CHAPTER 1

INTRODUCTION

Technological innovations for communication and computing have been advancing at an accelerated pace. The ability to co-ordinate and communicate between many devices by using wireless communication has had a major impact in many areas of life. One area that has seen slow advancement is medical care. There are many concerns about the security and integrity of the information created and stored in the systems that are being developed to help meet the needs of clinicians and patients. Patient privacy and safety are of major concern when applying many of the new innovations in wireless communication to the problems faced by the medical community. The general public is concerned about how their medical information is stored, transmitted and cared for. Clinicians are concerned about the quality and integrity of the medical data they receive.

To help alleviate the perceived issues of applying wireless technology to monitor patients, it is worthwhile to investigate existing security issues in wireless networks as well as how those issues have been resolved. By applying the experience gained from wireless deployments it will be possible to address the concerns and requirements of clinical systems, to ensure the safety of patients and staff. Before wireless technology can be applied to the clinical environment, which will bring many benefits and advantages to clinical care, the security issues need to be addressed. The ability to remotely track patient information will allow clinicians a more robust picture of patient health. The extended time that patient information
can be gathered will increase the understanding of the results of medical treatments and allow for stronger refinement of those treatments to create better results overall or tailored treatments for each patient. The technology will afford clinicians the ability to understand if a patient is in stable or in declining health over a long period of time.

1.1 WIRELESS MEDICAL SENSOR NETWORKS

Wireless Sensor Networks will have a very large impact on many aspects of society from military applications to common household appliances. The application of WSN to the field of medicine will have widespread consequences in the gathering of medical information and giving a more robust picture of patient health. Sensor networks can give real-time information and telemetry to the clinicians that require the information to properly respond to medical situations and emergencies.

Wireless Medical Sensor Networks (WMSN) are networks of medical sensors placed inside or outside the human body to sense the patient’s vital body signs and transmit the sensed data in a timely fashion to some remote location without human intervention. A MWSN can track many different aspects of the patient including movement inside their home, their temperature and other bio-medical information such as oxygen saturation. The telemetry will help reduce costs for healthcare facilities by allowing patients to be remotely monitored instead of being in a facility for observation. Long-term monitoring of patient’s vital signs such as heart beats, temperature, blood pressure, motion/acceleration, pulse-oximetry, etc. can be done continuously after returning home from the hospital (Ming et al 2010). Along with sensor information, there is a very real possibility of medication being delivered in minute doses to patients based on information gathered from medical sensor networks. The delivery of the medication would be controlled by wireless communication. When the information gathered from an MWSN
reaches this level of integration with the medical care of patients, it is imperative that all communication be very secure with high integrity and availability so that no mistakes can occur and to be certain that the medication needed is the medication delivered to the patient when needed.

Figure 1.1 Healthcare application using wireless medical sensor networks

As shown in Figure 1.1, Quality-of-care across a wide variety of healthcare applications such as ambulatory monitoring, vital physiological signal monitoring in hospitals, at-home-care monitoring of elderly people, monitoring in mass-casualty disasters and clinical monitoring can be carried out using WMSN. In addition, other applications called wireless Body Area Networks (WBANs) that also benefit from WMSNs include sports-person health status monitoring (Alonso et al 2010), and patients’ self-care.
1.2 WIRELESS BODY AREA NETWORK

A Wireless Body Area Network (WBANs) is defined by IEEE 802.15.6 as a communication standard devised for low power devices operating on, in or around the human body (but not limited to human) to serve a variety of applications such as medical, consumer electronics / personal entertainment and so on. Miniaturized low-power devices and biosensors that are worn on or implanted in the human body can be connected using WBANs. An idea of information exchange between electronic devices placed inside, on or near the human body was first introduced by Zimmerman (1996) in 1995 as Wireless Personal Area Network (WPAN). To reduce energy consumption, minimize interference, and secure the communication from eavesdropping, a low carrier frequency (fc<1MHz) is used.

1.2 shows how the battery-operated WPAN transmitter and WPAN receiver work when attached with the human body. The displacement current flows through the body when a biological conductor is formed. The “earth ground” is used to prevent the shorting of the communication circuit (Zimmerman 1996). Only in the year 2001, the term Wireless Body Area Network was introduced where communication among electronic devices were implemented in, on and around human body. WBAN sensors may be wearable, implantable or portable, and are integrated on various kinds of wireless communication motes (such as, Mica2, MicaZ, Telos, etc). A typical MicaZ mote contains a CPU of 7.3 MHz Atmel ATmega128L with 128 KB of ROM, and RAM of 4 KB for data. The radio operates at a bandwidth of 76.8 Kbps and at a range of a few meters. A sensor node typically has a limited battery power (e.g., AA-batteries), which is just enough for communication (e.g., unicast, multicast and broadcast) and computation (Malan et al 2004).
Figure 1.2 Block diagram of a PAN system (Zimmerman 1996)

The body implant or wearable sensors transmit their data to a central device called a Body Area Network Coordinator (BANC). Typically, the BANC is a computationally more powerful device than the body sensors. The BANC is responsible for reliably transferring the sensors’ data to the next node or destination. Emerging research trends of WBANs collect and jointly process biological data for continuous and long-term monitoring of health conditions (Bos et al 2004; Istepanian et al 2004; Yuce et al 2007; Poon & Zhang 2008).

1.2.1 Comparison of BAN with WSN

WBANs are different from generic WSNs and their differences are summarized in Table 1.1. As shown from the Table 1.1, generic WSNs are automatic and individual, deployed at a large scale in either a fixed or distributed behaviour, and their data rates depend specifically on the
applications, whereas WBANs have direct human involvement (i.e., patient, doctor, nurse, etc.), are deployed at a smaller level (i.e., depending on usability), must support mobility (a patient can carry the devices), and requires high data rates (e.g., ECG data is normally sampled at a rate of 250 Hz and blood pressure at 100 Hz (Dimitriou & Loannis 2008)), with reliable communication and multiple recipients (Muhammad et al 2010).

Table 1.1 Difference between generic WSN and WBAN (Mohammad et al 2010)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Generic WSNs</th>
<th>WBANs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Size</strong></td>
<td>Large area (metres to kilometres)</td>
<td>Smaller (within a few meters)</td>
</tr>
<tr>
<td><strong>Node Functionality</strong></td>
<td>Redundant nodes used. Each node performs a single dedicated task</td>
<td>No redundancy and multiple tasks are required from each node</td>
</tr>
<tr>
<td><strong>Node Size</strong></td>
<td>Smaller size preferable but not a limitation</td>
<td>Smaller node size required</td>
</tr>
<tr>
<td><strong>Resource Limitations</strong></td>
<td>More resources than WBAN node due to the larger acceptable size</td>
<td>Smaller nodes support less bandwidth, low energy source, slower processing, and less memory size</td>
</tr>
<tr>
<td><strong>Accessibility</strong></td>
<td>Depends upon the operational area. Normally accessible. Easy node replacement</td>
<td>Wearable nodes accessible but implant sensors are not easily accessible. Surgery is required to access implant sensors</td>
</tr>
<tr>
<td><strong>Node Accuracy</strong></td>
<td>Redundant nodes help to compensate for the accuracy</td>
<td>Highly robustness and accuracy is required</td>
</tr>
<tr>
<td><strong>Operational Environment</strong></td>
<td>Stable to inaccessible. Can be extreme in weather or noise</td>
<td>Operational area is in, on or around a human body</td>
</tr>
<tr>
<td><strong>Mobility</strong></td>
<td>Mostly fixed or static nodes</td>
<td>Depends upon the mobility of a human body. Biological variations and complexity</td>
</tr>
<tr>
<td><strong>Context Awareness</strong></td>
<td>Not important due to the static nodes used in known environment</td>
<td>Required due to mobile nature of human body</td>
</tr>
</tbody>
</table>
1.2.2 Components of Wireless Body Area Network

The basic components of the WBAN are the same as architecture of different types of WSN and are shown in Figure 1.2.

![WBAN sensor node structure](image)

**Figure 1.3 WBAN sensor node structure**

- **Energy Source:** Generally, the size of the batteries limits the source of energy available to WBAN nodes. The tiny size of sensor node batteries allows very low power levels as compared to the larger batteries used in the WSN nodes.

- **Processor:** This is the brain of the sensor node. The processor handles all computations in the node. The MSP430 from Texas Instrument (TI) is an example of a processor used in some of the WBAN nodes (Jacobsen et al 2011). The world’s Ultra-low power MSP430 is a 16-bit microcontroller platform. The speed of this processor is 8MHz to 15 MHz (Milenkovic et al 2006) and the number of pins is 14 to 113.
• **Memory:** Different kinds of memories are used in WBAN. A typical WBAN node with MSP430 processor contains 128B to 64KB RAM and 0.5KB to 512KB Flash memory (Milenkovic et al 2006).

• **Transceiver:** The transceiver is used to send or receive the data from or to the node. Chipcon CC2420 is used for low power and low voltage wireless communication in a WBAN node (Lo et al 2005). The current consumption of receiver and transmitter of CC2420 are 19.7 mA and 17.4 mA respectively.

• **Sensors:** The sensing unit in the sensor node contains multiple sensors which are used to monitor the physiological or biochemical parameters of the disease processes in the human body. The Electro Cardio Gram (ECG) sensors determine the heartbeat rate and any damage to the heart. The sensing unit in Blood Pressure (BP) sensor measures the pressure of circulating blood on the blood vessels.

• **Actuators:** Actuators are used to take action after getting the data from the sensor or from the user. Actuators convert motion into energy or energy into motion. An actuator placed with a body sensor allows the healthcare professional to inject the insulin in case it is required for a diabetic patient.

