



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJIRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 6, June 2023

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.423

9940 572 462

6381 907 438

ijirset@gmail.com

www.ijirset.com

An Overview: Health Surveillance Using Wireless Body Area Networks

Himanshu¹, Parvesh¹, Kirti Bhatia¹, Rohini Sharma²

P.G. Student, Department of CSE, Sat Kabir Institute of Technology and Management, Haryana, India ¹

Assistant Professor, Department of CSE, Sat Kabir Institute of Technology and Management, Haryana, India ¹

Assistant Professor, Department of CSE, Sat Kabir Institute of Technology and Management, Haryana, India ¹

Assistant Professor, Department of CS, GPGCW, Rohtak, Haryana, India ²

ABSTRACT: The use of wireless body area networks (WBANs), a recent innovation, has been used to improve the quality of human life by keeping track of patient conditions both inside and outside of hospitals, sports' activities, military applications, and entertainment. Intelligent micro- or nano-sensors that can process information and transmit it to the base station (BS) make up WBANs. Individuals, whether they are patients or not, will be able to provide accurate, complete vital signal measures from any location, just as if they had been taken in hospitals, in addition to receiving medical guidance from a distance. Individuals may be able to exchange critical information via wireless communication thanks to sensors installed in their bodies. In order to diagnose or treat a patient with a chronic condition, or to monitor the patient after surgery to handle crises, a network of these sensors is created that enables long-term medical treatment without interfering with patients' regular everyday activities. This study examines WBAN, its security issues, the architecture and operation of body sensor networks, and technology for communication.

KEYWORDS: Health Monitoring, WBAN

I. INTRODUCTION

In a few years, wireless sensor networks (WSNs) will play a crucial role in human existence and are already a significant area of research. WSNs are networks of sensor nodes that are spatially dispersed throughout the environment and each provide a specific function both alone and in conjunction with other nodes. These networks' primary objective is to gather environmental data and transmit it to the (BS) or remote server. The data is then carefully examined. The smallest part of a network, a wireless sensor has special properties including wide dispersion assistance, mobility, and dependability. The health of a patient can be remotely monitored thanks to wireless body area networks (WBANs), a specific type of sensor network that uses wireless sensor nodes on the body to record physiological parameters including arterial pressure, body temperature, heart rate, and sugar levels in the blood. WBANs come in wearable and implantable varieties. The major goal of WBANs is to protect people's health by placing sensors on the body to transmit physiologic data to medical servers so that doctors can comprehend the patient's health [1].

By supplying services like tracking and supplying pharmaceuticals and healthcare information, increasing patient's perception of data, managing appliances at home, and transmitting data, these systems can significantly help the medical board and individuals in situations. By tracking the patient's vital sign-related data over time, WBANs can also drastically lower the cost of their medical care. Body sensor networks (BSN) employ a star topology topology in contrast to wireless sensor networks. An approaching point (sinkhole) is situated in the body of this topology to collect data from nodes. There are less energy resources available to these networked sensor nodes. In physical sensor networks, sensors (such as mobility sensors) are mounted on a patient's body to track their vital signs or spot movement. The BSN keeps track of the vital signs of a person and instantly responds to the user so that they can follow the course of the patient's illness and take the appropriate safeguards. The energy use of the detectors in this type of network is crucial since once the energy supply runs out, the network's lifespan will be decreased [1].

In this study piece, efforts are made to look into potential solutions that could lengthen network lifespan and minimise node usage of energy simultaneously enhancing security and safety in the WBAN. In other words, the two issues regarding safety and usage of energy are considered and prioritised simultaneously. In order to achieve this, the WBAN and the associated structure are implemented along with the difficulties. The harmful repercussions of assaults and threats, such as the use of energy increase and longevity of networks a decrease, are then addressed after establishing and relying on safety issues and categorising network-related threats. The discussion concludes with protocols, models of mathematics, procedures, and cognitive techniques. It is suggested that this strategy can optimise node energy usage and lengthen the service life of the network in addition to security methods.

II. RELATED WORK

The research in [3-6] looked at design and implementation difficulties security concerns, diffusion modelling, and data routing, as well as real-life challenges like lowering energy usage and guaranteeing the quality of service. These papers gave a thorough explanation of every facet of WBANs, as well as the key considerations in creating multiple routing protocols, protection, and implementation-related technical difficulties. WBANs' major objective is to use biosensors in or near the human body to continuously monitor the condition of the individual and to sound an alarm when a risky scenario is found. The study in [7] included an overview of the many sensors utilised in body network systems and their functionality. The layout of WBAN, combining data, and data transmission in the network are the main topics of WBAN study. The research focuses on sensor deployment, energy usage, and sensor node routing capabilities in connection to network design. Features extraction, data reduction, and data classification are the main topics of data integration study. The authors of [8] investigated the use of energy in WBANs, and [9] offered appropriate strategies for rerouting sensors with other sensor and medical supplies.

