UNIT III

WIRELESS HEALTH SYSTEMS

Need for wireless monitoring, Definition of Body area network, BAN and Healthcare, Technical Challenges- System security and reliability, BAN Architecture – Introduction, Wireless communication Techniques.

3.1. INTRODUCTION

Wireless health system is the integration of wireless technology into traditional medicine, such as diagnosis, monitoring and treatment of illness, as well as other tools that can help individuals improve their personal health and wellbeing. Wireless health differs from mHealth in that wireless health solutions will not always be mobile and mobile health solutions will not always be wirelessly enabled. Mobile broadband connectivity is useful in reaching new patients in remote areas while improving productivity and convenience through data transmission.

Enabling Technologies

- 3G,
- 4G,
- Bluetooth low energy,
- BodyLAN (BodyLAN is a low-power wireless networking protocol that transmits data from medical and fitness devices),
- ANT+ (ANT+ is a wireless networking protocol that allows communication between multiple sensors and devices, designed for wireless sensor networks that require low-energy consumption and low data transmission.),
- Zarlink,

Examples

- Cardionet's 3G-enabled wireless service line, Mobile Cardiac Outpatient Telemetry (MCOT) allows for immediate arrythmia detection.
- Dexcom makes glucose sensing technologies with an FDA-approved product that enables users to manage diabetes with real-time glucose information and trends that can detect potentially dangerous glucose levels.
- A&D makes connected activity monitors, weight scales and blood pressure monitors with software to gather and analyze personal health data.
- Entra Health Systems makes integrated bluetooth-enabled, WiFi, and Cellular blood glucose meters that work with an online data collection network to upload and report patient blood glucose readings.

❖ A weight management system consisting of an armband and an online Activity Manager that automatically tracks activity and sleep. Used in combination with a food log, the system provides a complete picture of the three components of weight loss: calories in, calories out and sleep quality.

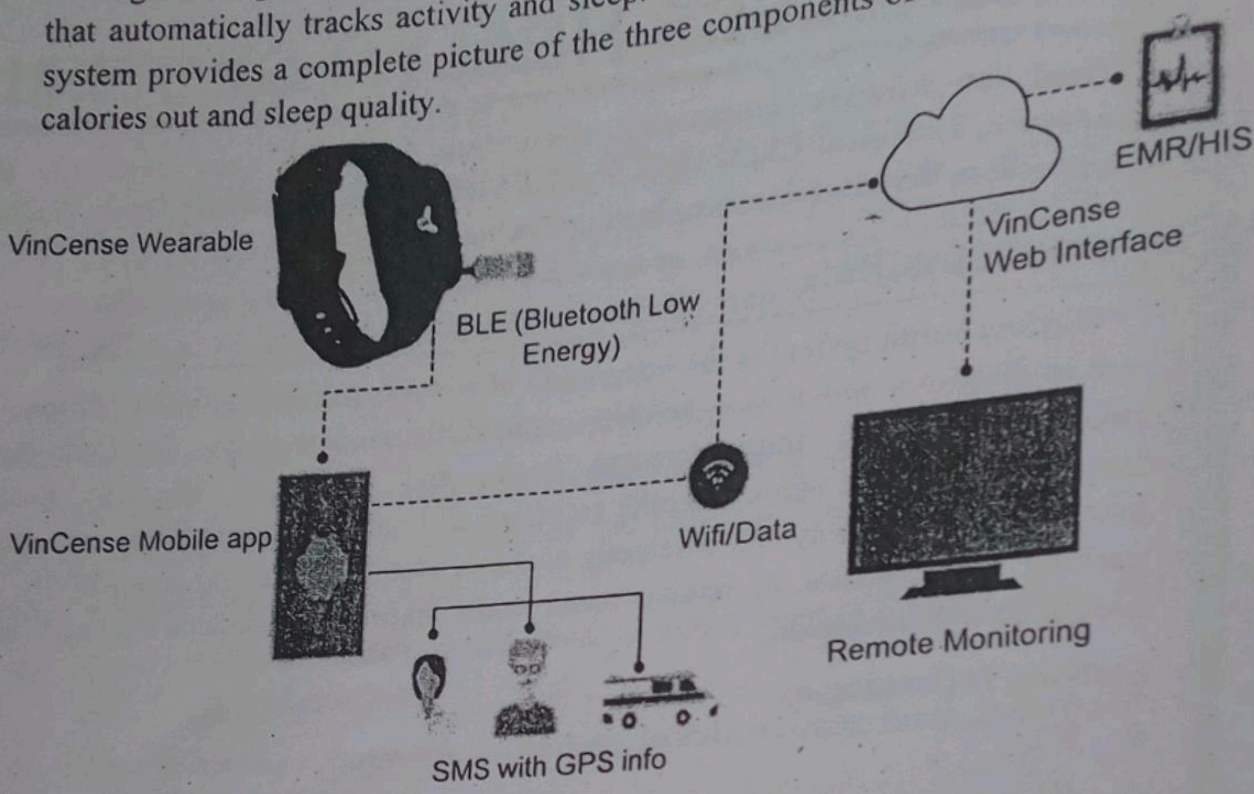


Fig. 3.1.

3.2. NEED FOR WIRELESS MONITORING

❖ A wireless health monitoring system, also known as a patient monitoring system or wireless Health wearables, includes remotely monitoring a patient's vital signs using devices that wirelessly communicate patient data to remote places.

❖ The use of communication equipment in healthcare reduces the challenge faced by medical professionals in simultaneously monitoring several patients.

❖ It allows them to keep an eye on patients without needing to be physically present at their bedside, whether in a hospital or at home.

❖ The devices use a wide range of sensors to monitor the patient's vitals, including heart rate, body temperature, ECG, respiration, non-invasive blood pressure, oxygen saturation, and so on.

❖ The use of wireless health monitoring eliminates geographic barriers to obtaining specialist care.

❖ Wireless health monitors not only send crucial physiological signs to medical workers but also make measuring easier, increasing patient monitoring efficiency.

❖ It also reduces measurement time and aids in receiving care at the optimal time during an emergency, potentially leading to better treatment outcomes.

- During treatment, it is critical to keep track of the patient's health. As a result, even in rural locations, the wireless health monitoring system plays a critical role in providing high-quality care to patients.
- The wireless health monitoring system provides healthcare providers with real-time actionable data in a user-centered interface, allowing them to closely monitor high dependency patients like postoperative, step down, and rehab patients. As a result, it aids in the transformation of healthcare delivery and management at a low cost.
- Wireless monitoring through wearable devices could be useful for hospitalized patients particularlythosewhoareunstableorathigherriskforseriouscomplicationssuchascritically ill patients. The use of wireless monitoring in the ICU setting.
- Wireless sensor network (WSN) technologies have the potential to change our lifestyle with different applications in fields such as healthcare, entertainment, travel, retail industry, dependent care and emergency management, in addition to many other areas.
- The combination of wireless sensors and sensor networks with computing and artificial intelligence research have built a cross-disciplinary concept of ambient intelligence in order to overcome the challenges we face in everyday life.

3.3. DEFINITION OF BODY AREA NETWORK

- A body area network (BAN), also referred to as a wireless body area network (WBAN) or a body sensor network (BSN) or a medical body area network (MBAN), is a wireless network of wearable computing devices.
- BAN devices may be embedded inside the body as implants or pills, may be surface-mounted on the body in a fixed position, or may be accompanied devices which humans can carry in different positions, such as in clothes pockets, by hand, or in various bags.
- Devices are becoming smaller, especially in body area networks. These networks include multiple small body sensor units (BSUs) and a single central unit (BCU).
- Despite this trend, decimeter (tab and pad) sized smart devices still play an important role. They act as data hubs or gateways and provide a user interface for viewing and managing BAN applications on the spot.
- The development of WBAN technology started around 1995 around the idea of using wireless personal area network (WPAN) technologies to implement communications on, near, and around the human body.
- About six years later, the term "BAN" came to refer to systems where communication is entirely within, on, and in the immediate proximity of a human body.

- A WBAN system can use WPAN wireless technologies as gateways to reach longer ranges. Through gateway devices, it is possible to connect the wearable devices on the human body to the internet. This way, medical professionals can access patient data online using the internet independent of the patient location.
- Body Area Network (BAN) technology uses small, low power wireless devices that can be carried or embedded inside or on the body. Applications include but are not limited to:
    - Health and wellness monitoring
    - Sports training (e.g., to measure performance)
    - Personalized medicine (e.g., heart monitors)
    - Personal safety(e.g., fall detection)
- A number of wireless BAN communication technologies have been implemented based on the existing radio technologies. However, if BAN technology is to achieve its full potential, it needs a more specific and dedicated technology, which is optimized for BAN.
- For example, solutions for monitoring people during exercise one or two hours a day, or a few days a week, may not be suitable for 24/7 monitoring as a part of the Internet of Things (IoT) concept.

Concept of BAN:

- The rapid growth in physiological sensors, low-power integrated circuits, and wireless communication has enabled a new generation of wireless sensor networks, now used for purposes such as monitoring traffic, crops, infrastructure, and health.
- The body area network field is an interdisciplinary area which could allow inexpensive and continuous health monitoring with real-time updates of medical records through the Internet.
- A number of intelligent physiological sensors can be integrated into a wearable wireless body area network, which can be used for computer-assisted rehabilitation or early detection of medical conditions.
- This area relies on the feasibility of implanting very small biosensors inside the human body that are comfortable and that don't impair normal activities.
- The implanted sensors in the human body will collect various physiological changes in order to monitor the patient's health status no matter their location.
- The information will be transmitted wirelessly to an external processing unit. This device will instantly transmit all information in real time to the doctors throughout the world.
- If an emergency is detected, the physicians will immediately inform the patient through the computer system by sending appropriate messages or alarms.

- Currently, the level of information provided and energy resources capable of powering the sensors are limiting. While the technology is still in its primitive stage it is being widely researched and once adopted, is expected to be a breakthrough invention in healthcare, leading to concepts like telemedicine and MHealth becoming real.

Applications

Initial applications of BANs are expected to appear primarily in the healthcare domain, especially for continuous monitoring and logging vital parameters of patients with chronic diseases such as diabetes, asthma and heart attacks.

- A BAN in place on a patient can alert the hospital, even before they have a heart attack, through measuring changes in their vital signs.
- A BAN on a patient with diabetes could auto inject insulin through a pump, as soon as their insulin level declines.
- A BAN can be used, to learn the underlying health state transitions and dynamics of a disease]

Other applications of this technology include sports, military, or security.

Standards

The latest international standard for BANs is the IEEE 802.15.6 standard.

Components

- A typical BAN or BSN requires vital sign monitoring sensors, motion detectors (through accelerometers) to help identify the location of the monitored individual and some form of communication, to transmit vital sign and motion readings to medical practitioners or care givers.
- A typical body area network kit will consist of sensors, a Processor, a transceiver and a battery. Physiological sensors, such as ECG and SpO_2 sensors, have been developed. Other sensors such as a blood pressure sensor, EEG sensor and a PDA for BSN interface are under development.

Wireless communication in the U.S

- The FCC has approved the allocation of 40 MHz of spectrum bandwidth for medical BAN low-power, wide-area radio links at the 2360–2400 MHz band.
- This will allow off-loading MBAN communication from the already saturated standard Wi-Fi spectrum to a standard band.
- The 2360–2390 MHz frequency range is available on a secondary basis. The FCC will expand the existing Medical Device Radio communication (Med Radio) Service in Part 95 of its rules.
- MBAN devices using the band will operate under a 'license-by-rule' basis which eliminates the need to apply for individual transmitter licenses.

