Data Security in Sensors of Wireless Sensor Networks

[1] Shanthi .K.Guru , [2]M.R. Ebenezar Jebarani
[1]Research Scholar [2]Associate Professor Sathyabama Instute of Science and Technology Chennai, India

ABSTRACT

The Wireless Sensor Network (WSN) has grown in importance as a technology that may be utilised in a variety of ways. Recent advancements in the WSN have enabled comprehensive health monitoring in both the home and hospital settings. Thanks to recent technological advancements in sensors, power-efficient integrated circuits, and wireless communication, compact, light-weight, affordable, and intelligent physiological sensor nodes have been created. One or more critical signals can be detected, processed, and transmitted by these nodes. They may also be used in wireless personal area networks (WPANs) or wireless corporate sensor networks for health monitoring (WBSNs). Many studies have been carried out and/or are currently being carried out in order to develop WBSNs for healthcare applications that are flexible, dependable, safe, real-time, and energy efficient. IEEE 802.15.4/ZigBee, a low-capacity wireless communication standard, has been developed as a new efficient technology in health monitoring systems to manage and monitor patient status while reducing power and maintenance costs.

Keywords - *Wireless Sensor Networks (WSNs), Sensor Nodes, sensor security,Health monitoring.*

I. INTRODUCTION

The Wireless Sensor Network (WSN) is a collection of small, self-contained devices that collaborate to solve problems. It is a unique technology that has advanced significantly during the previous decade. For research into nanostructures and sensors, real development opportunities for WSN were presented. It has been discovered that combining small, low-cost microcontrollers with sensors can lead to the production of extremely useful devices as an integral component. These gadgets are known as sensor nodes.

Nodes can communicate via a variety of protocols. In the subject of communication protocols for wireless sensor networks, studies are exciting and rely on a variety of network topologies. Power management, data transfer, movement patterns, and other issues are addressed through node communication. As previously indicated, WSNs provide new technology. The Smart Dust project, which was funded by DARPA[1], began at the University of California (University of California), Berkley. The goal of this study was to create a self-contained millimetre hardware platform for scattered WSNs. This was largely a military application that resulted in the development of huge sensor nodes. Later downsizing led in even smaller gadgets with excellent sensing and communication capabilities. The installation of an energy-efficient software platform, the Tiny OS operating system, which was also developed at UC, is an important part of the wireless sensor network's history. The WSN has also benefited from the development of numerous software platforms. Sensor nets are used in agriculture, environmental science, and tourism, but health is probably the subject where they will have the most impact.

LITERATURE REVIEW

II. REVIEW OF WIRELESS SENSOR NETWORKS IN HEALTH MONITORING:

This section discusses several specific apps that have been developed or are being studied for the purpose of health monitoring.

The MobiCare client and health care server Wireless Physiological Measurement System (WPMS) uses Bluetooth's short distance from the Body Sensor Network (BSN) to the BSN Manager (UMTS) and the BSN Manager to GPRS and health care providers (UMTS (General Packet Radio Service / Universal mobile telecommunications system) in MobiCare (Rajiv, 2006). This system makes use of Bluetooth, which enables for data speeds of up to 1Mbps. Despite this, it consumes a lot of power and has a tiny network size (up to 7 slave nodes). As a result, LR-WPAN is not ideal for many health applications (low-priced WPAN).

[Mangharam et al., 2006] at Carnegie Mellon University In coal mines, Firefly is an online rescue detecting device. Voice streaming through WSN is used in this way. The audio time requirements for a TDMA-based network are investigated. A dual radio architecture for worldwide synchronisation and data transfer was included in the hardware produced. This system is designed for rescue in a coal mine and has a small network size. For increased sound memory, it makes use of the codec chip and SD card. It's a high-powered device with a high sensor node cost and a huge dimension. WSN's various health applications are investigated by Harvard University's CodeBlue [Malan, et al., 2004]. They've developed a basic processing framework for detecting heart rate and catastrophic failure. They're presently working on a system prototype using in-house ECG samples and ZigBee wireless modules.