• **Operating Systems:** TinyOS is used as the operating system in the WBAN node. TinyOS, a Berkeley Software Distribution (BSD) licensed open source operating system, is specifically designed for all kinds of WSN platforms. TinyOS is ideally suited to the WBAN nodes due to its special design for low-power devices (Farooq & Kunz 2011).
1.2.3 WBAN Standards

The WPAN protocols were commonly used for the implementations of WBAN communication before the development of WBAN standards. The important WPAN protocols are ZigBee (IEEE 802.15.4) and Bluetooth (IEEE 802.15.1) (Paul et al 2013; Johansson et al 2001). There are several candidate wireless technologies that can be used for WBAN Communications. The IEEE 802.15 Working Group was formed to develop the standards for WPANs or short distance wireless networks. The communication between the portable and mobile computing devices like Personal Computers (PCs), Personal Digital Assistants (PDAs), peripherals, cell phones, tablets, and consumer electronics devices are supported by WPAN standards. The IEEE 802.15 group is a sub-group of the 802 local and metropolitan area network standards committee of the IEEE computer society. One of the IEEE divisions, IEEE-SA, is responsible for the standardization of the new protocols. Important issues of WBAN data transmission are to ensure high reliability, low latency, compatibility with movable sensors and low energy consumption. The specific needs of WBAN communication are not fulfilled by the existing Personal Area Network (PAN) standards (Zhen et al 2011). The first BAN interest group (IG-BAN) was formed in a meeting held at Jacksonville, FL, USA, in May 2006. IEEE Task Group 6 was assigned a job in November 2007 to suggest a WBAN communication standard IEEE 802.15.6 by considering short range transmission, reliability and latency requirements of Quality of Services (QoS) and less energy consumption (Latré et al 2011).

1.3 HEALTHCARE PROJECTS USING WBAN

The advancement of WMSNs in healthcare applications have made patient-monitoring more viable. In recent times, numerous wireless healthcare researches and projects have been proposed, which aim to offer continuous
monitoring of patients, ambulatory monitoring, monitoring in hospital & clinic, and open environment monitoring (e.g., athlete health-monitoring). This section describes a few popular research projects about healthcare systems using WMSNs

1.3.1 CodeBlue

CodeBlue (Malan et al 2004; Lorincz 2004) is a popular healthcare project developed, based on a medical sensor network at the Harvard Sensor Network Lab. Its architecture includes several medical sensors, board onto the Mica2 motes (Kumar & Lee 2012), which are placed on the patient’s body. The patient’s body data are sensed by these medical sensors and transmit it wirelessly to the end-user devices (PDAs, laptops, and PC) for further analysis. The basic idea of CodeBlue is that a doctor or medical professional issues a query for patient health data using a PDA, which is developed based on a publish-and-subscribe architecture. The relevant data are published by the medical sensors to a specific channel, and the end-user subscribes the channel by using hand-held devices (e.g., PDA and laptop). A Tiny ADMR routing component, based on an adaptive demand-driven multicast routing (ADMR) protocol, is used for facilitating multicast routing, node mobility, and minimal path losses. In addition, the CodeBlue architecture provides RF-based localization; called MoteTrack (Lorincz & Welsh 2006), which is accurate enough to locate a patient’s or medical professional’s location. More significantly, CodeBlue’s authors admit the need of security in medical applications, but until now security is still awaiting or they intentionally left the security aspects for future work. CodeBlue is anticipated for deployment in pre-hospital and emergency care in hospital, rehabilitation of stroke patient, and disaster response.
1.3.2 Alarm-Net

Alarm-Net (Wood et al 2006) was specifically designed at the University of Virginia as a heterogeneous network for patient health monitoring in the assisted-living and home atmosphere as shown in Figure 1.4. Alarm-net includes body sensor networks and environmental sensor networks in its architecture. Network tiers of three levels are applied to the proposed assisted-living and home environment as shown in Figure 1.3. In the first tier, a resident wears body sensor devices to sense individual physiological information, and in the second tier, environmental conditions are sensed by deploying environmental sensors in the living space, such as temperature, dust, motion, light (i.e., MicaZ boards). An Internet protocol (IP)-based network is used in the third tier, which consists of Stargate gateways called AlarmGate. The idea of Alarm-net is that body sensors broadcast individual physiological data using a single hop to the nearest stationary sensor (i.e., second tier). Thereafter, the stationary emplaced sensor nodes forward the body data using multi-hop communication to the AlarmGate, which is a gateway between the wireless sensor and IP networks and is also connected to a back-end server. In addition, authors have developed a circadian activity rhythms program to aid context-aware power management and privacy policies.

Further Alarm-Net facilitates network and data security for environmental, physiological and behavioural parameters about the residents. The Alarm-Net can be accessed only by the authenticated users and can query the sensor networks. The Internet protocols (IP) network is secured by Secure Remote Password (SRP) protocol for user authentication. Link-layer security suites are enabled in the wireless sensor networks. Sensors like MicaZ and Telos use built-in cryptosystems.
The major drawback of the built-in cryptosystem is that it does not offer AES-based decryption, so that the encrypted data cannot be accessed by an intermediary node during communication, if required. Also, hardware-based built-in cryptosystem makes the application highly platform-dependent. Pai et al.(2008) have pointed out some confidentiality infringement scenarios on Alarm-NET, such as the reality that it is prone to adversarial confidentiality attacks, which can leak resident’s position.

1.3.3 UbiMon

UbiMon (ubiquitous monitoring environment for wearable and implantable sensors) (Ng et al 2004) is a WBAN architecture composed of wearable and implantable sensors (e.g., electrocardiography (ECG), saturation of peripheral oxygen [SpO2], and blood oxygen) by an ad-hoc network. The objective of the project is to provide continuous monitoring of an individual’s
physiological states and to capture transient as well as life-threatening abnormalities that can be detected and predicted as shown in Figure 1.5.

![UbiMon system architecture](image)

_Figure 1.5 UbiMon system architecture (Ng et al 2004)

Although Ng et al (2004) proposed and demonstrated the ubiquitous healthcare- monitoring architecture, it is broadly accepted that without considering security for such applications they are often vulnerable to security attacks. So this project did not consider security for wireless healthcare monitoring, which is a vital requirement of healthcare applications, according to the government laws (Meingast et al 2006).

### 1.3.4 MobiCare

MobiCare (Chakravorty 2006) provides a wide-area mobile patient monitoring system that facilitates continuous and timely monitoring of a patient’s physiological status. Similar to UbiMon, as shown in the Figure 1.6 the MobiCare system comprises of a WBAN having wearable sensors (e.g., ECG, SpO2, and blood oxygen), a WBAN manager called “MobiCare client is through IBM wristwatch,” and a back-end infrastructure (MobiCare server). The medical sensors sense the patient’s body data in a timely manner and
broadcast it to the MobiCare client. The body data is aggregated by the MobiCare client and sends them using a cellular link to the MobiCare server. The MobiCare server can support the medical staff for offline physiological analysis and for patient care. Although the security issues were acknowledged in MobiCare, addressing security issues alone are not sufficient for real-time healthcare applications. It is suggested that the Wireless Application Protocol (WAP), which is based on Wireless Transport Layer Security (WTLS) protocol could be used to provide the patient’s privacy, data integrity and authentication. Thus, security and privacy are still not implemented in MobiCare healthcare monitoring.

![MobiCare patient monitoring architecture](image)

**Figure 1.6 MobiCare patient monitoring architecture**

### 1.3.5 MEDiSN

MEDiSN, a health care system developed at Johns Hopkins University, was especially designed for patients’ monitoring in hospitals and during disaster events (Ko et al 2010). It comprises multiple physiological monitors (called PMs), which are battery-powered motes equipped with
medical sensors for collecting patients’ physiological health information (e.g., blood oxygenation, electrocardiogram signals, pulse rate, etc.) as shown in Figure 1.7. The PMs are movable and temporarily store sensed data and transmit it (after encrypting and signing the sensed data) to the relay points (RPs). MEDiSN incorporates different stationary RPs that are self-organized into a bidirectional routing tree and forwards PM data to the gateways and vice versa. The RPs uses a collection tree routing protocol (CTP) to forward their measurements to the gateway. Also, MEDiSN is connected with a back-end database that constantly stores medical data and delivers them to authenticated GUI clients. Particularly, this research focused on reliable communication, routing, data rate, and QoS.

![Figure 1.7 Healthcare architecture of MEDiSN](image)

MEDiSN project acknowledged the need for encryption for PMs, but it did not describe which cryptosystem has been used for data confidentiality and how they have checked the authenticity of the delivered data. Thus, although the security is provided to MEDiSN, information about security implementation is not revealed. Further, only authenticated clients
can access and control the sensor network at back-end server, but the type of authenticated protocol used is unknown. As a consequence, from a security perspective, MEDiSN project failed to provide detailed information about the security mechanisms.

1.3.6 SATIRE

Ganti et al (2006), designed and developed a wearable personal monitoring service project, called SATIRE, with the association of the University of Virginia and the University of Illinois. SATIRE permits users to maintain a private searchable record of their daily routine activities (e.g., measured by two motion and location sensors). A person wearing a SATIRE jacket can record his/her normal daily activities. When the person wearing a jacket comes into the vicinity of an access mote which is connected to a personal computer, the aggregated data is uploaded reliably to a private repository associated with that person. This data may be used to reconstruct the activities and locations of the person later. Although, security and privacy issues are addressed by SATIRE, security and privacy for sensitive physiological data are not implemented and considered for future work.

