TWO TIER SECURITY SOLUTION FOR IMPLANTABLE MEDICAL DEVICES

A Thesis submitted to

Gujarat Technological University

for the Award of

Doctor of Philosophy

In

Computer Science

By

Monika Archit Darji

Enrollment No. 119997493008

Under Supervision of

Dr. Bhushan Trivedi

GUJARAT TECHNOLOGICAL UNIVERSITY

AHMEDABAD

June – 2016

DECLARATION

I declare that the thesis entitled Two Tier Security Solution For Implantable Medical Devices submitted by me for the degree of Doctor of Philosophy is the record of research work carried out by me during the period from March 2011 to June 2016 under the supervision of Dr. Bhushan Trivedi and this has not formed the basis for the award of any degree, diploma, associate ship, fellowship, titles in this or any other University or other institution of higher learning.

I further declare that the material obtained from other sources has been duly acknowledged in the thesis. I shall be solely responsible for any plagiarism or other irregularities, if noticed in the thesis.

Signature of the Research Scholar: Date: / /2016

Name of Research Scholar: Monika Archit Darji

Place: Ahmedabad

CERTIFICATE

I certify that the work incorporated in the thesis Two Tier Security Solution for Implantable Medical Devices submitted by Smt. Monika Archit Darji was carried out by the candidate under my supervision/guidance. To the best of my knowledge: (i) the candidate has not submitted the same research work to any other institution for any degree/diploma, Associateship, Fellowship or other similar titles (ii) the thesis submitted is a record of original research work done by the Research Scholar during the period of study under my supervision, and (iii) the thesis represents independent research work on the part of the Research Scholar.

Signature of Supervisor: …… Date: / /2016

Name of Supervisor: Dr. Bhushan Trivedi

Place: Ahmedabad

Originality Report Certificate

It is certified that PhD Thesis titled Two Tier Security Solution for Implantable Medical Devices by Monika Archit Darji has been examined by us. We undertake the following:

a. Thesis has significant new work / knowledge as compared already published or are under consideration to be published elsewhere. No sentence, equation, diagram, table, paragraph or section has been copied verbatim from previous work unless it is placed under quotation marks and duly referenced.

b. The work presented is original and own work of the author (i.e. there is no plagiarism). No ideas, processes, results or words of others have been presented as Author own work.

c. There is no fabrication of data or results which have been compiled / analysed.

d. There is no falsification by manipulating research materials, equipment or processes, or changing or omitting data or results such that the research is not accurately represented in the research record.

e. The thesis has been checked using https://**turnitin.com** (copy of originality report attached) and found within limits as per GTU Plagiarism Policy and instructions issued from time to time (i.e. permitted similarity index <=25%).

Signature of the Research Scholar: Date: / /2016

Name of Research Scholar: Monika Archit Darji

Place: Ahmedabad

Signature of Supervisor: Date: / /2016

Name of Supervisor: Dr. Bhushan Trivedi

Place: Ahmedabad

Thesis_Monika_Darji

ORIGINALITY REPORT

8%	1%	8%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Communications in Computer and Information Science, 2014. Publication	7%
2	Strydis, Christos, Robert M. Seepers, Pedro Peris-Lopez, Dimitrios Siskos, and Ioannis Sourdis. "A system architecture, processor, and communication protocol for secure implants", ACM Transactions on Architecture and Code Optimization, 2013. Publication	1%
3	dataspace.princeton.edu Internet Source	1%

EXCLUDE QUOTES	ON	EXCLUDE MATCHES	< 1%
EXCLUDE BIBLIOGRAPHY	ON		

PhD THESIS Non-Exclusive License to GUJARAT TECHNOLOGICAL UNIVERSITY

In consideration of being a PhD Research Scholar at GTU and in the interests of the facilitation of research at GTU and elsewhere, I, Monika Archit Darji having enrollment number 119997493008 hereby grant a non-exclusive, royalty free and perpetual license to GTU on the following terms:

a) GTU is permitted to archive, reproduce and distribute my thesis, in whole or in part, and/or my abstract, in whole or in part (referred to collectively as the "Work") anywhere in the world, for non-commercial purposes, in all forms of media;

b) GTU is permitted to authorize, sub-lease, sub-contract or procure any of the acts mentioned in paragraph (a);

c) GTU is authorized to submit the Work at any National / International Library, under the authority of their "Thesis Non-Exclusive License";

d) The Universal Copyright Notice (©) shall appear on all copies made under the authority of this license;

e) I undertake to submit my thesis, through my University, to any Library and Archives. Any abstract submitted with the thesis will be considered to form part of the thesis.

