CHAPTER – 1

Introduction

1.1 Background

The enormous growth in wireless communication, low power circuits, semiconductor technologies and biomedical sciences has enabled a new flavor of wireless sensor network termed as Wireless Body Area Network (WBAN) [1]. A subset of WBAN called Implantable Wireless Body Area Network (IWBAN) [2] is formed by networking implantable medical devices (IMDs) present in a human body and related external monitoring devices for continuous and autonomous health monitoring and prosthesis. Millions of patients get benefited by continuous monitoring and care provided by these devices. IMDs are becoming more sophisticated with increased functional complexity, software programmability, and wireless connectivity to other devices which aids in accurate and fast clinical decision making. However, incorporation of these features affects the trustworthiness of the device by inducing hardware failures, software malfunctions, wireless attacks on security and privacy. The implications of security attacks on these devices networked in an IWBAN would be exasperating as it will directly impact the health and life of the patient. FIGURE 1.1 shows the position of Implantable Body Area Network (IBAN). In this chapter we study such devices and their characteristics and then associate them to network security to imbibe on the importance of securing such devices. IMDs are enormously beneficial and have affected the lives of millions of patients living with chronic conditions quite easier. Our idea is not to discourage their usage but we would like to reemphasize on the importance of providing a secure wireless interfacing for such devices in order to increase their trustworthiness.

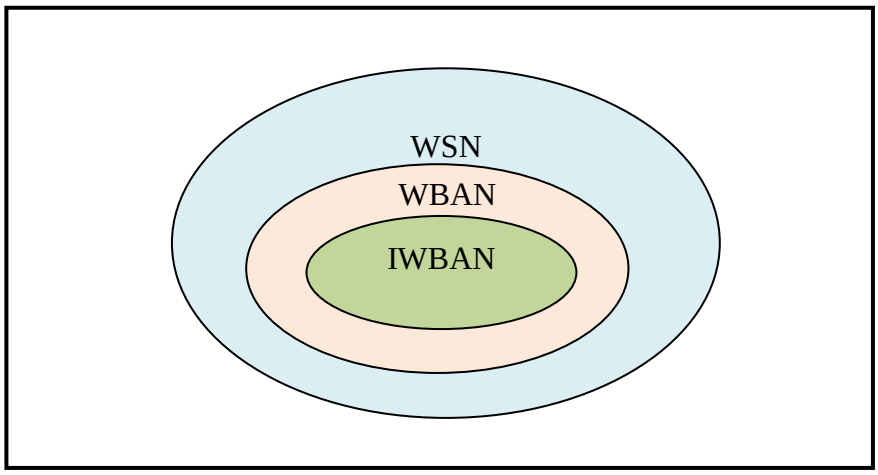

FIGURE 1.1 Position of Implantable Body Area Network

1.1.1 Implantable Medical Devices

The Implantable Medical Devices (IMDs) are deeply embedded inside human body to perform therapeutic tasks like sensing, diagnosing, monitoring, treating and communicating medical conditions [3]. These devices have eventually become an indispensable part of international healthcare industry in recent years due to the amount of flexibility it gives to the healthcare providers in terms of treatment automation and remote monitoring and to the patient in terms of mobility, continuous care and cost cutting by shunning the need of hospitalization.

According to [5] millions of people over the world use IMDs and the trend is ever increasing as visible in a report which states that over 2.6 million cardiac (heart) devices were implanted in patients in the U.S. alone between 1990 and 2002 [6]. FIGURE 1.2 shows pictures of a range of IMDs popular in the market today.