All the above healthcare-monitoring projects enable automatic patient monitoring and provide potentiated quality of healthcare without disturbing patient’s comfort. All the projects focus on the reliability, power consumptions of their prototypes and cost effectiveness, but even though most of the healthcare projects discussed above address the need for security and privacy for sensitive data (e.g., CodeBlue (Malan et al 2004; Lorincz et al 2004), MobiCare (Chakravorty 2006), STAIRE (Ganti et al 2006), only a few embed any security (e.g., ALARM-NET (Wood et al 2006), MEDiSN (Ko et al 2010), which is not sufficient for such critical applications. Hence, security and privacy have not been investigated in much depth, and challenges still remain for real-time wireless healthcare applications.
1.4 APPLICATION OF WBAN IN HEALTHCARE

According to the World Health Organization survey in 2005, the deaths of 17.5 million people were due to cardiovascular diseases. These deaths were the 30 percent of all the deaths during 2005. Currently 180 million people are found to be affected by diabetes worldwide and these numbers are expected to increase by the year 2030 to 360 million. More than 2.3 billion people will be overweight by 2015 (Patel & Wang 2010). The number of elderly people and chronic disease patients increase rapidly every year. The quality and quantity of healthcare services are also required to improve with respect to this increase. The most important application of WBAN is to monitor the patient’s medical data in the healthcare environment. The advancements of the medical field also bring new specialities of different areas in the healthcare. The continuous monitoring of the patient in indoor (hospital, home) and outdoor environments help physicians to get useful information that can be used in developing better treatment plans. Hospital, ambulatory, pre-operative, ER/Trauma units, Rescue, Maternity/Ob, and Nursing Homes are some of the healthcare environments where WBANs can be used.

1.4.1 Chronic Disease Patient Monitoring

Patients with a chronic diseases such as Cancer, Heart Disease, Stroke, Diabetes, Renal Failure, Vascular Diseases, Infectious Diseases, the formal procedure of routine visits is required to monitor the progress, development of complications or relapse of the disease. The choice of what to monitor, when to monitor, and how to adjust will affect the treatment plan. Poor choices can have a severe effect on the patient’s health. Specialized bio-sensors may be used to monitor the different physiological or biochemical parameters of different disease processes.
1.4.2 Elderly Patient Monitoring

As the world’s aging population is increasing at an extraordinary rate in the developed and developing countries. According to the “An Aging World: 2008” report (Zhen et al 2011), in 2008, the number of aging people worldwide (i.e., 65 years and older) was estimated at 506 million, and by 2040, that number is expected to touch 1.3 billion. Thus, the percentage of older age people will increase two times from 7% to 14% of the total world population in just over three decades (Zhen et al 2011). Even though a human success story of increased longevity is signified by the aging population, the steady and sustained growth of the older population also poses health challenges. When more and more people will be entering an elder age, the danger of developing certain chronic and debilitating diseases is significantly higher. For example, Alzheimer’s disease symptoms typically first appear after age 60, Heart disease, Diabetes, blood pressure and stroke rates rise after age 65 (Chen et al 2010). Further, if aged populations prefer to live alone they do however require long-term monitoring for better independent life (Khan et al 2013). Thus, the aging population desperately demands independent life and good quality-of-care without disturbing their comfort, but with their reduced care costs. In this context, wireless Body Area Network technology could provide cost effective, highly useful tools for elderly people’s health monitoring and patients who need continuous monitoring without disturbing their daily activities. Consequently, healthcare using wireless sensor networks constitutes an exciting and growing field for scientific exploration. In fact, the future of modern healthcare in an aging world will need ubiquitous monitoring of health with least actual interaction of doctor and patients (Khan et al 2012).
1.4.3 Hospital Patient Monitoring

Various levels of monitoring are necessary for the treatment of a patient in the hospital environment. The patient with stable conditions may require monitoring only four to six times per day in terms of measurement of vital physiological signs (blood pressure, ECG, heart rate, respiratory rate, and temperature), visual appearance (assessing their level of consciousness), and verbal response (asking them about the pain). The level of monitoring is very high for patients who are in an Intensive Care Unit (ICU). The monitoring of pre- and post-surgery is also very important. Different biosensors are used to monitor the different vital signs of a patient. Figure 1.8 shows the location of wearable sensors used with the human body. WBAN can be the most cost-effective solution for the continuous monitoring of a patient in the hospital environment.

![Figure 1.8 Location of wearable sensors on a human body](image-url)
1.5 SECURITY AND PRIVACY ISSUES

This section discusses: (i) which would be the possible threats to a wireless healthcare application without implementation of proper security and (ii) privacy issues. It is meaningful to assume the scale of deployment of healthcare applications using WMSNs before discussing the security issues in wireless healthcare applications. In this regard, three wireless healthcare scenarios are considered such as a nursing home care, home care monitoring, and monitoring in hospital, as shown in Figure 1.9.

Figure 1.9 Application scenarios for a nursing home, home care, and in-hospital

The wireless healthcare applications use medical sensors and environmental sensors (ES), mobile devices (i.e., PDA, laptop or iPhone), and more particularly wireless communication (i.e., IEEE 802.11, IEEE 802.15.4, Bluetooth etc.) protocols. Also, for physiological healthcare information (PHI) storage, and for offline analysis of PHIs, a back-end server is used. In
the nursing home scenario Figure 1.9 (left), medical sensors are placed on a patient’s body which sense the physiological data of an individual and transmit it in a timely manner to the PDA that may be held by a nurse. The patient’s sensors are queried by a nurse and analyze the real-time patient data conditions. Later nurse can send patient data to the central server either by using internet or through a wireless medium. Several ES, which are deployed in nursing homes, can form a wired or wireless network, sense the environmental parameters (e.g., ward temperature, humidity, etc.) and transmit the data to either a nurse or a distant center. Also, in an emergency situation the environmental sensors may forward an alarm to the remote server (e.g., suppose a severe condition is detected). In the home scenario, medical sensors are planted on a patient’s body that capture the health data from an individual and transmit it in a timely fashion to a PDA held by a nurse or family member. In addition, environmental sensors are necessary when a patient is usually alone at home. The environmental sensors are positioned at the corners of rooms, gathering the environmental conditions (e.g., room temperature, humidity, etc.), and patient movement data. Afterwards, they automatically send the collected environmental and patient’s abnormal conditions to the PDA which is held by either a nurse or a family member. Using Zigbee modules, the home local station can directly communicate with environmental sensors. To analyze the patient’s physiological information, an application program will be implemented at the back-end network. In the In-hospital scenario, the same deployment and sensing scenario (i.e., as in the nursing home and homecare scenarios) are now relevant to the hospital environment, where groups of patients are temporarily monitored using a wireless medical sensor network by nurses or physicians using their PDAs (Huang et al 2009).
1.5.1 Security Threats

As discussed in the above healthcare scenarios, WMSNs undoubtedly improve patient’s quality-of-care without disturbing their comfort. The medical sensor senses patient’s sensitive body data and transmits it over the wireless channels which are more susceptible than wired networks. Thus, patient’s sensitive physiological variables must remain secure and private from security threats. So the possible security threats that would be harmful for the wireless healthcare achievement are discussed, as follows:

- Monitoring and Eavesdropping on Patient Vital physiological Signs

  This is the most common threat to the patient’s privacy. By vital sign snooping of patient, an adversary can easily find out the patient information from communication channels. Furthermore, if the adversary has a powerful receiver antenna, then he/she can easily get the messages from the network. The physical location of the patient may be obtained from the captured message, allowing an attacker to locate the patient’s position and physically harm him/her. Also, an adversary can also detect the message contents such as message-ID, timestamps, source address, destination address and other related information. So, monitoring and eavesdropping can be a serious threat to patient’s privacy (Dimitriou & Loannis 2008; Chakravorty 2006).

- Threats to Information When in Transit

  As wireless communication ranges are not confined, they are easily vulnerable. In wireless healthcare applications, medical sensors sense the patient’s physiological and environmental data, and send them either to the physician or the hospital server. It may be attacked while sending the sensor’s
data (i.e., in transit). For example, an adversary can capture the physiological data from the wireless channels, and can alter the data. Later, he/she may pass the altered data to the physician or remote server, which could cause danger to the patient. There are different types of in-transit attacks: (i) Interception: Suppose, a WMSN has been compromised by a smart adversary, then he/she can illegally access the sensor node data such as cryptographic keys, sensor ID’s, type, etc. (ii) Message modification: In the message modification attack, the attacker can capture the patient’s wireless channels and extract the patient’s medical data; and later he/she may tamper with the patient data, which can mislead the involved users such as doctor, nurse, family member, etc. For example, suppose a cardiograph sensor transmits normal data to the medical staff, and if an attacker is able to modify the patient data during the communication and sends the modified data to medical staff, it may lead to an overdose of medicine being administered to the patient. Further, this modified data can generate a false alarm or can hide the true patient’s conditions, if abnormal. Message modification threatens the message integrity of medical sensor nodes.

- **Routing Threats in WSNs**

For the experimental scenario, consider the CodeBlue (Malan et al 2004) and MEDiSN (Ko et al 2010) architectures which need a multi-hop environment (i.e., one node to another node) from body sensors to a remote server. A malicious user could thus attack the network layer. An adversary may steal or modify the packets and forward the altered packets to the remote center (i.e., back-end) that may cause a false alarm. More specifically in the CodeBlue (Dimitriou & Loannis 2008) application, body sensors send their data using an ADMR routing protocol to the remote location (i.e., hospital). An attacker might modify the address fields of captured packets before forwarding them to the next hop, and therefore misguide the route or even
generate an endless routing loop (Kambourakis et al 2007). The routing attacks in a multi-hop environment are the following:

(i) **Selective forwarding**

In multi-hop environment (Malan et al 2004; Ko et al 2010; Huang et al 2009; Hande et al 2006), sensor packets (i.e., health data or environmental data) are expected to be forwarded to the base station or remote server via multi-hop routing. Malicious nodes may refuse to forward certain messages (e.g., ECG, temperature, etc.) in this threat, and may simply drop them, so that they cannot be broadcast further. If the attacker is explicitly included in the routing path, this threat can be stronger. Figure 1.10 illustrates an example; if an ECG sensor forwards packets, i.e., 1, 2, 3, 4... 10, to the next hop, but if a patient’s enemy deliberately captures and drops some ECG packets, and only forwards a few packets, i.e., 4, 5, 6, 8 and 10, to the remote location (Lo & Yang 2006), this could be life-threatening in a patient’s emergency condition. Further, Kambourakis et al (2007) pointed-out that the CodeBlue architecture is prone to grey-hole attacks. They claimed that if attackers modify the ADMR packet header of certain packets by small hop-count, they can make the adjacent nodes believe that the attacker is located in the shortest-path to the sink. Subsequently, the attacker can generously drop every packet, whatever he/she receives, which could cause life-threatening risks.

