ROHINI COLLEGE OF ENGINEERING AND TECHNOLOGY
AUTONOMOUS INSTITUTION
Approved by AICTE & Affiliated to Anna University
NBA Accredited for BE (ECE, EEE, MECH) | Accredited by NAAC with A+ Grade
Anjugramam - Kanyakumari Main Road, Palkulam,Variyoor P.O. - 629 401, Kanyakumari District.

Department of Biomedical Engineering

VI Semester

CBM 370 - Wearable Devices

Unit- 3 WIRELESS HEALTH SYSTEMS

3.6 Wireless communication Techniques

- ❖ Wireless communication technologies and wearable health-monitoring systems are unavoidably linked, as wireless capabilities allow devices worn by ambulatory patients to share data (and often power) in real time with other wireless nodes.
- ❖ Such systems incur little-to-no cost in terms of patient/device interaction and are a dramatic improvement over traditional store-and-forward wearable monitoring devices, such as Holter monitors.
- ❖ In addition, the ad hoc networking functionality supported by emerging plug-and-play wireless standards points to the inevitable reality of patient environments that host pervasive networks of wireless health care devices whose primary role is to increase their quality of life.
- ❖ Clearly, the realization of these wireless tools does not come without cost. Wires that may have once provided high data throughput and access to power, data storage, and processing resources are no longer available. The engineering challenge is therefore to incorporate adequate power, data storage, and processing capabilities on the wireless devices to balance the throughput and operational lifetime needs of the monitoring application. Concurrently, one must consider security issues associated with broadcasting previously local information.
- ❖ This chapter provides an overview of wireless technologies relevant to wearable health monitoring systems, including categories of wireless devices, networking

topologies, and standards (both existing and emerging) that will help to ease the transition into health monitoring environments pervaded by wireless wearable, nearby, and desktop medical sensors.

- These thoughts are followed by a synopsis of safety and security issues that inevitably arise from using wearable, wireless health monitoring systems as well as the design considerations that come into play when working with wireless links. Next, the authors briefly address technologies available to a developer to implement wireless solutions. This is followed by a synopsis of a few recent efforts that utilize wireless technology for human/animal health monitoring.

3.6.1 System-Level Consideration:

- Wireless communication links have been a mainstay in commercial and military domains for many years.
- Wearable health monitoring technologies also have a notable history of several decades in the form of devices, such as electrocardiogram, Holter monitors and accelerometer-based pedometers.
- The merger of the two technology classes, however, is relatively recent. It was not until the mid-to-late 1990s that medical-sensor-laden body area networks (BANs), a. k. a. personal area networks (PANs) or wireless personal area networks (WPANs), became a focus of discussion because of their potential to support continuous monitoring of high-risk patients without imposing severe mobility limitations affiliated with desktop clinical, home care, and telemedicine systems.
- Since that time, advances have occurred in the areas of wireless networking technologies and wearable devices that in aggregate make mobile health, “unwired e-med”, or wireless personal health, a feasible health monitoring alternative as opposed to an esoteric possibility.
- At the system level, wireless wearable systems by nature imply ***wireless transmission ranges*** of 10 m or less, ad hoc network creation, plug-and-play interoperability, the ability to stream data from multiple sensors when needed, and the capacity to operate at very low power levels for long periods of time.

- These requirements were not well met by traditional wireless technologies, including those that supported consumer applications, such as garage door openers and television remote controls.
- ***The embedded biomedical systems*** community therefore started to look toward emerging standards, such as Bluetooth and, more recently, ZigBee to meet those needs.
- During the same time frame, ***radiofrequency identification*** (RFID) technologies were developed for numerous security and inventory tracking applications, yet their promise for biomedical monitoring applications was clear.
- Even more recently, ***cell phone technology*** has become a focal point of discussion, as cell phones have the potential to offer both the functionality and the economy of scale desired for wearable data loggers that serve as BAN hubs.
- This section presents a comparative analysis of enabling wireless technologies for BAN implementation and the networking topologies they support. It then concludes with notes about information security and patient safety that are unique to wearable health monitoring systems

3.6.2 Body Area Networks:

- 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 [see Fig. 3.6.1] 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.
- 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 HomeRF implementations) are mature, and treatments of such subsystems are addressed in numerous wireless texts.