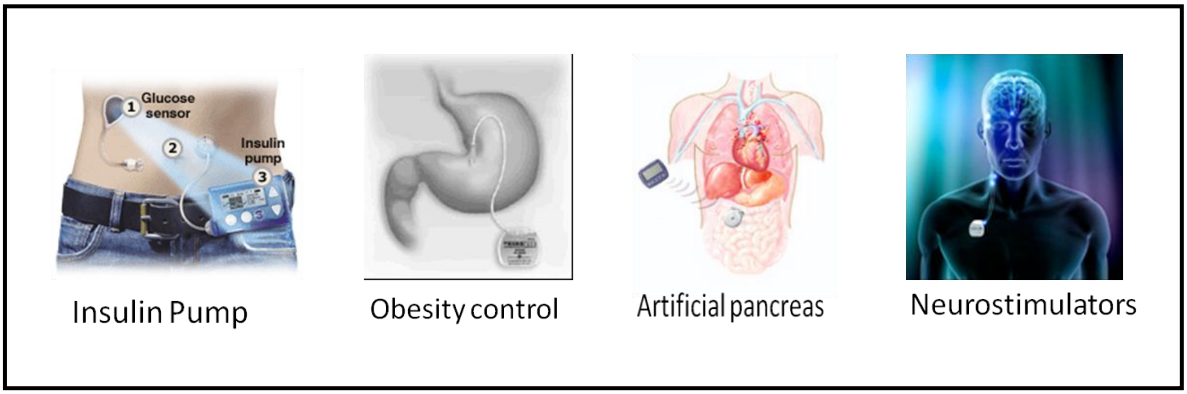

FIGURE 1.2 A range of IMDs (Photos: Medagadget)

Almost every aspect of human health can be monitored by IMDs thus providing highly accurate diagnostics and life sustaining functionalities. IMDs are being used for measuring

blood pressure [7], blood-glucose concentration [8], gastric pressure [9], tissue bio-impedance [10]. They are also used as electrical stimulators for paralyzed limbs [11], for bladder control [12], for blurred cornea in the eye [13]. Examples of IMDs are implantable pacemakers [14] , implantable cardiac defibrillators (ICDs) [15] , insulin pumps, neurostimulators, hearing aids, biosensors and automated drug delivery systems.

These devices in the current genre perform following tasks [23]:

1. Sense – IMDs are capable of collecting a variety of physiological information from the body which is further used for diagnosis of the medical condition of a patient.
2. Actuate – IMDs are capable of producing a therapeutic effect in the body either based on the sensed data or depending on the command it receives from an external device.
3. Information processing- IMDs may also perform some processing on collected or communicated information
4. Communication- IMDs communicate with other IMDs in the IBN and with external devices.

1.1.2 Classification of Implantable Medical Devices

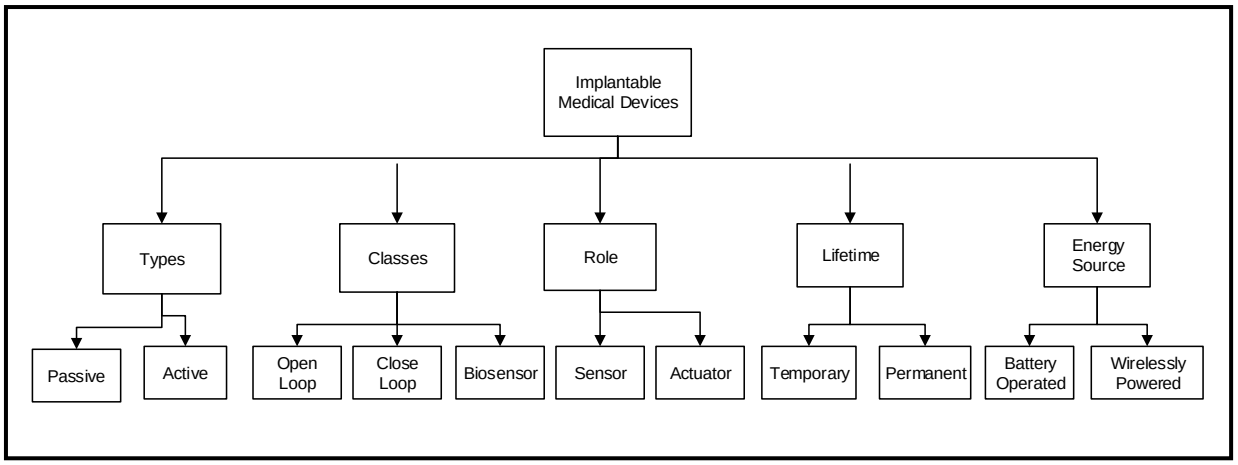

FIGURE 1.3 Classifications of IMDs

Fig.1.3 shows the classification of IMDs as per our understanding. They are broadly categorized as active and passive types. The active IMDs require power to run and uses wireless interface to communicate with external devices like a reader or a programmer or base station, and to receive commands or upgrades to optimize the delivered therapy. In this thesis, we have considered active devices only. Once these devices are inserted into human body, they remain in direct contact with the human body and organs for short or extended periods. Therefore, such devices are subjected to rigorous safety standards in the

interest of the IMD bearing patients. Active IMDs (AIMDs) are typically either sensors that sense physiological parameters and emit them like patient's ECG, temperature, blood glucose and oxygen levels as mentioned above; or actuators that deliver therapies, like cardiac pacing by pacemaker and drug injection by an insulin pump. Actuators can be further configured by external medical device using wireless means. These sensors and actuators are often combined into a closed-loop system performing sensing and actuation without patient intervention (e.g. in ICD) or in an open-loop system (e.g. in Insulin Pump) wherein actuator receives information from external device and need human intervention[16]. Biosensors are a special class of IMDs that collect, process, store and forward health information to a base station for further processing and analysis.

