Wireless Body Area Network (WBAN): A Survey on Architecture, Technologies, Energy Consumption, and Security Challenges

Journal of
Sensor and Actuator Networks

MDPI

Review

Wireless Body Area Network (WBAN): A Survey on Architecture, Technologies, Energy Consumption, and Security Challenges

Mohammad Yaghoubi, Khandakar Ahmed * and Yuan Miao

Intelligent Technology Innovation Lab (ITIL), Victoria University, Ballarat Road, Footscray, Melbourne, VIC 3011, Australia
* Correspondence: khandakar.ahmed@vu.edu.au

Abstract: Wireless body area networks (WBANs) are a new advance utilized in recent years to increase the quality of human life by monitoring the conditions of patients inside and outside hospitals, the activities of athletes, military applications, and multimedia. WBANs consist of intelligent micro- or nano-sensors capable of processing and sending information to the base station (BS). Sensors embedded in the bodies of individuals can enable vital information exchange over wireless communication. Network forming of these sensors envisages long-term medical care without restricting patients' normal daily activities as part of diagnosing or caring for a patient with a chronic illness or monitoring the patient after surgery to manage emergencies. This paper reviews WBAN, its security challenges, body sensor network architecture and functions, and communication technologies. The work reported in this paper investigates a significant security-level challenge existing in WBAN. Lastly, it highlights various mechanisms for increasing security and decreasing energy consumption.

Keywords: WBAN; security threats; energy consumption; routing protocols; attacker

check for updates

Citation: Yaghoubi, M.; Ahmed, K.; Miao, Y. Wireless Body Area Network (WBAN): A Survey on Architecture, Technologies, Energy Consumption, and Security Challenges. *J. Sens. Actuator Netw.* **2022**, *11*, 67. https://doi.org/10.3390/jsan11040067

Academic Editor: Chengwen Luo

Received: 2 August 2022
Accepted: 22 September 2022
Published: 18 October 2022

1. Introduction

Wireless sensor networks (WSNs) have become an important research issue and will become an integral part of human life in the near future. WSNs are a network of sensor nodes spatially distributed throughout the environment, each of which has a particular purpose independently and in cooperation with other nodes. The main goal of these networks is to collect data on the environment and transfer it to the base station (BS) or remote server. The information is then analyzed in detail. A wireless sensor is the smallest unit within a network, with unique characteristics such as support for wide dispersion, mobility, and reliability. WSNs can be applied to monitoring and controlling industrial processes, device monitoring, environmental monitoring, traffic control, intelligent houses, military and security uses, agricultural usage, and more. One application of the WSNs is in health and medical care. This application includes wearable sensors connected to the human body to monitor and track body movements and measure physiological parameters such as body temperature and heart rate. These sensors gather information and send it to the BS for analysis, storage, and processing. Then, the data are safely sent to remote medical servers via the Internet or other media. Security is vital because the data contain sensitive information obtained from physiological values. All personal data must be protected from unauthorized access.

Wireless body area networks (WBANs) are a particular type of sensor network using wireless sensor nodes on a person's body to measure physiological parameters such as blood pressure, body temperature, heart rate, and blood sugar level, enabling a patient's health to be monitored remotely. WBANs can be either wearable or implantable. The main purpose of WBANs is to ensure people's health by sending physiological information to medical servers using sensors on the body to enable physicians to understand the health of the patient [1]. These systems can offer significant assistance to the medical board and individuals in emergencies by providing services such as monitoring and delivering pharmaceutical and medical information, improving patient's processing data, controlling home appliances, and communicating data. WBANs can also significantly reduce patient's treatment costs by monitoring the patient's vital sign-related data over a long period of time. Unlike wireless sensor networks, body sensor networks use a star topology architecture. In this topology, an approaching spot (sinkhole) is located in the body to gather information from nodes. These sensor nodes in the network have access to limited energy resources. In physical sensor networks, sensors (like motion sensors) are installed on the body of a patient to observe the patient's vital signs or detect motion. By monitoring a patient's vital signs, the body sensor network provides an instant response to the user through which the user can follow the progression of a patient's disease and take the necessary precautions. In this type of network, the energy utilization of the sensors is critical because if the energy source is exhausted, the life duration of the network will be shortened [1,2].

In this research article, attempts are made to investigate solutions that, while increasing security and safety in the WBAN, can reduce the energy consumption of nodes and increase the network lifespan. That is, the two challenges of security and energy consumption are relied on and focused on the same time. To this end, the WBAN and the related architecture, along with the challenges, are introduced. Then, after introducing and relying on security challenges and categorizing network-related attacks, the destructive effects of attacks and threats including energy consumption increase and network lifespan reduction are addressed. Lastly, protocols, mathematical models, mechanisms, and intelligence methods are discussed. It is mentioned that, along with security mechanisms, this method can optimize the energy consumption of nodes and increase the lifespan of the network.

1.1. Related Work

Over the past 5 years, a large body of research has been conducted on WBANs, including design, challenges, and WBAN implementation issues. The studies in [1–9] examined the implementation and design challenges, security issues, diffusion modeling, and data routing, including reducing energy consumption and ensuring the quality of service, as well as practical issues. These articles provided a comprehensive overview of all aspects of WBANs and the significant points in designing different routing protocols and security along with the various technical challenges related to implementation.

The main goal of WBANs is to constantly monitor the patient's health using biosensors in or around the human body and to sound an alarm when a dangerous situation is detected. The study in [10] provided a summary of the various sensors used in body network systems along with their performance.

WBAN research focuses on the layout of WBAN, data integration, and the transmission of data in the network. In relation to network design, the focus of the research is on sensor deployment, energy consumption, and the ability to route sensor nodes. Data integration research focuses on feature extraction, data compression, and data classification. The authors of [11,12] studied energy consumption in WBANs, and the study in [13,14] provided suitable methods for routing sensors with medical devices and other sensors.

To ensure the security of all types of information, security algorithms protect the network so that the integrity, impeccability, verification, and privacy of information can be maintained. The study in [15] discussed privacy-preserving techniques to ensure the collected personal information is protected. The most important security issues considered in this article were privacy issues. First, in the storage process, the patient's data must be kept private and protected against malicious user nodes and collusion. Second, the data pertaining to a patient must not be changed while they are being stored. Instead, the data must be hashed through various movements. The third issue is to verify the sender of the data via authentication to ensure the data are valid, and invalid data other than those sent by the WBAN must be banned. Fourth, all information must be accessible even in the case of a denial of service (DoS) attack. The authors of [16,17] explained that the security of a secure communication session between biosensor nodes in an unfriendly environment must be based on the privacy of the security mechanisms so that the data can be made visible only to an authorized person. None of the studies reviewed and referenced in this article simultaneously addressed the two important challenges of security and energy consumption. The main goal of this review article is to fill this gap, i.e., this article simultaneously examines the two important issues of safety and power consumption, which are vital challenges to the WBAN.

In [18], after introducing a general perspective of WBANs and WSNs, the researchers conducted a more detailed and in-depth investigation of the security requirements of the WBAN. This article tried to discuss the importance, necessity, and problems of privacy in collecting and sending the vital information of the patient's body after focusing on two issues of security and privacy in the WBAN. In addition, the necessity of achieving a comprehensive and efficient security system that has complexity and simplicity in executive calculations and can save energy was pointed out. In this research article, although the importance of saving energy after applying security was mentioned, mechanisms for saving energy were not proposed in a comprehensive manner.

In [19], the researchers carried out detailed and in-depth investigations about the requirements and challenges of the WBAN. At first, they conducted an in-depth review of WBAN applications, and then focused on the requirements and challenges related to the WBAN. One of the unique features of this article was the review of technologies and requirements for data transmission in the WBAN. Next, the importance and characteristics of energy consumption and reducing the amount of energy in the WBAN were briefly mentioned. One of the limitations of this article is that the reference to the security and privacy challenge was too brief. To compensate for this gap, in this article, we try to introduce protocols and artificial intelligence algorithms that speed up and reduce energy consumption in the WBAN. In addition, the general and security challenges of the WBAN are stated and the attacks are categorized.

In [20], Ananthi and Jose conducted a thorough research on the WBAN security challenges for medical care applications. In this research, they investigated and tested the methods and events that lead to increasing security and speeding up the reliability of the WBAN. In this paper, they discussed the introduction and classification of security and security techniques in the WBAN along with the problems, methodologies, and results of each technique. The results and conclusions of this research showed that techniques such as clustering and selection of effective router protocols increase throughput and network lifetime in a safe and secure environment. In this article, the researchers introduced techniques to increase the life of the network along with the security of the WBAN, aiming at the improvement of high-speed information transmission. However, there was no reference to the effect of metaheuristic methods and artificial intelligence algorithms on improving the control parameters. They did not consider network quality and energy consumption optimization.

1.2. Contribution

WBANs are a powerful technological advance that greatly benefit both nonmedical and medical fields. A WBAN is a tool of communication designed to monitor inside or around the human body to collect a patient's health data and to direct physical or crucial information from biosensor nodes to a server for subsequent research. The problem with WBAN is that battery life constrains the energy of the biosensors, and many routing conventions are specifically designed to transfer the gathered information to a central station for further analysis, which may vary on the basis of the network design. This article presents a comprehensive review of the following:

- WBAN, its architecture, tasks, and communication technology, with a particular focus on new generation sensors to improve the quality of communication with different devices;
- The main challenges facing WBAN including security and power consumption;

- Accurate classification of attacks and threats affecting the WBAN;
- A detailed review (M. ATTEMPT, SIMPLE, HPOR, HEAT, GACA) of the essential routing algorithms proposed or used on existing medical devices and sensors in the network.

1.3. Article Structure

Section 2 introduces wireless body sensor networks. Sections 3 and 4 detail the architecture and tasks of WBANs. Section 5 outlines the main challenges of WBANs. In Sections 6 and 7, communication technologies, and a new generation of network sensors are introduced. Section 8 discusses the reduction in energy consumption, and Sections 9 and 10 cover the security challenges, attacks, and threats against WBAN. Section 11 presents the methods for routing in the WBAN. Lastly, the conclusion is given in Section 12.

2. Wireless Body Sensor Networks

Wireless sensor networks are networks based on the cooperation of sensor nodes with low energy consumption, low cost, and wireless communication. A sensor is a device that detects events or changes in its environment and sends this information to another electronic system. The significant limitations of sensor networks include memory capacity, computing power, and energy. However, due to the improved efficiency of data collection of the wireless sensor network, they have been applied in the medical field, and they have been used for environmental control, disaster reporting, military and security surveillance systems, and traffic control. Different applications in wireless sensor networks require the satisfaction of different quality parameters (such as latency, reliability, bandwidth, and security). The quality of service (QoS) needs to be ensured in each area. Some of the problems facing wireless sensor networks such as limited bandwidth power, unreliable communications, and node vulnerabilities make QoS requirements essential. Wireless sensor networks are used to collect data on the condition of hospital patients and observe the movements of rare diseases. Wireless sensors can also monitor the efficiency of agents. The cases in which these networks are used include remotely collecting physiological data of the human body, detecting patients and doctors in a medical setting, and organizing drugs in a hospital. Owing to the significant progress of wireless sensor network technology in the medical sector and the use of data provided by this technology outside the hospital, it is possible for medical practitioners to be alerted to any medical emergencies that arise, which will enable the medical team to take timely action. The various factors to be considered in relation to data delivery in telemedicine networks are availability, confidentiality, privacy, reliability, service quality, and mobility (portability) [1,2].

2.1. Using Sensors for Health Control

Most patients see a doctor when they experience abnormal health symptoms and, often, in serious cases, the patient needs to be treated immediately. In such cases, the patient needs to be quickly treated, and the patient may have to spend huge money on the treatment. However, employing a network of sensors can not only maintain the physical wellbeing of individuals but also identify disease occurrence, which helps with reducing further costs and risks throughout the therapeutic process [1,3].

Sensor networks will be widely used in healthcare in the future. Rudimentary types of sensors are currently being used in some advanced hospitals to monitor patients' physiology data, track courses of medication, and monitor physicians and patients in the hospital. One of the applications of sensor networks in this field is nursing the elderly. For this purpose, sensor cameras are used to detect muscle activity, which creates a complex network. This network monitors the elderly and can detect falls, a state of unconsciousness, vital signs, diet, and exercise. Experts say that, in the future, with the advances in technology and the use of broadband technology, such networks can be of great help to determine the actual health state of the body. Real-time health diagnostics using this technology can compensate for delays in identifying degenerative diseases, save lives, and consequently reduce health costs. Health can now be monitored remotely in some cases; however, remote monitoring systems are yet to be perfect. The current surveillance sensors described in earlier work using ultrawideband technology are very small and wearable, and they receive the energy they need from body warmth. Despite their small size, these devices are able to transmit large amounts of information that will significantly improve medical services and healthcare and can reduce treatment costs and help prevent disease. "For this type of health measurement and monitoring, an ultrawideband device will be designed," said Patrick Chiang, a specialist in wireless electronics and assistant professor of medicine at the School of Electrical Engineering and Computer Science (OSU). It can also collect and transmit data on heart health, bone volume, blood pressure, and insulin levels in the body. In addition to monitoring a patient's health, this device can also prevent disease; for example, it is possible to diagnose a patient with an arrhythmia and predict the onset of a heart attack. This device must be cheap and accessible to everyone and must also be able to store and deliver enormous amounts of data [1–4].

2.2. IoT Healthcare

The Internet of things (IoT) is a modern technology involving intelligent objects including physical components such as sensors that sense the internal state of an event or external environment and perform some actions on the basis of the data collected. The data generated by the sensors in smart objects can be further processed, and decisions can be made accordingly. These smart objects have embedded software to control the various parts and events generated in those objects. The IoT paradigm combines the benefits of different sections such as cloud computing, WBANs, edge computing, fog computing, and automated computing in communication technologies to create new ways and opportunities in various fields. By 2025, 75 billion devices are anticipated to be connected by IoT technology. Some of the areas that are affected by the IoT are business, manufacturing, healthcare, retail, and defense/security. There are many applications of the IoT, including smart parking, smart lighting, waste management, forest fire detection, earthquake detection, intelligent crop management, and remote care for the elderly [21].