Jovanov et al. (2005) aim to create wireless sensing technologies for human psychophysiological applications in both ambulatory and implanted contexts. They've developed heart monitoring devices, long-term prosthetic joints, and other bodies. Juyng and Lee[2008] described the device access control system. They proposed the reliable conveyance of physiological health data in a ZigBee-based health monitoring system. They designed wrist, chest, shoulder, and necklace physiological signal devices. They use a CC2430 microcontroller and two PDMS electrodes for ECG, the temperature sensor type ribbon, and SpO2 to monitor physiological indications. Their bracelet is 60x65x15 mm in size, and the total system, including one lithium-polymer battery, weighs 160 grammes. A trustworthy data transport mechanism is built via retransmission. A network device's power problem has been identified. It requires a small battery as a power source. It can be used for 6 hours without needing to be recharged. It's small, light, and easy to carry, however the battery life may be improved. Chien and Tai[2006] proposed the portable prototype measuring device (PCG), ECG, and body temperature. They establish a 3-wired ECG lead by inserting a condenser microphone into the PCG stethoscope tube. Bluetooth transmitter and receiver modules use a microcontroller and a PDA for wireless connection between a sensor module and a PDA. This method has some flaws as a health surveillance system. First and foremost, while assessing health issues, users should start with the PDA. As a result, this system is not automatically performed, driven by events, or scheduled. Second, this system contains multiple huge external circuits, coupled ECG pipework, and memory units. It is not designed to be worn, thus it is difficult to transport owing to its heavy weight and big proportions. Third, because of their complicated and many external equipment, they use a significant amount of electricity. As a result, wireless health surveillance is limited. Microsoft introduced the wearable health surveillance system [Oliver and Msngas, 2006]. HealthGear. It has various physiological sensors for monitoring and analysing blood oxygen levels (SpO2), heart rates, and multi-thysmographic signals. Multiparameter health monitoring in outpatient settings. Gyselinckx, et al. (2007) developed the Human++ cardiac monitoring system, which includes ECG, electroencephalography (EEG), and electromyography (EMG). The body area networks have three sensor nodes and a base station. The bio-signal is captured with a 12-bit ADC at 1024 Hz in the MSP430F149 microcontroller. Through a USB link, the base station collects data from each sensor node and transmits it to a PC or a PDA. This system is supposed to run for three months on two AA batteries. This system has been improved in [Brown, et al., 2009]. A tiny, lightweight WPMS platform is developed to monitor autonomous reactions for ambulatory and continuous monitoring in real-life applications. Human++ UniNode's applications include the MSP 430, the Nordic nRF24L01 2.2 GHz radio, 50 ohmes of antenna, and a 165 mAh lithium-ion battery. A node's battery measures 20x29x9 mm3. The topology of their network is a static TDMA protocol star network. Their wearable devices' medical sensors have grown into many types of chest and wristbands. The ECG and respiration sensors (20x22x4 mm3) are coupled to a Human++ UniNode and integrated into a chest belt, while the Skin Conductance and skin temperature sensors are merged into a wristband (20x25x5 mm3). The chest node consumes 2,6 mA while the wrist node consumes 4 mA and has a battery life of 63 hours and 41 hours, respectively, in full active mode. Fensli et al. [2005] introduced the wearable ECG device for continuous monitoring. The amplified ECG signal from a wearable device is sent into a normal PDA portable device. The ECG sensor has a sampling frequency of 500 Hz and is digitised with a 10 bit resolution. After digitising the signal, an operator receives a modulated RF link at 869,700 MHz on a continuous basis. The emergency has been the focus of this technology's implementation. Monton et al. [2008] were the first to introduce WPMS-based patient monitoring. This BSN uses a star network technology and is made up of two types of modules. A small device (34 to 48mm2), the sensor communication module, is coupled to one or more sensors for health signals (SCM). SCMs provide signals to a central processing unit (73 – 110 – 25 mm3) through ZigBee, which is referred to as Personal Data Processing (PDPU). PDP Using: 1) UWB, which links devices such as computers and PDAs, 2) WIFI, which connects to a LAN, or 3) GPRS, which connects to a WAN. A LAN connection is referred to as PDPU.

We describe the design of a wearable belt network in [Wang, et al., 2009]. A photoplethysmograph (PPG) sensor and a respiratory inductive plethysmograph (RIP) sensor are used to assess pulse rate and oxygen saturation for dynamic respiration monitoring. The main control unit of the WPMS node is the Microcontroller MSP430F149, the RF transceiver NRF905, and the external memory 64 Megabit AT25DF641. You communicate in a straightforward manner. The entire approach, which includes one sensor at each base station, is relatively simple. Milankovic et al. [2006] presented a single-hop WSN topology. Every health monitoring sensor is immediately connected to a personal digital assistant (PDA) that allows contact with a central server. They focus primarily on the difficulties of synchronisation and energy efficiency in the singlehop communication network between network devices and PDA. IEEE 802.15.4-enabled devices are used to construct a mobile wireless healthcare application. The CDMA network is used in hospitals and residential settings (Yan and Chung, 2007). Yan and Chung (2007) [Yan and Chung, 2007].