Depending on the ailment, IMDs may be implanted permanently or temporarily. Permanently implanted IMDs must be interfaced to external devices periodically for diagnosis, troubleshooting, and reprogramming, and to retrieve stored parametric and physiological data. Such external devices are called readers and/or programmers. Temporarily implanted IMDs either function autonomously or inter-operate through an external controller.

Most of the IMDs are battery powered with recharging a remote possibility due to their unique placement inside body. Some IMDs receive power through inductive coupling [17] e.g. cochlear implants and biosensors. Implanted biosensors receive power from a patch attached to human skin through inductive coupling. The patch is also responsible for transferring information to an external base station which in turn forwards the data to a remote station which is the doctor’s PC[17].

Multi-component IMDs can be hierarchically structured in master-slave fashion, or as peer-to-peer components. Information can be exchanged between the components of a multi-component IMD in point-to-point, end-to-end, broadcast, or multicast fashion.

1.1.3 Characteristics of Implantable Medical Devices

IMDs are unique devices with characteristics different from other wireless devices. The properties of interest for this study are summarized in Table 1.1 and are explained below:

TABLE 1.1 IMD Characteristics

Parameter	Value	Comments
Frequency Band	MICS Band 401-406 MHz[18]	Wavelength of 75 cm
Standard	IEEE 802.15.6	
Bandwidth	300 KHz	Ten channels of 300 kHz bandwidth each.
Data Rate	250 kbps and above	
Transmit Power	25 μw	Allows compact and lightweight implantable device design ; reduces the thermal effects and interference
Transmission Range	2-3 meter	To reduce thermal effects on the body
Transreceiver	MICS	Example ZL70101
Power Expense	5mA	Kept as low as possible to increase device lifetime.
Memory	2MB [14]	Less as devices are miniaturized

1.1.3.1 Implantable Medical Device Communication

These devices make use of RF-based wireless telemetry for transmission of physiometric data pertaining to patient and his medical condition in response to interrogation by an external device called reader/programmer or directly in case of a medical emergency. The wireless connection serves one or more of the following objectives:

1. It allows patient the flexibility to remain mobile while interrogation by an external device is going on.
2. It saves the patient from infections that may arise due to use of wires.
3. It allows the external devices to remotely monitor vital parameters and query IMD status parameters for continuous and autonomous care.
4. It allows external devices to access IMD for calibration purpose, program adjustments, software maintenance, upgrade patches and configuration.
5. It also allows in-body distribution of sensor data between two or more IMDs for control purposes or to form a loop of stimulation and actuation.
6. In case of an emergency, it allows healthcare providers to access the IMD to provide immediate relief to the patient.

Older models of IMD used 175 KHz band to communicate. The U.S. Federal Communications Commission (FCC) has allocated the Medical Implant Communication Service (MICS) band with frequency ranging from 401MHz to 406MHz specially for Medical Devices [19]. It allows bi-directional radio communication between IMDs or between IMD and external medical devices. The band is divided into ten 300 KHz

channels out of which any one is used by a pair of communicating devices. IMDs typically involves into two types of communication which are in-body and extracorporeal.

In-body Communication: In-body communication occurs when one IMD communicates with another IMD implanted inside the same human body.