3. Body Sensor Network Architecture

3.1. Sensor Network Architecture

The design of body sensors can be categorized into three levels as shown in Figure 1:

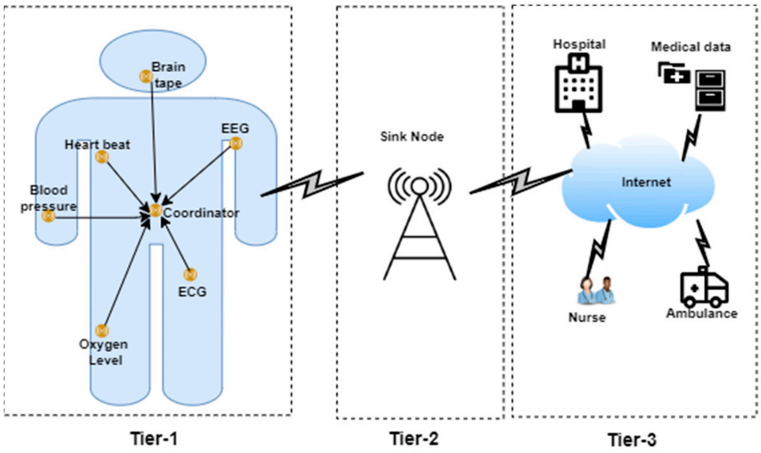

Figure 1. The architecture of wireless body sensor networks [1].

Level 1. Medical sensor nodes are implanted on or in the human body along with the sinkhole located at this level [1].

Level 2. Sensor nodes transmit the data to the sinkhole, and the data are then transmitted to the BS by aggregating and processing the data [1].

Level 3. After the data are received by the BS, they are transmitted to the medical center through the Internet infrastructure for remote monitoring and treatment. In general, in the architecture of this type of network, each sensor monitors the individual's health by receiving the sensory information from the patient's body, then sending the data to sink node before transfer to the BS to call for medical care [1].

3.2. How to Run the Body Sensor Network

Today, the use of wireless sensor networks is a significant issue in improving the degree of intelligence and synchronization of industrial or environmental systems. One of the major usages of wireless sensor networks in human healthcare systems is wireless body sensor networks. This sensor network sends physiological signals received from patients or the elderly to medical care centers after the patient has been discharged from the hospital and returns to their daily life. This enables physicians and emergency centers to monitor the condition of patients in real time or with a slight delay, as well as respond to their treatment needs accurately and in a timely manner. Figure 2 provides an example of a wireless sensor network in the healthcare system that collects physiological data from patients in different situations and sends these to the medical care coordinating unit. This information is provided to the doctor via various communication methods.

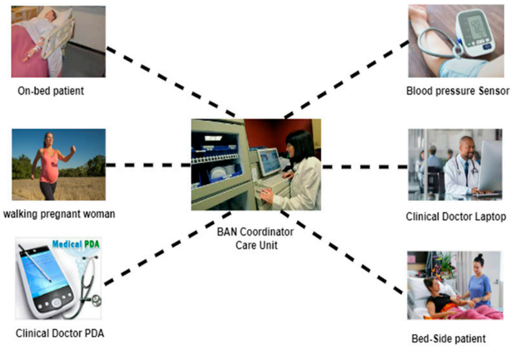

Figure 2. Example of a body sensor network [22].

The information received from the sensors is then sent to the BAN coordinator unit. Its primary role is to help extract valuable features from the dataset received from the patient's body and to set the data transmission timing. Another part of this node is the storage unit. Delayed data are archived in this unit and provided to the medical center upon request. Sometimes, the data need to be saved due to poor channel conditions or data traffic.

Other important parts of this network are the communication unit and the power supply unit. Typically, a transceiver with four radiofrequency channels between 850 GHz and 2.4 MHz is used to coordinate the nodes and send data to subsequent nodes. The required power is provided by batteries made for small and portable parts. Figure 3 shows the structure of a body sensor node called TEMPO developed by researchers at the University of Virginia, which is compared to the size of a coin [5].

Each of these body sensor nodes is connected to a central node with a star topology. In this topology, all nodes on the body send data to a collector unit. In the hybrid mesh star method, communication is established among the coordinating units of each group, and, in the case of problems in one node, the other nodes are notified immediately. This topology also connects collector units and bridges to connect to broader networks. Figure 4 illustrates the star topology, and Figure 5 demonstrates the mesh star composite topology.

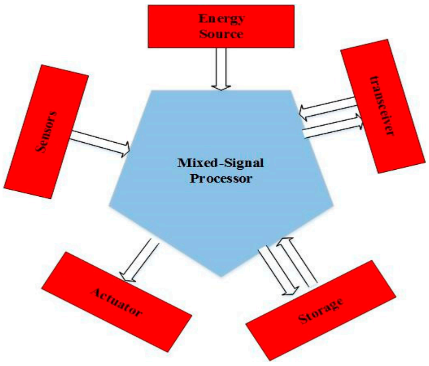

Figure 3. A body sensor node structure includes sensors, a mixed-signal processor, storage, a transceiver unit, an energy source, and an actuator unit [5,23].

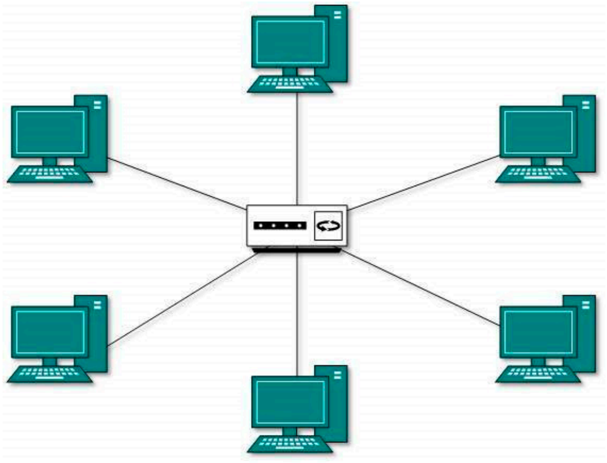

Figure 4. Star topology structure [24].

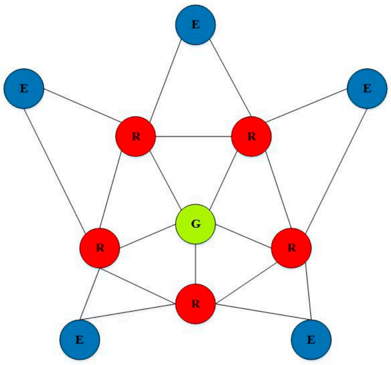

Figure 5. The structure of a mesh star composite topology in which nodes are connected to a central node [24].

Another characteristic of these networks is their hierarchical structure. This network continuously receives large amounts of data from which microprocessors must extract the necessary data and properties. Data collection is also hierarchical. This means that the data processing in each sensor node is performed locally, and then the network has several sensors in the next node of the dataset. The collecting unit has the leading role in data composition. These collectors combine the data from the nodes as an intermediary with higher levels of the network. The data obtained at each higher level can help as feedback to the lower levels to improve the classification, feature extraction algorithm, and coordination among the sensors. Figure 6 shows the path of the data in the wireless sensor network of the body [6].

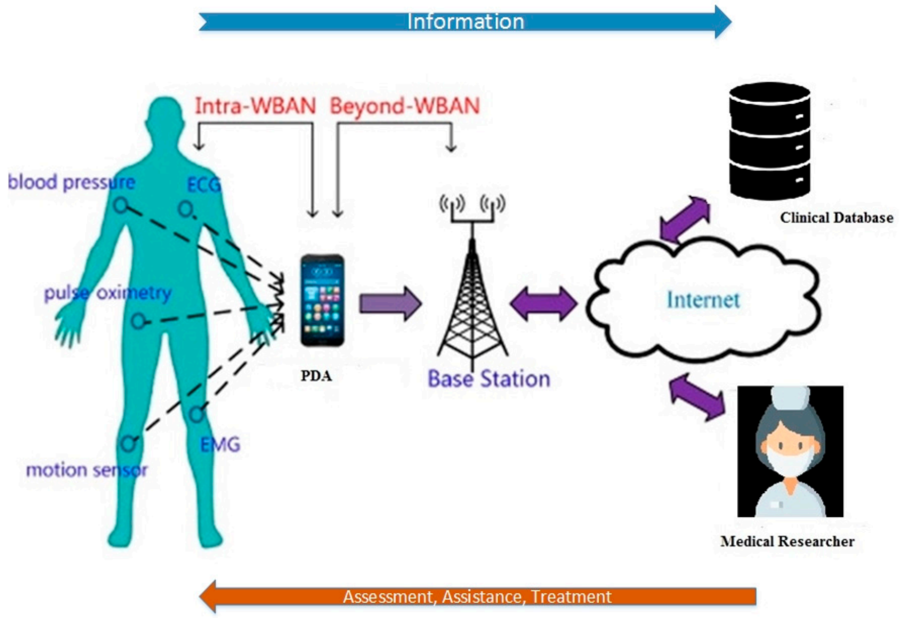

Figure 6. The path of the data in the wireless body sensor network of the body [6].

Another issue arising in wireless body sensor networks is the coordination of different parts in terms of technology. Standardization is one of the aids that harmonizes and coordinates the WBANs. Th next section introduces examples of new wireless technologies designed to be used in wireless body sensor networks [6].

4. The Body Sensor Network Function

Sensor nodes are responsible for monitoring important body parameters that indicate a person's disease status and vital signs. In a body sensor network, the vital signs mainly monitored are blood pressure, heart rate, respiration rate, blood oxygen level, body temperature, etc.

In addition to vital signs, other applications of medical sensors consist of ECG monitoring of cardiac activity, brain signals (EEG), muscle signals (EMG), glucose monitoring, and physical activity monitoring to determine the individual's health status [7].

When using sensor networks to obtain the best results of health data, different sensors should be placed in the network, and different sensor information should be used to monitor the patient's condition to enable medical professionals to make appropriate decisions. Examples of different types of sensors used in various ways, including dermal electrodes, and wristbands, are shown in Table 1 [7,19,25].

As shown in Table 1, different sensors are located on the body to collect data on the patient's symptoms. For example, body temperature is a key factor that should be measured to determine the patient's health status. A high body temperature is a sign of illness, and a low body temperature, to a certain extent, indicates an increased risk of illness. Blood pressure can be used to diagnose high blood cholesterol, clogged arteries, or irregular heartbeat. The heart rate sensor can also be used to indicate the patient's level of stress. When blood pressure is measured under the influence of stress, it is not at the normal level, and a person's heart rate and body temperature are directly related to a person's level of activity [7].

Table 1. Various medical sensors deployed on the human body [7,19,25].

Sensor	Description
ECG	The heart's electrical activity
Blood flow	Measurement of accelerating forces in three-dimensional space of the body
Blood pressure	The force applied by the circulation of blood on the walls of the blood vessels
Body temperature	An indicator of the body's ability to create and release heat
Respiration rate	Number of inhale and exhale movements per unit time
Oxygen level	Indicates the oxygen that is flowing in the patient's blood
Heart rate	The frequency of the cardiac cycle
Blood sugar	Measures the amount of sugar (type, source, energy) in the blood
Muscle signal	The electrical activity of skeletal muscles (nervous, muscular system)
Electroencephalography	Measures automatic brain activity and other brain capacities

The Performance of WBAN

For body implants, a set of radiant elements of WBAN receivers and transmitters work on curved surfaces of the body that are exposed to nearly 70% of body fluids (tissues). Absorption properties of body tissues increase the thermal effects of radiofrequency (RF) and attenuate the WBAN signal. In addition, the absorption properties of the tissues affect the signal transmission and other passages of the biosensor circuit. Changes in circuit transmissions may alter the operational characteristics of data acquisition devices, leading to data and device anomalies, as well as network errors. Furthermore, signal attenuation due to tissue absorption properties weakens the signal strength. Therefore, it can be easily disturbed by noise. Additionally, body motion due to different dynamics and WBAN topology affects the propagation of the RF signal, which leads to changes in packet transmission distance and disconnection, as well as impairs reliability. Given the limitations that WBANs face and the need for future healthcare, the emphasis is on improving performance and improving service quality for efficient operation in a resource-constrained and challenging environment. Hence, the future of modern healthcare services depends on the quality of services provided by empowering the current technologies via working on their cost-effectiveness, flexibility, and operational efficiency [26].

5. WBAN Challenges and Implementation Problems

5.1. WBAN Challenges

As a developing technology, there are many issues relating to WBAN that need to be addressed, both technically and ethically, such as privacy. Some of the most critical technical challenges that need to be addressed are listed in Table 2.

Table 2. WBAN challenges.

Challenges	Challenges in WBAN
Range	The WBAN range is limited, a few meters away from the body. Hence, reliable wireless communication is performed inside or close to the human body [8].
Energy consumption	WBAN requires constant energy to work properly, which necessitates a constant power supply [9].
Security	Due to the low power supply, it is difficult to add complex security mechanisms [27].
Service quality	One of the most important challenges in WBAN is to improve service quality [28].
Placement	It is difficult to put many nodes in a limited space [29].

5.1.1. Challenges Related to the Mac Layer

Since wireless sensor networks are always monitoring the human body, and they must send sensitive and important data of the human body to the medical teams at any moment, there are concerns about the delay in sending vital and important information. In order to reduce the dela in critical information sending, it is recommended to use quality control services that can prioritize essential and sensitive information and send it with the least delay. Using the technique of sending sensitive information directly is another method to reduce the delay, which is recommended [30].

5.1.2. Challenges Related to The Network Layer

WBAN body sensor network traffic by itself can cause energy consumption and create bottlenecks if proper routing protocols are not utilized. For this purpose, to reduce energy consumption and distribute traffic in a balanced way, it is recommended to use router protocols that have load-balancing capabilities. Furthermore, using quality and weight control and prioritizing network traffic can eliminate the bottleneck [31].