- Usage of the 2360–2390 MHz frequencies are restricted to indoor operation at health-care facilities and are subject to registration and site approval by coordinators to protect aeronautical telemetry primary usage.
- Operation in the 2390–2400 MHz band is not subject to registration or coordination and may be used in all areas including residential.

3.4. BAN AND HEALTHCARE

- Recent advances in microelectronics and wireless networking are moving closer to turning devices once thought of as science fiction into clinical reality.
- Ultra-small medical sensors/actuators can be either worn or implanted inside the body to collect or deliver a variety of medical information and services.
- The networking ability between these body devices and also possible integration with existing IT infrastructure could result into a pervasive environment that can convey health-related information between the user's location and the healthcare service provider.
- This flexibility for greater physical mobility (i.e. mHealth) directly translates into a significantly higher healthcare experience; and therefore, higher quality of life.
- Body Area Network (BAN) is a technology that allows communication between ultra-small and ultra low-power intelligent sensors/devices that are located on the body surface or implanted inside the body.
- In addition, the wearable/implantable nodes can communicate to a controller device that is located in the vicinity of the body. These radio-enabled sensors can be used to continuously gather a variety of important health and/or physiological data.
- Radio- enabled implantable medical devices offer a revolutionary set of applications among which we can point to smart pills for precision drug delivery, intelligent endoscope capsules, glucose monitors and eye pressure sensing systems.
- Similarly, wearable sensors allow for various medical/physiological monitoring (e.g. electrocardiogram, temperature, respiration, heart rate, and blood pressure), disability assistance, human performance management, etc.
- Wearable devices that work outside the confines of the hospital without expert medical assistance must fulfill a number of characteristics:
  - **Usability:** The device has to be worn on a continuous basis and must therefore be small and lightweight. The challenge is to compress the device size down.
  - **Power consumption:** The device should have low power consumption, reducing the need for frequent re-charging and disruptions in monitoring.
  - **Design:** The device must be elegant without the need to attach long wires and electrodes from the device to the patient and from the device to the mobile gateway that transmits data (to the remote medical care unit).

- **Cost:** If a patient is required to purchase the unit, it should cost sub US$200 to be affordable or for the hospital to give it away free as part of medical care.

❖ Devices that fulfill these conditions can expect to become popular. Manufacturers will find that users are able to easily integrate such devices into their daily lives for maximum benefit.

❖ The typical set of parameters that the device must monitor include heart activity, fetal heart rate, skin resistance, skin temperature, refractive index of blood etc. Based on what the device is required to measure and monitor, its components would include:

- **Bio sensors:** Application specific bio sensors that emit signals indicating measured parameters
- **Analog-to-digital converters:** Application specific analog front end to digitize the sensor signals. The device may also be equipped with signal conditioning circuitry.
- **General purpose microcontroller:** To process signals for the device to function. Signals could indicate battery levels, failure, etc. or signals received from accelerometer, displays and switches, memory and connectivity solutions.
- **Wireless interface:** In most instances, the device will connect to a mobile gateway over a Body Area Network (BAN) or the newer Bluetooth LE (low energy) suitable for continuous transfer of medical data.
- **Memory:** In modern wearable devices, the data is sent in real-time to a mobile gateway (smart phone or a tablet) and then to the patient's remote health care provider. These devices can also store data in off line mode, synchronizing the data when the device goes online.
- **Power management:** The device design must ensure that energy consumption is minimized for longer uninterrupted device deployment and stand by time.

Body Area Networks: Main Features and Requirements

A BAN is an evolution of a wireless sensor network (WSN). WSNs were first used for personal devices like cellphones, laptops, and cameras. These devices form a personal area network (PAN). The same concept is applied to a BAN. A BAN is a network of nodes with sensors and actuators which communicate with each other.

In addition to addressing aspects related to the lower layers of the OSI model, the design of BAN solutions should consider many general requirements such as safety, privacy and security and sustainability to ensure proper operation. However, in order to provide the best user experience, there are other aspects, e.g., quality of service and usability, which should be considered as well.

❖ **Safety:** These types of networks, which are in direct contact with the body, must be designed to ensure they are safe for the end user. Hence, this is a critical point in the development of BAN devices, especially when medical applications are being

- **Privacy and security:** BAN applications collect a great amount of sensitive information that must only be accessible to authorized people. Unauthorized use of private information may lead to abuse and discrimination. BAN solutions that have access or generate sensitive information need to implement authentication and encryption. However, security policies should not overhead the energy consumption of the BAN nodes.
- **Sustainability:** Finding a balance between energy consumption and energy source is mandatory in BAN products. Energy supply must be available when required to achieve a good performance of the BAN solution. Energy-supply models are divided into two groups: (1) the node is supplied directly by the harvesting energy source (SSCS), and (2) the harvesting source saves energy into a battery and the battery supplies energy to the node (SBCS). SSCS involves connecting the energy source (solar panel, wind turbine, etc.) to the computing unit without any energy storage in between. This configuration must be calibrated to match the power supply and the demand in order to be sustainable. The SBCS uses a battery to store energy for later use, which is useful in situations where the power supply is not available at any time, like solar power in the night. In SBCS, the energy generated must be in balance with the energy that the battery can store to reduce waste. Testing the energy consumption of nodes helps to choose the correct energy source needed for the deployment.
- **Quality of service:** Each type of BAN application has a different definition of quality of service (QoS) depending on the services offered. Some elements to measure QoS are latency, jitters, and bandwidth of the network, stats of data transmission, errors and useful information sent in a period of time. In any case, QoS includes adaptability, timeliness, reliability, robustness and credibility for most applications. QoS can be separated into two cases, namely application and network. The application perspective refers to the quality of the user interface (UI). The UI must be understandable and meet all the user's requirements. The network case measures the quality of the application's information provider (latency, reliability, error management, etc.).
- **Usability:** This is another requirement that has to be considered when developing BAN applications. Usability refers to how easily a person without information and communication technology (ICT) knowledge sets up the solution.

Body area network in Health care:

- Many high-level architectures have been proposed for health monitoring systems that employ sets of wearable sensors and their supporting communication and information storage networks
- The most common system-level, functional architecture includes
  1. a network of sensors on the body that stores its data to a wearable or handheld data logger/hub that then communicates wirelessly with a local base station or Internet gateway,

2. a central command center that receives data from these gateways, and
3. a network backbone infrastructure that facilitates the exchange of information between the command center and the appropriate medical service centers.

- While issues such as security and reliability as addressed in this chapter apply to all three levels of network communication, this chapter focuses on wireless technologies for the BANs themselves.
- This is because architectural topologies at the body level are quite limited, promoting a focused discussion in a single chapter.
- At the body level, sensors communicate bi-directionally with wearable/handheld data loggers, which then interact with the resources external to the wearer.
- Mesh sensor topologies, wireless routing schemes, and other more complex topological approaches are typically unnecessary at the body level due to the close proximity of the wireless nodes.
- In addition, the peripheral technologies that support the local gateways and the extended backbone network infrastructure (which may include cellular systems, wireless local area networks, or Home RF implementations) are mature, and treatments of such subsystems are addressed in numerous wireless texts

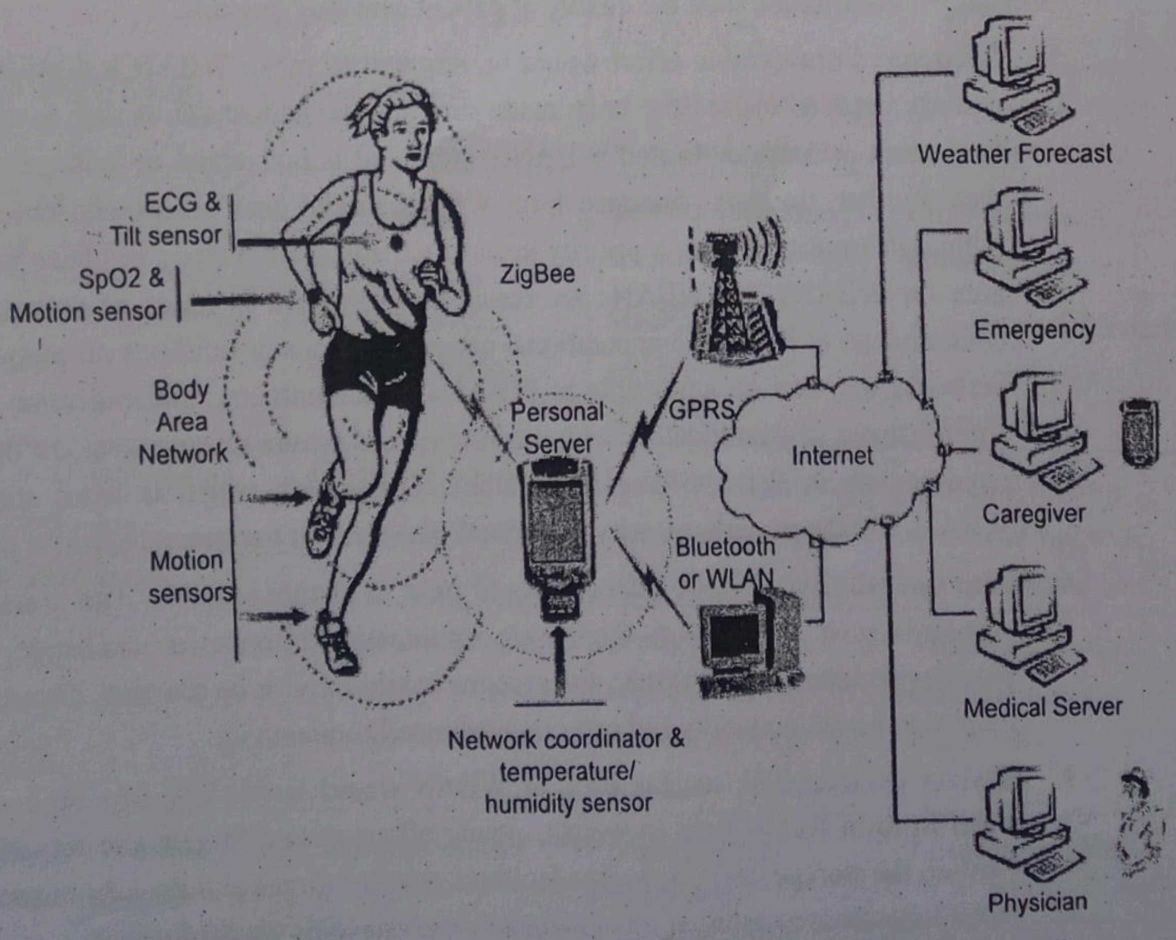


Fig. 3.2. Depiction of a body area network with its supporting information infrastructure

3.5. TECHNICAL CHALLENGES

1. **Data quality:** Data generated and collected through BANs can play a key role in the patient care process. It is essential that the quality of this data is of a high standard to ensure that the decisions made are based on the best information possible
2. **Data management:** As BANs generate large volumes of data, the need to manage and maintain these datasets is of utmost importance.
3. **Sensor validation:** Pervasive sensing devices are subject to inherent communication and hardware constraints including unreliable wired/wireless network links, interference and limited power reserves. This may result in erroneous datasets being transmitted back to the end user. It is of the utmost importance especially within a healthcare domain that all sensor readings are validated. This helps to reduce false alarm generation and to identify possible weaknesses within the hardware and software design.
4. **Data consistency:** Data residing on multiple mobile devices and wireless patient notes need to be collected and analysed in a seamless fashion. Within body area networks, vital patient datasets may be fragmented over a number of nodes and across a number of networked PCs or Laptops. If a medical practitioner's mobile device does not contain all known information then the quality of patient care may degrade.
5. **Security:** Considerable effort would be required to make WBAN transmission secure and accurate. It would have to be made sure that the patient secure data is only derived from each patient's dedicated WBAN system and is not mixed up with other patient's data. Further, the data generated from WBAN should have secure and limited access. Although security is a high priority in most networks, little study has been done in this area for WBANs. As WBANs are resource-constrained in terms of power, memory, communication rate and computational capability, security solutions proposed for other networks may not be applicable to WBANs. Confidentiality, authentication, integrity, and freshness of data together with availability and secure management are the security requirements in WBAN. The IEEE 802.15.6 standard, which is latest standard for WBAN, tried to provide security in WBAN. However, it has several security problems.
6. **Interoperability:** WBAN systems would have to ensure seamless data transfer across standards such as Bluetooth, Zigbee etc. to promote information exchange, plug and play device interaction. Further, the systems would have to be scalable, ensure efficient migration across networks and offer uninterrupted connectivity.
7. **System devices:** The sensors used in WBAN would have to be low on complexity, small in form factor, light in weight, power efficient, easy to use and reconfigurable. Further, the storage devices need to facilitate remote storage and viewing of patient data as well as access to external processing and analysis tools via the Internet.