III. Research Issues

When designing a tiny wireless sensor device and network for a real-world health monitoring system, a number of factors should be taken into account.

A. Reliability

The most crucial factor of a wireless health monitoring system is its dependability. Wireless health monitoring systems must convey measured data in a timely manner to a medical practitioner or other persons so that patient data may be monitored and analysed. There are three stages to the issue of dependability: 1) Trustworthy data gathering, 2) Trustworthy data transfer, and 3) Trustworthy data analysis [Hyun, 2008]. Hardware and software for effectively detecting and analysing data are the focus of Stages 1 through 3. Stage 2 necessitates more consideration than the previous stages since it entails communication between a sensor node and a coordinator or central monitoring server.

For trustworthy communication, Varshney [2007] recommended integrated wireless networks that include WSN, ad-hoc wireless networks, cellular networks, WLAN, and satellite networks. Juyng and Lee [2008] used a retransmission technique to achieve a reliable data transport. A sensor device sends the data via an ACK (Acknowledgement) request. During AckWaitDuration, if the sensor node does not get an ACK from a mobile device or coordinator, it broadcasts the same data frame until the mobile device answers. The number of times this operation can recur is limited by the MaxFrame-Retries [IEEE Std. 802.15.4-2003] parameter.

B. Power

The power issue is examined for a variety of WSN applications. Because most WSN devices are battery-powered, reducing power consumption is an important design consideration. Some WSN applications, such as passive RFID (Radio Frequency Identification) [RFID Handbook, 2003], do not require a battery. Instead, they rely on the reader's ability to backscatter information, a technique called as backscattering. They do, however, have a limited communication range and can only carry data that is very little. Energy harvesting systems for WSNs are used in applications such as solar cells [Hande, et al., 2007], vibration using piezoelectric devices [Roundy and Wright, 2004], temperature difference [Stark, 2006], and shoes insert [Paradiso2006]. However, for real-world WSN applications, these energy harvesting devices have various limitations, including the fact that their power output is reliant on their surroundings and that they are frequently over-sized. Van Dam and Langendoen [2003], Zheng et al. [2005], Ramakrishnan et al. [2004], and Miller and Vaidya [2005] created energy-efficient WSN protocols by developing energy-efficient MAC protocols. To save energy, Omeni et al. [2007] advocated that sensor node standby or sleep mode periods be managed. For MAC protocol operations, they propose three basic communication methods. Link setup is the process of connecting a process to a network. A wakeup service function wakes up a slave and master after a specified amount of time has passed. An alert method is only activated when a slave node needs to convey data to the master. These processes can only be started by the master node.

C. Portability

Sensor component integration into a wireless sensor node should be functional, long-lasting, small, light-weight, and cost-effective. As a result, most PANs use a small chip system (SOC) or a single MCU with an external transceiver, which comprises of a microcontroller and an RF transceiver. Various biomedical technologies for monitoring physiological signals that are easy to wear or attach to the body are already available [Barth, et al., 2009; Jung, et al., 2008]. As a consequence, they're simple to move.

D. Network Interference

A wireless connection is more sensitive to interference than a wired connection. In most WSN configurations, two or more communication techniques are merged into a single network. WPANs and WLANs are frequently found on the same ISM (Industrial, Science, and Medical) band. As a result, there's a chance they'll create network disturbance. Network interference or data collision challenges create intermittent network connections and packet loss, resulting in lower network performance and greater energy costs [Razvan and Andreas, 2008]. The concerns of Bluetooth and WLAN interference and cohabitation have been explored by [Jo and Jayant, 2003; Sakal and Simunic, 2003]. Interference issues between IEEE 802.15.4/ZigBee and WLAN are discussed in [Razvan and Andreas, 2008; Kim, et al., 2005; Kang, et al., 2007; Yang and Yu, 2009; Hauer, et al., 2009]. BER (Bit Error Rate), PER (Packet Error Rate), RSSI (Radio Signal Strength Indicator), or SINR (Signal Interference Noise Ratio) are all monitored and assessed for interference avoidance. Guo and Zhou [2010] provided interference prediction methods based on packet error rate data to explore the impacts of WiFi and microwave ovens on ZigBee communications.

E. Real Time and Continuous Monitoring

Heartbeat, lung sound, ECG, and RIP are examples of physiological data that should be continuously checked in real time. A biological sensor is also built to work for days, if not weeks, without requiring user input. A good example is a heartbeat monitoring device for a patient with cardiac difficulties. Because the heart rate is regularly monitored, a heartbeat sensor device should be turned on at all times and transmit continuously with minimal transmission delay and latency to enable for real-time monitoring. If a sensing device communicates periodic data discontinuously or consistently with a significant delay time, it is difficult for doctors to monitor and prepare for a patient's heart attack.