5.1.3. Challenges Related to The Transportation Layer

It is necessary to have a highly reliable transport mechanism to be able to provide vital and essential information instantly and quickly in the case of data loss since, in WBAN, correct data delivery is very sensitive, and the loss of, destruction of, and damage to vital body information during sending can increase the risk of death. In order to reduce energy consumption, this system can use a periodic or periodical system for recording and reporting unnecessary information [32].

5.1.4. Application Layer Challenges

As this layer is responsible for communicating with the user in the form of an interface at the highest level, having an intelligent mechanism that can send rich and meaningful information in medical environments seems crucial. For this purpose, it is possible to use intelligent methods of artificial intelligence and machine learning algorithms in this layer to use more valuable information to produce knowledge and experience [33].

5.2. Implementation Problems in WBAN

Advances in computer science along with the use of other sciences such as electronic technologies have led to the development and expansion of wireless sensors of the body, whereby these nanosized sensors have the ability to communicate and send physiological messages of the human body with minimal energy consumption. However, economic and technical obstacles destroy the necessary order for reliable and efficient decision making in WBAN. In this section, attempts are made to rely on a more detailed and efficient investigation of the infrastructure problems of WBAN sensors during implementation on the patient's body [34].

Physical Problems

(a) Unobtrusiveness

During the implementation and design of body sensors, keeping them covered and invisible when wearing and installing them on the human body poses a great challenge [35].

(b) Sensitivity of Sensors

Sensors implanted on the body in industrial environments that are always exposed to inflammable and flammable substances must have significant sensitivity so that they can react when necessary, when the surrounding environment heats up and when the temperature of the human body rises. However, in such cases, intense human sweat and steam from the surrounding environment can have a destructive effect on the sensitivity of these types of sensors, which causes damage and inaccurate recording of vital body data.

To solve this problem, it is recommended to utilize mechanisms and algorithms that have the ability to calibrate on time and quickly [36].

(c) Battery Charging and Maintaining Energy Consumption

In closed environments such as medical clinics that are not sufficiently exposed to direct sunlight, in cases that sensors are worn under clothing, or with people suffering from Alzheimer's and forgetfulness, charging the sensors can remain a potential problem. Using the natural heat of the patient's body and charging the batteries during the patient's movement can be feasible solutions [37].

(d) Body Data Collection Strategy

There are always concerns about the collection of vital information of the human body by sensors, which in some cases can cause wrong decisions after processing the physiological information. In some cases, the use of a sensor may not be efficient on its own for accurate and sensitive recording and conclusions. In such cases, integrating sensors for collecting and then processing can be more effective [38].

(e) Secure and Reliable Transmission to Send Information

Since sensors and wireless sensor devices have small antennas that lack the ability and power to send and transmit information in large volumes and long distances, there will always be a problem that transmission with high reliability cannot be achieved. To tackle this problem, reduce the risk of sending erroneous data, and increase the reliability, it is suggested to use coding and multiplexing methods [39].

6. Wireless Communication Technologies

Wireless networks have attracted increased attention from researchers. Although this technology seems beneficial and has many applications, the most crucial step that will determine the degree of satisfaction with it is to assess the needs and expectations of users and compare this with the features and capabilities of this technology. If the user's needs and expectations are not taken into account, the technical possibilities and applications of this technology will result in failure and dissatisfaction. Communication network technology plays a vital role in body sensor networks because of the sensitivity of the data on the body's vital signs for monitoring the human health condition, and it must be free of interference in the communication channels. In this section, we introduce some of the wireless technologies available in body sensor networks [19].

6.1. ZigBee Technology

ZigBee is an intelligent network used for high-level communication protocols and low-rate data transfer. This protocol is used in personal area networks (PANs) (small and low power), and its technology is fixed on the IEEE 802.15.4 standard. In body sensor networks, the ZigBee protocol is encrypted with 128 bit passwords. This system is supported through the tree, star, and mesh networks. Each device must have a coordinator on it. Its operating frequency is in the range of 2.4 GHz, and its transmission speed is 252 kbps [19,40–42].

6.2. Bluetooth Technology

Bluetooth is a standardized protocol for short-range communication with low energy consumption and low cost without the need for troublesome wires. The mainstay of Bluetooth technology is radio waves [19].

As shown in Figure 7, Bluetooth is an ideal technology for body sensor networks and enables information on the human body to be observed. When a tiny Bluetooth chip is installed in systems, it creates a personal wireless network that allows for communication with another user device nearby.

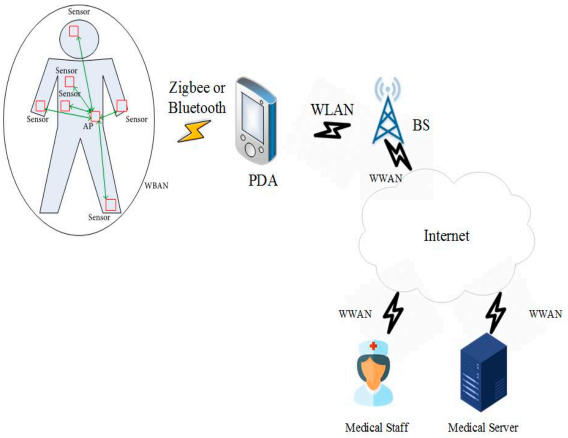

Figure 7. Bluetooth technology in the wireless body area network [19].

6.3. Ultrawideband (UWB) Technology

Ultrawideband technology is a radio technology that uses a very low energy level for short-range, high-bandwidth communications over a large portion of the radio spectrum.

In November 2007, an IEEE research team began examining body sensor networks and developed UWB wireless technology. As shown in Figure 8, one of the advantages of UWB wireless technology is the range over which it can send data, between 850 Mbps and 20 kbps, and it can be utilized to simultaneously observe many constantly sent physiological signals such as ECC/EEG. Although this standard still accepts instances for the body sensor network development, UWB wireless components are not currently widely available for the implementation of body sensor networks [19].

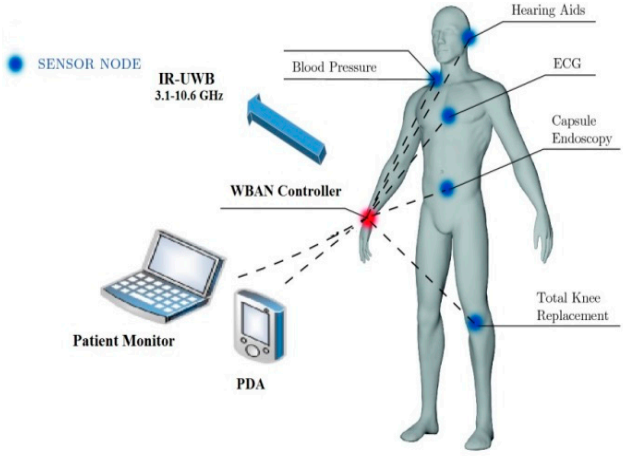

Figure 8. UWB technology in wireless body area networks [43].

6.4. Wi-Fi—IEEE 802.11

Wi-Fi is an IEEE 802.11 standard for wireless local area networks (WLANs). In general, Wi-Fi technology has four standards (802.11 a/b/g/n) that run on the 2.4 and 5 GHz ISM bands with an average coverage of 100 m. Wi-Fi allows users to transfer data at broadband speeds when connected to an access point (AP) or in temporary mode.

Wi-Fi is best suited for transferring large amounts of data via a high-speed wireless connection that allows for video conferencing, voice calling, and video streaming. A major advantage is that all smartphones, tablets, and laptops have built-in Wi-Fi. However, the main disadvantage of this technology is high energy consumption [44].

7. New Generations of Sensors for Body Sensor Networks

In biological monitoring, the "physical world" to be supervised is a living body. Therefore, the sensor nodes must be located near the body or implanted inside the body to form a network. Developing sensor nodes for biological monitoring is based on the need for "invisibility" that relies on all available technology options, from microelectronics to emerging technologies. Integrating various devices into a tiny physical volume achieves "invisibility" in sensor nodes for biological monitoring. This section describes four new-generation sensors for body sensor networks.

7.1. Obtrusive Nodes

The size and weight of these nodes are a barrier to their use. However, they can connect with other nodes or gateways and are portable. Current commercial sensors, such as electrical heart rate- and body-tracking systems that use a wearable camera and a marker, are now considered problematic due to two issues: the first is high energy consumption, which either demands a huge battery or a short charge time, and the second involves a hefty sensory interface [10].

7.2. Parasitic Nodes

Physical items whose size, weight, and structure do not obstruct regular functions are referred to as nodes. Biometric clocks and body tracking inertia sensors are examples of parasitic devices. These nodes should have a physical volume of a few cubic centimeters and a weight of a few tens of grams. These nodes should not use more than a few milliwatts as their electrical energy consumption, according to current battery technology. Recently, various parasitic nodes have entered the market commercially. These devices represent the latest technology in wireless sensor networks [10].

7.3. Symbiotic Nodes

The scientific community is working to revolutionize the use of new technology to create devices in cubic millimeters (called smart dust), which can support several new applications of in-body biological monitoring. However, there are several technical issues that need to be resolved. The first step is to put in place nodes that can give the energy they require. The body can provide the energy these nodes require (temperature changes, chemical reactions in the body, etc.). Secondly, the size restriction places difficult demands on the micro-processing and integration process. Lastly, there are concerns about safety regulations. The nodes must be biologically compatible in the short and long term. Since these nodes have a reciprocal benefit relationship with the target organism, their relationship is called coexistence [10].

7.4. Bio-Inspired Nodes

Bio-inspired nodes are offered as the technological and architectural apex of the progression of biologically inspired nodes. The interaction between the target sensor and the sensor itself vanishes when the physical scale of these devices approaches a few cubic microns (or less). Bio-inspired devices will become a reality in the near future thanks to molecular engineering and nanotechnology. Some research investigations have indicated that scale molecular devices, which are frequently created using biomolecules, can accomplish some of the features needed in sensor nodes. These nodes are self-contained and derive their energy from chemical processes inspired by biological systems. The manufacturing and architectural process of these devices is similar to natural processes in biology; in addition to safety and biological compatibility, bio-inspired nodes must be able to synthesize bottom-up, reproduce, and repair [10].

8. Energy Consumption Reduction in Body Sensor Networks

As wireless body sensor networks play a vital role in the quality and speed of medical treatments, attention must be paid to the needs of these networks, such as reducing energy consumption and improving the quality of service and security. In the last decade, many efforts have been made to optimize wireless sensor networks. When this network is specifically applied to the human body, we must also consider its unique features. Table 3 compares wireless sensor networks and specific applications for the wireless body sensor network. Among the issues raised in the construction of body sensor nodes are their weight and dimensions, as well as energy consumption limitations. Because these nodes are placed in or on the body, their size and weight are important in this network's design, and the energy supply or battery accounts for most of the weight and volume [11].

Table 3. Comparison between WSN and WBAN sensors [11,45].

Subject of Comparison	Wireless Sensor Networks	Wireless Body Sensor Network
Sensor node number	Many nodes in a wide range	Fewer than 10 nodes in a human body
Topology	Hybrid	Star
Sensor node type	Often homogeneous	Heterogeneous
Nodes' physical properties	Without special restrictions	Tiny, light, wearable, or implantable
Energy supply sources	Limited	Very limited
Energy efficacy	Requires high efficiency	Requires very high efficiency
Security	Unrestricted security	Patients' data requires high security
Communication	Less sensitive to service quality	Requires service quality
Example of node	MicaZ. IMote2	Sensium

On the other hand, these nodes are in direct contact with the user; hence, the number of times the battery is charged is important. One way to optimize these nodes is to reduce energy consumption, which leads to smaller batteries and a reduced need for charging. To optimize the energy consumption in a wireless body sensor network, the amount of energy consumed by its components, including the sensor unit, signal processor, power supply, and communication unit, will be examined [11].

8.1. Monitoring Patients

The leading cause of death worldwide is cardiovascular disease, which accounts for about 33% of all deaths globally. The frequent monitoring of patients can help control and decrease the risk of fainting, weakness, loss of blood circulation, and other complications. It is also important to monitor patients with other chronic diseases including hypertension, Alzheimer's, Parkinson's, postoperative monitoring, and stress monitoring.

Figure 9 depicts a body sensor network, where several sensors are placed directly on or beneath a person's skin in various locations. These sensors collect data on the patient's temperature, blood pressure, heart rate, the electrical activity of the brain, respiratory rate, oxygen saturation percentage, etc. The sensor network can be placed in home appliances such as MP3 players, headphones, headsets, and computers as a neural interface, and sensors can collect data when the patient is playing games, engaging in a leisure-time activity, or working, without attracting the patient's attention or resulting in boredom [12,46].

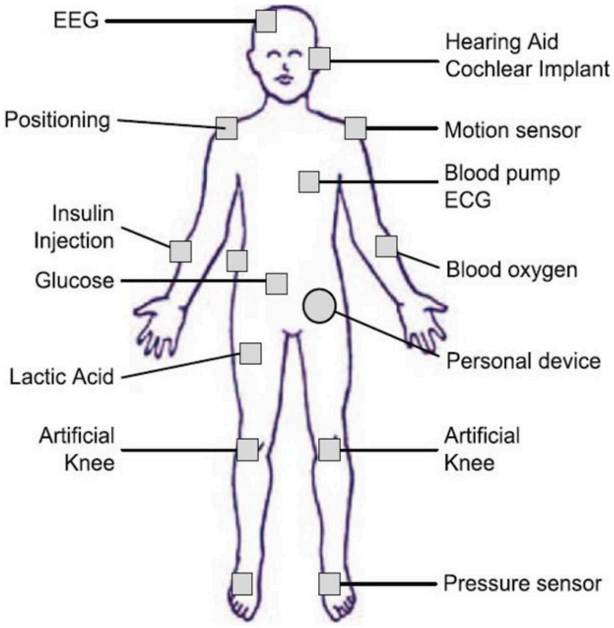

Figure 9. Patient monitoring [46].