8. **Energy vs. accuracy:** Sensors' activation policy should be determined to optimizing the trade-off between the BAN's power consumption versus the probability of patient's health state mis-classification. High power consumption often results in more accurate observations on the patient's health state and vice versa.

9. **Privacy:** People might consider the WBAN technology as a potential threat to freedom if the applications go beyond "secure" medical usage. Social acceptance would be key to this technology finding a wider application.

10. **Interference:** The wireless link used for body sensors should reduce the interference and increase the coexistence of sensor node devices with other network devices available in the environment. This is especially important for large scale implementation of WBAN systems.

11. **Cost:** Today's consumers expect low cost health monitoring solutions which provide high functionality. WBAN implementations will need to be cost optimized to be appealing alternatives to health conscious consumers.

12. **Constant monitoring:** Users may require different levels of monitoring, for example those at risk of cardiac ischemia may want their WBANs to function constantly, while others at risk of falls may only need WBANs to monitor them while they are walking or moving. The level of monitoring influences the amount of energy required and the life cycle of the BAN before the energy source is depleted.

13. **Constrained deployment:** The WBAN needs to be wearable, lightweight and non intrusive. It should not alter or encumber the user's daily activities. The technology should ultimately be transparent to the user i.e., it should perform its monitoring tasks without the user realising it.

14. **Consistent performance:** The performance of the WBAN should be consistent. Sensor measurements should be accurate and calibrated, even when the WBAN is switched off and switched on again. The wireless links should be robust and work under various user environments.

Effectiveness of the WBAN is important from both patients and healthcare perspective. As the time passes, challenges to the emerging technologies increases along with the advancements. There is variety of challenges faced by WBAN as explain below. These challenges are classified in six major classes such as energy, mobility, security and communications (i.e., networking, QoS and cooperation).

1. **Energy Requirements:** Since, most of the devices in WBAN are using the wireless medium, therefore they are portable. Such devices are small in size and carry power source too. Hence, the power is always limited. Wireless natures made them roam free, meaning the devices are free to move. The power to the device of the network is provided with the help of batteries. Things are not simplified by allowing the power

from battery but is encompasses some more challenges of power management of the battery supplies especially in case of implants. Since the sensors that are implanted in the body are so small that the battery cannot sustain more than a month. Removing the implants and re-installation require even more management of the complications generated. Different parameters that alter the power consumption include communication bandwidth and processing power. There is need to have better scheduling algorithm along with better power management schemes.

2. **WBAN Security**: In any network, communication data is of worth importance. In case of WBAN, it becomes more critical as it has been connected to the Physical system. These communication channels are very much visible to the attacker and if not securely implemented it could any of the attack including eavesdropping on traffic between the nodes, message injection, message replay, spoofing and off course compromise the integrity of physical devices. Upon successful attack, such actions not only invade privacy but may lead to catastrophic situation.

3. **Mobility Support:** WBAN provides two major advantages, i.e., portable monitoring and location independence. Regardless of the application, these are the key factors due to which WBAN is potential candidate in many venues. But these two advantages put some special limitations i.e., mobility. Mobility can pose serious problem in some application like E-Health care even posture do effect the communication. The mobility is defined between the user and the WBAN as a seamless link. One of the major issues is to reach to sink, which may be single or multi hop. Message is flooded to all nodes to reach sink node and the path with minimum delay is selected. Reliable multipath routing is another solution proposed. A path list is maintained depending upon different factors of the routing and the link is established accordingly.

4. **Quality of Service:** Quality of Service (QoS) is the requirements fulfilled by system as requested by the users. For more life critical system, timeliness may be the parameter for the quality. System, that cannot fulfill the said requirement, falls short of providing the QoS. Same is true for other factors like bandwidth, latency, jitter, robustness, trustworthiness, adaptability. Similarly, seamless roaming and end to end wireless connection between the body nodes and the sink nodes is another QoS factor.

5. **Cooperation between Nodes:** When the intermediate nodes help source destination pair in communication, the cooperation occurs. The intermediate nodes may refer as helper or relay. Cooperation offers a good solution for many of the limitations in WBAN such as distance, mobility, coverage and channel impairments.

3.6. SYSTEM SECURITY AND RELIABILITY

In wireless body area networks, many security techniques are involved to improve the authentication of data communication between patients and doctors. The most involved techniques are intrusion detection systems and cryptography with key management techniques. Table 1 shows the different security techniques used in the body area network.

research issues, and outcomes. Table 3.3 lists the merits of security-based techniques used in the body area networks.

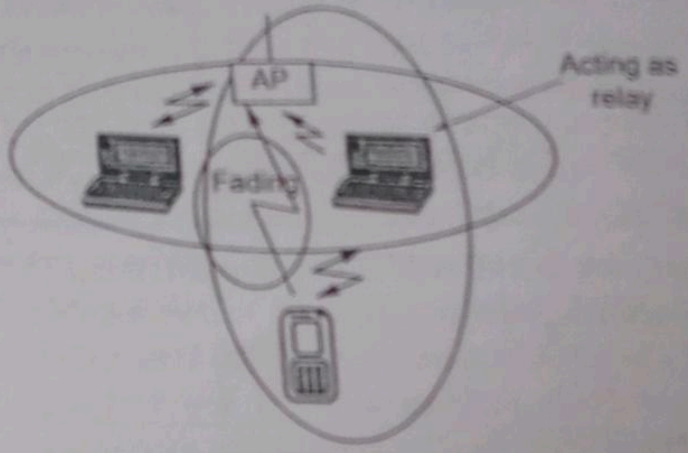


Fig. 3.3.

Table 3.1.

Technique	Research Issues	Methodology	Outcome
Intrusion detection system	Jamming Attacks	Two MAC Protocols involved (ZIGBEE and TMAC)	Successful packet delivery rate
IoT based health	Data Security	Constant monitoring for critical patients	Data authentication and authorization
Cloud- based WBAN	Lesser users	Increased storage level	More users and network lifetime
Mobile agent-based IDS	Network-level intrusion attacks	Machine learning and regression algorithms	Accurate results and lesser resource overhead
Signal propagation based mutual authentication	Active and passive network attacks	Enables mutual trust and used seed update algorithm	Minimal routing overhead and less computational cost
DMASK-BAN	Vulnerable attacks	Secret key extraction with movement aided from DoS attacks	Minimum power consumption with high QoS
Invariant feature-based approach	High-rate attacks	Maintain the bandwidth conditions in cooperative routing	Low-rate attacks

Identity-based anonymous authentication and key agreement	Several security issues	Cloud technology and wireless communication	High storage and low computation cost
Trust management	High residual power	Fuzzy logic technique	Secure and stable performance
Enhanced authentication and access control protocol	User impersonation attacks	Bilinear pairing and elliptic curve cryptography	High security

Different Security Aspects of Secure WBAN

Tan et al. explained the physical unclonable function (PUF) based cloud-assisted authentication scheme to improve the security performance in multi-hop body area networks. To increase the delivery rate, a lightweight authentication technique is implemented, which results in lower storage overhead, resource loss, conflict rates, channel utilization rate, and packet drop rate.

Demir et al. discussed the cyber-physical systems for 6G networks for security enhancement. Smart grid technology is used in the wireless body area network and is adaptable to all applications, including vehicles. The multilayer protection scheme is used to improve the network lifetime, reliability, and low latency which is suitable for real-time applications.

Mo et al. suggested the wearable health monitoring system for known session special temporary information with the two-factor authentications to enhance the security features in a wireless sensor network. A key agreement scheme is involved to improve the security enhancement with high network efficiency and it reduces the computational cost, communication overhead, and traffic computation.

Amel Zendehdel et al. introduced the telehealth monitoring scheme with Bluetooth for low energy applications in wearable devices. This scheme involves fingerprinting, biometrics, and vulnerability scanning for high security and high reliability on the internet of things.

Kong et al. suggested smart healthcare systems which promotes communication security in wireless body area networks.

Jithish et al. discussed the cyber-physical system and used the Markov decision process in wireless body area networks to increase network longevity and energy efficiency, as well as to defend against denial of service and deception attacks.

Vyas et al. discussed the remote health monitoring scheme for health care applications with the help of the Symmetric key generation method. Cloud-assisted technology is involved to improve the storage level in wireless communication channels. Complex encryption techniques are used to identify intruders and strengthen security.

Damasevicius et al. explained the network flow features to detect the different types of attackers by using the cyber security mechanism in wireless sensor networks.

Alzahrani et al. explained the cloud-based IoT scheme for remote patient health monitoring in body area networks. Authentication protocols with session key mechanisms to avoid smart card attacks and improves efficiency.

Irshad et al. described how to detect cyber-attacks in wireless networks using a smart grid-based authentication protocol for energy and internet-based vehicle to grid networks. These smart grid networks boost energy efficiency while also lowering computing and communication expenses.

Reliability Of BAN:

The process of adaptable secure data aggregation framework to improve the data integrity, security, and privacy measures in the wearable sensors for the wireless body area networks. This secure data framework improves the homomorphism security approach for the development of data integrity with the help of an aggregation framework.

Hasan et al. introduced the software-defined network (SDN) based WBAN for secure data transmission. This technique distributes the patient's health record information based on critical and non-critical patients. Furthermore, by employing the sector-based distance vector (DV) protocol for the earliest contact between patients and doctors, the suggested technique gives non-critical patient communications more priority.

Roy et al. explained the security and privacy issues in the wireless body area networks and also suggested adding a cybersecurity mechanism to defend the security challenges. Zhen et al. developed the privacy protection scheme with the cooperation of mobile edge computing for wireless body area networks.

Sammoud et al. proposed an innovative routing protocol for secure data communication with the aid of a biometrics-based cryptographic technique. This innovative routing protocol transfers the data with cryptographic keys and also concentrates on minimal power consumption in body area networks.

Wang et al. introduced the double hash chains for secure data transmission and it also enables data authenticity and reliability. This proposed scheme supports dynamic conditions and maintains the handover scheme.