f) I represent that my thesis is my original work, does not infringe any rights of others, including privacy rights, and that I have the right to make the grant conferred by this non-exclusive license.

g) If third party copyrighted material was included in my thesis for which, under the terms of the Copyright Act, written permission from the copyright owners is required, I have obtained such permission from the copyright owners to do the acts mentioned in paragraph (a) above for the full term of copyright protection.

h) I retain copyright ownership and moral rights in my thesis, and may deal with the copyright in my thesis, in any way consistent with rights granted by me to my University in this non-exclusive license.

i) I further promise to inform any person to whom I may hereafter assign or license my copyright in my thesis of the rights granted by me to my University in this non-exclusive license.

j) I am aware of and agree to accept the conditions and regulations of PhD including all policy matters related to authorship and plagiarism.

Signature of the Research Scholar:

Name of Research Scholar: Monika Archit Darji

Date: / /2016 Place: Ahmedabad

Signature of Supervisor:

Name of Supervisor: Dr. Bhushan Trivedi

Date: / /2016 Place: Ahmedabad

Seal:

Thesis Approval Form

The viva-voce of the PhD Thesis submitted by Smt. Monika Archit Darji (Enrollment No. 119997493008) entitled Two Tier Security Solution For Implantable Medical Devices was conducted on …….…… (day and date) at Gujarat Technological University.

(Please tick any one of the following option)

☐ We recommend that he/she be awarded the Ph.D. Degree.

☐ We recommend that the viva-voce be re-conducted after incorporating the following suggestions:

☐ The performance of the candidate was unsatisfactory. We recommend that he/she should not be awarded the Ph.D. Degree.

---------- ----------

Name and Signature of Supervisor with Seal 1) (External Examiner 1) Name and Signature

---------- ----------

2) (External Examiner 2) Name and Signature 3) (External Examiner 3) Name and Signature

ABSTRACT

The development of MEMS (micro electro mechanical systems), SoC (System on Chip) and ultra low power wireless communication technology enabled the evolution of Implantable Medical Devices (IMDs). Implantable medical devices (IMDs) diagnose, monitor, and treat a wide range of medical conditions. This has lead to paradigm shift of the healthcare industry from doctor centric to patient centric by providing home-based treatment and remote monitoring and hence cost reduction. While these features improve healthcare diagnostics and decision making, security and privacy remain critical design aspects in wireless communication performed by these devices. As compared to previous ones, IMDs of current genre are complex embedded systems with networking capabilities that aid in wireless communication amongst IMDs and with other external devices. Due to their unique placement in human body and resource constraints like low power availability, computation and storage capacity, achieving security and privacy for wireless communication is difficult. Security for medical devices has gained attention in the recent years following some well-publicized attacks on Implantable Medical Devices, like pacemakers and insulin pumps. This has resulted in solutions being proposed for securing these devices, which are usually device specific and useful only for secure communication with external devices. Multiple IMDs may be implanted in a single patient therefore we argue that securing individual devices will not serve the purpose as these devices will be integrated sooner or later for advance therapeutic implications. Security solution rather than being device specific should be patient specific to cater to the security needs of IMDs of a patient. We provide a simple solution to detect active attacks on IMDs and then we provide an emergency aware access control framework for IMDs and also provide a Buddy System for secure communication with external devices. Finally, we provide an application layer security solution which not only allows secure communication between IMDs and external devices but also between interoperable IMDs for a single patient. We consider extreme resource constraints of IMD and explore the tradeoffs among different cryptographic primitives for use in IMDs to carefully design a lightweight protocol optimized for IMDs for mutual authentication and secure communication between the IMD and the proxy device. We also design a secure publish-subscribe communication protocol between the “proxy device” and external devices. Finally, we provide a proof-of-concept for the proposed two-tier security solution.