8.2. Discussion of Energy Conservation in Body Sensor Networks

From a body sensor network perspective, the model shown in Figure 10 comprises four components: (a) a sensing subsystem consisting of one or more sensors (with analog converters to the relevant digital) for data acquisition; (b) a processing subsystem including a microcontroller and memory for local data processing; (c) a radio subsystem for wireless data communications; (d) the power supply unit. Depending on the specific application, sensor nodes can include additional components such as a locator to determine their positions, a relocation device or configuration, and so on. Nonetheless, we must consider the following statements in general:

Communication subsystems have much higher energy consumption than computing subsystems. Hence, transmitting a bit may consume as much energy as executing several thousand instructions.

Radiation energy consumption is often the same in reception, transmission, and idle modes, while power is cut off at least once in sleep mode. Therefore, the radio transceiver should go to sleep (or be shut down) whenever possible. Depending on the specific application, the metering subsystem can be a significant source of energy consumption, and its power consumption can be reduced [47–49].

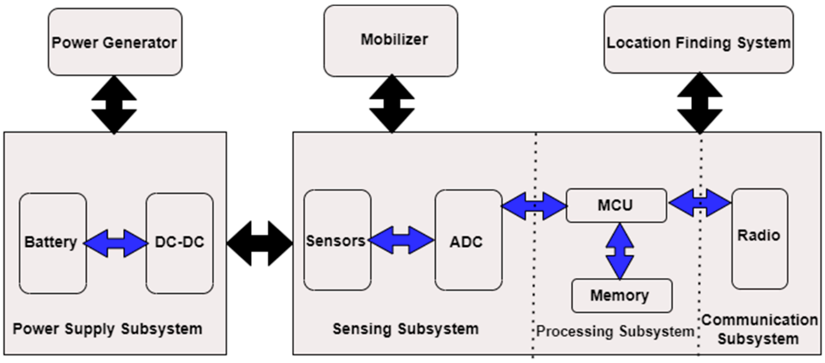

Figure 10. The architecture of a wireless sensor network [49].

In general, energy conservation exists at five different levels [50–52]:

- Efficient programming of the sensor node states between sleep and active modes;

- Efficient transmission power control to ensure a balance between optimal energy consumption and connectivity;
- Efficient routing of energy, clustering, and data aggregation;
- Data compression (source code) to reduce the amount of data transferred in vain;
- Access to efficient channels and packet retransmission protocols in the data-link layer.

9. Security in WBAN

Sensor nodes capture patients' physiological signals via the body control unit (BCU); hence, the transmission of messages between network members is extremely sensitive and plays a critical role in guaranteeing patients' physical wellbeing. This system can be hacked if it lacks a strong security mechanism. Attackers may listen in on and manipulate information sent between the sensors and the patient's digital assistant (PDA). Therefore, the necessary measures for data integrity, authenticity, privacy, and confidentiality must be taken during the design of the WBAN [15].

9.1. WBAN Security Requirements

The security needs of medical care programs using body sensor networks are as follows:

Data originality: Medical and nonmedical applications require both verification and licensing services. Authentication must be utilized for each sensor and base station in WBAN medical care applications to ensure that the data supplied by a sensor is reliable [15].

Data confidentiality: Inactive attackers can readily eavesdrop on radio communication between nodes due to the open wireless WBAN channel, resulting in the leaking of information to unauthorized parties. As a result, data must be encrypted before being transmitted [53].

Data integrity: Attackers can alter the intercepted data and deliver it to the intended recipient to achieve illicit goals, resulting in system failure and patient injury. As a result, the data must be checked for integrity [54].

Data availability: Availability ensures that services and information are available when needed. Thus, the availability of medical sensor nodes ensures that health data are consistently available for medical care. If an unauthorized individual captures a sensor node, data access will be lost. Therefore, accessibility must always be maintained in medical care applications [15].

Data freshness: The freshness technique ensures that the old data have not been recycled by preventing data recording, replaying, and publishing by the attacker node [55,56].

Data authentication: Using the authentication system, each node must have the ability to identify and authenticate the nodes from which it receives information. For this purpose, methods such as symmetric authentication can be utilized [56,57].

Secure management: To maintain integrity in decoding and authentication between nodes, a safe and secure method is needed to distribute and remove keys. To this end, a coordinator can independently manage the distribution of keys between network nodes [56].

Dependability: A security system must have high reliability. A secure and reliable WBAN system must have the ability to recover correct information. Techniques such as error coding can be used to restore broken information [57,58].

Safe positioning: Since the WBAN has a dynamic environment and the location of the patient is constantly changing, there is always a need to update all applications that are responsible for registering the physical location of the patient. However, it should be noted that these movements and updating the location of the patient can provide an opportunity for an attacker to enter fake signals and information into the location registration system [53,56,59,60].

Accountability: In relation to medical and care facilities that need to record and maintain patient information, it should always be considered that keeping patient information is one of the important duties of the staff. In case of a patient's personal information misuse, the medical center and related staff are responsible [58,61,62].

Flexibility: In case of need or request from the patient, there is always a possibility that the patient's emergency information is sent to another person or hospital. In this case, the secondary person and the hospital must have the possibility and permission to access the patient's information [54].

Privacy and compliance requirement: In order to protect the personal and vital data of the patient, international rules and regulations have been developed to protect the patient's information. One of the most important ones is HIPPA. Civil and criminal consequence for this code in case of violation is an amount equivalent to 250,000 USD or 10 years in prison [57,63–65].

Data authenticity: Authenticity provides a method for guaranteeing that the information is sent by the individual who is thought to be sending it. It is useful to use both public keys and private keys when attempting to ensure the authenticity of data [18,66].

Data authorization: To restrict users' access to a system's resources and services to a given degree, the method of authorization is practical. The combination of an ACL with an access policy enables the granular regulation of user access to resources and services [66].

9.2. Security Threats

In this section [67–69], we examine the security threats that may be detrimental to medical care.

Surveillance and monitoring of the patient's vital signs: This is the most prevalent threat to a patient's privacy; an attacker may quickly uncover the patient's information through communication channels by spying on the patient's vital signs. Furthermore, if the attacker has a powerful receiver antenna, they may quickly collect network communications. If the patient's physical location is included in the intercepted communication, the attacker can maliciously substitute the patient's location with the intent to cause physical harm. The attacker can also obtain the communication content, such as the message ID, time tags, and source and destination addresses. As a result, eavesdropping poses a major danger to patients' privacy.

Information threats during transmission: The communication range of wireless networks is not limited and is easily vulnerable. Sensors in medical care applications collect patient and environmental data and communicate it to the physician and hospital server. The information may be attacked while being sent. For example, an attacker could obtain and modify physiological information and then direct it to a server, thereby endangering the patient.

Different Types of Information Delivery Attacks

Interception: Assuming a body surface sensor network is compromised by a smart attacker, the attacker can illegally access sensor data such as encryption keys, sensor ID, etc. [70].

Message change: The attacker extracts and modifies the patient's medical data, and then misleads the involved users such as the patient, physician, nurse, and family. For example, a sensor sends normal heart rate information but the attacker modifies it and sends it to the users, which may result in the physician overprescribing a drug that endangers the patient's health. In addition, manipulated data can generate false alarms or obscure the patient's condition when it is abnormal. Message change threatens data integrity [71].

Wireless sensor routing threats: A malicious user can attack the network layer. They can steal or modify packets, and then forward them to the remote-control center to trigger a false alarm. An attacker can change the address field of the captured packet before sending it to the next node, causing it to deviate from the correct path or even creating an endless routing loop [71].

9.3. Security Mechanisms

Security mechanisms are procedures used to detect and prevent security attacks. In this section, we discuss the issues related to existing security mechanisms.

9.3.1. Cryptography

Medical WBANs deal with physiologically sensitive information; thus, robust encryption functions are among the basic requirements of these networks. These cryptographic functions protect the security and privacy of the patient against harmful attacks. Strong encryption necessitates substantial computation and resources; therefore, selecting the right cryptography for the hungry sources of medical sensor nodes that can give optimal security with the least number of resources is difficult. Furthermore, the communication and computing capabilities of the sensor nodes influence the encryption system used. Some claim that asymmetric cryptography systems are typically too costly for medical sensors, whereas symmetric cryptographic methods are insufficiently complete. Due to the restricted resources of medical sensors, security techniques should be chosen on the basis of several factors. The energy needed to conduct cryptographic operations is determined by the amount of memory required (for example, read-only memory and random-access memory) and runtime (how long it takes to activate security mechanisms) [16].

9.3.2. Key Management

Key management is the management of the keys contained in an encryption system, which includes the birth, exchange, storage, and use of keys. If the cryptographic algorithms and protocols used are invincible, the use of weak keys or the improper use of the required keys can leave many weaknesses for security analysis. The most difficult aspect of cryptography in the real world is key management. It is not simple to create safe cryptographic algorithms, yet academic research in this field can yield solid results. Nevertheless, since the keys used to encrypt communications are crucial in terms of security, maintaining their safety is a challenging task. Many nodes and decryption analyzers attack public key encryption systems and symmetric algorithms through their key management. Therefore, the reliable and robust design of key management has a profound effect on the security of information exchanges [72].

9.3.3. Secure Routing

Sensor nodes must communicate data to nodes that are not within their radio range. As a result, data transmission and routing are crucial. There have been several routing protocols suggested so far, but none have been developed with great security in mind. Denial-of-service attacks affect routing protocols. In addition, an attacker might introduce malicious routing data to the network, resulting in routing irregularities and conflicts. Furthermore, many routing methods are built for static wireless networks, but medical care applications require mobility and dynamism. The security requirements of real-time medical applications may also complicate these protocols [73].

9.3.4. Trust Management

Trust represents the interrelationship of two trusted nodes that have shared their data. Trust is the degree of secure reliability and the reliability that one node has in relation to another node. A distributed collaboration among sensor nodes depends on medical programs. Therefore, one of the critical aspects of these programs is the trust evaluation in the behavior of a node. Therefore, trust management systems help identify the degree of trust in a node [17].

9.3.5. Blockchain Technology

With the integration of wireless sensor networks and the Internet of things, the smart grid is envisioned as a solution to future power supply challenges. However, security and privacy issues in data consumption and commerce pose serious challenges for smart grid adoption. To address these challenges, blockchain technology for smart grid applications such as WBAN is being developed and researched. Blockchain is a decentralized technology that is used to record various transactions performed in the network right from the beginning of the chain. Each block in this chain is connected to the previous block using cryptographic techniques, keys, etc., which secure the system and make it resistant to malicious attacks and malfunctions. A pair of blockchain keys usually consists of a private key and a public key. A public key is like a bank account number used to receive digital assets. A private key is like an account password. Blockchain key encryption is based on the principle of cryptography of specific mathematical functions (e.g., multiplication of an elliptic curve) that makes the generated digital key irreversible and unchangeable [74]. Table 4 reviews related works for securing WBAN.

Table 4. Related work.

	Issue	Papers	Method
1	Cryptography	Hybrid encryption algorithm in wireless body area networks (WBANs)	This paper introduced a new concept, the hybrid encryption algorithm (HEA), which is suitable for ad hoc networks as well as wired networks. This algorithm not only considers data security, but also considers various limitations of sensor networks such as battery power, bandwidth, limited processing capability, and dynamic topology [75].
2	Key management	Trust key management scheme for wireless body area networks	In this paper, the authors presented an approach that uses physiological signals (electrocardiograms (ECGs)) to address security issues in the WBAN: a trusted key management scheme for the body area wireless network. This approach manages the production and distribution of symmetric cryptographic keys to the sensors of a WBAN (using an ECG signal) and protects privacy [76].
3	Secure routing	Secure routing of WBAN with monarchy butterfly optimization	Transfer of healthcare data was centralized in this paper. The WBAN is a mobile ad hoc network (MANET) used to transmit healthcare data. Efficient parameters for secure routing in the WBAN are specified and then optimized simultaneously. Secure routing in the WBAN is modeled as an optimization problem. Because the secure routing parameters are individual and the WBAN structure is dynamic, the optimization is performed simultaneously. Multi-objective optimization algorithms can optimize multivariate simultaneously. Monarchy butterfly optimization was used as a new and powerful multi-objective optimization algorithm in this paper [77].
4	Trust management	Naïve Bayes-based trust management model for wireless body area networks	In this paper, the authors proposed a trust management model based on the naïve Bayes classifier to classify a sensor node as trustworthy or malicious. On the basis of the classification, the trusted node selects a trusted node for data exchange. The authors trained the proposed model in MATLAB, and the experimental results showed that the proposed model can successfully classify a sensor node as malicious or reliable [78].

10. Security Attacks on Wireless Sensor Network

Because of the diffusing nature of the transmission medium, the wireless sensor network is subject to several assaults. Figure 11 depicts many types of attacks on the WSN, which can be divided into active and passive attacks.

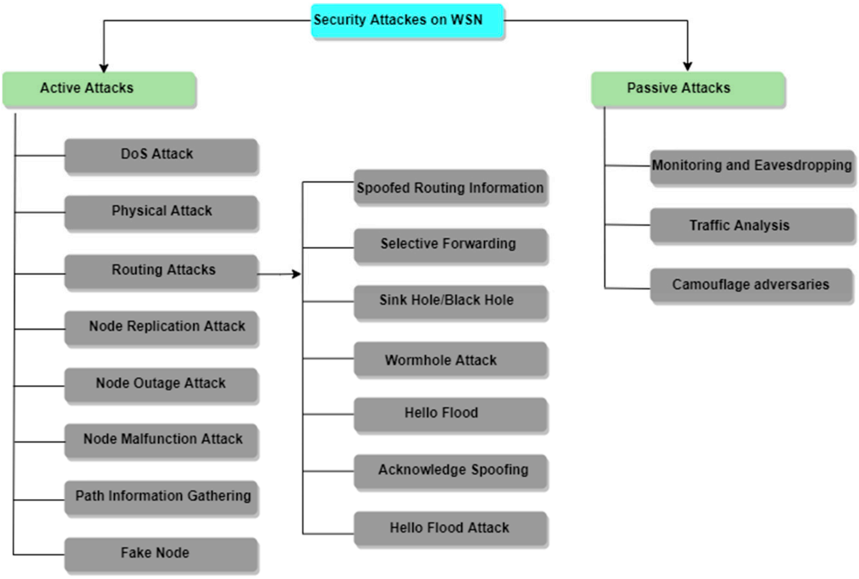

Figure 11. Security attacks on wireless sensor networks [79].