Sensor nodes/actuators represent essentially the wireless sensor network, and the sensor node senses acoustic factors including temperature, pressure, sound, pulse rate, ECG, blood pressure, and heart rate of the human body. In healthcare, this form of sensor network is known as a wireless body area network (WBAN).

Wireless body area networks consist of sensors, biological parameters, body control unit, personal device assistant, transmission factor, and user access. Figure 3.4 shows that the wireless body area network along with the sensor senses the biological factors continuously in order to obtain the human health information from the body control unit. The electro cardiogram (ECG)sensor records the patient's electric impulse as it passes through the heart muscle. This assists in monitoring the patient's heartbeat, which is used to track various movements such as resting and moving. The temperature of the human body's ears, skin, and forehead are detected by the body temperature sensor.

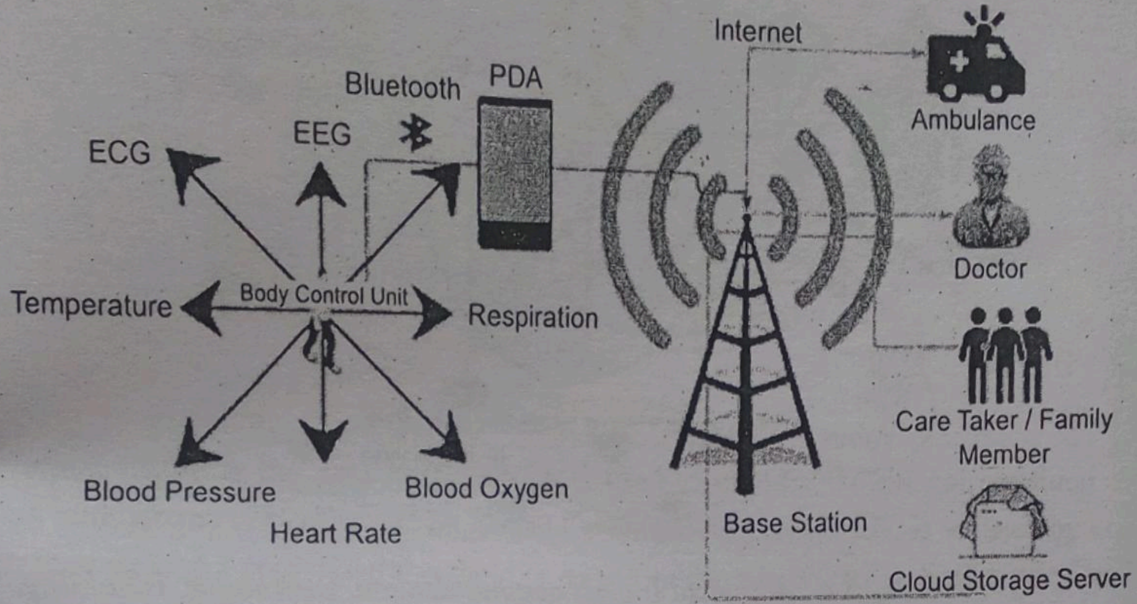


Fig. 3.4. Wireless body area network architecture

The pressure of blood as it travels through the arteries is measured by blood pressure andthepulsewaveismeasuredbytheheartratesensorasitpumpsbloodthroughthepatient's body. The saturation level of oxygen in the blood is measured with a pulse oximeter. The airflow sensor can be positioned near the human body's nasal to assess the body's respiration. The collected information will be transferred and stored in the personal device assistants(PDA) and later transmitted to the base station. From the base station, the data will be transferred to the respective user applications such as cloud databases, ambulances, family members, and doctors via the Internet.

A cloud database's purpose is to store the patient's data on a server so that the doctor can access it and then send the patient's information to the user via the internet. Star topology is used in the body area network. The body control unit acts as a central node and then each sensor will sense and communicate to the center node. The center node interfaces the human body by using Bluetooth or ZigBee or Personal Device Assistants(PDA),and then the patient's information can be accessed by the doctors using the Internet.

Security Issues in WBAN

The purpose of network security is to protect data from threats during data transmission. There are two forms of attacks in network security: active and passive attacks, both of which contribute to the detection of malicious data. An active attack is primarily focused on data and has a significant impact on the system's operation. A passive attack damages or modifies data but does not degrade information resources. The security flaws are applied at various levels. Each layer of the TCP/IP layered architecture generates attacks. IP attacks are introduced in the second layer (logic link control),resulting in address spoofing for incorrect communication. Internet Control Message Protocol (ICMP) attacks is generated in the media access control layer, which results in sniffing and man-in-the-middle attacks. In the third network layer, routing attacks such as blackhole and eavesdropping attacks are created. TCP attacks are originated in the transport layer, resulting in high synchronization flooding in data communication. Application layer attacks are generated in the OSI model's application layer, resulting in authentication issues such as accessing the user's username and password

A denial of service (DoS) attack will restrict data from authorized users and prevent them from accessing their resources. Because of the week password, distributed denial of service (DDoS) attacks is generated. The main difference between a DOS and a DDOS attack is that a DOS attack targets a single host at a time, but a DDoS attack targets numerous hosts simultaneously. These types of attacks will degrade network performance.

The term "reliability" refers to the fact that health-care practitioners receive monitoring data in a timely and accurate manner. WBAN sensors must be capable of viewing and detecting essential active signs of human health; therefore, reliability is critical. WBAN sensors must be capable of viewing and detecting essential active signs of human health; therefore, reliability is critical.

3.7. BAN ARCHITECTURE

WBAN is designed with special purpose sensor which can autonomously connect with various sensors and appliances, located inside and outside of a human body.

Below Figure demonstrates a simple WBAN architecture where the architecture is divided into several sections. Here we have classified the network architecture into four sections. The first section is the WBAN part which consists of several numbers of sensor nodes. These nodes are cheap and low-power nodes with inertial and physiological sensors, strategically placed on the human body. All the sensors can be used for continuous monitoring of movement, vital parameters like heart rate, ECG, Blood pressure etc. and the surrounding environment. There are vast monitoring systems are being used already based on wired connections. Any wired connection in a monitoring system can be problematic and awkward worn by a person and could restrict his mobility. So, WBAN can be a very effective solution in this area especially in a healthcare system where a patient needs to be monitored continuously and requires mobility.

The next section is the coordination node where the entire sensor nodes will directly connected with a coordination node known as Central Control Unit (CCU). CCU takes the responsibility to collect information from the sensor nodes and to deliver to the next section.

For monitoring human body activities there is no such wireless technology is fixed for targeting WBAN. Most popular wireless technologies used for medical monitoring system are WLAN, WiFi, GSM, 3G, 4G,WPAN (Bluetooth, ZigBee) etc. . Except Cellular network standard all of these technologies are commonly available for short distance communication.

WMTS (Wireless Medical Telemetry Service) and Ultra-Wide Band are another technology that could be used for body monitoring system as they operate in low transmission power.

The third section is the WBAN communication which will act as a gateway to transfer the information to the destination. A mobile node can be a gateway to a remote station to send Mobile Message to a cellular network using GSM/3G/4G. A router or a PC can be a remote node to communicate via email or other service using Ethernet which is shown in Figure 3.5.

The last section will be a control center consists of end node devices such as Mobile phone for message, PC for monitoring and email and server for storing the information in the database.

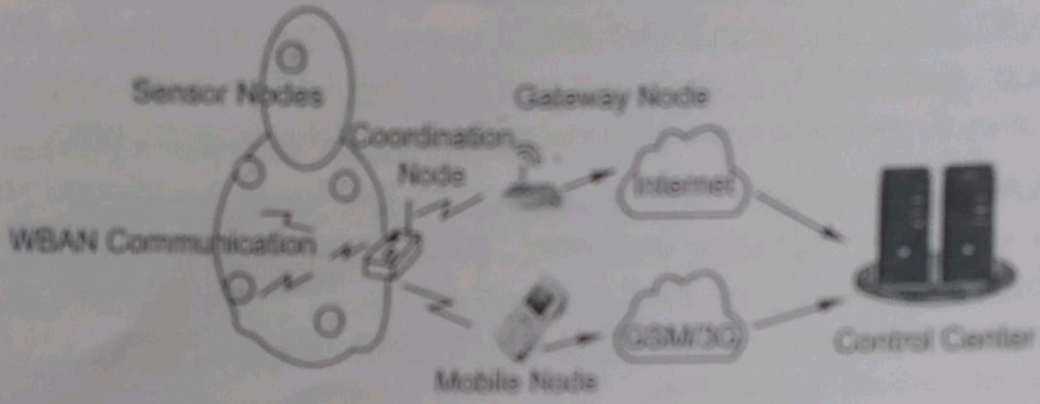


Fig. 3.5.

WBAN Requirements and Workflow

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads—the template will do that for you.

Requirements for Wireless Medical Sensors in WBAN

Wireless medical sensors should satisfy the following main requirements such as

Wearibility: To achieve non-invasive and unobtrusive continuous monitoring Wearibility is a very important issue. These sensors must be lightweight and small. Size and weight of sensors are mainly determined by the size and weight of batteries . But, a battery's capacity is directly proportional to its size.

Reliability: Reliable communication in WBANs is of paramount importance for any WBAN application. So the designer should target a reliable communication technique which will ensure uninterrupted communication and optimal throughput .A careful trade-off between communication and computation is very crucial for a reliable system design.

Security: Another important issue is the security of the network. All the wireless medical sensors must meet the requirements of privacy and should ensure data integrity authentication.

Interoperability: Wireless medical sensors should allow users to easily build a robust WBAN. Standards governing that interaction of wireless medical sensors will help vendors competition and eventually lead to more accessible systems .

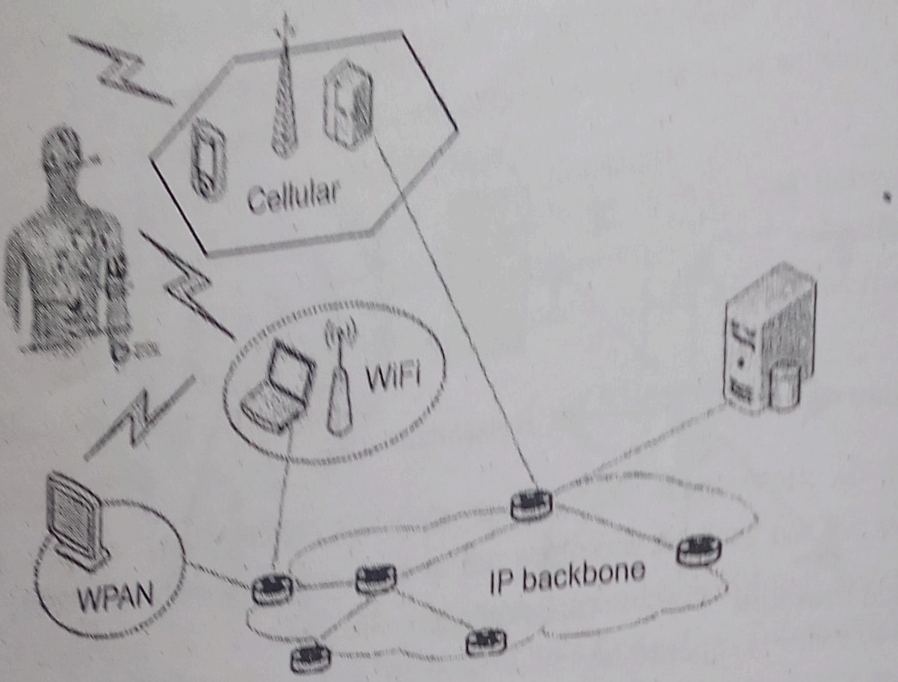


Fig. 3.6. A Typical WBAN communication. wearability, reliability, security, and interoperability

Monitoring Sensors

Wireless body area network is a system which can continuously monitor a person's activities. Based on the operating environments the monitoring sensors can be classified into two types.