Extracorporeal Communication: When IMD communicates with external devices, it is termed as extracorporeal communication. Such external devices can be IMD programmer, a reader, a base station, a gateway or even a smartphone. Some IMDs like Pacemakers and implantable cardioverter defibrillator (ICDs) contain a magnetic switch that is activated by an external magnetic wand to gain access to the device [20]. The programmer (or reader) initiates a session with the IMD during which it either queries the IMD for its telemetry data or sends it commands. To save power IMD are designed in a manner that they do not initiate transmissions; they transmits only in response to a transmission from a programmer [18]. But in case of an emergency, IMD may initiate a transmission when it detects an event that endangers the safety of the patient. A programmer and an IMD share the medium with other devices as follows [1]: To select a channel for their session, they must "listen" for a minimum of 10 ms to confirm the channel is idle. Once an unoccupied channel is found, a session is established and alternate request-responses occur between the programmer transmitting a query or command, and the IMD responding to it immediately without sensing the medium [21]. As power is a scarce resource, IMDs employs a duty-cycling operating system to conserve power. As transceiver is known to consume a large share of available power, it employs sleeping state for most of time. The power required to look for a communicating device at regular intervals must be kept extremely low (less than 1μA). The power required to transmit and receive is also kept low(less than 6mA) [20].

1.1.3.2 Implantable Medical Device Design

Typically, IMDs are designed using system-on-chip(SoC) technologies. For wireless data transmission ultralow-power Zarlink MICS transceiver is used. Zarlink ZL70101, 402 MHz MICS transceiver is world's first ultralow-power RF wireless chip that is used for implantable communication [22] at the MICS band. ZL70101 supports a typical raw data transmission rate of 200 to 800 kb/s. These transceivers are commercially available as an implantable-grade bare die [23] and can be stacked on the sensing unit or the actuation unit. For long-term active implantable biomedical system, Lithium-ion (LI) batteries are used [23] which has approximate capacity up to 10 mWh and energy in range of 3000

joules [22]. The transceiver of an implant is idle most of the time and activates after a large time interval (several hours or even weeks) to save power[12]. IMDs use RF-based communications for bidirectional data and command transfer that extends upto 2-3 meter. This range allows a data transfer rate of 250 kbps and above. Modern implants heavily rely on software rather than pure, hardwired circuitry.

In implantable biosensors, inductive links are used for delivering power to an implanted device via a patch put on human skin. The same link is also used to perform bidirectional data communication with the implanted devices not needing RF Transmitter. Downlink communication (from the external transmitter to the implanted device) acquires a bit-rate of 100 kbps. Uplink communication (from the implanted device to the external transmitter) acquires bit-rate of 66.6 kbps[24].

1.1.3.3 Implantable Medical Device Networking

An implantable medical device generally works as an isolated standalone device rather than as a connected and coordinated system. Recently these devices are being internetworked and made interoperable to aid in improved decision making, patient care, patient context awareness, reduced medical errors, and improved patient safety[25]. Recent work has proved that it is feasible to develop implantable wireless body sensor networks (IWBSNs) by adding network function to multiple standalone implantable devices [26]. The introduction of internetworking makes medical devices rely on each other for diagnostic decision making. For example, the implanted drug delivery device may get information from the targeted areas where sensors are implanted in order to release the right amount of dosage in the required place.

1.1.4 Classification of Implantable Medical Device Data

IMDs perform therapy delivery, sensing, diagnosing, monitoring, and related functions, either autonomously or through cooperation from another device. Transmitted data in medical applications usually contain sensitive information that is either private or critical for the proper operation of the IMD. In general, telemetry data include the following:

1. Patient data: It includes quantitative physiometric data that is measured by an IMD. It also includes non-patient information, such as parametric data that reports the status and operational characteristics of the IMD and environmental data that includes information like ambient temperature or time of day.

2. Commands: They are the instructions, which are issued to control, effect an operational result, and communicate. Commands can be originated by an IMD or other external device, and include program or instructional codes and messages that direct an IMD or other device to operate in a certain manner.
3. Other Data: The operational parameters of IMD may be given reprogramming commands. Also firmware may be given patching commands. Metadata that is data about data may also be sent by IMD.

1.1.5 Our Findings

From the above discussion, we draw following summary:

1. Number of IMDs per human may be one to many.
2. Existing IMDs may be removed or replaced and new IMDs may be added for the patient depending on his medical ailment.
3. IMDs have a unique placement inside the human body.
4. IMDs perform life-critical functions.
5. IMDs have limited energy, computational power and available memory.
6. All IMDs of a patient are equally important and no redundant devices are available.
7. IMDs require an extremely low transmit power in order to minimize interference and cope up with health concerns.
8. The communicated data to and fro IMDs must have high reliability and low delay.
9. IMDs are heterogenous having different demands and requirements in terms of data rates, power consumption, lifetime and reliability.
10. A wide range of devices may be needed to interact with these devices.