10.1. Active Attacks

In active attacks, there is an enemy who is listening and introducing malicious code, stealing or tampering with the content of the message, and breaking the security mechanism [79].

Active Attacks on WSNs Are Described Below

I. DOS Attack

A DOS attack is an attack that reduces the capacity of networks to perform tasks and is generated by malicious activity or the unintentional failure of nodes. Various types of DoS attacks can occur in a wireless sensor network [80].

In this attack as illustrated in Figure 12, the attacker overloads the server, which renders the server incapable of processing the request. For example, node X sends a request to node Y for connections, and node Y sends information to node X, but node X continuously sends a request to Y. As a result, node Y is unable to communicate with any other node [80,81].

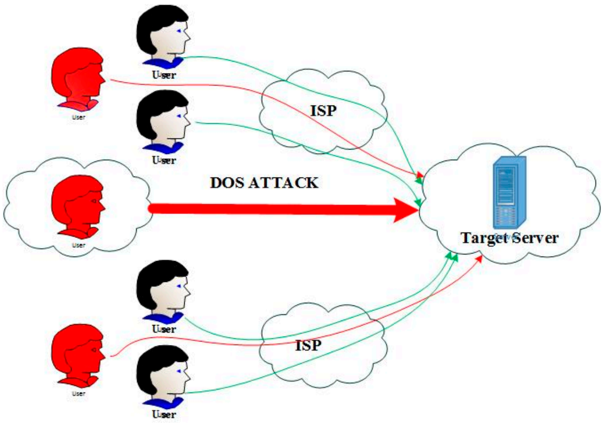

Figure 12. DOS attack demonstration [81].

Blocking a node or a group of nodes is the simplest DOS attack on a wireless sensor network. The transmission of a telecommunication signal that interferes with telecommunication frequencies and is used by the sensor network is referred to as obstruction [80].

II. Physical Attacks

Outdoor wireless networks are the most common target for physical attacks. Wireless networks are vulnerable to physical assaults due to their scattered and unsecured nature. As demonstrated in Figure 13, Sensor nodes can continually be damaged by physical attacks, which may be irreparable. An attacker might steal sensitive data or change the software code [79,82].

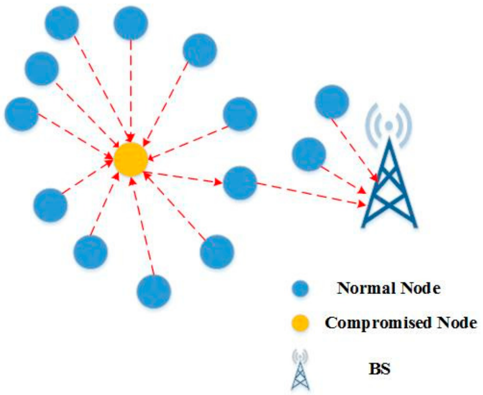

Figure 13. Physical attack on WSN [82].

III. Routing Attacks

Routing attacks are assaults that target the network layer. The attacks that arise when routing messages are listed as follows [83]:

(a) Deceptive Routing Information

In the sensor network, the sensor nodes receive values and send them to the BS. When this information is routed to the main station, an attacker may modify that routing information to interrupt the network traffic [84]. Figure 14 depicted deceptive routing information attack.

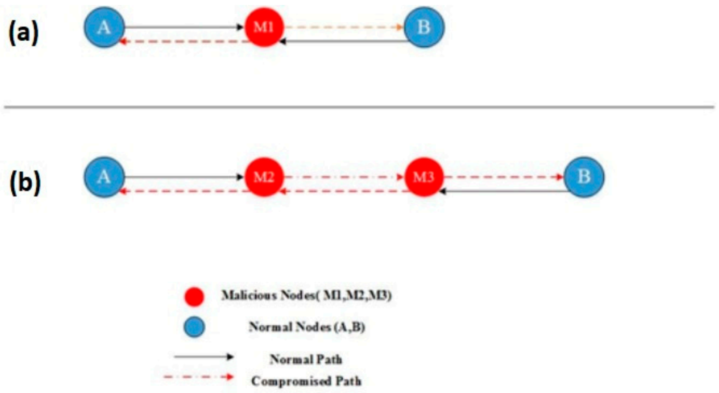

Figure 14. Deceptive routing information on WSN [84].

(b) Sending the Selected Package

It is thought that all nodes in a wireless sensor network communicate the complete received packet correctly; however, in this attack, an attacker constructs a rogue node that does not relay the entire received message [83].

(c) Blackhole Attack

In blackhole attack, as shown in Figure 15, an attacker develops an endangered node that looks the most like adjacent nodes in a high-capacity sensor network in this sort of assault. As a result, all nodes in the vicinity of the data are routed via this affected node, and when data go through this infected node, the attacker has complete control over the packet [83].

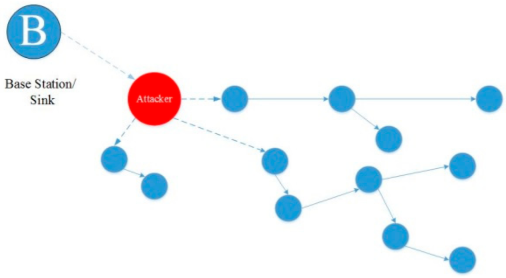

Figure 15. Blackhole attack on WSN [85].

(d) Sybil Attack

Each sensor node in a wireless sensor network may need to collaborate to complete a task. In this type of attack as demonstrated in Figure 16, a malicious node masquerades as a group of hostile nodes, impersonating other healthy nodes and disrupting the routing method, dispersing the source, changing the data density, and delivering misleading information to the network [86].

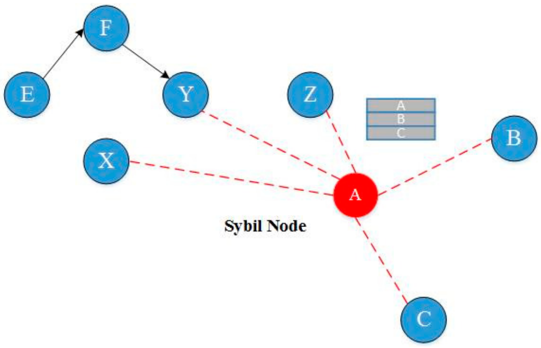

Figure 16. Sybil attack on WSN [10,87].

This false information can relate to a variety of issues, such as the position of the nodes and the signal strength to build a node that does not exist [86].

(e) Wormhole

In the wormhole attack, the attacker catches the packet (bits) at one site on the network and retransmits it to another location [88].

When the base station or any other sensor node (assume node B) needs to communicate data, it sends out a routing request packet. An attacker gets a routing request packet and delivers the data to node B when it is released. When node B provides data, the attacker receives it and, while concealing its identity, sends it back to the nearby node. A wormhole is created when a nearby node believes it is within node B's range, but it is actually far away from the B node [88]. Figure 17 represented wormhole attack.

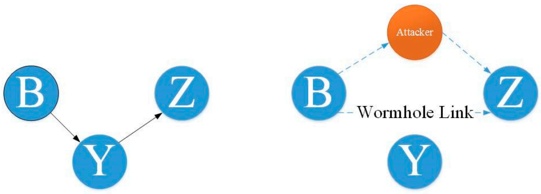

Figure 17. Wormhole attack on WSN [88,89].

(f) Hello Flood

This is the most basic assault on a wireless sensor network, in which an attacker uses a high-power Hello packet as a weapon to persuade the sensor nodes to spread across a vast region of the wireless sensor network. The victim nodes try to convey the data to the base station through the attackers because they see the attacker as a neighbor. As a result, the node is deceived by the attacker [90]. Figure 18 depicted Hello flood attack on WSN.

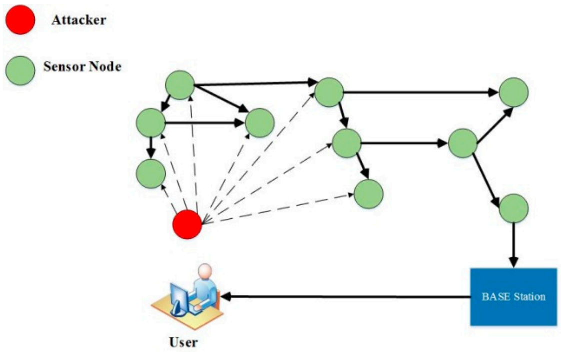

Figure 18. Hello flood attack on WSN [91].

(g) Acknowledgment Spoofing

Sensor network routing methods must sometimes be tested before they can be utilized. In this type of attack as shown in Figure 19, an attacker might eavesdrop on a packet transmitted by one of its nearby nodes and tamper with it by verifying or transmitting fake information, such as sending information that a node is alive while it is actually dead and providing false information to other nodes [92–94].

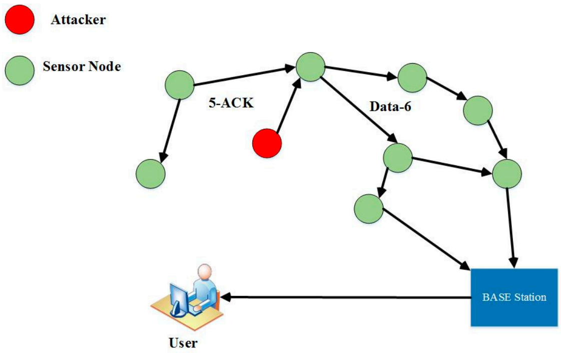

Figure 19. Acknowledgment spoofing attack on WSN [95,96].

IV. Node Reflection Attacks

In a node reflection attack, an attacker copies the ID of an existing sensor node and adds it to the current sensor network. Using packet diversion or bogus packet routing, this attack slows down the network operations [42].

V. Node Disconnection

When a node stops operating, this is known as node disconnection. When a group guide stops the operation, the sensor network protocols must be resilient enough to generate a recommended way to reduce the node's certain consequences [97].

VI. Node Malfunction

A faulty node might create erroneous data, which can jeopardize the sensor network's health, especially if the node is a dense data node such as a group guide [97].

VII. Collecting Passive Information

An intruder with a powerful receiver and a well-designed antenna can easily eliminate data propagation. Blocking messages that involve the sensor nodes' physical locations allows the attacker to locate and destroy the nodes. In addition to the locations of the sensor nodes, an unauthorized person can view the specific content of messages, including message IDs, timestamps, and other fields [13,98].

VIII. Artificial Node (False)

An artificial node attack is an attack in which a malicious node is added to a wireless sensor network that encourages artificial data or halts appropriate data transmission. Most attacks on the wireless sensor network are caused by artificial information [99].

10.2. Passive Attacks

In passive attacks, the attacker tracks the traffic from which the data are transferred rather than altering or modifying the data as in active attacks. The goal of this assault is to intercept the information being transferred.

A number of common passive attacks on the WSN are described below.

- *Monitoring and Eavesdropping*

This is the most prevalent privacy breach. An intruder snoops the data, and by snooping the data, they easily comprehend the message's contents. When the traffic transfers control data about the sensor network configuration, eavesdropping can effectively undermine privacy protection [99].

- *Traffic Analysis*

Another passive covert attack on a wireless sensor network is called traffic analysis. An enemy examines traffic to detect the activities of a wireless sensor network and a number of sensor nodes that are critical to the wireless sensor network. This approach might result in a denial-of-service attack that targets the most critical nodes [97].

- *Hidden Enemies*

This attack is a passive covert attack on the wireless sensor network. In this attack, an enemy inserts a sensor node into the wireless sensor network. These camouflage nodes absorb packets from other nodes and give incorrect addresses to those nodes that perform the covert analysis [99].

10.3. Attacks on The Physical Layer

Congestion: This is a well-known attack on wireless communications that easily interferes with the radiofrequencies used by a transceiver of the device. The only difference between congestion and normal radio broadcast is a delay in the service status of the former. The degree of congestion is determined by physical characteristics such as high power, antenna design, obstacles, and a wide field. This type of attack is particularly effective against single fixed-frequency networks when the nodes are in a small, single-spectrum mode. Standard defense against congestion includes the use of a wide range of frequency techniques [100].

Frequency transmission: This is a type of broad-spectrum in which a sequence is used to change the transmission frequency. The receiver, also called a sequence, can re-transmit a signal to reconstruct the original message. Frequency transfer resists unexpected congestions, i.e., interferences. Broad-spectrum techniques resist noisy environments in which sensor networks are destroyed. Although this set of inverse criteria has been carefully studied, their inherent complexity includes broad-spectrum systems which bear a heavy cost for sensor particles [100,101].

Frequency jump: This attack requires two important sources, high power and a high financial cost. Preventing service attacks is a difficult task because most sensor networks use single-frequency communications. Wood, Stankovic, and Son proposed a jammed-area mapping that emphasizes identification and compatibility in response to congestion [102].

They assumed that only a part of the network is congested, and then tried to map the area. Therefore, the attack can be avoided. Nodes in the affected area are synchronized with the low-power state. Information about congested areas is transferred to the network layer. Hence, packets can be easily routed around congested areas. If broad-spectrum techniques cannot be integrated into particles, detection algorithms such as Jam can be significant in the case of defending against congestion attacks [101].

Tapping: A secondary problematic issue in the physical layer is the relative ease and potential difficulty of tapping the device. The risk of this attack is increased by the large-scale, robustness, and special nature of sensor networks. Access to thousands of nodes over several kilometers cannot be completely controlled. Attackers can gain more access to nodes than network operators. Nodes may be abducted or trapped without emerging problems. Although node destruction is undesirable, node inclusion can be dangerous due to the cryptographic process [101].

One type of defense involves regulating the physical temperature of the devices. Nodes must react to knocking by removing sensitive cryptographic information; nevertheless, tapping-resistance packing increases the cost of the device and reduces their economic utility.

The best solution is an algorithmic solution. Algorithms that reduce the impact of a single key factor on a perfect network have a security impression. For example, if each node has a key with its agents and neighbors, a smaller part of it is included than the time the network has a set of keys. Although this software achievement is less costly, it does not provide significant protection. In fact, tapping is one of the most important problems in sensor network security [103].