IV. OVERVIEW OF WIRELESS SENSOR NETWORKS

A. Basic Components in Wireless Sensor Nodes:

A wireless sensor network (WSN) is a collection of wireless nodes that detect and transmit information about specific objects or entities across wireless networks. The information is transferred to a base station or a PDA/cell phone, which can link to other networks, such as the Internet, through a single or several hops. A wireless sensor node consists of one or more sensors for measuring physical variables, as well as a primary processing unit (a microcontroller or low-power consumption CPU), an analog-to-digital converter (ADC), flash memory, and an RF transceiver. It typically has a power source that is insufficient.

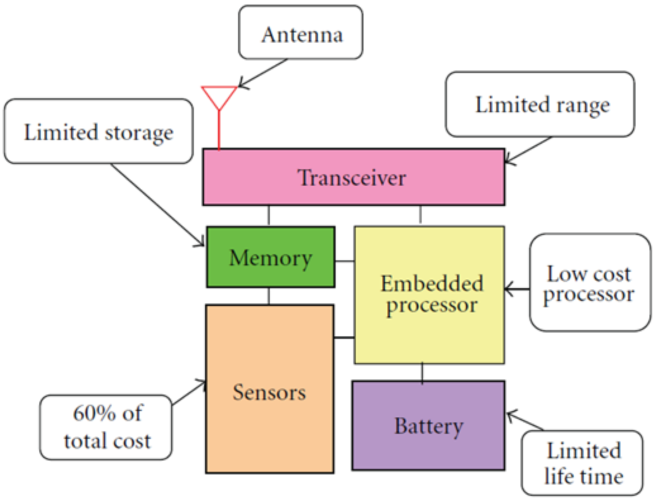

Figure 1: A basic setup of a sensor node [4]

Figure 1 depicts the major components of a typical wireless sensor node. Most WSN nodes utilise an 8051 microcontroller as their main processing unit because of its low cost, low power consumption, and small size [Barth, et al., 2009; Chen and Wang, 2008; Choi, et al., 2007; Choi and Song, 2008; Zhang, et al., 2009]. Some systems, such as the CC2430 [Chai and Yang, 2008], use a system-on-chip (SOC), which includes an ADC, flash memory, and an RF transceiver. The compact size of SOC allows for the creation of a small and low-power sensor node. The ADC's poor quality and limited memory space are disadvantages. Some sensor nodes use a microcontroller unit (MCU), such as the MSP430F1611 or an Atmel with an external RF transceiver [Jovanov et al., 2005]. Other developers [Mangharam, et al., 2006] employ MCUs with external ADCs or external extra flash memory to increase service quality.

B. Wireless Sensor Network in Health Monitoring

In a wireless physiological data monitoring system, wearable biomedical sensor devices broadcast real-time vital sign data to a coordinator through a radio channel. Patients can wear wireless devices that track their physiological indicators and provide data to their doctors in real time.

Wireless health monitoring systems provide a number of benefits over wired healthcare equipment. To begin with, patients no longer have to wait for an appointment with their doctor. Furthermore, the use of wireless healthcare systems outside of the hospital saves money for healthcare providers. It also allows many patients to work while still being monitored by their physicians. Second, if some important signals, such as heart rate, vary considerably from the norm, such gadgets can identify any medical emergency. A heart attack occurs when a blood clot blocks a coronary artery, causing heart muscle death. If blood flow to the heart muscle is not restored, 20 million Americans will have a heart attack each year. [2010, Medicinenet] A heart attack claims the lives of 40% of them. Because heart attacks can hit older people or patients at any time, continuous and real-time monitoring of their heart rates can help them live longer. The majority of heart rate monitors, such as electrocardiography (ECG), are now only available in a few places, such as hospitals and doctors' offices. They entail the implantation of a large number of wired electrodes on the skin of a patient. Stethoscopes are commonly used by medical personnel to listen to a patient's heartbeat. Regrettably, in terms of heart rate monitoring, these have considerable limits. As previously indicated, continuous heart rate monitoring is very important in the case of a sudden heart attack. However, with today's connected medical equipment, it's practically impossible. Wireless health monitoring devices certainly have numerous advantages over current wired healthcare equipment. Figure 2 depicts a typical wireless sensor network for healthcare applications. The data collected by the sensor nodes is relayed to the base station, coordinator, or PDA/cell phone through an RF channel, which is physically or wirelessly connected to other networks. In real time, a server manages and monitors the whole network. Depending on the application, wireless communication methods such as Wi-Fi, Bluetooth, ZigBee, UWB, and cellular networks are used.