Protection algorithms safeguard the network to preserve the integrity, impeccability, veracity, and privacy content while ensuring the security of all forms of data. The research conducted in [10] examined privacy-preserving strategies to guarantee the confidentiality of the gathered personal data. In this article, privacy concerns were prioritised as the most significant security concerns. The patient's data must first be maintained secure and shielded from hostile user nodes and cooperation during the storage procedure. Furthermore, no modifications may be made to patient data while they are being stored. Data must be substituted with hashed using other operations. The third concern is ensuring the data are valid by authenticating the sender, and any faulty data supplied by sources other than the WBAN must be prohibited. Fourth, even in the event of a denial of service (DoS) attack, all information must be available. The authors of [11] indicated that the privacy of the security procedures must be the foundation of a secure communication session between biomarker nodes in a hostile environment so that the data can be made accessible only to an authorised individual.

After providing an overview of WBANs and WSNs in [12], the researchers performed a more thorough analysis into the security needs of the WBAN. After concentrating on two issues of security and privacy in the WBAN, this article attempted to examine the significance, necessity, and issues of privacy in the collection and transmitting of the patient's body's critical information. Additionally, it was emphasised the importance of developing a thorough and effective security system that can conserve energy and has complexity and simplicity in executive computations. Although the need of energy conservation after implementing security was mentioned in this research piece, full energy conservation strategies were not offered.

III. WIRELESS BODY SENSOR NETWORKS

A sensor is an appliance that monitors its surroundings and communicates information about occurrences or modifications to another electrical system. Memory size, computational power, and energy consumption are some of the major restrictions on sensor networks. The wireless sensor network has been utilised in the medical industry, as well as for environmental management, disaster coverage, military and safety monitoring systems, and traffic management, thanks to its improved effectiveness in data collecting. The WSNs are employed to gather information on hospital patients' health and track the progression of rare diseases. The effectiveness of agents can also be tracked via wireless sensors. Such systems are used for tasks including organising medications in a hospital, locating patients and healthcare professionals in a medical setting, and remotely collecting physiological data about the human body. Doctors may be made aware of any emerging health emergencies, allowing medical professionals to respond quickly. This is made attainable by the significant advancements made in wireless sensor network technology in the medical field and the use of data supplied by these devices far beyond the hospital.

The majority of patients visit a doctor when they have unusual health problems, and in many grave cases, the individual requires to be handled right away. In such circumstances, the individual desires to have treatment as soon as possible, and the cost of the treatment may be very high. Yet using a network of sensors can assist preserve people's physical welfare as well as detect disease, which lowers further expenses and dangers throughout the course of therapy.

In some cutting-edge hospitals, rudimentary sensor types are already being utilised to manage drug regimens, monitor doctors and patients in the hospital, and monitor patient physiology data. Nursing the elderly is one of the uses for sensor networks in this area. Muscle action is detected for this purpose using sensor cameras, which builds a complicated network. The elderly are watched over by this network, which can spot falls, unconsciousness, vital signs, food, and activity. According to experts, these networks will be very useful in the future for determining the actual health status of the body as a result of technological advancements and the usage of broadband technology.

The use of this equipment enables real-time health monitoring that can make up for missed degenerative conditions, save people's lives, and thereby save medical expenses. There are some situations when health can currently be monitored from home, nevertheless these systems are not yet flawless. The ultrawideband espionage sensors used today are tiny, wearable, and get their energy from body heat, as was previously detailed in earlier studies. Even though they are small, these devices are able to send a lot of information, which will greatly enhance healthcare and medical services, lower the cost of treatment, and aid in disease prevention. An ultrawideband gadget will be created for this kind of health tracking and measurement. Additionally, it can gather and provide information about the body's insulin levels, cholesterol levels, bone density, and heart health. This gadget can identify a patient with an atrial and foretell the start of a cardiac event, for example, in besides evaluating a patient's health and preventing sickness. This device needs to be affordable, available to everyone, and capable of storing and sending large volumes of data.