(ii) **Sinkhole threat:**

In this threat, an attacker tries to attract all neighbouring nodes to establish routes through a malicious node. Figure 1.11 illustrates a sinkhole attack; once the attacker is successful in the sinkhole attack, then the network is also open to other attacks (Lo & Yang 2006), for example, eavesdropping
or selective forwarding. Sinkhole attacks are very difficult to detect (Nasser & Chen 2007).

![Selectiv forwarding attack](image1)

**Figure 1.10 Selective forwarding attack**

![Sinkhole attack](image2)

**Figure 1.11 Sinkhole attack**

(iii) **Sybil Attack**

In this attack, a compromised node shows multiple fake identities to other neighbouring nodes in the network (Muraleedharan & Osadciw 2008). Figure 1.12 illustrates how the multiple fake identities of a compromised node
are sent to other neighboring nodes (Yang 2006). Also, Kambourakis et al (2007) state that the CodeBlue system is susceptible to Sybil attack, especially, when it operates in an ad-hoc manner (Misic et al 2007). The Sybil attack poses a major threat in geographic and multipath routing protocols, because the compromised node may emerge in more than one place (Karlof & Wagner 2003). There are more routing attacks in the framework of healthcare applications using sensor networks, e.g., sleep attack, fairness attack and wormhole attack (Muraleedharan & Osadciw 2008; Misic et al 2007).

**Figure 1.12 Sybil attack**

iv. Clone Attack

In this attack, an adversary extracts all information including identity, cryptographic keys of a benign node in the WSN and produces a large number of nodes same as benign nodes with same identity. These nodes are called clones. (Choi et al 2007; Parno et al 2005). Then, this adversary deploys these malicious clones into the network. These clones perform several attacks to the network. Figure 1.13 illustrates the clone/replication attack.
v. Masquerade and Replay Threats

In a home care application, an attacker can easily rogue a wireless relay point while patient data is being transmitted to the remote location. In general, wireless relay nodes are unguarded. So, it may happen that a rogue relay node can provide unrestricted access to an attacker who can then cause a masquerade. In this threat, an illegal relay node acts as a real node to the network. This can lead to false alarms to remote sites and an emergency team could start a rescue operation for a non-existent person. A masquerade node can apply easily denial-of-service attacks, and can disrupt the application operation. It can even defeat the purpose of wireless healthcare. Thus, masquerading nodes can be very dangerous for healthcare applications. More importantly, if a masquerade relay node captures the patient’s physiological data, later, these captured messages can pose replay threats to the real-time healthcare application. Obviously the patient treatment depends on freshly received messages from medical sensor networks. If masquerade nodes replay the old messages again and again, this could cause of mistreatment and
overtreatment (i.e., medicine overdose) to the patients. Thus, masquerade and replay threats endanger real-time healthcare applications using wireless medical sensors.

vi. Location Threats

Medical sensor networks support patient mobility. So, the exact patient location knowledge is needed since it allows reaching medical staff in a short time, in case of any emergency (Redondi et al 2010). Generally, location-tracking systems are based on radio-frequency (Lorincz & Welsh 2006), ultrasound, received signal strength indicator or some other technologies (Lorincz et al 2004). Curtis et al (2008) have used geopositioning to locate the patient and care-giver in their project called SMART (Scalable Medical Alert Response Technology). As the localization system is required for the patients and medical staff, if an adversary constantly receives the persons’ radio signals and analyzes them, then he/she would gain details of those persons’ locations, which could directly infringe a person’s privacy.

vii. Activity Tracking Threats

An adversary can obtain someone’s health status while he/she is busy, exercising in a health-club. Based on a sensor’s captured facts, a malicious user can deduce the current action of a patient and may propel the incorrect work out instructions to the patient that possibly will root them stern ache. In view of a further pattern, a sportsperson is being monitored using a wireless sensor network while he/she is working in the society (Baca & Kornfeind 2006). Medical sensors are located on the athlete’s body, which brain physical condition information, e.g., heart-rate, instance and site, and send health response to the base station (Alonso et al 2010). Hence, it might be likely for an opponent to adapt to the athlete’s health information, which
may bring the athlete under thought in doping tests that could even mess up the athlete’s profession.

viii. Denial-of-Service (DoS) Threats

Wood & Stankovic (2002) stated that “a denial-of-service attack is any event that diminishes or eliminates a network’s aptitude to execute its predictable purpose.” Denial-of-service threat could be even more troublesome in healthcare applications because such a network needs always-on patient health monitoring (i.e., in-home, in-hospital, ambulatory etc.). As DoS threats are destructive to every request, it could attempt to give many problems in each layer. A list of denial-of-service attacks is shown in Table 1.2.

Table 1.2 Denial-of-service attacks at each network layers

<table>
<thead>
<tr>
<th>Layers</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical layer</td>
<td>congestion, Node tampering</td>
</tr>
<tr>
<td>Link layer/medium access</td>
<td>conflict, exhaustion, and unfairness</td>
</tr>
<tr>
<td>control</td>
<td></td>
</tr>
<tr>
<td>Network and routing layer</td>
<td>Neglect and greed, homing, misdirection, spoofing, replaying, routing-control traffic or clustering messages</td>
</tr>
<tr>
<td>Transport layer</td>
<td>Flooding and De-synchronization</td>
</tr>
<tr>
<td>Application layer</td>
<td>Overwhelming sensors, reprogramming attack</td>
</tr>
</tbody>
</table>

a. Physical layer: congestion and tampering are the most common attacks on the physical layer. In congestion, generally, an invader can clutch the message using high radio frequency (RF) signals, which bother the network functionality. For example, medical sensor networks are small
networks that clutch early. Tampering is also known as a type of physical attack. A malicious user steals the medical sensor and automatically interrogates it to take out the patient information from the sensor mote.

b. Link/medium access control layer: This layer mainly suffers from conflict, collapse, and unfairness attacks. In conflict attacks, an opponent concurrently sends the packets at the same frequency, resulting in packet conflict and ruin of the network presentation. In exhaustion attacks the battery source is altruistic, since wireless motes most of the times maintain the guide active. In unfairness attacks, network presentation degrades because medium access control layer precedence is generally disrupted according to the function supplies.

c. The network and routing layer: Routing-disturbance attacks lead to DoS threats in multi-hop medical sensor surroundings. Generally, the routing attacks involve spoofing, changing routing paths or replaying packets, selective forwarding, sinkhole, warm-hole, etc.

d. Transport layer: It suffers mainly from two accepted types of attacks, namely, flooding attacks and de-synchronization attacks. Flooding attacks generally are used to exhaust the memory income by transferring the control signals. In de-synchronized attack, invader may disturbs the recognized connection between two lawful ends nodes (i.e., body sensor and base station) by re-synchronizing their broadcast. As a product, it disturbs network message and network income collapse (Wood & Stankovic 2002; Raymond & Midkiff 2008). DoS attacks may spoil the wireless healthcare function
network and can lead to the defeat of the patient’s life. Thus, these (DoS) attacks are always destructive to the mission-critical applications such as site tracking, ambulatory, home-care monitoring, etc. (Muraleedharan & Osadciw 2008; Wood & Stankovic 2002; Raymond & Midkiff 2008).