Wearable sensor devices worked on the human body surface. v Implantable devices operated inside human body

Wearable sensor devices allow the individual to follow closely the changes in her or his functions and in the surrounding environment and provide feedback for maintaining optimal and instant status. For example ECG, EEG, Blood pressure sensor can be used to monitor a critical patient, GPS sensor can be used to locate an area and different types of sensor that can be used to measure the distance, temperature, movement etc.

To measure heath parameters, implantable sensors are planted in close contact with the skin, and sometimes even inside the human body. Implantable biosensors are an important class of biosensors based on their ability to continuously measure metabolite levels, without the need for person interference and regardless of the person's physiological state(sleep, rest, etc.).the implantable biosensors have great impact to diabetes and trauma care patients, as well as soldiers in action (military). Figure 3.7 focuses on the sensor nodes with wireless capabilities.

Traffic Types

In a WBAN traffic can be divided into three categories such as: v Normal traffic v Emergency traffic v On-demand traffic

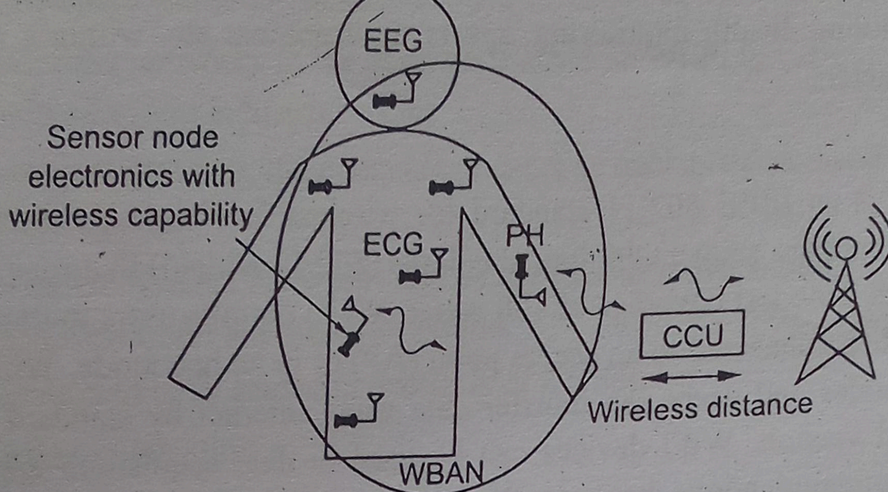


Fig. 3.7. Sensor nodes in WBAN.

Normal traffic is the data traffic which is used to monitor the normal condition of a person without any criticality and on demand events. Emergency traffic is initiated by nodes when they exceed a predefined threshold or in any emergency situation. Such type of traffic is totally unpredictable.

On-demand traffic is initiated by the authorized personnel like doctor or consultant to acquire certain information for diagnostic purpose .

Work Flow

Figure 3.8 shows the work flowchart of WBAN. In the flowchart workflow is divided in to two sections. First section is the WBAN where all the sensors devices will collect data and process them to the control center. While processing if any error occurs then it will read data again from the sensor and will forward for processing.

The control center will send the data to the desired location. If any problem occurs then it will generate an error where resend option should be needed again.

WBAN Standards and Technologies

As WBAN is a short range wireless networks so different types of wireless short range technologies can be involved in different stages. In this segment we will describe most common technologies such as Bluetooth, ZigBee, WiFi, IEEE 802.15.6 etc. that can be used to deploy WBAN.

Bluetooth

Bluetooth is an IEEE 802.15.1 standard commonly known as WPAN (Wireless Personal Area Network). Bluetooth technology was designed as a short range wireless communication standard, anticipated to form a network with security and low power consumption. A typical

Bluetooth network forms a Piconet where a Bluetooth device works as a master and another seven Bluetooth devices

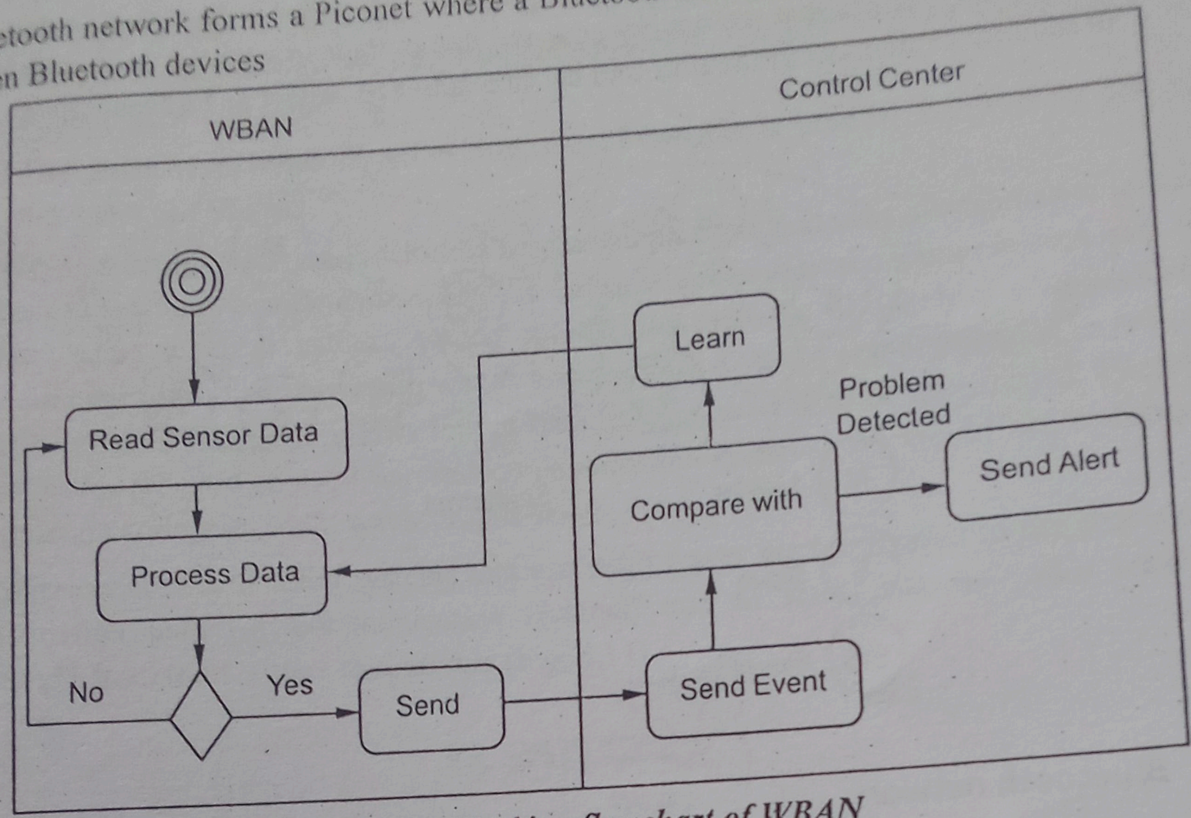


Fig. 3.8. Working flowchart of WBAN

work as slaves which gives each device to communicate with each other simultaneously. An other type of Bluetooth network can be formed with more than one Piconet known as Scatternet. In Scatternet a node of a Piconet (can be a master or a slave) joins as a slave in another Piconet. Figure 3.9 shows how a Piconet and Scatternet are formed using Bluetooth nodes. Though, the basic Bluetooth protocol does not support relaying but it is possible to join together numerous Piconet into a large Scatternet, and to expand the physical size of the network beyond Bluetooth's limited range using this method.

Bluetooth devices operate in the 2.4GHz ISM band(Industrial, Scientific and Medical band), utilizing frequency hopping among 79 1 MHz channels at a nominal rate of 1600 hops/sec to avoid interference. It is classified with three classes of devices with coverage ranging from 1 to 100 m and different transmission powers ranging from 1 mW to 100 mW with 3 Mbps data rate. A very key feature of Bluetooth is that all the Bluetooth devices can communication with each other in NLOS condition. Bluetooth is suitable for short distance data transmission applications such as between servers of WBANs or between a WBAN and a personal computer.

ZigBee

ZigBee is an IEEE 802.15.4 standardized solutions for wireless telecommunications designed for sensors and controls, and suitable for use in harsh or isolated conditions. One of the biggest advantages of ZigBee network is its low power consumption. Figure 3.10 shows a typical ZigBee network topology which consist of three kinds of devices or nodes such as coordinator, router and end device. One coordinator exists in every ZigBee network. It starts the network and handles management functions as well as data routing functions. End devices are devices that are battery-powered due to their low-power consumption. They are in standby mode most of the time and become active to collect and transmit data.

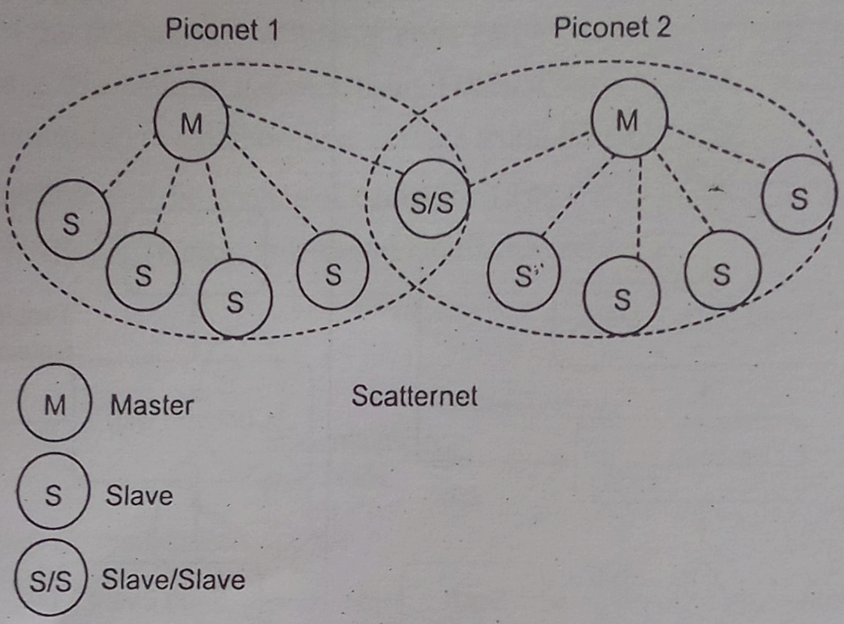


Fig. 3.9.

Bluetooth network

Devices such as sensors are configured as end devices. They are connected to the network through the routers. Routers help to carry data across multi-hop ZigBee networks. In some cases ZigBee network topology are formed without routers when the network is point to point and point to multipoint.

ZigBee is aimed at RF applications that require low data rate, long battery lifespan and secure networking. Through the standby mode, ZigBee enabled devices can be operational for several years. ZigBee-based wireless devices operate in three different frequency bands such as 868 MHz, 915 MHz, and 2.4 GHz.