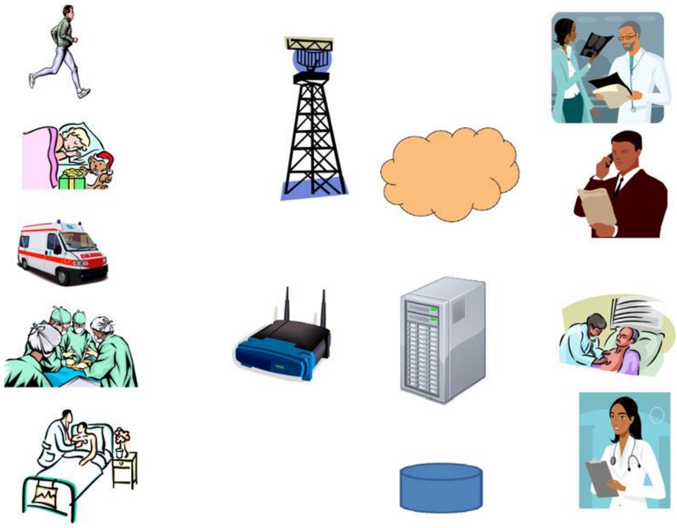

Fig. 2 Typical architecture of wireless sensor networks in healthcare applications [11]

C. Technologies for WSN in Health Monitoring

IEEE 802.15.1 (Bluetooth), IEEE 802.15.4 (ZigBee), and IEEE 802.15.3a (UWB) for PAN, and one IEEE 802.11 a/b/g (Wi-Fi) for WLAN are briefly examined in this section for their applicability in wireless health monitoring systems. WSN collects medical data with small, low-power devices. Their nodes sense and collect data, then communicate with a coordinator or a remote monitoring device, such as a PDA, mobile phone, or PAN coordinator, using wireless data transmission technology. The PAN coordinator has a large memory and fast CPUs to analyse and show data. The operating frequency, modulation technique, network data rate, and hardware interface between nodes and the central server are all determined by the physical radio layer.

1. ZigBee

IEEE 802.15.4 and ZigBee, both standard-based protocols, offer the network infrastructure required for WSN applications. ZigBee defines the network and application layers, whereas 802.15.4 defines the physical and MAC levels. They can be used to build low-data-rate, low-complexity, low-power, and low-cost WSNs. The physical layer (PHY) supports three radio bands: the 2.4GHz ISM band, which has 16 channels worldwide, the 915MHz ISM band, which has 10 channels in the Americas, and the 868MHz band, which has a single channel in Europe. The data speeds are 250kbps at 2.4GHz, 40kbps at 915MHz, and 20kbps at 868MHz. The IEEE 802.15.4 PHY uses direct sequence spread spectrum coding to reduce packet loss due to noise and interference. It also offers two PHY layer modulation options. The 868/915 MHz PHY uses binary phase shift keying modulation, while the 2.4 GHz PHY uses offset quadrature phase shift keying. The three types of ZigBee devices are the coordinator (MAC Full Function Device-FFD), router (MAC FFD), and end device (MAC FFD) (MAC Reduced Function Device- RFD). An FFD may serve as both a network coordinator and a standalone device. It is capable of interacting with any other gadget. Simple applications, such as a light switch or a tiny sensor device, need for an RFD.

Only FFD can communicate with it. A ZigBee coordinator is a base station node that manages the entire network and composes the network automatically. It needs a significant amount of memory and processing power. An FFD that links groups and facilitates multi-hop packet transport is known as a ZigBee Router. It can connect with other routers as well as end-devices. With ZigBee end devices, only an FFD may connect. It has a limited set of capabilities. In theory, ZigBee can support up to 65,536 nodes. For security, it uses 128-bit Advanced Encryption Standard (AES) encryption and authentication.

2. Bluetooth

Bluetooth, also known as IEEE 802.15.1, is a low-cost, low-power wireless radio frequency standard for short-range communication. The Bluetooth protocol stack is highly advanced in contrast to other IEEE networking stacks. Many components are defined at a higher level than the PHY and MAC. Some of them are optional, adding to the protocol's overall complexity [Hackmann, 2006]. In the unlicensed 2.4 GHz ISM band, Bluetooth uses 79 channels. The PHY layer uses frequency hopping spread spectrum coding to reduce interference and fading. The highest data rate in enhanced data rate mode is 3Mbps.