Therefore, we conclude that IMD is a critical device that collects and transmits sensitive data and perform functions that directly or indirectly impact the life of a patient.

1.1.6 Network and Communication Security

IMDs which perform life saving jobs are miniaturized computers empowered with wireless communication and are becoming essentially networked therefore a discussion on network security is of prime importance here.

1.1.6.1 Definition

Network security refers to the basic provision of security services including confidentiality, authentication, integrity, authorization, non-repudiation, and availability, and some augmented services, such as duplicate detection and detection of stale packets (timeliness) [107].

The use of wireless telemetry in IMDs makes them vulnerable to potentially serious security issues. IMDs are becoming complex with the feature of software programmability and network connectivity. For improvements in quality of monitoring and therapy adjustments, remote monitoring[27] has also been added into some devices. These devices were designed with limited power and storage and miniaturized size constraints therefore data and communication security which require resources were not considered a priority. But, with the increasing sophistication of security attackers, security no more remains an afterthought. The sensitive nature of medical data and the unprecedented access that a malicious adversary can gain to human body by compromising these devices may threaten the safety and trustworthiness of the device leading to a life-threatening condition. Health Insurance Portability and Accountability Act (HIPAA) and the European Privacy Directive (EPD), states that it is mandatory for medical information systems to protect patient privacy as patient health information (PHI) is a non-disclosable and private affair. According to Health and Human Services (HHS), vulnerabilities of medical devices has become a major concern to the Healthcare and Public Health (HPH) Sector. Current research shows that IMDs do not employ any security mechanisms and these devices are easily accessible for people with the right equipment [28]. As mentioned above, devices like Pacemakers and implantable cardioverter defibrillator (ICDs) can be activated by use of a magnetic switch[29]. The current magnetic-switch-based access does not provide any security from unauthorized access. The pivotal role of IMD in human body and its significance in sustaining life leaves a scope of zero error and zero tolerance towards security and thus safety breach.

1.1.6.2 Security Objectives of Implantable Medical Device

Looking at the criticality of these devices, the key security objectives can be directly referenced from X.800 [30] which is an international standard by the International Telecommunication Union (ITU). The security services of X.800 for interconnection of open systems are categorized as Access Control, Data Confidentiality and Data Integrity. Authentication service is also included here. These security services are explained below:

1. **Data Confidentiality:** Confidentiality refers to the protection of the exchanged data, identity, and context information from unauthorized disclosure by eavesdropping on unprotected wireless communication. This limits the use of data by other external devices or other IMDs.
2. **Data and Command Integrity:** Integrity service ensures that the exchanged data is not deleted, replicated to replayed, forged or fabricated. Physiological data communicated by IMD are vital for diagnosis and decision making and therefore manipulated data may lead to disastrous consequences. Unauthorized manipulation of the data during storage or transmit must be detectable and preventable. Integrity must also be ensured in the commands issued to the IMDs by healthcare staff as it has the capability of altering the IMD functionalities.
3. **Availability:** Ensures that sensed telemetry data and the IMD itself are available and functioning in the correct manner to provide deemed services to the patient. IMD especially needs to be protected from battery depletion, which renders it unusable or from commands which shuts it down. It should perform the expected life critical functionalities seamlessly. Also in any condition, access should not be denied to authorized healthcare staff as access failure may become a life threatening matter for patients.
4. **Authentication:** Authentication is the assurance of genuineness of the communication and communication party. It allows verification of the identities of peer entity devices that attempt to interface wirelessly before transmission of the data. It also deals with the authentication of the origin of the data. It is mandatory to authenticate the devices and users before granting them access to the IMDs which gives an unprecedented view of the inner workings of the human body.
5. **Access Control:** With access control, unauthorized use of a resource is prevented. Once a device is authorized does not mean that it may send any command to the IMD. Such flattened communication will increase the risk of aggravated access either mistakenly or maliciously. The security service is essential for addressing patient's concerns by actively controlling which IMD or external device can query and send what commands and under which circumstances.