3.5.2 Wireless Standards Comparison:

- ***WPANs*** are a class of networks that subsumes ***BANs***. Specifically, WPANs are short-range networks usually confined to the personal operating spaces of users.
- The first WPAN effort was initiated in 1998 with the emergence of ***Bluetooth technology.***
- In 1999, the ***IEEE 802.15*** standards working group was created, and this group has since been actively involved in developing ***wireless standards*** for the personal area network arena.
- The ***IEEE 802.15.1*** standard based on ***Bluetooth technology*** was the first standard to address WPANs.
- This was followed by efforts of the ***IEEE 802.15.3*** task group which led to the ***ZigBee standard***.
- Finally, the ***IEEE802.15.4 task group*** is developing a standard for ***low-data-rate sensor*** network applications. In the following subsections, we provide a brief discussion of these enabling wireless technologies, which are expected to provide most BAN implementations in the near future. Table 3.1 provides a comparison between features of candidate WPAN technologies.

Table 3.5.1 WPAN comparison

	Bluetooth (802.15.1)	WiMedia (802.15.3)	ZigBee (802.15.4)
Operational spectrum	2.4 GHz	3.1 10.6 GHz	2.4 GHz and 868/915 MHz
PHY layer details	Frequency hopping spread spectrum (FH SS), 1,600 hops/s	Multiband OFDM	DSSS with BPSK or MSK
Channel access	Master slave polling	CSMA/CA	CSMA/CA
Max data rate	1 Mbps	480 Mbps	868 MHz to 20 kbps 915 MHz to 40 kbps 2.4 GHz to 250 kbps
Coverage radius	<10 m	<10 m	<20 m
Typical current drain	1 60 mA	Up to 400 mA	Very low (20 50 μA)
Relative cost per node	Low	Medium	Very low

3.5.2.1 Bluetooth– IEEE 802.15:

- In 1998, a group of companies wanted to develop technology to enable wireless interconnectivity between personal devices (e.g., laptops, personal digital assistants, digital cameras, etc.), respectively, separated by ***10 m*** or less.
- ***Bluetooth technology*** was developed to meet this need. In 1999, ***the IEEE 802.15.1*** working group adopted the Bluetooth specifications as the basis of a ***1 Mbps WPAN standard*** (IEEE 2004). (The name Bluetooth comes from the Danish king Harald Blatand (Bluetooth), who united the Scandinavian people in the tenth century.)
- Bluetooth links operate in the ***2.4 GHz unlicensed band***. More specifically, the 2,402 2,480 GHz industrial, scientific, and medical (ISM) band is divided into 79 equally spaced 1 MHz channels, which each Bluetooth device employs using random hops.
- During transmission, these hops occur at a rate of ***1,600 hops/s***. The modulation scheme uses ***binary Gaussian-shaped frequency shift keying*** (GFSK) at a 1 Mbps rate. Typical transmitter output power is about ***1 mW*** with an option to scale up to 100 mW for larger transmission ranges.

- The ***low transmission power*** makes Bluetooth devices suitable for battery operation.
- Additionally, when operating within the 10 m communication range, Bluetooth devices can organize themselves into piconets.
- Each piconet has a master node which controls and communicates with at most seven slaves; this master slave mode of operation avoids contention within the system.
- Piconets can operate independently, and their configurations can change spatially and over time. Every new device that wishes to enter a piconet must register with the master node.
- If the master node is already full with seven slave nodes, the new device registers in "parked" mode. Devices may also exist in standby mode when they do not associate with a piconet.
- Communication among members of a piconet is defined in the IEEE 802.15.1 standard.