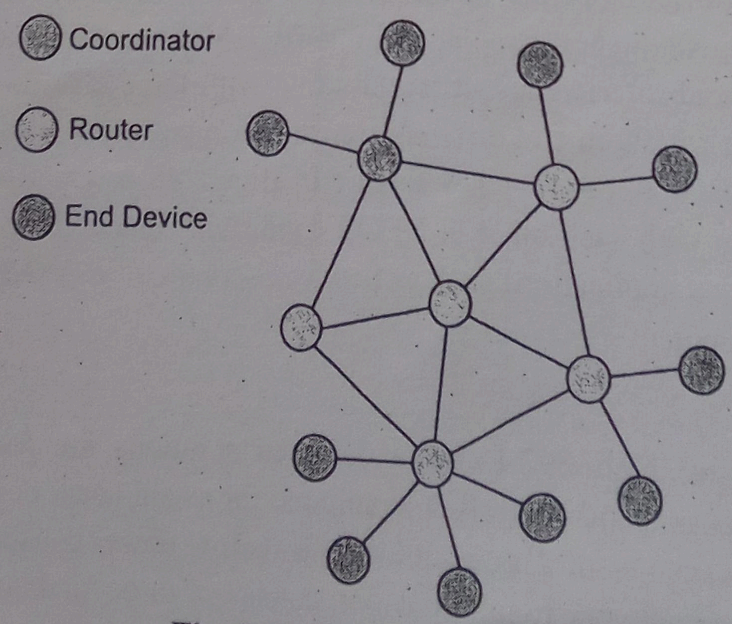


Fig. 3.10. ZigBee network.

Therefore, one substantial drawback of using ZigBee network for WBAN applications is due to interference with wireless local area network WLAN) transmission, especially at 2.4GHz. As ZigBee devices operate at low data rate so it can be unsuitable for large-scale and realtime WBAN applications. But, it can be very much suitable for personal use like assisted living, health monitoring, sports, environment etc. within a modest range between 50 - 70 meters.

WiFi

WiFi is an IEEE 802.11 standard for wireless local area network (WLAN). Generally WiFi technology comes with four standards (802.11 a/b/g/n) that runs in ISM band 2.4 and 5 GHz with a modest coverage of 100 meter. Wi-Fi permits users to transfer data at broadband speed when connected to an access point (AP) or in ad hoc mode. WiFi network where WiFi sensor nodes and users can transfer data using internet by standard WiFi router. In some modified version, WiFi devices can be used in data acquisition applications that allow a direct communications between the sensors and the smart phones/ PC even without an intermediate router.

WiFi is preferably suitable for large amount of data transfers with high-speed wireless connectivity that allows videoconferencing, voice calls and video streaming. An important advantage is that all smartphones, tablets and laptops have Wi-Fi integrated; however the main disadvantage of this technology is high energy consumption.

IEEE802.15.6WBAN

IEEE802.15.6 is the latest addition in WPAN which is known as WBAN standard that provides various medical and non medical applications and supports communications inside and around the human body. This standard supports communication inside and outside of human body which can be used for different medical and non medical applications such as e-Healthcare monitoring, sports, environment etc.

IEEE 802.15.6 standard is classified by three physical layer standards. Each standard uses different frequency bands for data transmission with data rate 10 Mbps maximum. First one is Narrowband (NB) which operates within the range of 400, 800, 900 MHz and 2.3, 2.4 GHz bands. The Human Body Communication (HBC) is another standard which operates at range of50 MHz. The Ultra Wideband (UWB) technology operates between 3.1 GHz to 10.6 GHz which supports high bandwidth in short range communication.

Wireless Communication Techniques

Wireless networking technology is an alternative to traditional cable and fibre optic networks. It is fast becoming a vital productivity tool for today's mobile workforce.

A wireless network uses radio waves instead of cables to connect devices such as laptops to the internet, or to your business network. It removes the need for expensive and messy wires, and allows you or your staff to access your company's documents, emails and other ... from any location within your network's coverage area or any Wi-Fi hotspot. By removing the need for wiring, wireless networks can be a quick and cost-effective small business networking solution.

- In today's world, wireless communication has a major application in sharing of information anywhere and at anytime.
- We can use wireless networks in the form of WLAN or Wi-Fi in various fields such as education, healthcare, and industrial sector.
- As the technology is growing, the demands of users as well as the demand of ubiquitous networking is increasing.
- WBAN(Wireless Body Area Network) allows the user to move another without having the restriction of a cable for sharing information.
- The communication in body sensor networks is of 2 types:
  - In-body communication
  - On-body communication
- In-body communication is the communication between sensor nodes that are implanted inside human body. The MICS (Medical Implant Communication System) communication can be used only for in-body communication.
- On-body communication occurs between wearable devices which consist of sensor nodes. The ISM(Industrial Scientific and Medical)band and UWB (Ultra-wideband) communication can be used only for on-body communication.
- A body area network(BAN),also referred to as a wireless body area network(WBAN) or a body sensor network (BSN) or a medical body area network (MBAN), is a wireless network of wearable computing devices.
- BAN devices may be embedded inside the body, implants, maybe surface-mounted on the body in a fixed position Wearable technology or may be accompanied devices which humans can carry in different positions, in clothes pockets, by hand or in various bags.
- A WBAN system can use WPAN wireless technologies as gateways to reach longer ranges. Through gateway devices, it is possible to connect the wearable devices on the human body to the internet.
- This way, medical professionals can access patient data online using the internet independent of the patient location.
- In modern technology wireless communication provides a lot of possibilities to be able to share its information to each other at anytime and anywhere.
- Intelligent mobile communication network and WLAN, Wi-Fi are applied to various sectors such as education; healthcare service and industry in order to provide people a convenient way to communicate with each other.

- As the demand of ubiquitous network is increased, the devices for home, office and other information devices that can communicate wireless in short range have been getting more attention.
- The standard and technique development of ubiquitous network has rapidly put itself into the world market.

Wireless communication is wireless telecommunication that uses electromagnetic waves (radio waves), magnetic fields, and electric fields, whereas optical communication uses light without using wires or cables. Among the various methods of wireless communication, telecommunication that uses radio waves enables long-distance communication in the order of kilometers or more and allows lots of data (information)*1 to be transmitted. Therefore, radio waves are used in most wireless communication systems. We would like to focus our explanation mainly on radio waves in this series.

Wireless communication systems that use radio waves are configured to use space as the transmission path (or communication channel) and to send data on radio waves as signals*1 from transmitters to receivers (Fig. 3.11).

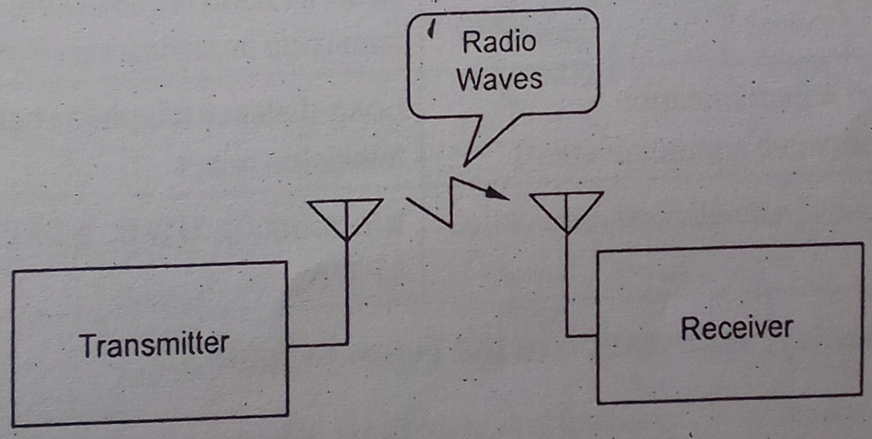


Fig. 3.11. Configuration of a Simple Model for a Wireless Communication System

- **Data:** A collection of symbols and codes that represent facts.
- **Information:** Data including audio, text, and images that can be interpreted by humans and used in ways such as to determine things and take actions.
- **Signals:** Data or information transmitted over time across transmission paths (communication channels) such as space or cables.

Examples of Wireless Communication Applications

Table 1 summarizes the approximate categories of wireless communication that transmit data using radio waves and the typical applications of each category. Wireless communication is used in various fields. The applications and types of wireless communication are also wide-ranging.

We should note here that wireless communication is also being developed beyond the boundaries of these categories in recent years. For example, various countries have begun satellite mobile communication services that incorporate satellite communication into mobile communication (smartphones equipped with a function to connect to satellites).

Table 3.2. Categories of Wireless Communication and their Applications

Categories of Wireless Communication	Typical Applications
Mobile communication	Mobile phones
Aviation communication	Radio altimeters, radars for air traffic control
Satellite communication	Satellite broadcasting, GPS weather observation
Ship communication	LF beacons, MF/HF/VHF wireless communication
Broadcast communication	AM/FM radio broadcasting (audio) television broadcasting (Video)
Fixed communication (microwave communication)	Long-distance telephone call relays, television relays
Wireless network communication	Bluetooth ⊙, UWB, Wi-Fi, Wi-MAX, LPWA, etc.

Supplementary Information to the Terms in Table 3.2

Table 3.3.

Term	Description
Global Positioning System (GPS)	A satellite positioning system for the entire earth
Low Frequency (LF)	Also called long wave. The frequency range is 30 kHz to 300 kHz
Medium Frequency (MF)	Also called medium wave . The frequency range is 300 kHz to 3,000 kHz (3 MHz)
High Frequency (HF)	Also called short wave The frequency range is 3 MHz to 30 MHz
Very High Frequency(VHF)	Also called ultra-short wave The frequency range is 30 MHz tp 3,000 MHz (3 GHz)
Microwaves	Also described as Super Very High Frequency (SHF) The frequency range is 3 GHz to 30 GHz
Amplitude Modulation (AM)	A type of communication technology that transmits analog audio over long distances.

Frequency Modulation (FM)	A type of audio communication technology similar to AM. FM broadcasts have a reach of about 100 km. However, Am broadcasts can go beyond that and even reach overseas. Nevertheless, AM broadcasts are more susceptible to the impact of noise.

Basic Configuration and Elements of Wireless Communication Systems

The basic model configuration of wireless communication systems (and wired communication systems) is as in Fig. 3.12.

We call the data transmitted through a transmission path a "signal." We refer to the unnecessary components that negatively affect these signals and make it difficult to transmit the data we want to send to the recipient "noise." In practice, noise may occur in both transmitters and receivers and then cause interference with the operation of devices and other problems. In other words, we can call a communication system completely unaffected by this noise the ideal communication system.

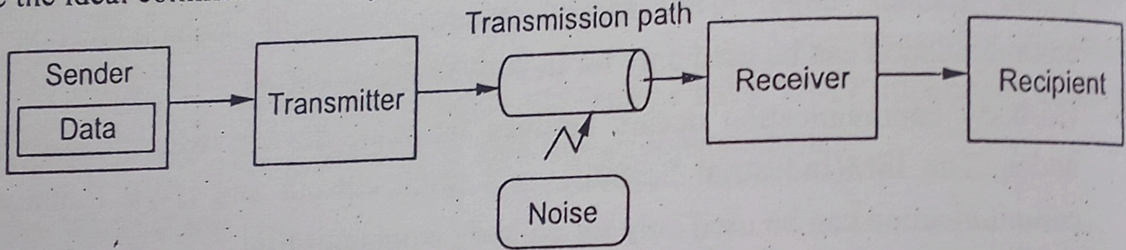


Fig. 3.12. Configuration of the Basic Model for Communication Systems

Table 3.4. Constituent Elements of the Basic Model for Communication Systems

Constituent Elements	Description
Sender	The person sending data
Data	Audio, text, still images, videos etc
Transmitter	The device that converts the information you want to pass along the transmission path into signals.
Transmission path (communication channel)	The medium in which signals are transmitted from the transmitter to the receiver (the transmission path is a wire or cable in wired communication)
Receiver	The device that converts the signals passed along the transmission path into data.
Recipient	The person who received data

Wireless Body Area Network (WBAN) is becoming a special application of such technique. WBAN differs with other wireless sensor networks(WSN) with some significant points. First difference between a WBAN and WSN is mobility. In WBAN user can move with sensor nodes with same mobility pattern whereas WSN is generally used to be stationary. Energy consumption is much less in WBAN than other WSNs arrangement. In addition, WBAN sensor devices are found cheaper than WSNs. For reliability, node complexity and density, WBAN nodes are however traditional. WSNs do not tackle specific requirements associated with the interaction between the network and the human body. The WBAN performs like Virtual Doctor Server, by keeping the different responsibilities like-maintain the history of the patient, giving advices to the patient in general/emergency (first aid help from second person) case etc. To understand the communication approach of this emerging WBAN technology, we first need to know the conceptual structure of WBAN so that, one can easily know the flow of communication within the system and to the outside world, this has been achieved by the demonstration of a simple WBAN communication architecture. Where this architecture is mainly comprised with three different layers namely: Tier 1, Tier 2 and Tier 3 and these are further described better in the given figure 3.14.