1.1.6.3 Challenges in Securing IMDs

For IMDs to avail these security services, stringent security mechanisms are required to render above mentioned services for medical data. Adding security mechanisms even if seems obvious, is a complex task for IMDs due to following reasons:

1. **Resource Constraints:** As mentioned in [31], IMDs are resource constraint devices that are miniaturized in order to be placed in human body. Most of the IMDs are expected to run for 5- 10 years on a limited battery power. If battery is exhausted, replacement requires surgery. Their unique placement and deployment technique places stringent limits on processor capability and memory size. Authors states memory sizes of implants ranges from 1 KB to 10 KB [3]. Secure communication [32] in particular require use symmetric-key cryptography to ensure confidentiality of the transmitted data; message authentication for integrity protection and validation of source of origin, and public-key cryptography for peer authentication and key exchange. Such cryptographic transformations present higher processing, memory, and energy requirements unless optimized for these devices.
2. **Key Distribution Constraints:** Use of symmetric key cryptosystem require sharing of secret key between legitimate parties and key renewal which is difficult to manage as only non-invasive means of accessing these devices is available. Well-established public-key cryptosystems such as RSA, Diffie-Hellman, and elliptic curve cryptography (ECC) provide flexibility for key management and distribution without requiring a physical access of the IMDs but remain prohibitively expensive due to higher resource requirements and code size [33].
3. **Environmental Constraints:** IMDs are used in insecure physical environments and are prone to greater exposure to the attackers.
4. **Manageability Constraints:** IMDs per user may tend to increase making it impractical for users to manage separate security administration tasks such as security patching and credentials management.
5. **Inalterability Constraints:** In the U.S. alone, there are millions of people who already have wireless IMDs, and about 300,000 such IMDs are implanted every year [34]. Therefore, altering existing IMDs is very difficult.
6. **Safety Constraints:** It is crucial to ensure that health care professionals always have seamless access to an implanted device for safety assurance. However, if

cryptographic methods are embedded in the IMD itself, the device may become inaccessible unless provided with the right credentials. Imposing stringent access control may work in normal conditions but during emergency may rendering them inaccessible.

7. **Deployment Constraints:** These devices are carried inside patients therefore cannot be put into a restricted physical environment.

For secure communication under tight power budget, these devices can only support minimalistic security transformation for wireless communication making it infeasible to simply borrow conventional security solutions without modifications from the province of Wireless Sensor Networks. The key solution is use of algorithms and protocols that optimize the resource consumption. While designing the security scheme it is crucial to balance security, privacy, safety and utility goals to get high acceptability [16, 27].

1.2 Motivation and Objectives

As stated above, the use of wireless communication for IMDs gives rise to unique security and privacy challenges. Attackers may compromise the confidentiality of the transmitted data which may lead to unwilling disclosure of patient's medical conditions. Attackers may even send unauthorized commands to change the settings of an IMD which may create a life threatening situation. Computer and network security is a matured field, providing security solutions to a wide range of data processing systems. But the due complexity of the human body, safety concerns, resource bottlenecks like low power, processing and storage capacity poses a challenge in using existing security solutions for these devices.

In this thesis, we address the following research question: "How can we define a system that provides confidentiality and integrity, authentication and access control of sensitive information during the communication between an IMD and a legitimate programmer, or between two or more IMDs of a patient in an IWBAN while ensuring seamless availability of information to legitimate users?"

Since the design of IMDs is proprietary, little information about the details of its architecture is publicly available. This thesis considers the existing problems in securing IMDs which need to be addressed and are taken as the baseline for motivation and objectives of this research. These problems are mentioned below:

Problem 1: Existing solutions fail to work for multiple IMDs implanted in a human body and internetworked with each other communicating in-body as well as extracorporeal.

Existing solutions address security issues of a specific IMD but fail to address the security requirements when there are multiple IMDs networked in an IBAN.

Problem 2: Existing solutions fail to handle the heterogeneous nature of IMDs to find a universal security solution applicable to all IMDs.

Solutions proposed in literature can mainly used for a specific type of IMD which limits its usability for a wide range of devices.

Problem 3: Existing security solutions do not handle emergency situation well and majorly provide a fail open access.
Majority of solutions fail open in case of an emergency which makes these systems vulnerable to attacks.

Problem 4: Existing security solutions do not provide a sophisticated authentication and access control mechanism and only provides proximity based access control.
Majority of solutions only provide a few security services which limits their usability.