3.1.2.2 IEEE 802.15.3 and WiMedia:

- Since the Bluetooth standard is ***not intended for high-rate*** multimedia applications, the ***IEEE 802.15.3*** working group pursued a high rate (11-55 Mbps) WPAN standard in 2003 with a focus on medium access control (MAC) and physical layer (PHY) specifications.
- This standard specifies an ad hoc PAN topology similar to the master slave Bluetooth architecture: devices can assume either master or slave functionality and exit or enter the ad hoc network without complicated setup procedures.
- The MAC is based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) (Rappaport 2002).
- In CSMA, each device ***first listens to the channel*** for a predetermined amount of time to verify if it is idle. If the channel is idle, then the device transmits; if it is not, the device defers its transmission. The PHY layer of the 802.15.3 standard specifies operation in the unlicensed 2.4 GHz frequency band with four 15 MHz channels.
- Depending on the data rate supported (11, 33, 44, or 55 Mbps), one of the five modulation techniques is used. The base modulationis differentially

encoded ***QPSK (quadrature phase shift keying)*** with options to switch to uncoded QPSK, trellis coded QPSK, and 16/32/64-QAM (quadrature amplitude modulation). Transmit power complies with the FCC specification of 0 dBm, and range is limited to 10 m.

- ❖ The 802.15.3a group was formed to create a high-speed enhancement of the 802.15.3 PHY layer. The focus of this group was to develop a standard that would support bit rates up to 480 Mbps using principles of ultrawideband (UWB) communication.
- ❖ However, the task group was unable to unify the two candidate proposals for the standard (multiband orthogonal frequency division multiplexing (MB-OFDM)-based UWB and direct sequence UWB) and was therefore dissolved in 2006.
- ❖ The ***WiMedia alliance***, a consortium of more than 350 organizations, has adopted MB-OFDM-based UWB as the enabling technology for high-rate PANs (WiMedia 2010).
- ❖ Wireless USB is based on the WiMedia Alliance's MB-OFDM-based UWB PHY layer and is capable of sending up to 480 and 110 Mbps at distances up to 3 and 10 m, respectively. It operates in the 3.1 10.6 GHz frequency range.
- ❖ Recently, the Wimedia Alliance released an enhanced UWB PHY specification that supports up to 1,024 Mbps.

3.1.2.3 IEEE 802.15.4/ZigBee:

- ❖ The ***IEEE 802.15.4*** specification defines a standard for low-rate, low-power WPANs that are well suited for body area and home networking applications (e.g., home automation, security, etc.).
- ❖ In 2000, ***the ZigBee Alliance*** and the IEEE 802 working group came together to build the specifications for low-rate PANs.
- ❖ The IEEE working group addressed the PHY and MAC layers, while the ZigBee Alliance defined the higher layer protocol specifications.
- ❖ ***IEEE 802.15.4*** supports both ***star and peer-to-peer network topologies***. The MAC layer is once again based on CSMA/CA.

- The PHY layer is based on direct sequence spread spectrum techniques operating in the unlicensed 2.4 GHz ISM band worldwide.
- There is also a provision for use of the 868/915 MHz bands in Europe and in the United States, respectively. The 2.4 GHz band supports data rates up to 250 kbps, while the 868/915 MHz band supports rates of 20 and 40 kbps.
- BPSK modulation is specified, and spectrum spreading is accomplished using a 15-chip m-sequence. A choice of aggregating four bits and using minimum shift keying (MSK) modulation is also provided.
- A typical coverage radius for each of these devices is envisioned to be around 10 20 m.

3.1.3 Device and Information Surety:

- “Surety” is a broad term that aggregates the concepts of security, safety, reliability, verifiability, redundancy, usability, and other system properties that speak to the ability of the system to always work as anticipated and in the best interest of the user.
- In the case of wireless, wearable health monitoring systems, surety is essential. For example, the transition from wired to wireless connections makes it more difficult to control who can access patient data.
- These wireless data should therefore be ***encrypted*** a straightforward design problem given encryption facilities provided in cellular phone products and base wireless standards, such as Bluetooth and ZigBee.
- A system designer must also make reasonable decisions about on-body connections, balancing the power and computational costs of encryption and on-body key distribution against the likelihood that, e.g., sensor to-data-logger transmissions will be intercepted.
- Means must be in place to authenticate the identity of patients that use these devices, since data corruption (e.g., storing health data in the wrong patient record) is arguably in some contexts a greater concern than a breach of patient confidentiality.