The actual data payload is usually decreased to maintain compatibility among all Bluetooth sensor nodes owing to differences in unit addresses and other header information. Bluetooth's core connection technology is the piconet, which is based on a star network architecture. It consists of a single master device capable of communicating directly with up to seven active slave network devices. The master's clock and frequency hopping pattern are used to synchronise all devices in a piconet, while slave devices only interact with their master one-to-one. Bluetooth has three different power-saving modes. Only designated slots for synchronous connections are processed by devices in hold mode. They then fall into a deep slumber. When in sniff mode, a device is in sleep mode for the most of the time. It communicates by waking up at intervals set by the user. All other links to the master device are disabled since the device only keeps the parked slave broadcast (PSB) link in parked mode. If the latter wishes to wake up parked devices, it sends beacons across the PSB link [Hackmann, 2006]. A slave device in active mode can reduce its power consumption by entering one of the several power saving modes.

3. Ultra Wide Band (UWB)

UWB (IEEE 802.15.3a) is a wireless radio technology that uses a greater section of the radio spectrum to provide short-range, high-bandwidth communication at extremely low energy levels. The IEEE 802.11 standards have a hidden adversary in the form of UWB. One of its most notable features is its massive bandwidth. Wireless USB now offers up to 480 Mbps at 3 metres and 110 Mbps at 10 metres of distance. It may handle multimedia applications in home networks, including as audio and video transmission. It may also be used to replace high-speed serial buses like USB 2.0 and IEEE 1394 with a wireless connection [Lee, et al., 2007]. IEEE 802.11 is a wireless networking standard that is intended to replace Ethernet cables in data networking applications like WLAN. Bluetooth is increasingly widely used in applications that span a limited area network, such as a wireless mouse and a phone set. Bluetooth, on the other hand, has a much less bandwidth than UWB. It uses very low-power, short-pulse radio emissions to convey data over a wide range of frequencies.

4. Wireless Fidelity (WIFI)

Wi-Fi refers to any network that uses the IEEE 802.11 standard (wireless fidelity). 802.11 networks include the 802.11a (up to 54 Mbps), 802.11b (up to 11 Mbps), and 802.11g networks (up to 54 Mbps). These networks are referred to as WLANs. Three 802.11 standards offer different bandwidth, coverage, security support, and hence applications. 802.11a is better suitable for multimodal audio, video, and large-image applications in densely populated user environments. However, because it has a shorter range than 802.11b, it needs fewer access points to cover large areas.

V. Limitations and Challenges in WSN

To achieve low power consumption and compact gadget size, MCU is employed as a control unit in medical applications. Furthermore, AAA, AA, and Li-ion batteries are used to power all of the devices. The batteries have the greatest impact on the size and weight of gadgets. A battery's capacity is proportional to its size. 2 AA or 2 AAA batteries are used by [Juyng and Lee, 2008] and [Monton, et al., 2008], whereas Li-ion or Li-P batteries are used by [Malan, et al., 2004], Oliver and Msngas [2006], Gyselinckx, et al. [2007], and Milenkovic, et al., 2006. A compact Li-P battery has a life span of around 6 hours [Juyng and Lee, 2008], whereas an AA or AAA battery has a life span of several days or even three months in full active mode [Gyselinckx, et al., 2007]. As a result, battery types utilised in different healthcare applications must be carefully selected for mobility and power consumption. Several applications for health monitoring systems make advantage of numerous wireless networks. With a PDA, a cellphone, or a wireless network, Rajiv [2006], Chien and Tai [2006], and Oliver and Msngas [2006] utilise Bluetooth. To link a BAN with a PDA or a WLAN for a broader network, Milenkovic et al. [2006], Yan and Chung [2007], and Juyng and Lee [2008] all employ ZigBee. When numerous wireless infrastructures are established in the same network region, interference and data collision can occur in overlapping channels. Multiple network topologies, such as star, peer-to-peer, and mesh, should be investigated for diverse health data applications. Each software addresses some of the issues mentioned above, such as dependability, power, mobility, network interference, and QoS, in real-world applications. None of them, though, are totally content. Some programmes, such as [Jung, et al., 2008; Milenkovic, et al., 2006], provide high reliability, portability, and QoS, but they use too much power for real-world applications. [Mangharam, et al., 2006; Mangharam, et al., 2006; Mangharam, et al., 2006; Mangharam, et al., 2006; Mangharam, et al., 2006;

Mangharam, et al., 2006; Mangharam, Despite their remarkable performance, Oliver, et al., 2006]'s devices are too bulky and heavy to carry or attach to the body in real-world applications. The FireFly project [Mangharam et al., 2006] can send continuous speech data in real time, but it uses a lot of power, requires a large device, and has a limited network. Existing health monitoring clearly faces a number of challenges and concerns, including reliability, mobility, low battery consumption, and real-time communication, as outlined. The bulk of the solutions we looked at were focused on single hop topologies and offered little real-time monitoring. Certain systems are challenging to install or transport due to their size and weight.