11. Methods Presented for Health Monitoring Systems of Wireless Body Sensor Networks

Recently, wireless body area networks have attracted great interest in medical and non-medical fields due to the growth and usefulness of the subject. In WBAN, small wearable and implantable sensors are used, either on or inside the body to monitor physiological parameters such as blood pressure and blood sugar levels. WBANs continuously monitor health which can significantly reduce treatment costs. Unlike wireless sensor networks, star topologies are commonly used in WBANs. In this topology, an access point (sinkhole) is available to collect data from nodes 1.5 m away. The access point is like a personal digital device that normally has enough power resources. The activities of the sensors can play an essential role in saving energy, and the access point can be a coordinator of all activities. An access point with multiple nodes (typically 10) makes routing protocols viable for data collection at the access point in an asymmetric architecture. However, sensor nodes suffer from limited energy resources. Efficient routing protocols have been proposed to forward the body's sensor data to the medical server; the operation of each is described below.

The construction of an effective health monitoring system in the research community has been studied. Many solutions and techniques have been proposed to solve the significant design challenges associated with these systems. In this section, we take a brief look at the body of research conducted in this field.

Much work has been conducted regarding health monitoring systems. The researchers in [104] proposed the mHealth Mon project, an energy-efficient mobile health monitoring system based on cloud computing. The main idea is to run some program components in parallel in the cloud to avoid wasting the battery charge of mobile devices.

Prioritization of patients' health status, support for quality of service, multi-interface design, and multi-directional routing have been studied in many research projects.

The developed system can identify the patient's emergency information and guide the medical staff to the most appropriate management of emergencies. Prioritization of emergencies and evaluation of the most appropriate ambulance and care measures are the features of this system. A priority-based and interference-sensitive monitoring system was introduced in [13]. The system transmits the patient's vital signs based on their current state of health and the current state of the network, such as congestion, interference, and multichannel access. and latency. The work presented in [99] examined multidirectional routing and interfering design in systems based on WBANs. Researchers in [94] proposed a multifrequency/multichannel communication framework for wireless body area networks to prevent the effects of fading in health monitoring systems. The goal is to increase data rates to support multimedia data and improve overall network performance. A handoff protocol for wireless body area networks was provided in [105] to support user mobility in the environment. There have been many articles in recent years focusing on medical system security issues; in 2013, Jiang et al. [106] proposed a privacy enhancement scheme for remote medical information systems, but Kumari and colleagues [107] showed that their plan was attacked by a stolen inspector, an online password guess attack, and an identity forgery attack.

11.1. M-ATTEMPT Routing Protocol

This protocol uses a multistep routing scheme for heterogeneous body area networks. While the connection is multistep for delivery, this protocol uses direct communication to route and send data when emergency data or wanted data are requested. One of the main challenges of this protocol is the heat generated by the sensors [108].

In the first phase of this protocol, all nodes broadcast a hello message, as shown in Figure 20. This message comprises information about the nodes' neighbors, as well as the distance between them and the sinkhole. In this way, all nodes know their neighbor, and the location of the sinkhole and the accessible node-to-sinkhole routes are determined. The second phase of this protocol is to calculate the routes with fewer steps to the sinkhole. The path with the fewest steps is selected as the data transmission path [108].

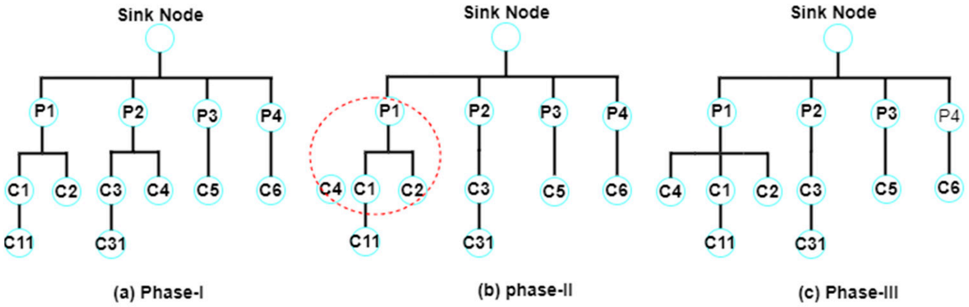

Figure 20. Execution steps of M-ATTEMPT protocol [108,109].

11.2. SIMPLE Routing Protocol

A reliable and efficient SIMPLE protocol has been proposed to increase the routing power of wireless body area networks. This protocol uses multistage technology to lower energy consumption and maximize network life. The protocol uses a cost function to select a parent node or data carrier. The goal is to select the parent node whose cost function has the highest amount of energy and the shortest distance to the sinkhole [97]. In this protocol, after placing the sensors on the human body, a message containing the spatial information of the sinkhole on the human body is broadcast to all the nodes to identify the position of the sinkhole on the body. When the information is received, each sensor becomes aware of the location of the sinkhole, and a package containing information such as residual energy and the distance to the sinkhole is broadcast to all. By doing this, each sensor will be aware of its neighbors. The sinkhole selects a node as the parent node (forwarder) according to the information received from all sensors by calculating the cost function, which can be elicited from the following formula [110]:

$$C.F\ (i) = (d\ (i))/(R.E\ (i)), \tag{1}$$

where *d (i)* is the distance of node *i* to the sinkhole, and *R.E (i)* is the energy of node *i.*

The sinkhole selects a node as a forwarder according to the calculation of the cost function of each node. The node with the most residual energy and the shortest distance to the sinkhole is selected as the forward node. After selecting the forwarder node, all nodes send their information to the forwarder node, and the forwarder node transports them to the sinkhole at specified intervals [110].

11.3. HPOR

The purpose of this protocol is to improve the energy and high routing power for body area networks. In this protocol, the energy consumption needs to be maximized, and network life is maximized by hierarchical routing. In this protocol, one node collects data from the other nodes as a cluster head and then sends it to the base station. The basis is the use of energy in a clustering scheme as a function of the minimum control rate for data transfer. In this method, sensors divide smaller nodes into clusters and each cluster into a cluster. The cluster head manages the connection of nodes with the base station. Therefore, the sensor nodes are no longer directly connected to the base station [111].

11.4. HEAT

The approach to using wireless body area networks in healthcare programs is very limited as currently used. The purpose of the proposed protocol (adaptive power protocol to save energy by horizontal displacement) is to move the routing horizontally over the body, using direct communication for emergency data and multistep communication for standard data. This protocol increases the lifespan of the network and provides the best period of stability, in which the human body moves horizontally in a walking position, and the sinkhole is placed on the abdomen. When the human body is in a fixed position, the nodes are arranged according to the table. The position of the nodes is shown in Table 5. Each node is placed on the human body according to the distance [112].

Table 5. The position of the nodes on the body [112].

Node No.	X Coordinate (CM)	Y Coordinate (CM)
1	40	90
2	60	90
3	50	60
4	50	60
5	50	30
6	50	30
7	50	08
8	50	08

All nodes are located on different parts of the body. Due to the movement of the human body, they send their data to the sinkhole. For example, nodes 2 and 1 are on the chest, and nodes 4 and 3 are on the arms. In this method, there are two types of data: emergency and normal data. In an emergency, a direct data connection to the sinkhole is utilized, whereas, in normal times, a multistep connection is used to send the data [112].

11.5. Ant-Based Genetic Algorithm Routing Protocol

One of the most important issues in relation to body sensor networks is the energy consumption of the nodes. Because the nodes have battery limitations, it is either impossible to replace and charge them, or it is not easy to do so. Therefore, to optimize energy consumption, proper routing and the long duration of nodes in the network are required. In this algorithm, the idea of using the ant-based genetic mechanism to navigate the body sensor networks was proposed in [14]. The proposed algorithm consists of two phases. In the first stage, device and energy aware routing (DEAR) is proposed. This stage interacts with the total amount of network energy in the body area sensor networks to maximize the lifespan of the network. In the second phase, the GACA algorithm is proposed. The purpose of this algorithm is to select the optimal path using an ant-based genetic algorithm. Figure 21 shows the architecture of this proposed algorithm [14].

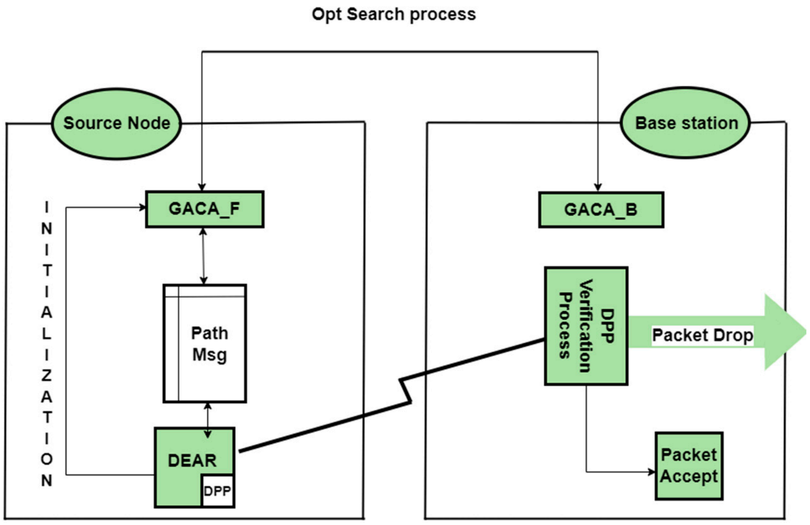

Figure 21. The architecture of the proposed algorithm [14].

As shown in Figure 21, an optimal path is sought from the origin to the base station. There are three types of packages in this plan: data packets, ant packages, and neighbor packages. Data packets are packets referred to in the sensor network. This algorithm is irrelevant to the contents of this pack, and only the ants move the packet forward (GACA-F) and backward (GACA-B). These packages update the routing table. These packages consist of four sections: destination addresses, starting time, final destination reaching time, and a stack of nodes that pass through them. The information in this package is stored for control [14].

11.6. Absorbing Markov Chain Model (AMC)

A mathematical model based on the absorbing Markov chain (AMC) was used to detect sleep denial attacks in sensor networks in [113], and the possible nature of the sensor nodes was detected using the AMC model. Taking into account the expected time of death using this method, the sleep denial attack is detected by sensor networks under a common scenario.

The method of investigating the behavior of high-risk sensor nodes is executed according to the Markov chain with an absorption mode. In the absorption method, the Markov chain is used to model each of the sensor nodes. That is, instead of focusing on the behavior of a sensor node, the network stream is monitored by an intrusion detection method. In this method, the absorption expectation time of the sensor network is examined, which indicates the life span of the network. If the state of the network is prone to rapid death, we compare the common death time of the sensor networks. After this, the network is attacked by sleep denial (affected by the sleep denial attack). This method is much more accurate than the definitive model method.

A hierarchical framework based on the distributed collaboration method [114] was used to detect sleep denial attacks in WSN. This method uses a two-step anomaly detection to minimize the possibility of incorrect intrusion. As a result, a heterogeneous WSN with effective and reliable performance is presented. These variables are compared with specific predefined parameters in a normal index to detect anomalies. The task of each node is to make dynamic changes to minimize the burden created by another node. To decrease the possibility of this attack, the physical method prevents the malicious node from entering the network and rejects fake packets. In [115], a layer of efficient energy with a security mechanism was used to protect the network from sleep denial attacks. The simulation showed that, using this approach, significant efficiency of sleep denial attacks is obtained by preventing network nodes from going to sleep mode. This layer-by-layer interaction concept was used to prevent sensor nodes from wasting energy attacks.

11.7. Scheduling Sensor Nodes Using Phase Logic

Bagci and colleagues [116] proposed a method for sleep/wake scheduling in phase logic-based wireless sensor networks. The method presented in this paper is centralized, i.e., all the collected data as well as the calculations of how to cover the areas are performed in the central station. In this paper, the following two criteria or parameters are used for phase construction:

- The average distance between live nodes and the main station;
- Residual energy (in living nodes).

Three-phase states are considered for the remaining energy parameters. Each of these three modes is displayed as low-energy residue, medium-energy residue, and high-energy residue. The next parameter is the distance between the live nodes and the main station. Three-phase modes are considered for this parameter: low distance, medium distance, and large distance (high). These if-then phase rules are provided in Table 6.

Table 6. If-then phase rules [116].

Distance to Base	Residual Energy	Competition Radius
Close	Low	Very small
Close	Medium	Small
Close	High	Rather small
Medium	Low	Medium small
Medium	Medium	Medium
Medium	High	Medium large
Far	Low	Rather large
Far	Medium	Large
Far	High	Very large

12. Limitation

No comprehensive systematic review in the literature concurrently addresses security challenges and energy usage. The arrival of 5G networks has expedited the use of WBAN for mobile health applications. However, open challenges such as optimizing power consumption, improving the reliability of communications, and achieving transparency with devices and security are still some of the available difficulties yet to be solved; additionally, most approaches in this discipline attempt to use a single metaheuristic algorithm. In short, finding the optimal combination of protocols for improving security and decreasing energy usage is still a significant challenge.

13. Conclusions

Medical science development is very closely related to other fields of science and technology, and it is described by the profound effects that occasional leaps in various branches of science have on human life and how medical services are provided. The advent of body sensor networks represents such a leap. These networks are an innovative and exhilarating branch in the world of remote health monitoring. Furthermore, to assess the status of patients being treated in hospital settings and after discharge at home and work, or to provide the necessary care for the elderly, this new technology enables health monitoring by physicians or intensive care units so that treatment protocols can be applied if necessary. A number of small wireless sensors are installed in or on the body, creating a wireless body network that can sample, process, and transmit various vital signals or environmental parameters. These nodes allow the independent monitoring of a person's location in everyday environments and for long periods, and they provide the user and medical staff with real-time feedback on the patient's health status. One of the issues discussed is optimizing energy consumption in these networks, the central part of which is receiving data through sensors and transmitter and receiver units. One way to reduce energy consumption in wireless sensor networks is to reduce the amount of sent data.