- ❖ Like encryption, a designer must balance the ***computational, power***, and throughput costs of these approaches against the available system resources, which can be minimal at the BAN sensor level.
- ❖ A large body of work exists that addresses information surety as it relates to patient safety within the context of health monitoring systems, and guidelines published by the U.S. Food and Drug Administration are changing to address the use of wireless, wearable systems in home environments.
- ❖ In a more general way, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 includes a broad mandate to protect data in health networks from unauthorized access and tampering.

Wireless communication technologies used in wearable devices:

Wearable devices rely on various **wireless communication technologies** to enable data transmission, connectivity, and interoperability. The choice of technology depends on factors like **power consumption, range, data rate, and latency**. Here are the main wireless communication technologies used in wearable devices:

Short-Range Wireless Technologies

1. **Bluetooth (Classic & Low Energy - BLE)**
   - **Most common for wearables** (smartwatches, fitness trackers, earbuds).
   - BLE consumes **low power**, making it ideal for battery-operated devices.
   - **Range:** 10–100 meters.
   - **Data Rate:** Up to **2 Mbps** (BLE).
2. **Wi-Fi (IEEE 802.11x)**
   - Higher data transfer speeds, suitable for **smart glasses, AR/VR headsets**.
   - Consumes more power than Bluetooth.
   - **Range:** Up to 100 meters indoors.
   - **Data Rate:** Up to **9.6 Gbps** (Wi-Fi 6).
3. **Near-Field Communication (NFC)**

   - Used for **contactless payments, authentication, and data exchange**.
   - Ultra-low power, but **very short range (~4 cm max)**.
   - **Data Rate:** Up to **424 kbps**.
4. **Zigbee & Z-Wave**
   - Common in **smart home integration** (wearables as control hubs).
   - Low power consumption but slower data rates.
   - **Range:** 10–100 meters.
   - **Data Rate:** Zigbee (250 kbps), Z-Wave (100 kbps).

Long-Range Wireless Technologies

5. **Cellular (4G LTE, 5G, NB-IoT, LTE-M)**
   - Used in **standalone smartwatches, smart clothing, and medical wearables**.
   - 5G enables **low latency and high-speed data** transfer.
   - **Range:** Several kilometers (depends on network).
   - **Data Rate:** Up to **10 Gbps** (5G).
6. **LoRa (Long Range) & Sigfox**
   - **Low-power, long-range** communication for **health monitoring wearables**.
   - Used in industrial and medical IoT applications.
   - **Range:** Up to **15 km**.
   - **Data Rate:** LoRa (0.3–50 kbps), Sigfox (~100 bps).
7. **Ultra-Wideband (UWB)**
   - **High precision** positioning and tracking for smart wearables.
   - Used in **smart tags, AR/VR applications**.
   - **Range:** 10–50 meters.
   - **Data Rate:** Up to **27 Mbps**.
8. **RFID (Radio-Frequency Identification)**
   - Used in **wearable tags, smart badges, and inventory tracking**.
   - **Short to medium range (a few meters to several meters, depending on frequency band).**
   - **Data Rate:** Typically **low**.

Emerging Wireless Technologies

9. **Wi-Fi HaLow (IEEE 802.11ah)**
    - **Low-power, long-range** Wi-Fi for wearables in IoT applications.
    - **Range:** Up to **1 km**.
    - **Data Rate:** Up to **347 Mbps**.
10. **Visible Light Communication (VLC) / Li-Fi**

- Uses **LED light** for data transmission.
- Secure and interference-free (suitable for medical and industrial wearables).
- **Range:** A few meters.
- **Data Rate:** Up to **Gbps**.

Choosing the Right Technology for Wearables

- For fitness trackers & smartwatches: Bluetooth Low Energy (BLE), Wi-Fi, NFC.
- For standalone smart wearables: 4G LTE, 5G, Wi-Fi.
- For medical wearables: NB-IoT, LTE-M, LoRa, RFID.
- For high-precision tracking: UWB, RFID, Wi-Fi HaLow.

Challenges on Wireless Communication Technologies:

1. Signal Throughput

- ❖ One of the challenges when designing a reliable wearable wireless system is to understand the throughput variability that occurs in practice. A common approach for designing wireless solutions is to first calculate throughput requirements based on

    (1) the number and types of sensors used,

    (2) the sampling rate, and

    (3) the amount of information that is to be exchanged.