1.5.2 Privacy Issues

As wireless healthcare applications are not meant to monitor the patient’s physiological information alone, they also comprise urgent situation organization, healthcare information admission, electronic health account, etc. Further, folks contribute their information to physicians (in a doctor-patient association), cover companies (for insurance protraction), and health-coaches (as sports squad trainers) or to relations (as relatives’ hold up for revival). So, it is worth addressing the seclusion issues that are moral from the communal point of view. National Committee for Vital and Health Statistics (NCVHS), the consultative board of the United States Department of Health and Human Services, says “Health information privacy is an individual’s right to control the acquisition, uses, or disclosures of his or her identifiable health data. To sustain solitude, patients should have the rights to decide which information should be composed, used or disclosed. Any unofficial compilation or outflow of patient information could damage the patient. For example, an unofficial person may use the patient’s information (such as, patient identity) for his/her individual advantage, such as for medical scam and deceptive indemnity claims, that sometimes may even pose critical risks. As the medical data is very sensitive, who owns medical information, and how to manage the admittance to medical statistics are important factors for consideration. Further, in wireless healthcare applications, huge quantity of health and lifestyle statistics are collected that need secure awareness to who wheel it, what is collected, who has rights to contact it and where/how/whether that statistics
is stored or not (Brown & Adams 2007). Mingiest et al (2006) have raised alike questions concerning patient solitude: (i) Who can have authorization to possess the statistics; (ii) what type of medicinal facts, how much, and where the facts should be composed; (iii) who can have authorization to examine the medical facts; and (iv) to whom the medical facts should be exposed to without the patient’s approval. Ramli et al (2010) have discussed the privacy threats that hoist questions about healthcare achievement: Identity threat: if a patient loses or allocate his/her uniqueness that can sham major economic, bodily and touching damage to a human being. An insider may use patient’s individuality for their personal advantage, e.g., he/she may abuse the uniqueness to get compensation (insurance claims) or abuse the uniqueness to get medical services. Access threats: Generally a patient is self-concerned in the access threats, if he/she fails to communicate their approval correctly. For example, in the absence of patient approval, an insider may spoil the patient’s information and hurt the patient for their personal reasons. In a patient medical proof scheme, insiders may change the medical report deliberately. For example, an insider may imperfectly alter the patient’s medical statistics such as infirmity situation, severe allergies, and purposely blood nature, all of which being front-grave risks (Kotz 2011). Ramli et al (2010) have reviewed the solitude issues in an enveloping healthcare monitoring scheme and recognized a few solitude issues in enveloping healthcare such as abuse of medical information, outflow of prescriptions, eavesdropping on medical data, and social implications for the patient. Misuse of medical information: The patient health data flows on a wireless guide and therefore, it is released to all the wireless threats like eavesdropping and snooping. Thus, patient solitude could be breached if an unauthorized person captures the wireless facts and misuse them (Ramli et al 2010). Leakage of prescriptions: The medical prescription can be a big basis of privacy violations. For example, to move or trade the prescription facts from pharmacy/doctor to third parties, since the medical prescriptions hold full order concerning a patient, i.e., name,
credentials, diseases, etc. (Ramli et al 2010; Kosseim & Emam 2009) . Thus, the outflow of prescription facts becomes a privacy subject. Eavesdropping on patient medical information: Patient’s medical information drifts on the wireless links, so that it can be easily monitored. The monitoring system reports patient data from communication channels and extracts the pricey private patient information. Thus, eavesdropping is very simple for an attacker, while the patient data is transmitted from the Wireless Body Area Network to the care-giver device. Hence, the patient privacy is breached. Social implications for the patient: Another privacy problem concerns the social implications, where a patient aged 65 and above, for instance, is not able to make decisions for his/her own solitude, particularly if he/she suffers from dementia, a condition characterized by the loss of mental skills that affects every-day life.

This part has shown that security and privacy issues directly influence patient’s life and the healthcare system, if there is any dodge in the application security. So, it is required to explore that robust security should be measured from the start of the application plan. In addition, as the security and privacy issues could breach patient’s physiological information, there is a need for rigorous directions and laws that can act to permit scrupulous standards for shielding the patient’s sensitive information.

1.6 THREAT MODEL IN WMSN

The Figure 1.14 gives the detailed categorization of security attacks on WMSN. The attacks are classified in view of the various aspects like scratch level, position, type of tool and function (Mohammadi & Jadidoleslamy 2011).
Figure 1.14 Classification of attacks on wireless sensor networks on different bases

1.6.1 Attacks based on Damage/Access Level

Here are presented the classifications of WMSNs’ physical layer attacks based on their smash-up level or attacker's access level.

i. **Active attacker:** This attacker does operations such as:

   - Injecting defective facts into the WMSN.
   - Impersonating
   - Packet change
   - Unauthorized admission, observe, eavesdrop and changing resources and information flow
   - Creating hole in security protocols
   - Congestion in the WMSN.
• The WMSN functionality interruption.
• The WMSN presentation degradation.
• Sensor nodes damage.
• Data modification.
• Incapability in utilizing the WMSN services.
• Obstructing the operations or to cut off definite nodes from their neighbours.

ii. **Passive attacker:** Passive attacker may do following functions:

• Attacker is similar to a usual node and gathers information from the WMSN.
• Monitoring and eavesdropping from communication channel by unauthorized attackers.
• Performing logically against privacy.
• Eavesdropping, gathering and stealing information
• Compromised privacy and discretion requirements.
• Storing energy by self-centred node and to avoid from cooperation.
• The WMSN functionality degradation.
• Network separation by non-cooperate in operations.
1.6.2 Attacks based on Attacker Location

Attacker can be deployed inside or outside the WSN, if the attacker is into the WMSN's choice, called insider (internal), and if the attacker is deployed out of the WMSN's choice, called outsider (external). The WMSN link layer attacks based on attacker’s position are including:

i. **External attacker (outsider):** Some of the most familiar features of this type of attack are:
   - External to the network (from out of the WMSN range).
   - Device: Mote/Laptop class.
   - Dedicated by illegally parties.
   - Initiating attacks without even being legitimate
   - Congестing the entire communication of the WMSN.
   - WSN's property consumption.
   - Triggering DoS attacks

ii. **Internal attacker (insider):** The meaning of insider attacker is:
   - Sourced from inside of the WMSN and access to all other nodes within its range.
   - Authorized node in the WMSN is malicious / compromised.
   - Executing wicked information or use of cryptography filling of the legitimate nodes.
- Legitimate unit (authenticated) compromising a number of WMSN nodes.
- Access to cryptography keys or other WMSN codes
- Enlightening secret keys
- An elevated threat to the functional efficiency of the whole collective network.

1.6.3 Attacks based on Attacking Devices

Attackers can use different types of devices to assault to the WMSN; these devices have different power, radio antenna and other capabilities. There are two general categories of them, including:

i. **Mote-class attacker**: Mote-class attacker is every one that using devices similar to common sensor nodes and this means:

- Happening from inside the WMSN.
- Using WMSN nodes (compromised sensor nodes) or access to similar nodes/motes (which have similar functionality as the WMSN nodes).
- Executing malicious codes/programs
- Congestion in radio link.
- Stealing and access to cryptography keys

ii. **Laptop-class attacker**: Laptop-class attacker is every one using more influential devices than regular sensor nodes, including:
• Using more powerful devices by attacker, thus access to high bandwidth and low-latency statement channel.

• Traffic inoculation (Karlof & Wagner 2003).

• Passive eavesdrop (Krontiris et al 2007) on the entire WMSN by a single laptop-class device.

• Replacing legitimate nodes.

• Launching more serious attacks and then leading to more serious harm.

• Jamming radio links on the WMSN completely (by using more powerful transmitter).

• Access to high bandwidth and low-latency statement channel.

1.6.4 Attacks based on Function (Operation)

Link layer attacks in WMSNs have been classified into three types, based on their main functionality and they include:

i. Secrecy: Its definition and techniques are:

• Operating stealthy on the communication channel.

• Eavesdropping.

• Packet replay, spoofing or modification.

• Injecting false data into the WMSN

• Passive eavesdrop.

• Packet replication, spoofing or modification.
ii. **Availability:** This class of attack known as Denial-of-Services (DoS) attacks which leads to WMSN unavailability and degrade the WMSN presentation. Some of the most common goals and effects of this attack group are the following:

- Performance degradation.
- The WSN services destruction/disruption.
- The WMSN services useless/unavailable.

iii. **Stealthy:** This kind of attack is operating stealthy on the communication channel such as:

- Eavesdropping.
- False data injection into the WMSN.
- Partial/entire degradation/disruption of the WMSN services and functionality.

### 1.7 EFFECTS OF LINK LAYER ATTACKS ON WMSNs

WMSNs are intended in layered form. This layered architecture makes these networks susceptible and leads to damage against many kinds of attacks. For each layer, there are some attacks and defensive mechanisms. Thus, WMSNs are vulnerable against diverse link layer attacks, such as DoS attacks, Collision, unfairness and other attacks to link layer protocols (Sharma & Ghose 2010; Zhou et al 2008). WMSNs are susceptible to relation layer attacks. Attackers can gain access to transmission media, create radio intrusion, prevent from lawful sensor nodes to communicate/transmit (access to the communication channel) or launch DoS attacks against link layer. Now, Table 1.3 presents the definitions of link layer attacks on WMSNs, and it classifies and compares them to each other based on their strategies and effects.
Table 1.3 Link layer attacks on WSNs

<table>
<thead>
<tr>
<th>Attack/Criteria</th>
<th>Attack Definition</th>
<th>Attack Techniques</th>
<th>Attack Effects</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Node outage</strong></td>
<td>• Stopping the functionality of WSN workings, such as a sensor node or a cluster-leader</td>
<td>• Physical</td>
<td>• Stop nodes' services;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Logical</td>
<td>• Take over/compromise the partial/entire WSN and prevent from some communication;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Unfeasibility of reading gathered information;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Launching other attacks;</td>
</tr>
<tr>
<td><strong>Link layer jamming</strong></td>
<td>• Finding data packet and to squashing it (Znaidi et al 2008)</td>
<td>• Looking at the prospect distribution of the inter-arrival times between all types of packets;</td>
<td>• Colliding packets during transmission;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• This attack can be applied on S-MAC, B-MAC and L-MAC protocols (Znaidi et al 2008);</td>
<td>• Exhausting nodes resources;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Confusion;</td>
</tr>
<tr>
<td><strong>Denial of Service (DoS) attacks</strong></td>
<td>• A general attack includes several types of attacks in different layers of WSN, simultaneously (Wood &amp; Stankovic 2002);</td>
<td>• Physical layer, link layer, routing layer, transport layer and application layer attacks techniques;</td>
<td>• Effects of physical layer, link layer, routing layer, transport layer and application layer attacks;</td>
</tr>
<tr>
<td>Attack/Criteria</td>
<td>Attack Definition</td>
<td>Attack Techniques</td>
<td>Attack Effects</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Collision          | • Message transmission by two nodes on a same frequency (Znaiidi et al 2008; Zia 2008) concurrently;  
• There are two types of collision: environmental and probabilistic collision; | • Environmental collision;  
• Probabilistic collision;  
• Verifying and isolate radio transmissions;  
• Change packet's fields;  
• Alter the ack message; | • Interferences (Znaiidi et al 2008);  
• Data/control packets corruption /cripple (Znaiidi et al 2008);  
• Discarding packets;  
• Energy exhaustion;  
• Cost effective; |
| Resource Exhaustion| • Repeated collisions and continuous retransmission until the sensor node fatality(Znaiidi et al 2008); | Continuously retransmission;  
• Interrogation attack (RTS/CTS);  
• Message modification;  
• Ack corruption/change; | • Resources exhaustion;  
• Compromise accessibility; |
| Desynchronization   | • Disrupting the established connections between two lawful nodes by re-synchronizing their transmission; | • Sending frequently forged or false messages;  
• Re-synchronizing transmissions; | • Disrupt communication;  
• Go out the synchronization;  
• Resource collapse; |
Table 1.3 (Continued)