Given that the body's wireless sensor networks play an essential role in communicating between sensors that are installed on the human body to monitor the health status of patients and the activities of people in daily life, much research in this area has been carried out to establish reliable, secure, and efficient communication between these sensors. In this article, we reviewed several methods proposed in recent years to route the wireless body sensor networks with regard to the issue of energy consumption, and we provided a good overview of these methods. Given that there are few articles on the conscious energy management of the wireless body sensor networks, the purpose of this article was to introduce a number of these articles to create a proper mindset for researchers who are interested in working in this field. The methods examined can be implemented and used according to the existing goals and policies; therefore, it is not necessary to use all of them in one environment. It can be concluded that, if wireless sensor networks are implemented without considering issues such as reliability, security, and energy consumption, adverse results, such as increased network implementation costs and the reduced service life of the network, can be expected.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bangash, J.I.; Abdullah, A.H.; Anisi, M.H.; Khan, A.W. A survey of routing protocols in wireless body sensor networks. *Sensors* **2014**, *14*, 1322–1357. [CrossRef] [PubMed]
2. Mainanwal, V.; Gupta, M.; Upadhayay, S.K. A survey on wireless body area network: Security technology and its design methodology issue. In Proceedings of the 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 19–20 March 2015.
3. Tavera, C.A.; Ortiz, J.H.; Khalaf, O.I.; Saavedra, D.F.; Aldhyani, T.H. Wearable wireless body area networks for medical applications. *Comput. Math. Methods Med.* **2021**, *2021*, 5574376. [CrossRef] [PubMed]
4. Javaid, N.; Khan, N.A.; Shakir, M.; Khan, M.A.; Bouk, S.H.; Khan, Z.A. Ubiquitous healthcare in wireless body area networks-a survey. *arXiv* **2013**, arXiv:1303.2062s.
5. Kour, P.; Kang, S.S. Hybrid Routing Protocol for Wireless Body Area Networks. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 1926–1932. [CrossRef]
6. Nadeem, A.; Hussain, M.A.; Owais, O.; Salam, A.; Iqbal, S.; Ahsan, K. Application specific study, analysis and classification of body area wireless sensor network applications. *Comput. Netw.* **2015**, *83*, 363–380. [CrossRef]
7. Gupta, M.; Tanwar, S.; Rana, A.; Walia, H. Smart Healthcare Monitoring System Using Wireless Body Area Network. In Proceedings of the 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 3–4 September 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–5.
8. Saleh, Y.N.; Chibelushi, C.C.; Abdel-Hamid, A.A.; Soliman, A.H. Privacy Preservation for Wireless Sensor Networks in Healthcare: State of the Art, and Open Research Challenges. *arXiv* **2020**, arXiv:2012.12958.
9. Rahangdale, H. A Review on WMSN (Wireless Medical Sensor Networks) for Health Monitoring Systems. *ECS Trans.* **2022**, *107*, 1973. [CrossRef]
10. Adarsh, A.; Kumar, B. Wireless medical sensor networks for smart e-healthcare. In *Intelligent Data Security Solutions for e-Health Applications*; Academic Press: Cambridge, MA, USA, 2020; pp. 275–292.

11. Qu, Y.; Zheng, G.; Ma, H.; Wang, X.; Ji, B.; Wu, H. A Survey of Routing Protocols in WBAN for Healthcare Applications. *Sensors* **2019**, *19*, 1638. [CrossRef]
12. Abidi, B.; Jilbab, A.; Mohamed, E.H. Wireless body area network for health monitoring. *J. Med. Eng. Technol.* **2019**, *43*, 124–132. [CrossRef] [PubMed]
13. Rady, A.; El-Rabaie, E.S.M.; Shokair, M.; Abdel-Salam, N. Comprehensive survey of routing protocols for Mobile Wireless Sensor Networks. *Int. J. Commun. Syst.* **2021**, *34*, e4942. [CrossRef]
14. Xu, G.; Wang, M. An energy-efficient routing mechanism based on genetic ant colony algorithm for wireless body area networks. *J. Netw.* **2014**, *9*, 3366. [CrossRef]
15. Zou, S.; Xu, Y.; Wang, H.; Li, Z.; Chen, S.; Hu, B. A Survey on Secure Wireless Body Area Networks. *Secur. Commun. Netw.* **2017**, *2017*, 3721234. [CrossRef]
16. Huanan, Z.; Suping, X.; Jiannan, W. Security and application of wireless sensor network. *Procedia Comput. Sci.* **2021**, *183*, 486–492. [CrossRef]
17. Salau, A.O.; Marriwala, N.; Athaee, M. Data security in wireless sensor networks: Attacks and countermeasures. In *Mobile Radio Communications and 5G Networks*; Springer: Singapore, 2021; pp. 173–186.
18. Naik, M.R.K.; Samundiswary, P. Wireless body area network security issues—Survey. In Proceedings of the 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kumaracoil, India, 16–17 December 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 190–194.
19. Zhong, L.; He, S.; Lin, J.; Wu, J.; Li, X.; Pang, Y.; Li, Z. Technological Requirements and Challenges in Wireless Body Area Networks for Health Monitoring: A Comprehensive Survey. *Sensors* **2022**, *22*, 3539. [CrossRef]
20. Ananthi, J.V.; Jose, P. A perspective review of security challenges in body area networks for healthcare applications. *Int. J. Wirel. Inf. Netw.* **2021**, *28*, 451–466. [CrossRef]
21. Naresh, V.S.; Pericherla, S.S.; Murty, P.S.R.; Sivaranjani, R. Internet of things in healthcare: Architecture, applications, challenges, and solutions. *Comput. Syst. Sci. Eng.* **2020**, *35*, 411–421. [CrossRef]
22. Kateretse, C.; Lee, G.W.; Huh, E.N. A practical traffic scheduling scheme for differentiated services of healthcare systems on wireless sensor networks. *Wirel. Pers. Commun.* **2013**, *71*, 909–927. [CrossRef]
23. Hanson, M.A.; Powell, H.C., Jr.; Barth, A.T.; Ringgenberg, K.; Calhoun, B.H.; Aylor, J.H.; Lach, J. Body area sensor networks: Challenges and opportunities. *Computer* **2009**, *42*, 58–65. [CrossRef]
24. Vera, D.; Costa, N.; Roda-Sanchez, L.; Olivares, T.; Fernández-Caballero, A.; Pereira, A. Body area networks in healthcare: A brief state of the art. *Appl. Sci.* **2019**, *9*, 3248. [CrossRef]
25. Al-Saud, K.A.; Mohamed, A.; Mahmuddin, M. Survey on Wireless Body Area Sensor Networks for healthcare applications: Signal Processing, data analysis and feedback. In Proceedings of the 3rd International Conference on Computing and Informatics (ICOCI 2011), Bandung, Indonesia, 8–9 June 2011.
26. Liu, Q.; Mkongwa, K.G.; Zhang, C. Performance issues in wireless body area networks for the healthcare application: A survey and future prospects. *SN Appl. Sci.* **2021**, *3*, 155. [CrossRef]
27. Huynh, D.T.; Chen, M. An energy efficiency solution for WBAN in healthcare monitoring system. In Proceedings of the 2016 3rd International Conference on Systems and Informatics (ICSAI), Shanghai, China, 19–21 November 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 685–690.
28. Moungla, H.; Touati, N.; Mehaoua, A. Efficient heterogeneous communication range management for dynamic WBAN topology routing. In Proceedings of the 2013 First International Symposium on Future Information and Communication Technologies for Ubiquitous HealthCare (Ubi-HealthTech), Jinhua, China, 1–3 July 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 1–5.
29. Cornet, B.; Fang, H.; Ngo, H.; Boyer, E.W.; Wang, H. An Overview of Wireless Body Area Networks for Mobile Health Applications. *IEEE Netw.* **2022**, *36*, 76–82. [CrossRef]
30. Ullah, S.; Shen, B.; Islam, S.R.; Khan, P.; Saleem, S.; Kwak, K.S. A study of MAC protocols for WBANs. *Sensors* **2009**, *10*, 128–145. [CrossRef] [PubMed]
31. Kurian, A.; Divya, R. A survey on energy efficient routing protocols in wireless body area networks (WBAN). In Proceedings of the 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 17–18 March 2017; IEEE: Piscataway, NJ, USA, 2007; pp. 1–6.
32. Sagar, A.K.; Banda, L.; Sahana, S.; Singh, K.; Singh, B.K. Optimizing quality of service for sensor enabled Internet of healthcare systems. *Neurosci. Inform.* **2021**, *1*, 100010. [CrossRef]
33. Filipe, L.; Fdez-Riverola, F.; Costa, N.; Pereira, A. Wireless body area networks for healthcare applications: Protocol stack review. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 213705. [CrossRef]
34. Asam, M.; Jamal, T.; Adeel, M.; Hassan, A.; Butt, S.A.; Ajaz, A.; Gulzar, M. Challenges in wireless body area network. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 336–341. [CrossRef]
35. Channa, A.; Popescu, N.; Skibinska, J.; Burget, R. The rise of wearable devices during the COVID-19 pandemic: A systematic review. *Sensors* **2021**, *21*, 5787. [CrossRef] [PubMed]
36. Darwish, A.; Hassanien, A.E. Wearable and implantable wireless sensor network solutions for healthcare monitoring. *Sensors* **2011**, *11*, 5561–5595. [CrossRef]

37. Barakah, D.M.; Ammad-uddin, M. A survey of challenges and applications of wireless body area network (WBAN) and role of a virtual doctor server in existing architecture. In Proceedings of the 2012 3th International Conference on Intelligent Systems Modelling and Simulation, Kota Kinabalu, Malaysia, 8–10 February 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 214–219.
38. Bouhassoune, I.; Saadane, R.; Chehri, A. Wireless body area network based on RFID system for healthcare monitoring: Progress and architectures. In Proceedings of the 2019 15th International Conference on Signal-Image Technology Internet-Based Systems (SITIS), Sorrento-Naples, Italy, 26–29 November 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 416–421.
39. Bedi, R.K. An improved energy efficient TDMA based MAC protocol for WBAN. *Int. J. Comput. Eng.* **2018**, *6*, 34–39.
40. Aishwarya, C. Wireless Body Area Networks–A Review. *Int. J. Res. Eng. Sci. Manag.* **2022**, *5*, 88–91.
41. Abbas, A.M. Body Sensor Networks for Healthcare: Advancements and Solutions. In *Pervasive Healthcare*; Springer: Cham, Switzerland, 2022; pp. 87–102.
42. Hajar, M.S.; Al-Kadri, M.O.; Kalutarage, H.K. A survey on wireless body area networks: Architecture, security challenges and research opportunities. *Comput. Secur.* **2021**, *104*, 102211. [CrossRef]
43. Kołodziej, J.; Grzonka, D.; Widłak, A.; Kisielewicz, P. Ultra wide band body area networks: Design and integration with computational clouds. In *High-Performance Modelling and Simulation for Big Data Applications*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 279–306. [CrossRef]
44. Dhawankar, P.; Kumar, A.; Crespi, N.; Busawon, K.; Qureshi, K.N.; Javed, I.T.; Kaiwartya, O. Next-Generation Indoor Wireless Systems: Compatibility and Migration Case Study. *IEEE Access* **2021**, *9*, 156915–156929. [CrossRef]
45. Khan, R.A.; Pathan, A.S.K. The state-of-the-art wireless body area sensor networks: A survey. *Int. J. Distrib. Sens. Netw.* **2018**, *14*, 1550147718768994. [CrossRef]
46. Mile, A.; Okeyo, G.; Kibe, A. Hybrid IEEE 802.15. 6 wireless body area networks interference mitigation model for high mobility interference scenarios. *Wirel. Eng. Technol.* **2018**, *9*, 34–48. [CrossRef]
47. Chugh, A.; Panda, S. Energy efficient techniques in wireless sensor networks. *Recent Pat. Eng.* **2019**, *13*, 13–19. [CrossRef]
48. Junaid, M. Wireless network sensors applications and challenges in a real-life environment. *IEEE-SEM* **2020**, *7*, 111–117.
49. Khriji, S.; El Houssaini, D.; Kammoun, I.; Kanoun, O. Energy-efficient techniques in wireless sensor networks. In *Energy Harvesting for Wireless Sensor Networks: Technologies, Components and System Design*; De Gruyter Oldenbourg: Berlin, Germany, 2018.
50. Akram, J.; Munawar, H.S.; Kouzani, A.Z.; Mahmud, M.P. Using Adaptive Sensors for Optimised Target Coverage in Wireless Sensor Networks. *Sensors* **2022**, *22*, 1083. [CrossRef]
51. Xiong, C.W.; Tang, M.; Wang, X.H.; Liu, Y.; Shi, J. Evolution model of high quality of service for spatial heterogeneous wireless sensor networks. *Phys. A Stat. Mech. Appl.* **2022**, *596*, 127182. [CrossRef]
52. Roselin, J.; Latha, P.; Benitta, S. Maximizing the wireless sensor networks lifetime through energy efficient connected coverage. *Ad Hoc Netw.* **2017**, *62*, 1–10. [CrossRef]
53. Kargar, M.J.; Ghasemi, S.; Rahimi, O. Wireless body area network: From electronic health security perspective. *Int. J. Reliab. Qual. E-Healthc.* **2013**, *2*, 38–47. [CrossRef]
54. Fatema, N.; Brad, R. Security requirements, counterattacks and projects in healthcare applications using WSNs-A review. *arXiv* **2014**, arXiv:1406.1795.
55. Han, N.D.; Han, L.; Tuan, D.M.; In, H.P.; Jo, M. A scheme for data confidentiality in cloud-assisted wireless body area networks. *Inf. Sci.* **2014**, *284*, 157–166. [CrossRef]
56. Kavitha, T.; Sridharan, D. Security vulnerabilities in wireless sensor networks: A survey. *J. Inf. Assur. Secur.* **2010**, *5*, 31–44.
57. Kumar, R.; Mukesh, R. State of the art: Security in wireless body area networks. *Int. J. Comput. Sci. Eng. Technol.* **2013**, *4*, 622–630.
58. Li, J.; Ren, K.; Zhu, B.; Wan, Z. Privacy-aware attribute-based encryption with user accountability. In Proceedings of the International Conference on Information Security, Pisa, Italy, 7–9 September 2009; Springer: Berlin/Heidelberg, Germany, 2009; pp. 347–362.
59. Ferdous, M.S.; Chowdhury, F.; Moniruzzaman, M. A taxonomy of attack methods on peer-to-peer network. In Proceedings of the 1st Indian Conference on computational intelligence and information security (ICCIIS, 07), Pune, India, 1 January 2007; pp. 132–138.
60. ur Rehman, O.; Javaid, N.; Bibi, A.; Khan, Z.A. Performance study of localization techniques in wireless body area sensor networks. In Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, 25–27 June 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 1968–1975.
61. Sharma, D. Wireless health care monitoring system with data security and privacy. *Int. J. Res. Comput. Eng. Electron.* **2013**, *2*, 1–2.
62. Javadi, S.S.; Razzaque, M.A. Security and privacy in wireless body area networks for health care applications. In *Wireless Networks and Security*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 165–187.
63. Malik, M.S.A.; Ahmed, M.; Abdullah, T.; Kousar, N.; Shumaila, M.N.; Awais, M. Wireless body area network security and privacy issue in e-healthcare. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 2018. [CrossRef]
64. Li, M.; Lou, W.; Ren, K. Data security and privacy in wireless body area networks. *IEEE Wirel. Commun.* **2010**, *17*, 51–58. [CrossRef]
65. Al Ameen, M.; Liu, J.; Kwak, K. Security and privacy issues in wireless sensor networks for healthcare applications. *J. Med. Syst.* **2012**, *36*, 93–101. [CrossRef]
66. Narwal, B.; Mohapatra, A.K. A survey on security and authentication in wireless body area networks. *J. Syst. Archit.* **2021**, *113*, 101883. [CrossRef]