- ❖ This is followed by identifying wireless modules that claim to provide a certain data rate and then integrating them with the sensors.

- Unfortunately, more often than not, this exercise does not offer the expected performance. Practical data rates tend to be lower than the maximum rates indicated in the specifications. This is due to a number of factors. First, a system's usage environment plays a major role. For example, Bluetooth and wireless LAN devices operate in the unlicensed 2.4 GHz ISM band.
- Many household devices such as cordless phones, microwave ovens, and car alarms also operate in this band and serve as interferers that can lower transmission rates.
- Second, network specifications usually denote the aggregate data rate supported and state that the rate per device may not be guaranteed as the number of deployed devices increases. Finally, the rated throughput values typically indicate "raw data rates", whereas actual data rates must accommodate information transmission overhead such as

  (1) channel coding,

  (2) training data for channel estimation,

  (3) frame synchronization packets,

  (4) addressing/authentication information, and

  (5) higher MAC/Network/ Application-layer-related information.

- In summary, it is important for the designer to understand the practical variability in throughput and account for this at the design stage.

2. Resource Allocations

- Another important consideration in wearable systems is the means to distribute the information processing load.
- A typical wearable system consists of a network of sensors that measure complementary (sometimes redundant) health information.
- An initial vision was to have the sensors store their raw data and periodically upload those data to a central processing unit. However, with advances in embedded processing and the low cost of memory, it is now practical to perform local data processing at the sensor level prior to communication, saving battery life in the meantime.

- For example, a wearable pulse oximeter may decide to calculate and transmit only the blood oxygen saturation level rather than send raw photo-plethysmographic (PPG) data.
- This distributes the information processing task to the sensor and minimizes the amount of data communicated over the wireless link.
- The key benefit of distributed signal processing is that power spent on communication is lowered at the cost of more processing power at the sensor level.
- Since wireless communication is the dominant drain for battery power, ***distributed signal processing approaches*** have received attention in the sensor networking arena. At the same time, it is important to remember that communicating “quantized” or “partial” information to the central processing unit limits the ability of the system and its users to detect and act on information. For example, the knowledge one can gain from postprocessing a complete ECG or PPG waveform is no longer available if only a summative health metric is communicated.
- Distributed processing variants can be implemented to overcome this drawback. For example, if the wearable devices detect abnormal health metrics, they can then send entire wave forms to the central processing unit for post processing. If the patient is healthy, devices can communicate summative health metrics periodically and sleep in the interim.

3. Power Optimization:

- The battery life in wearable sensor networks is important. One way to increase the lifespan of a BAN is by improving the batteries that power the sensors.
- Since communication uses most of the power, it makes sense to first think about how to best manage transmit power for a specific BAN setup.
- The discussion of distributed signal processing in the previous section is closely related to power optimization.
- Effective data compression/quantization at the sensor level also reduces the amount of information to transmit, which in turn reduces the power consumed to complete the transmission.

- A central processing unit can similarly act as the power manager in a BAN.
- Additionally, power can be indirectly reduced if the sensors can be programmed to determine the best modulation and coding characteristic for each transmission.
- In a sense, the idea of software defined radio modules can be used to ensure that power utilized to exchange information is always minimized.
- ***Piezoelectric systems*** can convert motion from the human body into electrical power. As a result, one can harness energy from leg/arm motion and foot falls: piezoelectric materials can be embedded in shoes to recover “walking energy”.
- Additionally, ***miniature thermo couples*** have been developed that convert body heat into electricity. Another method to harvest energy is through the oxidation of blood sugars as demonstrated by researchers at Saint Louis University. This approach can power implanted electronic devices (e.g., implanted biosensors for diabetics, implanted active RFID devices, etc.).
- In all of these cases, the ***harvested energy*** can power sensors and radios to form sensor networks. It is important to note that the energy/power levels harvested from these sources can be intermittent and quite small (on the order of microwatts).
- Recently, the IEEE 802.15.4f task group has started working on developing guidelines for such low power sensor systems.

****