<table>
<thead>
<tr>
<th>Attack/Criteria</th>
<th>Attack Definition</th>
<th>Attack Techniques</th>
<th>Attack Effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic manipulation</td>
<td>• Usual monitoring transmissions and computing some parameters based on the affected MAC protocol carefully transmitting messages just at the moment when normal nodes do so; • Similar to Collision attack;</td>
<td>• Regular monitoring of the communication channel and computing require parameters; • Misusing from the wireless nature of communications in WSNs; • Disobeying the coordination rules of MAC schemes in use; • Collision attack techniques; • Unfairness attack techniques; • Continuously collisions and unfairness;</td>
<td>• Excessive packet collisions; • Artificially increased contention; • Decreasing signal quality and network availability; • Aggressively competition for channel usage; • Break the protocols' operations; • Unfair bandwidth usage; • Degradation of the WSN performance; • Traffic distortion; • Effects of collision and unfairness attacks; • Confusion;</td>
</tr>
<tr>
<td>Unfairness</td>
<td>• Partial DoS attack; • Using other attacks such as collision and exhaustion continuously;</td>
<td>• Intermittent application of collision and exhaustion attacks; • Misusing/abusing a cooperative MAC-layer priority mechanism; • Continuously request to access to channel by attacker;</td>
<td>• False view/information of the WSN; • Launch selective forwarding attack; • Packet loss/corruption;</td>
</tr>
<tr>
<td>Attack/Criteria</td>
<td>Attack Definition</td>
<td>Attack Techniques</td>
<td>Attack Effects</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------</td>
<td>------------------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
| Sinkhole        | • A special selective forwarding attack;  
|                 | • More complex than black hole attack;  
|                 | • Attracting (Zia 2008; Padmavathi, & Shanmugapriya 2009) or drawing all the possible network traffic to a compromised node by placing a malicious node closer to the base station (Krontiris et al. 2007) and enabling discriminating forwarding;  
|                 | • Centralizing traffic into the malicious node  
|                 | • Possible scheming another attack during this attack;  
|                 | • Sinkhole detection is very hard; | • Luring (Sharma & Ghose 2010) or compromising nodes (Karlof & Wagner 2003);  
|                 | | • Tamper with application data along the packet flow path (selective forwarding);  
|                 | | • Receiving traffic and altering or fabricating information (Krontiris et al. 2007);  
|                 | | • Identity spoofing for a short time;  
|                 | | • Using the communication prototype;  
|                 | | • Creating a large sphere of manipulate;  
|                 | | • Based on used routing protocol: Mint Route or Multi Hop LQI protocol;  
|                 | | • Luring and to attract almost all the traffic;  
|                 | | • Triggering other attacks such as eavesdropping, trivial selective forwarding, blackhole and wormhole;  
|                 | | • Usurp the base station position;  
|                 | | • Message modification;  
|                 | | • Information fabrication and packet dropping;  
|                 | | • Suppressed messages in a certain area;  
|                 | | • Routing information modification/fake;  
<p>|                 | | • Resource exhaustion; |</p>
<table>
<thead>
<tr>
<th>Attack/Criteria</th>
<th>Attack Definition</th>
<th>Attack Techniques</th>
<th>Attack Effects</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Eavesdropping</strong></td>
<td>• Detecting the filling of communication by overhearing/stealthy crack to data; • Abusing of wireless nature of WSN transmission medium; • Using powerful resources and strong devices, such as powerful receivers and well-intended antennas;</td>
<td>• Interception; • Abusing of wireless nature of WSN transmission medium; • Using powerful resources and strong devices, such as powerful receivers and well-intended antennas;</td>
<td>• Launching other attacks (wormhole, blackhole); • Extracting sensitive WSN information; • Delete the privacy defence and reducing data Confidentiality</td>
</tr>
<tr>
<td><strong>Impersonation</strong></td>
<td>• Wicked node impersonates a cluster leader and lures nodes to a mistaken position; • Impersonating a node within the path of the data flow of attacker's interest by modifying routing data or implying itself as a trustworthy communication partner to neighbouring nodes in parallel;</td>
<td>• The WSN reconfiguration; • Admission to encryption keys and authentication information; • Man-in-the-middle attack and fake MAC addresses; • Node replication • Physical access to the WSN; • False or malicious node attack techniques; • Sybil attacks techniques; • Misdirection/misrouting; • Changing routing information; • Luring/convince nodes;</td>
<td>• Routing information modification; • False sensor readings; • Making network congestion or collapse; • Disclose secret keys; • Network partition; • False and misleading messages generated; • Resources exhaustion; • Degrade the WSN performance; • Invasion; • Carrying out further attacks to disrupt operation of the WSN; • Confusion and takes over the entire WSN;</td>
</tr>
</tbody>
</table>
Table 1.3 (Continued)

<table>
<thead>
<tr>
<th>Attack/Criteria</th>
<th>Attack Definition</th>
<th>Attack Techniques</th>
<th>Attack Effects</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wormholes</strong></td>
<td>• Tunneling (Zia 2008; Karlof &amp; Wagner 2003) and duplicating messages from one location to another through alternative low latency links (Sharma &amp; Ghose 2010; Zhou et al 2008) that connect two or more points (nodes) of the WSN with fast communication medium (Khokhar et al 2008) (such as Ethernet cable, wireless communication or optical fibre), by colluding two active nodes (laptop-class attackers (Sharma &amp; Ghose 2010) in the WSN, by using more powerful communication resources than normal nodes (Xing et al 2005; Maheshwari et al 2007) and establishing improved real communication channels (tunnel); • Wormhole nodes operate fully invisible (Maheshwari et al 2007)</td>
<td>• Compromising/luring nodes (Sharma &amp; Ghose 2010) with false and fake routing information; • An attacker locates between two nodes and forwards messages between them; • Using out-of-band or high bandwidth Fast (Khokhar et al 2008) channel; • Wormholes may be used along with Sybil attack; • This attack may combine with selective forwarding or eavesdropping;</td>
<td>• Routing disruption /disorder (false routes, misdirection and forged routing); • False/forged routing information; • Confusion and WSN disruption; • Enable other attacks; • Exploiting the routing race conditions; • Change the network topology; • Prevention of path detection protocol; • Packet destruction /alteration by wormhole nodes; • Changing normal messages flow;</td>
</tr>
</tbody>
</table>
1.8 REGULATIONS AND LAWS

1.8.1 Legislated Requirements

Privacy of medical information is a very important requirement as the information has a large potential for abuse. To address the issue of privacy and security the United States, Canada and many other countries have developed legislative requirements on how the data can be handled by the organizations that need access to the information. Many different organizations need information related to MSNs that are deployed with patients. The clinicians, pharmacies and health care providers each need some, if not all, of the telemetry that is received from the sensors. Insurance providers need to know which MSN has been deployed with what sensor types and what billable actions have been taken with the system. Researchers need a variety of information collected to be able to conduct research and increase knowledge and positive outcomes of clinical care. Public health organizations may need information collected to understand if there is a public health issue in an area.

1.8.2 Health Insurance Portability and Accountability Act (HIPAA)

The United States passed legislation dealing with patient information that requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. HIPAA required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. There are two rules that are the foundation of the legislation, the Privacy Rule and the Security Rule. The Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that
information while still permitting the disclosure of personal health information needed for patient care and other important purposes.

The patient has rights related to the health information collected and can request to see a copy of the health records. Patients can have corrections added to their health information, receive a notice that tells them how their information is used and shared, decide whether to give permission before information can be used or shared for certain purposes and get a report on when and why the health information was shared. The entities covered under the law must teach the people who work for them how patient information may or may not be used and shared and they must take appropriate and reasonable steps to keep your health information secure.

The Security Rule establishes national standards for protecting the integrity, confidentiality and availability of electronic protected health information (e-PHI). The requirements state that entities must ensure the confidentiality, integrity and availability of all e-PHI they create, receive, maintain, or transmit. They must identify and protect against reasonably anticipated threats to the security or integrity of the information. They must protect against reasonably anticipated, impermissible uses or disclosures. They must also ensure compliance by their workforce. The technical safeguards that are required are Access Control, Audit Controls, Integrity Controls and Transmission Security.

1.8.3 Personal Information Protection and Electronic Documents Act (PIPEDA) and Other Relevant Laws

Canada passed legislation that governs how organizations collect, use and disclose personal information in the course of business. Unlike the American legislation, PIPEDA applies to all organizations that have access to personal information for commercial purposes. This requirement makes
hospitals exempt from many of the regulations but physicians’ commercial activities and private practice is covered under the law. Private group homes are also covered under PIPEDA and need to meet the requirements. There are laws that apply to hospitals and other primary care facilities on a provincial basis such as the Personal Health Information Protection Act (PHIPA) and the Freedom of Information and Protection of Privacy Act (FIPPA) in Ontario. PIPEDA requires that all organizations receive consent for collection of information, except in a few specific limited circumstances. The information can only be used or disclosed for the purposes for which consent has been given. Even with consent, the collection, use and disclosure must be limited to purposes that a reasonable person would consider appropriate under the circumstances. The law also requires that individuals have a right to see the personal information and the ability to correct any inaccuracies. The acts that relate to hospitals in the different provinces have many of the same requirements as stated in PIPEDA. PIPEDA and the other laws generally require that safeguards be put in place to protect personal information against loss, or theft. The information must be protected from any unauthorized access, disclosure, copying, use or modification. The information must be protected regardless of the format in which it is held.