IV. BODY SENSOR NETWORK CONFIGURATION

In addition to the sinkhole situated at this level, medical sensor nodes are implanted on or within the human body. Data from sensor nodes are relayed to the sinkhole, where they are aggregated and processed before being sent to the BS. The data are sent to the medical centre over the Internet infrastructure for remote monitoring and treatment after being received by the BS. In the design of this kind of network, each sensor typically keeps tabs on a person's health by gathering sensory input from the patient's body and transferring it to a sink node before being transferred to the BS to request medical attention (Fig. 1). An illustration of a WSN in a healthcare system is shown in Fig. 1. This network gathers health information from patients in various settings and transmits it to a unit that coordinates medical care. The doctor receives this knowledge via a variety of communication channels.

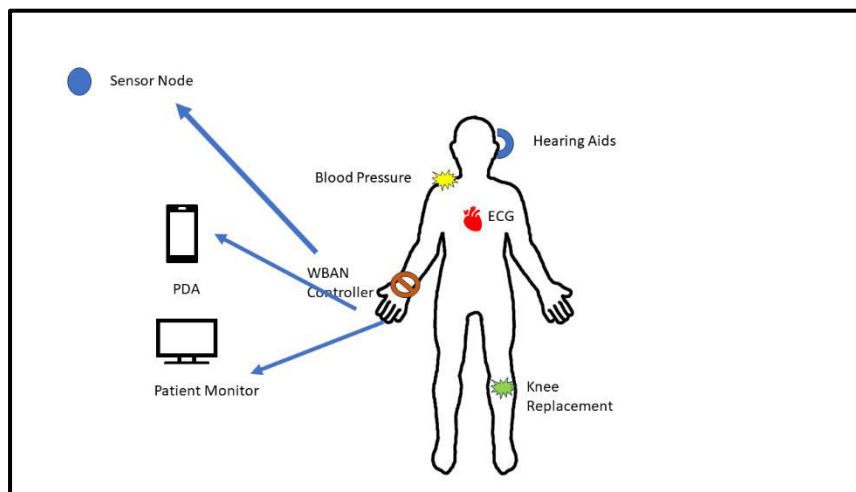


Fig 1.: Comparison of Supervised and Unsupervised Categorization

The BAN coordinating unit then receives the data given by the sensors. Its main function is to time the data transfer and aid in the extraction of useful information from the dataset obtained from the patient's body. The storage unit is another component of this node. In this unit, delayed data are archived and made available to the medical centre upon

request. Sometimes it's necessary to store the data because of bad channel circumstances or high data traffic. The interface unit and the power generation unit are two additional crucial components of this network. To organise the nodes and communicate with following nodes, a transceiver with four frequency channels between 850 GHz and 2.4 MHz is typically employed. Batteries designed for tiny and portable parts offer the necessary power. Figure 2 depicts the design of the TEMPO body sensor node.

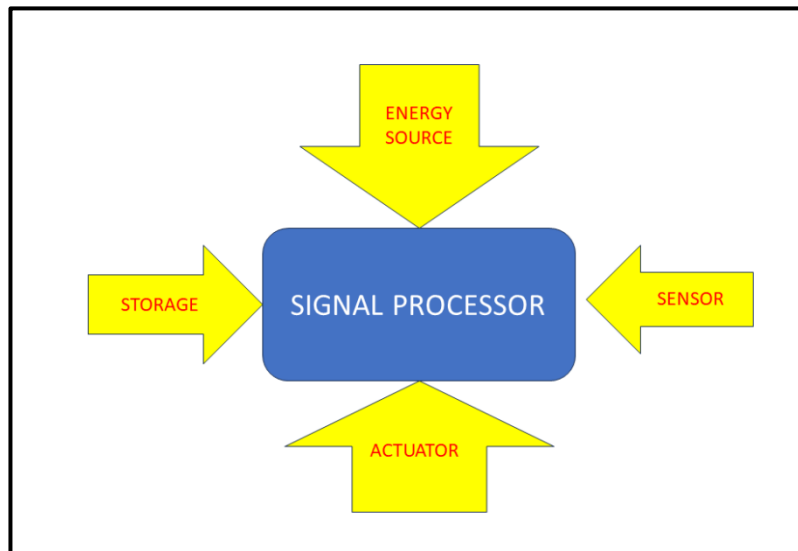


Fig 2: Structure of Body Sensor Node

These body nodes with sensors are all linked together by a central node using a star topology. All nodes on the body deliver data to a collector unit in this design. In the combined mesh star approach, communication is built up between the controlling units of each group, and the other nodes are alerted right away in the event of a problem in one node. In order to connect to larger networks, this design also links collector modules and bridging. Vital body metrics that reflect a person's health and vital signs are tracked by sensor nodes. BP, heart rate, breathing rate, oxygen level in the blood, temperature in the body, etc. are the key vital signs tracked in a body sensor network.