67. Jabeen, T.; Ashraf, H.; Ullah, A. A survey on healthcare data security in wireless body area networks. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *12*, 9841–9854. [CrossRef]
68. Ren, Y.; Leng, Y.; Zhu, F.; Wang, J.; Kim, H.J. Data storage mechanism based on blockchain with privacy protection in wireless body area network. *Sensors* **2019**, *19*, 2395. [CrossRef]
69. Al-Janabi, S.; Al-Shourbaji, I.; Shojafar, M.; Shamshirband, S. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egypt. Inform. J.* **2017**, *18*, 113–122. [CrossRef]
70. Butun, I.; Österberg, P.; Song, H. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Commun. Surv. Tutor.* **2019**, *22*, 616–644. [CrossRef]
71. Usman, M.; Asghar, M.R.; Ansari, I.S.; Qaraqe, M. Security in wireless body area networks: From in-body to off-body communications. *IEEE Access* **2018**, *6*, 58064–58074. [CrossRef]
72. Chen, C.Y.; Chao, H.C. A survey of key distribution in wireless sensor networks. *Secur. Commun. Netw.* **2014**, *7*, 2495–2508. [CrossRef]
73. Tropea, M.; Spina, M.G.; De Rango, F.; Gentile, A.F. Security in Wireless Sensor Networks: A Cryptography Performance Analysis at MAC Layer. *Future Internet* **2022**, *14*, 145. [CrossRef]
74. Zhang, J.; Zhong, S.; Wang, J.; Yu, X.; Alfarraj, O. Alfarraj: A Storage Optimization Scheme for Blockchain Transaction Databases. *Comput. Syst. Sci. Eng.* **2021**, *36*, 521–535. [CrossRef]
75. Farooq, S.; Prashar, D.; Jyoti, K. Hybrid Encryption Algorithm in Wireless Body Area Networks (WBAN). In *Intelligent Communication, Control and Devices*; Advances in Intelligent Systems and Computing; Singh, R., Choudhury, S., Gehlot, A., Eds.; Springer: Singapore, 2018; Volume 624. [CrossRef]
76. Gautam, A.K.; Kumar, R. A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks. *SN Appl. Sci.* **2021**, *3*, 50. [CrossRef]
77. Hashemi, S.M. Secure routing of WBAN with Monarchy Butterfly Optimization. In Proceedings of the 2017 2nd International Conference on Communication and Information Systems, Wuhan, China, 7–9 November 2017; pp. 155–158.
78. Remu, S.R.H.; Faruque, M.O.; Ferdous, R.; Arifeen, M.M.; Sakib, S.; Reza, S.S. Naive Bayes based Trust management model for wireless body area networks. In Proceedings of the International Conference on Computing Advancements, Dhaka, Bangladesh, 10–12 January 2020; pp. 1–4.
79. Butun, I. Prevention and Detection of Intrusions in Wireless Sensor Networks. Ph.D. Thesis, University of South Florida, Tampa, FL, USA, 2013.
80. Ali, M.H.; Jaber, M.M.; Abd, S.K.; Rehman, A.; Awan, M.J.; Damaševičius, R.; Bahaj, S.A. Threat Analysis and Distributed Denial of Service (DDoS) Attack Recognition in the Internet of Things (IoT). *Electronics* **2022**, *11*, 494. [CrossRef]
81. Han, T.; Jan, S.R.U.; Tan, Z.; Usman, M.; Jan, M.A.; Khan, R.; Xu, Y. A comprehensive survey of security threats and their mitigation techniques for next-generation SDN controllers. *Concurr. Comput. Pract. Exp.* **2020**, *32*, e5300. [CrossRef]
82. Butani, B.; Shukla, P.K.; Silakari, S. An exhaustive survey on physical node capture attack in WSN. *Int. J. Comput. Appl.* **2014**, *95*, 32–39. [CrossRef]
83. Virmani, D.; Soni, A.; Chandel, S.; Hemrajani, M. Routing attacks in wireless sensor networks: A survey. *arXiv* **2014**, arXiv:1407.3987.
84. Zhu, Q.; Clark, A.; Poovendran, R.; Başar, T. Deceptive routing games. In Proceedings of the 2012 IEEE 51st IEEE Conference on Decision and Control (CDC), Maui, HI, USA, 10–13 December 2012; pp. 2704–2711.
85. Baviskar, B.R.; Patil, V.N. Black hole attacks mitigation and prevention in wireless sensor network. *Int. J. Innov. Res. Adv. Eng.* **2014**, *1*, 167–169.
86. Majid, M.; Habib, S.; Javed, A.R.; Rizwan, M.; Srivastava, G.; Gadekallu, T.R.; Lin, J.C.W. Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. *Sensors* **2022**, *22*, 2087. [CrossRef] [PubMed]
87. Wadii, J.; Rim, H.; Ridha, B. Detecting and preventing Sybil attacks in wireless sensor networks. In Proceedings of the 2019 IEEE 19th Mediterranean Microwave Symposium (MMS), Hammamet, Tunisia, 31 October–2 November 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–5.
88. Teng, Z.; Du, C.; Li, M.; Zhang, H.; Zhu, W. A Wormhole Attack Detection Algorithm Integrated with the Node Trust Optimization Model in WSNs. *IEEE Sens. J.* **2022**, *22*, 7361–7370. [CrossRef]
89. Ouafaa, I.; Salah-ddine, K.; Jalal, L.; Said, E.H. Review on the attacks and security protocols for wireless sensor networks. *Eur. J. Sci. Res.* **2013**, *101*, 455.
90. Srinivas, T.A.S.; Manivannan, S.S. Prevention of hello flood attack in IoT using combination of deep learning with improved rider optimization algorithm. *Comput. Commun.* **2020**, *163*, 162–175.1. [CrossRef]
91. Dhakne, A.R.; Chatur, P.N. Detailed Survey on attacks in wireless sensor network. In Proceedings of the International Conference on Data Engineering and Communication Technology, Maharashtra, India, 15–16 December 2017; Springer: Singapore, 2017; pp. 319–331.
92. Hussain, M.; Mehmood, A.; Khan, S.; Khan, M.A.; Iqbal, Z. Authentication techniques and methodologies used in wireless body area networks. *J. Syst. Archit.* **2019**, *101*, 101655. [CrossRef]
93. Patil, R.A.; Dhanvijay, M.R.; Patil, S.M.; Dhanvijay, M.M. Comparative Analysis and Simulation of Routing Protocols for Wireless Body Area Networks. In *Recent Advances in Manufacturing Modelling and Optimization*; Springer: Singapore, 2022; pp. 107–119.

94. Alrajeh, N.A.; Khan, S.; Campbell, C.E.; Shams, B. Multi-channel framework for body area network in health monitoring. *Appl. Math. Inf. Sci.* **2013**, *7*, 1743. [CrossRef]
95. Daia, A.S.A.; Ramadan, R.A.; Fayek, M.B.; AETiC, A. Sensor networks attacks classifications and mitigation. In *Annals of Emerging Technologies in Computing (AETiC)*; International Association of Educators and Researchers: Paris, France, 2018; pp. 28–43. ISSN 2516-0281.
96. Sen, J. A survey on wireless sensor network security. *arXiv* **2010**, arXiv:1011.1529.
97. Bangash, Y.A.; Al-Salhi, Y.E. Security Issues and Challenges in Wireless Sensor Networks: A Survey. *IAENG Int. J. Comput. Sci.* **2017**, *44*, 94–108.
98. Keerthika, M.; Shanmugapriya, D. Wireless Sensor Networks: Active and Passive attacks Vulnerabilities and Countermeasures. *Glob. Transit. Proc.* **2021**, *2*, 362–367. [CrossRef]
99. Wahid, A.; Kumar, P. A survey on attacks, challenges and security mechanisms in wireless sensor network. *Int. J. Innov. Res. Sci. Technol.* **2015**, *1*, 189–196.
100. Shi, E.; Perrig, A. Designing secure sensor networks. *IEEE Wirel. Commun.* **2004**, *11*, 38–43.
101. Wang, X.; Gu, W.; Chellappan, S.; Schosek, K.; Xuan, D. Lifetime optimization of sensor networks under physical attacks. In Proceedings of the IEEE International Conference on Communications, ICC 2005, Seoul, Korea, 16–20 May 2005; IEEE: Piscataway, NJ, USA, 2005; Volume 5, pp. 3295–3301.
102. Shin, I.; Cho, M. On Localized Countermeasure against reactive jamming attacks in smart grid wireless mesh networks. *Appl. Sci.* **2018**, *8*, 2340. [CrossRef]
103. Jouini, O.; Sethom, K. Physical Layer Security Proposal for Wireless Body Area Networks. In Proceedings of the 2020 IEEE 5th Middle East and Africa Conference on Biomedical Engineering (MECBME), Amman, Jordan, 27–29 October 2020; pp. 1–5.
104. Ahnn, J.H.; Potkonjak, M. Toward energy-efficient and distributed mobile health monitoring using parallel offloading. In Proceedings of the 2013 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), Osaka, Japan, 3–7 July 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 7257–7261.
105. Bhanumathi, V.; Sangeetha, C.P. A guide for the selection of routing protocols in WBAN for healthcare applications. *Hum.-Cent. Comput. Inf. Sci.* **2017**, *7*, 24. [CrossRef]
106. Jiang, Q.; Ma, J.; Ma, Z.; Li, G. A privacy enhanced authentication scheme for telecare medical information systems. *J. Med. Syst.* **2013**, *37*, 9987. [CrossRef] [PubMed]
107. Kumari, S.; Khan, M.K.; Kumar, R. Cryptanalysis and improvement of 'a privacy enhanced scheme for telecare medical information systems'. *J. Med. Syst.* **2013**, *37*, 9952. [CrossRef]
108. Rahman, H.U.; Ghani, A.; Khan, I.; Ahmad, N.; Vimal, S.; Bilal, M. Improving network efficiency in wireless body area networks using dual forwarder selection technique. *Pers. Ubiquitous Comput.* **2022**, *26*, 11–24. [CrossRef]
109. Javaid, N.; Abbas, Z.; Fareed, M.S.; Khan, Z.A.; Alrajeh, N. M-ATTEMPT: A new energy-efficient routing protocol for wireless body area sensor networks. *Procedia Comput. Sci.* **2013**, *19*, 224–231. [CrossRef]
110. Selem, E.; Fatehy, M.; Abd El-Kader, S.M. mobthe (mobile temperature heterogeneity energy) aware routing protocol for wban iot health application. *IEEE Access* **2021**, *9*, 18692–18705. [CrossRef]
111. Renu, B. An Energy Efficient Routing protocol in Wireless Body Area Networks. *Sci. Eng. Res. J.* **2014**, *2*, 101–106.
112. Afridi, A.; Javaid, N.; Jamil, S.; Akbar, M.; Khan, Z.A.; Qasim, U. Heat: Horizontal moveable energy-efficient adaptive threshold-based routing protocol for wireless body area networks. In Proceedings of the 2014 28th International Conference on Advanced Information Networking and Applications Workshops, Victoria, BC, Canada, 13–16 May 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 474–478.
113. Udoh, E.; Getov, V. Performance analysis of denial-of-sleep attack-prone MAC protocols in wireless sensor networks. In Proceedings of the 2018 UKSim-AMSS 20th International Conference on Computer Modelling and Simulation (UKSim), Cambridge, UK, 27–29 March 2018; pp. 151–156.
114. Moudni, H.; Er-rouidi, M.; Mouncif, H.; El Hadadi, B. Black hole attack detection using fuzzy based intrusion detection systems in MANET. *Procedia Comput. Sci.* **2019**, *151*, 1176–1181. [CrossRef]
115. Boubiche, D.E.; Bilami, A.; Athmani, S. A Cross Layer Energy Efficient Security Mechanism for Denial of Sleep Attacks on Wireless Sensor Network. In Proceedings of the International Conference on Networked Digital Technologies, Dubai, United Arab Emirates, 24–26 April 2012; Springer: Berlin/Heidelberg, Germany, 2012; pp. 151–164.
116. Bagci, H.; Yazici, A. An energy aware fuzzy unequal clustering algorithm for wireless sensor networks. In Proceedings of the International Conference on Fuzzy Systems, Barcelona, Spain, 18–23 July 2010; pp. 1–8.