The HITECH Act includes provisions to enlarge the use of information technology (IT) to store, capture, transmit, properly share and use health data. It introduces the new Act that states that those who manage patient’s health information (PHI) should notify the affected individuals if there is any breach that discloses their PHI.

Although the involvement of wireless technology and Internet access are providing a low-cost communication infrastructure that is suitable for home care monitoring, ambulatory monitoring, hospital and clinical monitoring, and so on. It should also be considered that in some special cases
such as medical emergencies and disaster medical management, there may a need to disclosure the patient information with many people involved in the rescue activities. Therefore, the regulations should have some flexibility and the users also have to compromise with their privacy to some extent. The next section discusses the existing security mechanisms that can provide security to wireless healthcare applications and ensure patient’s privacy.

1.9 SECURITY MECHANISMS

Security mechanisms are the processes that are used to detect, prevent and recover from security attacks. Although there are significant security mechanisms for traditional networks (i.e., wired and ad hoc), they are generally not directly applicable to resource constrained wireless medical sensor networks. So, this sub-section discusses the issues concerning existing security mechanisms, as follows:

1.9.1 Cryptography

As wireless medical sensor networks deal with sensitive physiological information, the strong cryptographic functions (i.e., encryption, authentication, integrity, etc.) are paramount requirements for developing any secure healthcare application. These cryptographic functions provide patient privacy and security against many malicious attacks. Strong cryptography requires extensive computation and resources, and therefore selecting appropriate cryptography is a challenging task for resource-hungry medical sensor nodes that can provide maximum security whilst utilizing the minimum resources. Further, the selection of cryptography system depends on the computation and communication capability of the sensor nodes. Some argue that asymmetric crypto systems are often too expensive for medical sensors and symmetric crypto systems are not versatile enough (Le et al
However, applying the security mechanisms to resource-constrained medical sensors should be selected based on the following considerations:

- **Energy**: how much energy is needed to perform the crypto functions.
- **Memory**: how much memory (i.e., read only memory and random access memory) is needed for security mechanisms.
- **Execution-time**: how much time is required to execute the security mechanisms.

### 1.9.2 Key Management

Key management protocols are fundamental requirements to develop a secure application. These protocols are used to set up and distribute various kinds of cryptographic keys to nodes in the network. Generally, there are three types of key management protocols such as trusted server, key pre-distribution and self enforcing (Ng et al 2006; Shaikh et al 2006). (i) Trusted server protocols rely on a trusted base station responsible for establishing the key agreement in the network. It is considered that the trusted server protocols are well-suited to hierarchical networks in the presence of unlimited resource gateways. Although, trusted server-based schemes provide stronger security to hierarchical networks, in a real-time environment, a trusted server could become a single point for the entire network failure. Hence, they are not suitable for critical applications (e.g., healthcare) (Ng et al 2006). (ii) Key pre-distribution protocols are based on symmetric key cryptography, where secret keys are stored in the network before the network deployment. The key pre-distribution protocols are easy to implement and offer relatively less computational complexity, making them more suitable for resource-constrained sensor networks. (iii) Self-enforcing protocols using a public-key infrastructure provide many advantages such as strong security, scalability,
and memory efficiency. Earlier public key based solutions were thought to be too computationally expensive (i.e., RSA and Diffie-Hellman key exchange (Ebrahim et al 2013)) for wireless sensor networks. However, some researchers (Malasri & Wang 2009; Seo 2009; Malasri & Wang 2006) have shown that Elliptic curve cryptographic based schemes are viable on resource-constrained networks. In fact, in real-time implementation, the ECC based necessary cryptographic primitives (e.g., signature generation and verification) are still expensive in term of the time complexity.

1.9.3 Secure Routing

In home care or disaster scenarios, sensor devices might require sending their data to other devices outside their immediate radio range (Lorincz et al 2004). Therefore, routing and message forwarding are a crucial service for end-to-end communication. So far, numerous routing protocols have been proposed for sensor networks, but none of them have been designed with strong security as a goal (Nasser & Chen 2007; Chen et al 2009). Karlof & Wagner (2003) discussed the fact that routing protocols suffer from many security vulnerabilities such as an attacker might launch denial-of-service attacks on the routing protocol. An attacker could also inject malicious routing information into the network, resulting in inconsistencies in the routing. Further, most of the current proposals are designed for static wireless sensor networks but mobility has not been taken into consideration, whereas healthcare applications require mobility- supported routing protocols. In addition, designing secure routing protocols for mobile networks is a complex task and current WMSNs healthcare security requirements will make it more complex when they become real-time applications.
1.9.4 Resilience to Node Capture

Resilience against node capture is one of the most challenging problems in sensor networks. In real-time healthcare applications, the medical sensors are placed on a patient’s body, whereas, the environmental sensors are placed on hospital premises (e.g., ward room, operation room etc.) which may be easily accessible to attackers. Thus, an attacker might be able to capture a sensor node, get its cryptographic information and alter the sensor programming accordingly. Later, he/she can place the compromised node into the network, and that could endanger application success. The current cryptographic functions (i.e., node authentication and identification) may detect and defend against node-compromised attacks to some degree, but these compromised node attacks cannot be detected instantly (Kavitha & Sridharan 2010), which is a big issue for healthcare applications. For example, consider the case of a false alarm. One possible solution to prevent this attack is to use tamper-resistant hardware. However, tamper-resistant hardware is not a cost effective solution.

1.9.5 Secure Localization

WMSNs facilitate mobility for patient’s comfort. Therefore, patient location estimations are needed for the success of healthcare applications. Since, medical sensors sense physiological data of an individual, they also need to report the patient’s location to a remote server. As a result, medical sensors have to be aware of patient’s location, i.e., called localization. Boukerche et al (2008) discussed localization systems, which were divided into: distance/angle estimation, position computation and localization algorithms, and further, they discussed attacks on localization systems. Chen et al (2009); Kavitha & Sridharan (2010) argue that mobility supported secure localization protocols still need to be explored.
1.9.6 Trust Management

Trust signifies the mutual association of any two trustworthy nodes (i.e., sensor node and data aggregator node), that are sharing their information (Boukerche & Ren 2009). Trust is defined as “the degree to which a node should be trustworthy, secure, or reliable during any interaction with the node”. Wireless healthcare applications depend on distributed cooperation among the network nodes. The key aspect of healthcare applications is a trust evaluation on the behaviour of a node (i.e., data delivery and quality). So, trust management systems are useful to detect the degree of trust of a node. Boukerche & Ren (2009) evaluated the trust for mobile healthcare system. However, trust management must still be implemented in real-time healthcare application using WMSNs, to ensure a clearer picture of trustworthiness of the parties i.e., medical sensors, etc. involved.

1.9.7 Robustness to Communication Denial-of-Services

An attacker attempts to disrupt the network operation by broadcasting high-energy signals. If the broadcasting is powerful enough, then the entire network communication might be jammed. Other attacks are also possible. For instance, an adversary may delay communication by violating the medium access control protocol. Moreover, an adversary can transmit packets while a neighbour node is also transmitting. Raymond & Midkiff (2008) have discussed the details of DoS attacks and their countermeasures at different layers of WSN routing. Most of the DoS countermeasures are suitable for static wireless sensor networks, as shown in Table 1.4. Since the WMSN healthcare applications are mobile in nature, as a result, secure DoS attack counter measures still need a further investigation for real-time healthcare application using WMSNs.
Table 1.4 Denial-of-Service attacks and countermeasures at each network layer

<table>
<thead>
<tr>
<th>Network Layer</th>
<th>Attacks</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical layer</td>
<td>Jamming</td>
<td>Detect and sleep, route around jammed areas</td>
</tr>
<tr>
<td></td>
<td>Node tampering</td>
<td>Temper-proof boxing</td>
</tr>
<tr>
<td>Link layer/medium access control</td>
<td>Collision, unfairness</td>
<td>Authentication and anti-replay protection</td>
</tr>
<tr>
<td></td>
<td>Denial of sleep</td>
<td>Authentication and anti-replay, detect and sleep, broadcast attack protection</td>
</tr>
<tr>
<td>Network and routing layer</td>
<td>Neglect and greed, misdirection, spoofing, replaying, routing-control traffic or clustering</td>
<td>Authentication and anti-replay protection, Secure cluster formation</td>
</tr>
<tr>
<td></td>
<td>Homing</td>
<td>Header encryption and dummy packets</td>
</tr>
<tr>
<td></td>
<td>Hello floods</td>
<td>Pair-wise authentication, geographic routing</td>
</tr>
<tr>
<td>Transport layer</td>
<td>Flooding</td>
<td>SYN cookies</td>
</tr>
<tr>
<td></td>
<td>De-synchronization</td>
<td>Packet authentication</td>
</tr>
<tr>
<td>Application layer</td>
<td>Overwhelming sensors</td>
<td>Sensor tuning, data aggregation</td>
</tr>
<tr>
<td></td>
<td>Reprogramming attack</td>
<td>Authentication and anti-replay protection</td>
</tr>
<tr>
<td></td>
<td>Path-based DoS</td>
<td>Authentication streams</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Authentication and anti-replay protection</td>
</tr>
</tbody>
</table>
There are tremendous robust security mechanisms but these mechanisms are not directly applicable to healthcare applications where resource-constrained devices are used. Consequently, the security gap between the above securities measures still needs to be explored for healthcare applications.