ECG monitoring of heartbeat, EEG surveillance of brain impulses, EMG monitor of muscle signals, glucose monitoring, and physical activity surveillance are additional uses of medical devices in alongside vital signs. diverse sensors should be installed in the network and diverse information gathered from them should be employed for tracking the patient's status so that medical practitioners may make the best judgements possible when using networks of sensors to collect health data. Examples of numerous sensor types employed in diverse contexts include bracelets and dermal electrodes. In order to gather information on the patient's symptoms, various sensors are placed on the body. To establish the patient's health status, body temperature is one important component that should be measured. A low body temperature, to some extent, denotes a higher risk of sickness, and a high body temperature is an indication of illness. High blood cholesterol, blocked arteries, and irregular heartbeats can all be identified using blood pressure readings. The patient's degree of stress can also be determined using the heart rate sensor. Under the effect of stress, blood pressure readings are abnormal, and a person's heart rate and body temperature are closely related to their degree of activity.

For use in body implants, a set of radiant WBAN receiver and transmitter elements operate on the curved body surfaces that are in contact with almost 70% of bodily fluids (tissues). The WBAN signal is diminished and the thermal impacts of radiofrequency (RF) are amplified due to the bodily tissues' absorption qualities. Additionally, the biosensor circuit's signal transmission and other pathways are impacted by the tissues' absorption characteristics. Changes in network communications may change how data acquisition devices operate, resulting in anomalous data and devices as well as network failures. Additionally, the signal power is diminished by signal attenuation caused by tissue absorbance characteristics. As a result, noise might easily upset it. In addition, variations in packet distance during transmission and disconnections as well as decreased reliability are caused by body motion as a result of various dynamics and WBAN topology. The emphasis is on enhancing performance and improving service quality for efficient operation in a

resource-constrained and complex environment given the limits that WBANs confront and the need for future healthcare. Therefore, the quality of services given by leveraging current technology by focusing on their cost-effectiveness, adaptability, and operational efficiency will determine the future of contemporary medical care [13].

V. SANCTUARY ISSUES IN WBAN

The body control unit (BCU), which is used by sensor nodes to gather patients' physiological signals, makes message transmission between network members exceedingly sensitive and essential to ensuring patients' physical well-being. If this system doesn't have a robust security system, it could be compromised. Attackers have the ability to eavesdrop on and alter data transferred between the sensors and the patient's personal digital assistant (PDA). Therefore, when designing the WBAN, the required precautions for data integrity, authenticity, privacy, and secrecy must be taken.

Monitoring and keeping an eye on the patient's vital signs: The greatest risk to a patient's privacy is this: by monitoring the patient's vital signs, an attacker can swiftly learn the patient's information through communication channels. Furthermore, the attacker may swiftly gather network communications if they have a strong receiver antenna. If the intercepted communication contains the patient's physical location, the attacker can intentionally substitute that location with the intention of doing the patient physical harm. The communication content, including the message ID, time tags, source and destination addresses, can also be obtained by the attacker. As a result, eavesdropping puts patients' privacy in grave jeopardy.

Threats to information delivery: Wireless networks' unrestricted communication range makes them easily vulnerable. Medical care applications use sensors to gather and transmit patient and environmental data to the server used by the doctor and hospital. When being transmitted, the information could be attacked. For instance, an attacker might seize and alter physiological information before sending it to a server and putting the patient in danger.

VI. ATTACKS ON INFORMATION DELIVERY

Interception: In the event that a body surface network of sensors is breached by a cunning attacker, the attacker may get unauthorised access to sensor data, including encryption keys, sensor IDs, and other information [14].

Alteration in message: After extracting and altering the individual's medical information, the attacker deceives all parties involved, including the patient, doctor, nurse, and family. For instance, if an attacker alters a sensor's normal heart rate data and sends it to users, the doctor can overprescribe a prescription that is harmful to the patient's health. Additionally, falsified data may cause false alarms or hide an individual's unhealthy condition. Data integrity is threatened by message modification [15].

Threats to wireless sensor routing include network layer attacks from malevolent users. In order to set off a false alarm, they can steal or alter packets before forwarding them to the controlling centre. As the packet is sent to the next node, an attacker can alter the address field, leading it to veer off course or possibly enter an unending routing cycle.