1.3. Objective and Scope of work

The major objectives of this research are:

1. Understanding the security and privacy implications of future networked implantable medical devices that provide an unprecedented view into the inner workings of the human body.
2. To perform threat modeling for a network of IMDs and external devices.
3. To provide taxonomy of security solutions for IMDs that is proposed in literature.
4. To explore design alternatives that effectively provides a single security solution for a system involving heterogeneous IMDs of a patient and which communicate with each other and with external devices by wireless means.
5. To propose an application layer security solution which is patient specific rather than device specific.
6. To greatly reduce overhead of security related processing on IMDs
7. To propose a two-tier model which can allow secure communication between resources constrained IMDs and resource rich external devices simultaneously.

8. To understand energy issues, including power depletion and replay attacks that exploit the lightweight nature of the IMDs and propose a solution model that offload security related processing from IMDs.
9. To impose security policies on IMDs as well as external devices for fine-grained access control.

We define our scope as:

1. Developing a detailed threat model for wireless communication of implantable medical devices.
2. Developing a secure two-tier communication protocol for Implantable Medical Devices. We may assume typical IMD for our case. The assumption might not be exactly in terms of some typical IMD. The proposed protocol will work at application layer while assuming a specific transport layers services present. The protocol also assumes a key exchange and renewal technique to be in place.
3. Providing a proof of concept.
4. This thesis focuses on the IMD and its related radio attacks, considering the communication between an IMD and an ED and also IMD-IMD. Hardware failures, software errors, malware and vulnerability exploits and side-channel attacks as described in [45] are out of the scope of this work.
5. By making realistic assumptions about the architecture of the IMDs based on modern technologies, a system can be made that solves the lack of security mechanisms in the future. This thesis focuses on the IMDs and its related radio attacks.

1.4. Contribution of the Study

The thesis first discusses the vulnerabilities and threats related to wireless access of IMDs and come up with the threat model.

The thesis then discusses the available security solutions for IMDs and provides taxonomy of available schemes.

The thesis proposes a trusted external device based security solution for IMD – External Device communication called Buddy System. It is a simple intuitive scheme which makes use of friendly jamming for key exchange. Buddy System can be used for providing

minimally invasive security to IMDs. It runs authentication and access control protocols on behalf of IMDs to grant access to the external devices. We also propose a Session Key generation scheme on IMD which harvests Physiological Values (PVs) randomness and therefore shuns the need of a Pseudo Random Number Generator (PRNG). Finally, we propose a friendly jamming scheme by Buddy Device for secure transmission of thus generated one time session key from IMD to authenticated external device.

The thesis discusses the insufficiencies of current solutions in handling access control in emergency condition especially when the patient bearing IMD is unconscious and proposes a trusted external device based Emergency Aware Access Control Framework for IMDs.

The thesis proposes a trusted external proxy device based solution for the detection of active attacks for wireless IMDs by use of Angle of Arrival (AoA) signature.

The thesis proposes a novel external-based two-tier solution for achieve secure data transmission in wireless IMDs. We design a suitable defense framework for resource constrained IMDs. The proposal combines, for the first time, a request-response protocol for IMDs with publish-subscribe protocol, a powerful and general approach for asynchronous unicast and multicast communication, which allows usage of security mechanism based on the requirement and constraint of communicating parties and handles heterogeneous nature of IMDs well. The frameworks include light weight secure communication protocol for IMDs for which components have been carefully selected to reduce the overhead on IMDs. The thesis thereafter presents a novel countermeasure against replay attacks on IMDs by use of nonces which are generated using Physiological Values that are sensed by IMDs therefore not needing usage of the pseudo random number generator (PRNG). The communication protocol provides authentication, encryption and integrity checking of the communicated data along with fine-grained access control for IMDs by defining topics and controlling who is allowed to publish and to subscribe to which topic. The most important feature is its ability to secure IMD-IMD communication and IMD-External Device communication. The proposed scheme is lightweight and adaptable as it is applicable to a wide range of devices and saves IMD critical resources like memory, computation and communication.

We also implement the proposed system for a proof of concept. Evaluation results show the feasibility of the system in practice.

1.5. Research Methodology adopted for this Work

The data for the study has been collected mainly from secondary sources comprising various books, periodicals, journals. Our Research is:

Qualitative since we continuously strive to maintain optimal balance between safety and security without compromising any of the performance measures.

Experimental since our proposed model follows hybrid approach for deployment, which we have used for proof of concept.

Exploratory as we are combining two popular communication models to find the right balance for securing IMD to IMD as well as IMD to External Device communication.