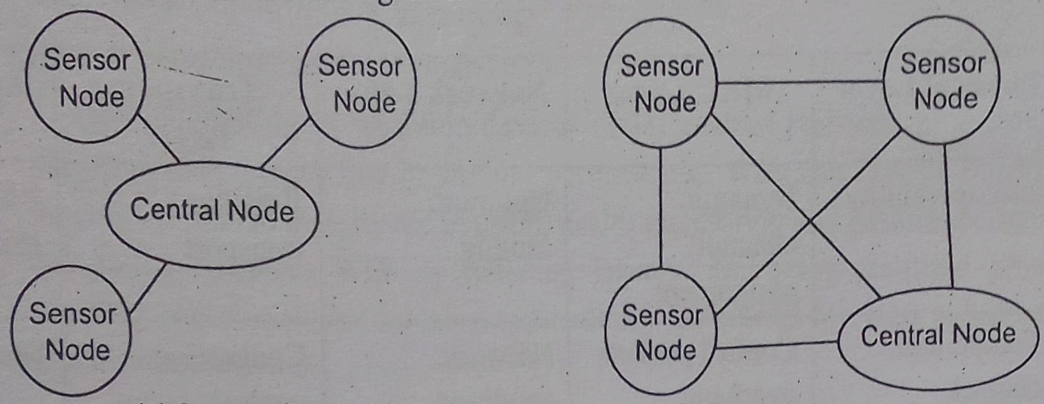
WBAN Architectures and Communication Protocols

There are different WBAN architectures proposed by many different research groups for specific applications. The architecture and communication protocols are application specific for optimizing the performance. Three-tier WBAN architecture is the most common architecture while body-to-body (B2B), machine-to-machine (M2M), and ad-hoc type architectures are there. Figure 1.shows an example of the three-tier WBAN architecture used in healthcare systems.

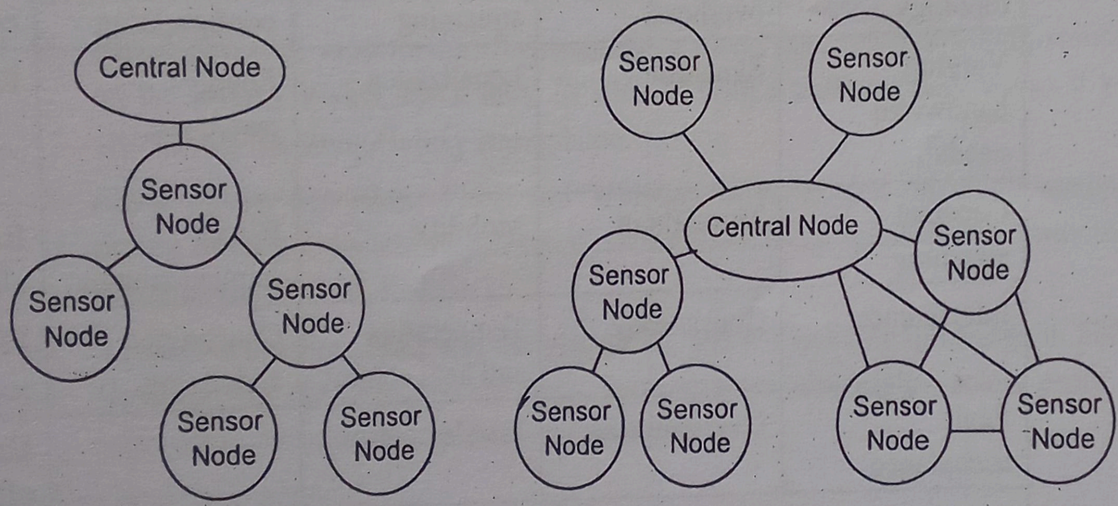
Tier 1 has the sensors including electroencephalography (EEG) sensors, electrocardiography (ECG) sensors, electromyography (EMG) sensors, and peripheral oxygen saturation (SPO_2) sensors attached on the body, implanted in the body, or swallowed. This tier is called the intra-WBAN tier where all the communications happen within the WBAN. Tier 2 has external communication gateways such as a mobile phone or a wi-fi router connected to the internet. There may be one WBAN communicating with another WBAN and this is called the inter-WBAN tier, but still categorized under tier 2. The communication between the gateways and end users is categorized as tier 3, commonly known as the beyond-WBAN tier. Cloud computing sits between tiers 2 and 3.

WBAN Topologies

WBANs have four common network topologies as shown in Fig.3.13, where the star topology has equal access levels for all peripheral sensor nodes to the access point or the central node. This is preferred when the sensor nodes do not need to communicate with each other. In case one sensor node needs to talk to another node, it must go through the central node. In contrast, the mesh topology provides all sensor nodes the same level of access rights as in star topology and each sensor node can talk to the other sensor nodes individually. However, this comes with the cost of high signal collision probability and therefore may cause delays in successful data transmission. Therefore, the fully meshed network topology is not used unless it is essential for a particular application. The tree network topology has different priority levels for different sensors and the number of hops needed to access the central node is also dependent on how they are configured. Sensor-to-sensor communication in a tree network always needs more than one hop unless it is between parent and child nodes. The hybrid topology has all the above-mentioned configurations within it dependent on the configuration and this is the most common WBAN configuration used in the field when the sensor node number grows.



(a) Star topology (b) Mesh topology



(c) Tree topology (d) Hybrid topology

Fig. 3.13.

WBAN Communication Protocols

IEEE has derived several network standards related to WBANs. The first one was IEEE 802.15.1 developed in 2002 for Wireless Personal Area Network (WPAN) which was based on Bluetooth. It defined the physical layer (PHY) and the media. IEEE 802.15.4 low rate WPAN was also introduced in 2003 for longer battery access control (MAC) layer specifications for fixed and mobile WPAN [20]. Later IEEE 802.15.2 was developed as a coexisting network and IEEE 802.15.3 was developed as the high rate WPAN in 2003 life networks and had a couple of amendments thereafter to accommodate different country-specific regulatory changes. IEEE 802.15.5 is the standard provided for interoperable, scalable, and stable WPANs. The IEEE 802.15.6 standard was specifically developed for-

WBAN. The body area network node locations have three major zones namely, implant, on the surface, and external where the external devices can operate from a maximum of 5 m away from the body. Dependent on the scenario of transmission, the channel models (CMs) and frequency bands have been allocated.

Table 3.5. Designing and implementation challenges in different layers of WBAN protocols

Physical Layer	MAC Layer	Network Layer	Transport Layer	Application Layer
Interoperability	Dynamic channel assignment	Optimum routing	Reliable transport	Efficient interface
Temperature control	Control packets overhead	Network condition	Congestion control	Security
Changing topology	Protocol overhead	Real-time streaming	Self-configuration	Congestion control
Varying bandwidth needs	Synchronization	Localization	Energy awareness	Flow control
Constant signaling	Throughput	Mobility	Biased implementation	Bandwidth allocation
Interference	Consistency	Temperature and heat control	Constrained addressing	Packet-loss recovery
Fault acceptance	Over-emitting	Traffic control	-	Energy efficiency
Security	Packet scheduling	Multi-path routing	-	-
Quality of Service (QoS)	Error control	Security	-	-
Varying data rates	Overheating	QoS	-	-
-	Calibration	Fault tolerance	-	-
-	Fault acceptance	-	-	-
-	Energy conservation	-	-	-
-	QoS	-	-	-

-	Multi-radio and multi-channel design	-	-	-
-	Data flow control	-	-	-
-	Idle listening	-	-	-
-	Security	-	-	-
-	Delay control	-	-	-

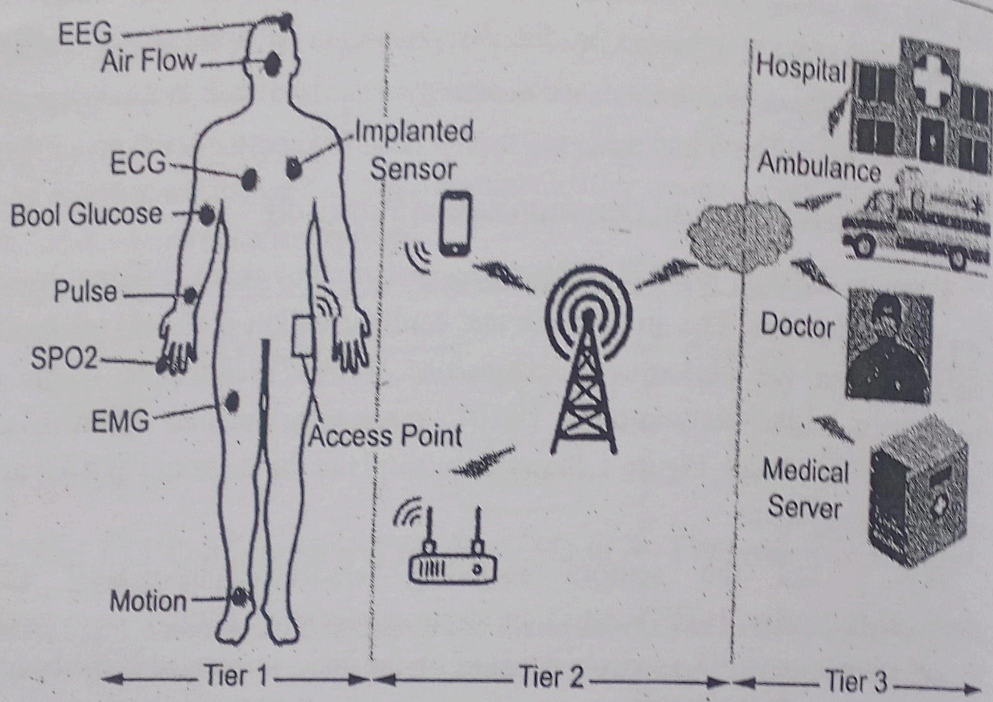


Fig. 3.14.

TWO MARK QUESTIONS WITH ANSWERS

1. ***Brief note on need for Wireless monitoring.***

   Wireless monitoring through wearable devices could be useful for hospitalized patients, particularly those who are unstable or at higher risk for serious complications such as critically ill patients.