VII. SECURITY METHODS

Cryptography: Medicinal WBANs deal with medically sensitive data, hence strong encryption capabilities are among its fundamental requirements. These cryptographic features defend the patient's confidentiality and privacy from damaging attacks. It is challenging to choose the best cryptography for resource-hungry medical sensor nodes that can provide excellent security with the fewest resources since strong encryption requires a lot of processing and resources. The encryption system in use is also influenced by the sensor nodes' connectivity and computing capacities. Some contend that symmetric encryption techniques are inadequately comprehensive while asymmetric cryptography technologies are often too expensive for use in medical sensors. Medical sensors have limited resources, so security measures should be selected based on a number of considerations. The quantity of memory necessary to perform cryptographic operations determines the amount of energy consumed.

Secure Routing: Data must be sent from sensor nodes to nodes outside of their radio range. Data transmission and routing are therefore essential. Numerous routing protocols have been proposed so far, but none have been created with high security in mind. Routing protocols are impacted by denial-of-service attacks. Additionally, an attacker might inject harmful routing data into the network, causing conflicts and anomalies in the routing. Additionally, a lot of routing techniques were developed for stationary wireless networks, whereas medical applications need mobility and dynamism. Real-time medical applications' security concerns could make these methods more difficult.

Trust Management: The link between two trusted nodes who have shared their data is represented by trust. The level of secure dependability and dependability one node has in respect to another node is known as trust. Medical programmes are required for a distributed collaboration between sensor nodes. The confidence assessment in a node's behaviour is thus one of the crucial components of these programmes. As a result, trust management systems aid in determining a node's level of trust.

Blockchain Procedure: The smart grid has been envisaged as a solution to upcoming power supply issues through the integration of wireless sensor networks and the Internet of things. Nevertheless, the adoption of the smart grid faces significant obstacles due to security and privacy concerns in the use of data and commerce. Blockchain software for applications related to smart grids like WBAN is being developed and studied as a solution to these problems. Blockchain is a decentralised technology that is used to register different network transactions from the very start of the chain. Cryptographic methods, such as keys, are used to link each block in this chain to the one before it, securing the system and making it immune to fraudulent attempts and malfunctions.

VIII. CONCLUSION

A wireless body network that can the specimen, process, and communicate different vital signals or environmental factors is made possible by the installation of a number of small wireless sensors inside or on top of the body. These nodes enable independent location monitoring of a person over extended periods of time and in commonplace settings. They also give the user and medical personnel real-time input on the patient's health. Energy consumption optimisation in these networks, whose core function is data collection via sensors and transmitter and receiver units, is one of the topics covered in the discussion. Reducing the amount of data sent can help wireless sensor networks use less power.

Given the crucial role that WSNs play in the body, a lot of research has been done to establish dependable, secure, and effective communication between these sensors. These sensors are installed on the human body to monitor patients' health statuses and their daily activities. In this article, we analysed a number of strategies put out in recent years to route wireless body sensor networks in light of the problem of consuming energy. We gave a thorough summary of these strategies.

REFERENCES

- [1] Anjali Rana, Kirt Bhatia, Rohini Sharma, "ETM: A survey on Energy, Thermal and Mobility Efficient Routing Protocols for Wireless Body Area Sensor Network," International Research Journal of Commerce , Arts and Science, Vol. 8, issue 4 2017, pp.26-38.
- [2] Anjali Rana, Kirt Bhatia, Rohini Sharma, "IIEPDR: Improved Information and Energy Proficient Data Relaying Routing Protocol for Wireless Body Area Networks", International Research Journal of Science Engineering and Technology, Vol. 7, Issue 2, 2017, pp. 4-11.
- [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.
- [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:1303.2062.
- [5] Kour, P.; Kang, S.S. Hybrid Routing Protocol for Wireless Body Area Networks. *Int. J. Innov. Technol. Explor. Eng.* 2019, 8, 1926–1932.
- [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.
- [7] 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.
- [8] 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.
- [9] 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.
- [10] 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.
- [11] Huanan, Z.; Suping, X.; Jiannan, W. Security and application of wireless sensor network. *Procedia Comput. Sci.* 2021, 183, 486–492.



- [12] 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.
- [13] Yaghoubi M, Ahmed K, Miao Y. Wireless Body Area Network (WBAN): A Survey on Architecture, Technologies, Energy Consumption, and Security Challenges. *Journal of Sensor and Actuator Networks*. 2022; 11(4):67.
- [14] Butun, I.; Österberg, P.; Song, H. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Commun. Surv. Tutor.* 2019, 22, 616–644.
- [15] Usman, M.; Asghar, M.R.; Ansari, I.S.; Qaraq, M. Security in wireless body area networks: From in-body to off-body communications. *IEEE Access* 2018, 6, 58064–58074.



INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.423



ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 **6381 907 438** **ijirset@gmail.com**



www.ijirset.com

Scan to save the contact details