Even if they can monitor health issues, they will not be practical in everyday situations. For their various health indicators, situations, and places, they employ various wireless technologies. Despite its low data rate, IEEE 802.15.4/ZigBee is utilised to transmit small data such as body temperature and patient ID. Furthermore, real-time time synchronisation has little impact on this sort of data. Some physiological data, such as ECG, EEG, and EMG, must, nevertheless, be sent in real time. Furthermore, they demand a high data rate for reliable transmission. As a result, each application on a health monitoring system must review or improve its weak areas for real-world use.

VI. SECURITY IN SENSORS

Security breaches in sensor networks in healthcare applications are a critical issue. Because healthcare sensor network applications are almost same to WSN application settings, most security challenges are likewise nearly identical and hence comparable. The two main levels of security concerns are system security and information security. The authors in [11] categorised the threats and attacks [12] into two categories: passive and aggressive. While data packets are being delivered across the system, a passive attack might occur. The attackers may change the destination of packets or cause routing errors. Attackers might possibly employ wireless communication channel eavesdropping to steal health data. Threats that are active provide a greater risk than passive threats. Criminals may be able to trace down the user's location through eavesdropping. This might place you in a dangerous situation. Sensors are frequently constructed with few external security features, leaving them open to physical manipulation. This increases the vulnerability of the gadgets and makes security more challenging.

The authors of [11] go into great detail on eavesdropping and manipulation of medical data, forging of warnings on medical data, denial of service, location and activity tracking of users, physical tampering with devices, and jammer assaults. People with bad motivations might use the knowledge for their own gain.

The attacker can erase or modify part or all of the eavesdropped data and send the changed data back to the original receiver to achieve some illegal aim. The importance of health data cannot be overstated. Modifying them might result in a system failure and the death of a person.

Impersonation attack—If an attacker acquires a wireless sensor node's identity information, they can use it to fool other nodes.

Eavesdropping—Any attacker can easily and freely intercept radio talks between wireless nodes due to the open nature of wireless channels used by sensor networks. Stolen data might be used for malicious reasons.

Replaying—An attacker can intercept valid data and send it back to the original receiver over a period of time to accomplish the same purpose in a different environment.

The authors argued in [13] that the availability, scalability, efficiency, and quality features of inter-node communication should all be deemed secure in light of current security concepts. System Reliability In a WBAN situation where a person wears many devices, a centralised control device can be used for data transfer from within and outside the network. This control device can also act as a link between the internal network and the outside world. Sensor network security in health-care applications must not be compromised. Extreme steps are necessary in this scenario.

Layer	Attacks	Security Approach
Physical layer	Jamming and Tampering	Use spread spectrum techniques and medium access control (MAC) layer admission control mechanisms
Data link layer	Jamming and Collision	Use error correcting codes and spread spectrum techniques
Network layer	Sinkhole	Redundancy checking
	Sybil	Authentication, monitoring
	Wormhole	Authentication, probing
	Hello flood	Authentication, packet leashes by geographical and temporal info.
	Ack. flooding	Authentication, bidirectional link authentication, verification
Transport layer	Injects false messages and energy drain attacks	Authentication
	Flooding	Client puzzles
	De-synchronization	Authentication
Application layer	Attacks on reliability	Cryptographic approach

Security at the administrative level

Effective administrative control is essential to administer the system. To prevent security breaches, staff or those in control of the overall system functioning should be subjected to security protocols. A well-defined user hierarchy paired with strong authentication techniques may help to prevent security breaches at this level. Only authorised users should be able to access the data, hence access methods must be included in security measures. Similarly, data forwarding may be restricted to previously approved places or persons.

Security at the Physical Level

Controls at this level include restricting access to physical equipment and data in the system to prevent claimed theft or manipulation. The devices are vulnerable to malicious individuals as well as natural wear and tear. The system may fail in the case of a natural disaster, posing serious hazards to the entire system's operation. As a result, careful device design is essential to ensure that they are temperature resistant. It is acknowledged, however, that avoiding physical tempering of circuits is difficult. Allowing only authorised personnel to physically handle the devices while they are in operation might be another protective measure.