2. ***Write the applications of Wireless technology in wearable devices.***

   Some of the wireless technologies used in wearable devices include [1]:

   - **Near Field Communication (NFC):** This technology is used in wearables that require low power consumption. It involves the transfer of tiny amounts of data over a very short range.
   - **Bluetooth Low Energy (BLE):** This technology is known for being easy to implement and low cost. It requires very little power from your wearable.

- **ANT:** This technology is typically used for monitoring of heart rate, cycling power, distance and speed.
- **Bluetooth Classic:** This technology is used for wireless communication and is the standard for audio streaming.
- **Wi-Fi:** This technology is best for streaming huge amounts of data, like video, but it has high power consumption.
- **Cellular:** This technology is used in devices that need to talk directly to the cellular network.

3. ***Mention the advantages of Wireless technology.***

The advantages of wireless technology in wearable devices include:

1. **Convenience:** Wireless connectivity allows for easy data transfer and communication without the hassle of cables.
2. **Comfort:** Wireless wearables are more comfortable to wear, as they don't have cumbersome cords or wires.
3. **Portability:** Wireless wearables are lightweight and easy to carry, making them perfect for fitness and outdoor activities.
4. **Real-time data tracking:** Wireless technology enables real-time data tracking and monitoring, providing instant feedback and insights.
5. **Seamless connectivity:** Wireless wearables can connect to smartphones, tablets, or computers, enabling easy data sync and sharing.

4. ***Mention the challenges of Wireless communication in WD.***

The challenges of wireless technology in wearable devices include:

1. **Power consumption:** Wireless connectivity consumes power, reducing battery life and requiring frequent recharging.
2. **Interference:** Wireless signals can be disrupted by other devices, causing interference and data loss.
3. **Security:** Wireless connectivity poses security risks, making wearables vulnerable to hacking and data breaches.
4. **Connectivity issues:** Wireless connections can be unreliable, leading to dropped signals and lost data.

5. ***Define Wireless sensor network***

Wireless sensor networks (WSNs) are networks of sensors that monitor and record physical conditions in the environment and send the collected data to a central location. WSNs can be used for a variety of purposes, such as monitoring the environment, tracking security threats and monitoring patients in hospitals. These networks are built of "nodes" that are connected to other sensors and can vary in size from a shoebox to a grain of dust.

6. ***Define Cellular network.***

A cellular network is a wireless network distributed over land areas called cells, each of which has a fixed location base station [1]. These networks are used to provide services such as wireless communication, personal communication systems, wireless networking, etc. They are designed to provide radio coverage over a wide geographic area, which can be divided into smaller areas or cells

7. ***Write a short note on Edge computing.***

Edge computing in wearable devices (WD) enables real-time processing of sensor data, reducing latency and improving performance. WDs can execute machine learning models for human activity recognition, health monitoring and gesture recognition . Edge computing enhances WDs by reducing latency, improving real-time processing and enabling robust machine learning applications. It's crucial for WDs to provide efficient and accurate services.

8. ***Mention the future trends in wireless communication.***

Here are some future trends in wireless communication in wearable devices

- **Blood pressure monitoring:** Samsung has a blood pressure monitoring solution on the Galaxy Watch, but it must be verified with a cuff and only works if you also have a Samsung Galaxy smartphone.
- **Sleep apnea detection:** Fitbit and Withings offer oxygen variation readings during sleep, but devices stop short of talking about sleep apnea due to limitations of not being medical devices.
- **AI and wearables:** 2023 was the year of AI, and it's unlikely to change in 2024. However, we may see a move from impressive yet ultimately useless proof of concepts to meaningful implementations.

9. ***Define Body area network.***

A Body Area Network (BAN) is a wireless network of wearable devices or sensors that are worn on or implanted in the body to monitor various physiological parameters, such as heart rate, blood pressure, body temperature, and other health metrics. BANs are also known as Wireless Body Area Networks (WBANs) or Body Sensor Networks (BSNs).

10. ***Mention the components of Body area network.***

BANs typically consist of:

1. **Sensors:** Wearable devices or implantable sensors that collect physiological data.
2. **Hub or Coordinator:** A device that collects data from sensors and transmits it to a remote server or smartphone.
3. **Communication Technology:** Wireless communication protocols like Bluetooth, Wi-Fi, or Zigbee enable data transmission between devices.

11. *Mention the applications of Body area network.*

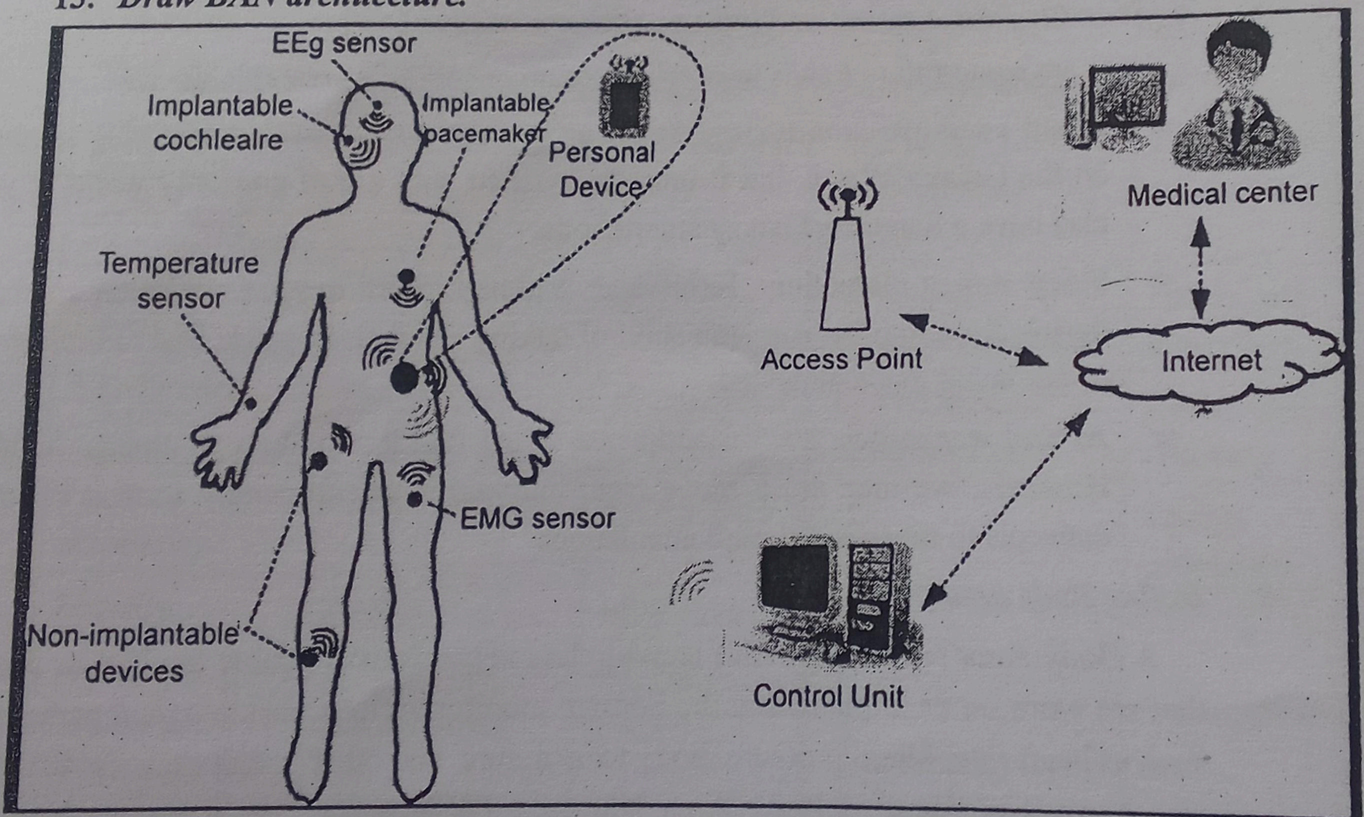
BANs have various applications, including:

1. **Healthcare:** Monitoring chronic conditions, tracking vital signs, and remote patient monitoring.
2. **Fitness and Sports:** Tracking physical activity, performance, and biometric data.
3. **Military and Emergency Response:** Monitoring vital signs in extreme environments.
4. **Gaming and Entertainment:** Enhancing gaming experiences with biometric feedback.

12. *Write the characteristics of BANs.*

- Body area networks (BANs) are networks of wireless sensors and medical devices embedded in clothing, worn on or implanted in the body, and have the potential to rev-olutionize healthcare by enabling pervasive healthcare.

13. *Draw BAN architecture.*



14. *Mention the Requirements for Wireless Medical Sensors in WBAN.*

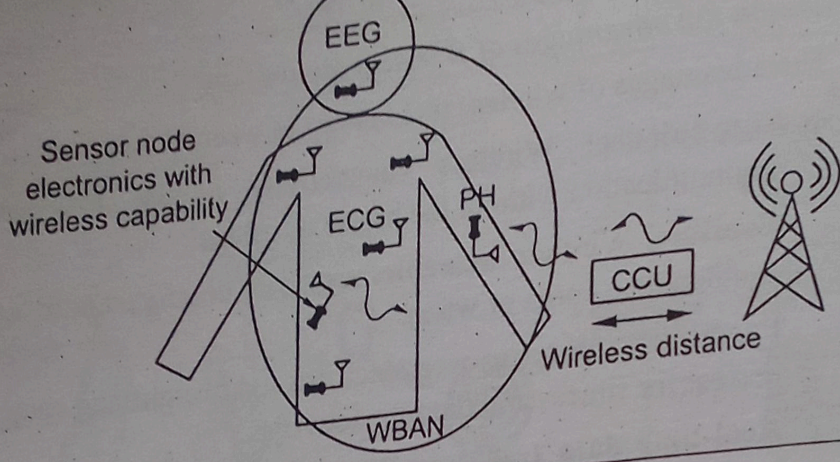
Wearibility: To achieve non-invasive and unobtrusive continuous monitoring Wearibility is a very important issue. These sensors must be lightweight and small. Size and weight of sensors are mainly determined by the size and weight of batteries. But, a battery's capacity is directly proportional to its size.

Reliability: Reliable communication in WBANs is of paramount importance for any WBAN application. So the designer should target a reliable communication technique which will ensure uninterrupted communication and optimal throughput .A careful trade-off between communication and computation is very crucial for a reliable system design.

Security: Another important issue is the security of the network. All the wireless medical sensors must meet the requirements of privacy and should ensure data integrity and authentication.

Interoperability: Wireless medical sensors should allow users to easily build a robust WBAN. Standards governing that interaction of wireless medical sensors will help vendor competition and eventually lead to more accessible systems.

15. ***Sketch the sensor nodes in BAN.***



REVIEW QUESTIONS

1. (*i*) Explain the need of Wireless communication in wearable devices in detail.
   (*ii*) Explain the advantage and applications of wireless communication in WD.
2. Explain BAN in detail with neat diagrams.
3. Explain the Bluetooth and Zigbee wireless technology in detail.
4. Explain the signal throughput in detail.
5. Explain in detail about the Body Area Networks in Healthcare.
6. Describe about the advanced technologies and tools used for technical challenges in wearable device.
7. Describe about the different wireless technologies used in BAN.
8. Explain the four different layers of Body area network in detail.
9. Explain the different types of wireless communication used in Wearable devices in detail.
10. Describe about the different wireless communication techniques.
11. Explain Resource allocations and Power optimization in detail.
12. Explain about the characteristics of Body area network in detail.
13. Explain Body Area Network Architecture in detail with neat diagrams.
14. Explain in detail about Recent Applications of Wireless Technology in Wearable Health Monitoring Systems.