculum since its establishment however, he is currently responsible for teaching courses in the area of Network and Information Security..



Qusay Al-Maatouk An innovative and knowledgeable professional with more than 10 years of experience as a senior lecturer, published more than 50 research articles in international journals and conferences, supervised more than 75 undergraduate research projects, and reviewed more than 50 research articles for international conferences and journals. currently serving as Guest Editor for a special issue hosted by MDPI (Switzerland). achieved more than 30 technical certifications and 30+ professional memberships such as IEEE senior member, MBCS, MIET, MACM.

Travis Atkison is an Associate Professor of Computer Science, the Computer Science Cyber Security Program Director, and the director of the Digital Forensics and Control Systems Security Lab (DCSL) at the University of Alabama. His current research efforts focus on the topics of cyber security, transportation infrastructure, and control systems security. These efforts include malicious software detection, threat avoidance, digital forensics, and security in control system environments (previous efforts in power systems and transportation). Dr. Atkison has been employed with the National Security Agency, Louisiana Tech, and the University of Alabama. He has authored over 70 peer reviewed articles in outlets such as IEEE Transactions on Dependable and Secure Computing, International Journal of Critical Infrastructures, and IEEE Eurographics Visualization Symposium. Dr. Atkison has been awarded funding from multiple agencies including NSF, DOE, ALDOT, and AFOSR among others. His work has spanned a wide range of topics, including computer security using both static and dynamic methods, cyber security, information assurance, network security, control system security, transportation infrastructure security, intrusion detection, information retrieval, data mining, distributed data mining, ensemble and hierarchical modeling, and architecture and application development. Dr. Atkison currently holds an active CISSP (Certified Information Systems Security Professional) certification.