Security at the technical level

Hardware security checks, such as servers, discs, and other similar devices, are generally necessary at the technological level. If data is sent over the network to central servers, server-based security on the server side and client-based security on the end-user side should be used. This is especially crucial when it comes to safe information dissemination. This may put more demand on sensors at the user's end, resulting in a higher total cost. As a result, compromises between these issues will be necessary. More powerful motes will probably definitely be necessary to fulfil the increased demands for processing and communication [14].

The system's security mechanism is responsible for providing the following security services on specified biological data when the applications request it.

a. Data Encryption— Data is encrypted in transit to prevent its disclosure. The data encryption service safeguards information from eavesdropping.
b. Data Integrity— The data integrity service is made up of the data integrity and data origin authentication services. If data integrity is preserved, the recipient may be certain that the data has not been tampered with or modified. The receiver can verify that the data originated from the designated sender by using data origin authentication. It's an effective approach to guard against data tampering.

Individuals offer critical questions from time to time. Writers in [8], for example, have highlighted worries regarding safeguarding an individual's privacy, such as where health data should be stored and who should have access to a patient's medical record. There are also issues regarding who should have access to this information without the patient's consent, as well as who will be responsible for storing these data and who will be held accountable if something goes wrong. These are only a few of the primary challenges that must be addressed in order to protect privacy and, to some extent, data security.

VII. Conclusion

The WSN research community has done an exceptional job of overcoming some of the present health-care application constraints. The bulk of plans have focused on the deployment of tiny wearable medical sensors, while some have built infrastructures for monitoring individual patients throughout daily activities, whether at home or in a hospital. In this paper, we examine the present status of wireless sensor network research, highlighting the gaps between existing technologies with respect to security to data stored in sensors and the requirements of a Wireless Sensor Network for Health Care.

VIII. Acknowledgment

I'd like to thank Dr.P. Malathi for all of her assistance, encouragement, advice, patience, and support during the writing of this work.

IX. References

1. Jin Soo Choi and Mengchu Zhou, "Recent Advances in Wireless Sensor Networks for Health Monitoring," International Journal of Intelligent Control and Systems, Vol. 15, No. 4, pp. 49-58, December 2010.
2. Jin Soo Choi and Mengchu Zhou, "Performance analysis of ZigBee-based body sensor networks,"
3. IEEE International Conference on Systems Man and Cybernetics (SMC), Istanbul, Turkey, pp. 2427-2433, October 2010.
4. "Wireless networks in the medical and health care field "Kaja Najumudeen, Sarath Barathi *M.Sc in Wireless Communication, LTH, Lund, Sweden*
5. Akyildiz I. F., Su W., Sankarasubramaniam Y., and Cayirci E., "Wireless Sensor Networks: a Survey," Computer Networks, vol. 38, pp. 393-422, 2002.
6. WBAN http://en.wikipedia.org/wiki/Body_area_network .
7. Wireless Sensor Networks http://en.wikipedia.org/wiki/Sensor_Networks.
8. JeongGil Ko, Chenyang Lu, Mani B. Srivastava, John A. Stankovic, Fellow IEEE, Andreas Terzis, and Matt Welsh "Wireless Sensor Networks for Healthcare" Vol. 98, 0018-9219/$26.00 2010 IEEE No. 11, November 2010 | Proceedings of the IEEE.
9. "The Outdoor Wireless Healthcare Monitoring System for Hospital Patients Based on ZigBee"

Xiaoxin Xu et.al Vol. 98, 0018-9219/$26.00 2011 IEEE No. 11.

10. Zhang J., Li W., Xia Z., Wang G., and Wan Z., " The Implementation of Communication for CC2430-Based wireless Sensor Network Nodes," *5th International Conference on Wireless Communications, Networking and Mobile Computing, WiCom '09*, pp. 1-4, Beijing, China, Sept. 2009.

11. Kargl, F., Lawrence E., Fischer M., and Lim Y. Y., Security, privacy and legal issues in pervasive ehealth monitoring systems. 7th International Conference on Mobile Business icmb, pp. 296–304, 2008.

12. Ng, H. S., Sim, M. L., and Tan, C. M., Security issues of wireless sensor networks in healthcare applications. BT Technol. J. 24 (2):138–144, 2006.

13. Yong, W., Attebury, G., and Ramamurthy, B., A survey of security issues in wireless sensor networks. IEEE Commun.Surv. Tutor. 8 (2):2–23, 2006. Second Quarter.

14. Ashraf, A., Rajput, A., Mussadiq, M., Chowdhry, B. S., and Hashmani, M. SNR based digital estimation of security in wireless sensor networks. In Communications Infrastructure. Systems and Applications in Europe , Vol. 16: 35–45, 2009.