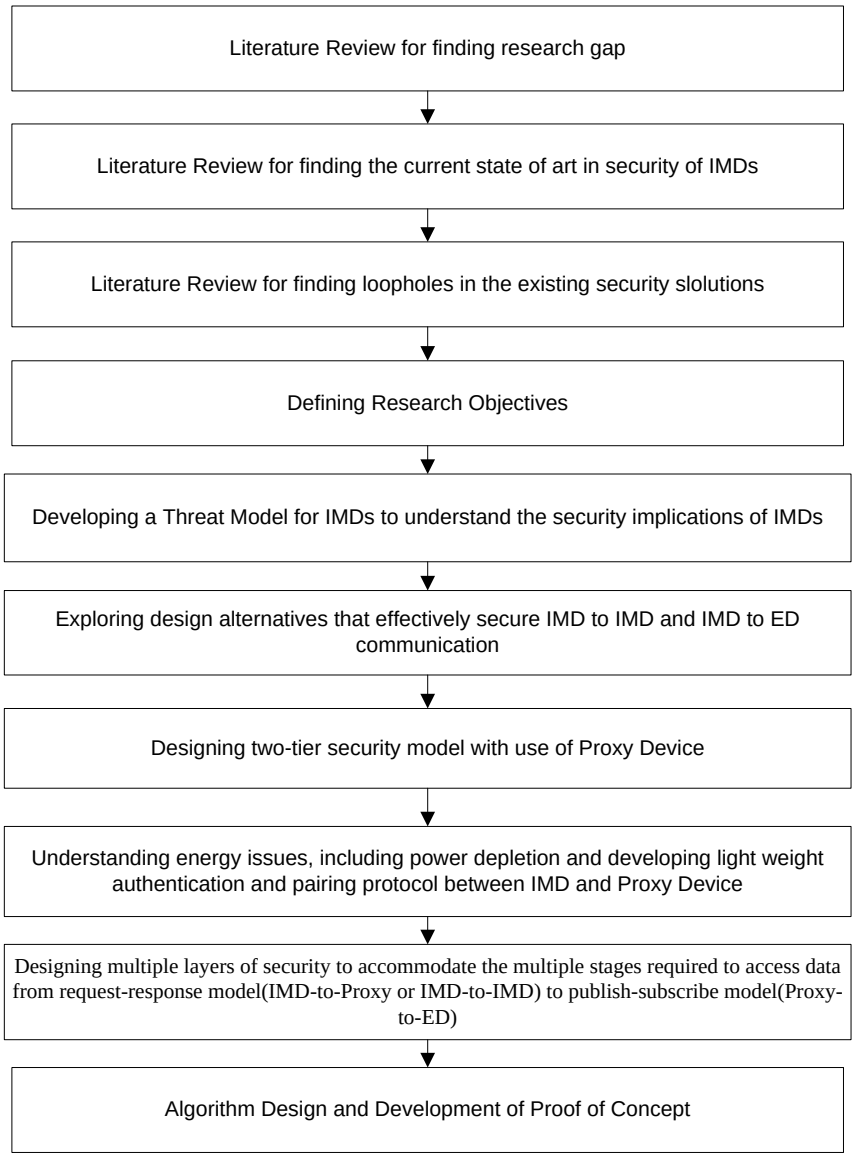

FIGURE 1.4 Phases Covered in Research Work

1.6. Organization of Remainder of the Thesis

In Chapter 2, we study the security related vulnerabilities and threats and their implications to derive a threat model for IMDs which helps us in identifying a set of security services required for secure communication between IMDs and also with external devices.

In Chapter 3, we perform literature study of the most promising existing solutions and techniques that address the security problem of wirelessly communicating IMDs to derive taxonomy of solutions. Furthermore, emergency access related solutions are discussed.

In Chapter 4, we propose a trusted external device based security solution for IMD – External Device communication called Buddy System.

In Chapter 5, we propose a trusted external device based Emergency Aware Access Control Framework for IMDs.

In Chapter 6, we propose a trusted external proxy device based solution for the detection of active attacks for wireless IMDs by use of Angle of Arrival (AoA) signature.

In Chapter 7, we propose a novel external proxy device based two-tier solution to achieve secure data transmission in wireless IMDs.

In Chapter 8, we provide a security analysis of the proposed protocols for two-tier solution.

In Chapter 9, we provide the implementation details for the proof of concept of our two-tier solution.

In Chapter 10, we conclude our work with a description of objectives achieved, conclusions of our work, and directions of future enhancement.