1.10 SECURITY AND PRIVACY REQUIREMENTS FOR WIRELESS MEDICAL SENSOR NETWORKS

Based on the above application scenarios, security issues and regulatory laws, this section points out the paramount security and privacy requirements for healthcare applications using wireless medical sensor networks, as follows:

(1) Data confidentiality: Patient health data are generally held under the legal and ethical obligations of confidentiality. These health data should be confidential and available only to the authorized doctors or other care-givers. Thus, it is important to keep the individual health information confidential, so that an adversary cannot eavesdrop on the patient’s information. Data eavesdropping may cause damage to the patient because the adversary can use the patient’s data for many illegal purposes and hence, the patient’s privacy is breached. Therefore, data confidentiality is an important requirement in healthcare applications using WMSNs.

(2) Data authentication: Authentication services provide authorization which is necessary for both medical and non-medical applications. In WMSN healthcare applications, authentication is a must for every medical sensor and the base-station to verify whether the data were sent by a trusted sensor or not.
(3) Strong user authentication: The major problem in a wireless healthcare environment is vulnerability of wireless messages to an unauthorized user. So, it is highly desirable that strong user authentication should be considered, whereby each user must prove their authenticity before accessing any patient’s physiological information. Furthermore, strong user authentication, also known as two-factor authentication, provides greater security for healthcare applications using wireless medical sensor networks.

(4) Data integrity: Data integrity services guarantee at the recipient end that the data has not been altered in transit by an adversary. Due to the broadcast nature of the sensor network, the patient’s information could be altered by an adversary; this could be very dangerous in the case of life-critical events. To verify the data integrity, one must have the ability to identify any data manipulation done by illegal parties. Thus, proper data integrity mechanisms ensure that the received data has not been altered by an adversary.

(5) Key distribution: If two parties exchange information, they must share a session key and that key must be protected from others. A secure session key helps secure subsequent communication and safeguards data against various security attacks. Thus, in order to preserve the patient’s privacy, an efficient key distribution scheme is a major requirement in wireless healthcare applications (Misic & Misic 2008).

(6) Access control: In healthcare applications many users (e.g. doctors, nurses, pharmacists, insurance companies, lab staff, social workers, etc.) always directly deal with the patient’s
physiological data. So, it is highly desirable that a role-based access control mechanism should be implemented in real-time healthcare applications that can restrict the access of the physiological information, as user’s roles. For example, the HL7 Standard Development Organization uses a role-based access control model.

(7) Data availability: Availability ensures that services and information can be accessed at the time when they are required. Thus, medical sensor node availability ensures that the patient’s data are constantly available to the care-giver. If a sensor node is captured by an adversary, then its data availability will be lost. Therefore, it is required to maintain always the operation of the healthcare applications in the case of loss of availability.

(8) Data freshness: In healthcare applications, data confidentiality and integrity are not enough, if data freshness is not considered. Data freshness implies that the patient’s physiological signs are fresh or resent; and thus an adversary has not replayed the old messages. There are two kinds of freshness: weak freshness, which gives partial message ordering but does not carry time-delay information; and strong freshness which gives a total order on a request-response pair and allows for delay estimation (Saleem et al 2011).

(9) Secure localization: In healthcare applications, estimation of the patient’s location is very important. In real-time applications, a lack of smart patient tracking allows an attacker to send incorrect patient’s location by using false signals (Saleem et al 2011).
Forward and backward secrecy: In a real-time healthcare application, generally new medical sensors are deployed when old sensors fail. So, it is important to consider forward and backward secrecy. In forward secrecy, a medical sensor cannot read future messages transmitted after it leaves the network, while in backward secrecy a sensor joining the network cannot read any previously transmitted messages (Wang et al. 2006).

Communication and computation cost: Since wireless medical sensors are resource-constrained devices, healthcare application’s functions also need room for executing their tasks and the security schemes must be efficient in terms of the communication and computational cost.

Patient’s permission: A patient’s permission is needed when a healthcare provider is disseminating his/her health records to another healthcare consultant including medical researcher, insurance company, etc. In addition, patient’s anonymity is also needed for healthcare applications because medical sensor networks are wireless in nature. Thus, anonymity hides the source of a packet (i.e., medical sensor data) during wireless communication. It is a service that can enable confidentiality. Further, a wireless healthcare application should enable minimum survivability in the presence of power loss, failures or attacks.

1.11 MOTIVATION AND BACKGROUND

The development of a wireless healthcare application offers many novel challenges such as reliable data transmission, node mobility support and
fast event detection, timely delivery of data, power management, node computation and middleware (Koch & Hagglund 2009; Chung et al 2007; Gravina et al 2008; Lorincz et al 2009; Lee et al 2008; Omeni et al 2007; Lamprinos et al 2005; Waluyo 2009). Further, deploying new technologies in healthcare applications without considering security often makes patient’s privacy vulnerable (Dimitriou & Loannis 2008; Xiao et al 2006; Venkatasubramaniam & Gupta, 2006; Leon & Garcia 2009; Halperin et al 2008). As WMSNs share individual data with physicians (in a doctor-patient relationship), insurance companies (as insurance protection), and health-coaches (as sports team trainers) or with family (as relatives’ support) (Kotz 2011), unauthorized collection and use of patient data by potential adversaries (such as insurance agents, for political reasons, rival coaches, personal enemies etc.) can cause life-threatening risks to the patient, or make the patient’s private matters publically available (Meingast et al 2006). For instance, in a simple scenario, a patient’s body sensors transmit his/her body data to a nurse/care-giver; a third person may drop the patient data while the data is transmitted, and consequently the patient’s privacy may get breached. Later, the attacker may post the patient data on a social site (Face Book or Twitter, etc.), thus posing risks to the patient’s privacy. Indeed, wireless healthcare can offer many advantages to patient-monitoring, but the physiological data of an individual are highly vulnerable. So, security and privacy become some of the big concerns for healthcare applications, especially when they come to adopt wireless technology. More importantly, a healthcare provider is subjected to strict civil and criminal penalties (i.e., either fine or imprisonment) if Health Insurance Portability and Accountability Act (HIPAA) rules are not followed properly (Meingast et al 2006). Thus, security and privacy of a patient are the central concerns in healthcare applications.
WBAN is vulnerable to insider physical attack called cloning attack or node replication attack. In this attack, the adversary physically captures one or a few legitimate nodes, reads the secret credentials of compromise node, clones or replicates them with the same identity and finally deploys a capricious number of clones throughout the network (Conti et al 2011; Lu et al 2012; Parno et al 2005; Zeng et al 2010; Zhu et al 2010). Using these clones, the attacker can launch several kinds of attack without being easily detected: (i) unauthorized access to health data, (ii) false data injection, where the attacker injects false results which are different from true health data sensed by bio-sensors, (iii) selective reporting where the attacker changes the reports of events by dropping legitimate packets that pass through the compromised node and (iv) alteration of health data of a patient, thereby leading to incorrect diagnosis and treatment (Dimitriou & Ioannis 2008). If these replicated nodes or clones remain undetected or unattended for a long time, they can further make changes in protocol behavior and intrusion into the system security (Gautam 2008). Several clone node detection schemes have been proposed to detect such attacks. However, these solutions are not suitable because they demand in terms of energy, memory and execution time.

The resource constraint nature of the sensors in WMSN such as low computational power, limited memory, small power supplies and limited communication range (Ngai et al 2006; Martins & Guyennet 2010), create great opportunities are laid for attackers. When the attacker node manages to attract neighbouring nodes, it becomes a sinkhole and can be used to launch other attacks (Samundiswary et al 2010). In a sinkhole attack an intruder compromises an existing node or introduces a counterfeit node inside the network and uses it to launch an attack. Here the compromised node sends fake routing information to its neighbours to attract network traffic to itself (Pandey & Tripathi 2010). Due to the ad hoc network setup and many to one
communication pattern of WMSNs, where many nodes send data to a single base station, WMSNs are particularly vulnerable to sinkhole attacks (Ngai et al 2007).

The main aim of the present study in this connection is to propose innovative and novel mechanisms for detection and prevention of cloning or replication attack in WBANs and detection mechanism for sinkhole attack in WMSNs. Improved resilience against cloning attacks and sinkhole attacks under various conditions is an added advantage of the proposed protocols

1.12 CONTRIBUTIONS

In this study, two major contributions are made in regard to the WBANs and WMSNs associated with two major severe attacks namely cloning or replication attack and sinkhole attack. The detailed discussion of these contributions is given in the remaining chapters of the research work and is summarized below.

i. Proposal of a novel clone detection and prevention strategy for WBAN by leveraging inconsistent collisions so that legitimate nodes of WBAN are alone allowed to participate in communication, while preventing the cloned nodes.

ii. Proposal of an approach to detect Sinkhole attack in WMSNs. It provides a centralized approach to detect suspicious regions in the network using Energy-hole estimation followed by explicit identification of sinkhole attacker node using trust.

1.13 OUTLINE OF THE RESEARCH WORK

The five chapters of this study cover the background work and the details of the contributions. The remainder of the work is organized as follows.
Chapter 2: Literature Review

This chapter starts with a discussion of existing cloning attack detection protocols and sinkhole detection protocols for WSNs, their sub-categories and their advantages and limitations.

Chapter 3: A Novel Protocol for Detection of Cloning Attack and Sinkhole Attack in Wireless Medical Sensor Networks

In this chapter, the motivation, algorithm, and advantages of the proposed cloning attack detection and prevention protocol framework are described in detail. Also this chapter presents the algorithm and working mechanism of the energy-aware sinkhole detection along with Trust mechanism.

Chapter 4: Security analysis and performance evaluation

In this chapter, the security analysis and performance evaluation of the proposed algorithms for detection of cloning attack in WBANs and sinkhole detection in MSNs are discussed.

Chapter 5: Conclusions and Future direction

This Chapter summarizes the research contributions in the present study along with future research directions and suggestion.