Acknowledgement

The perseverance required to come till here is the result of unmatched inspiration from my Guide, **Dr. Bhushan Trivedi,** Dean, Faculty of Computer Technology, GLS University; Director, GLS Institute of Computer Technology; Dean, Zone-I, MCA Programme, GTU. He never compromised in bringing out the best in me but at the same time gave me complete freedom to finish the work at my own pace. He allowed me to unfold my research work and never forced me to follow others footsteps. His go ahead would make me discover new ways of doing things and his remainder alarms helped me to stay focused and never wander too far. His expertise in the field helped me in developing a state-of-art solution.

The Doctorate Progress Committee (DPC) members: **Dr. Haresh Bhatt,** ISO, CIO and Mission Director, Information Security, Space Application Center (SAC), Indian Space Research Organization (ISRO) and **Dr. Devesh C Jinwala,** Professor and Dean, Research & Consultancy, Department of Computer Engineering, S V National Institute of Technology have helped me immensely in the entire work by giving their expert advises and by conducting earnest reviews.

I am also truly indebted to my co-guide **Dr. Pramode K. Verma,** Professor of Computer Engineering and Director of Telecom Engineering, University of Oklahoma, USA for supervising my work, providing invaluable inputs and motivating me.

I heartily thank **Prof. Urja Mankad** and **Mr. Hetansh Mankad** who supported me throughout this endeavor. I also appreciate the work of all the researchers whose work helped me to understand my field of research and contribute to it in however small manner possible.

Dr. Akshai Aggarwal, Vice Chancellor, Gujarat Technological University initiated this programme and I am thankful to him for giving me this once in a lifetime opportunity.

I express my gratitude towards the reviewers who took out their precious time to read the thesis and review it.

At the end I wholeheartedly thank my husband, **Mr. Archit Darji** who made this journey an epitome of memorable moments by always being there for me. I can’t thank God enough for bestowing oodles of luck on me in the form of a supportive family who stood

next to me in the thick and thins. My beloved son **Meghant** and adorable mother **Hasumatiben Darji** supported me immensely. My father **Mr. Sapan Mukherjee** was there for me whenever I needed his help. It is their unparallel love and good wishes that worked along with me in this journey. At the end I would like to dedicate this work to my papaji, **Prof. Arvindbhai Darji**, who was a wonderful teacher, an ace author, an orator and most importantly a marvelous human being!

Table of Content

CHAPTER – 1 Introduction		1
1.1.	Background	2
1.1.1.	Implantable Medical Devices	2
1.1.2.	Classification of Implantable Medical Devices	3
1.1.3.	Characteristics of Implantable Medical Devices	4
1.1.3.1.	Implantable Medical Device Communication	5
1.1.3.2.	Implantable Medical Device Design	6
1.1.3.3	Implantable Medical Device Networking	7
1.1.4.	Classification of Implantable Medical Device Data	7
1.1.5.	Our Findings	8
1.1.6.	Network and Communication Security	8
1.1.6.1.	Definition	9
1.1.6.2.	Security Objectives of Implantable Medical Device	9
1.1.6.3.	Challenges in Securing IMDs	11
1.2.	Motivation and Objectives	12
1.3.	Objective and Scope of work	13
1.4.	Contribution of the Study	14
1.5.	Research Methodology adopted for this Work	16
1.6.	Organization of Remainder of the Thesis	17
CHAPTER 2 Threat Modeling		18
2.1.	Introduction	18
2.2.	Threat Model	18
2.3.	Related Work	19
2.4.	Vulnerability and Threats in Existing IMDs	21
2.5.	A Hypothetical Attack Scenario	22

2.6.	Adversarial Model	23
2.7	Threat Modeling using SDL Tool	25
2.8.	Conclusion	27
CHAPTER – 3 Literature Survey		28
3.1.	Security Dimensions	28
3.2.	Design Dimensions	29
3.3.	Taxonomy of Security Models proposed in Literature	29
3.3.1.	Inhibiting Long Range Communication	29
3.3.1.1.	Use of small-range communication channel	30
3.3.1.2.	Enforcing Proximity	30
3.3.2.	Using Cryptography	31
3.3.2.1.	Using Symmetric Cryptography	32
3.3.2.2.	Using Asymmetric Cryptography	32
3.3.3.	Key Distribution and Management	33
3.3.3.1.	Putting Patient in the Loop	33
3.3.3.2.	Use of Patient Biometrics	33
3.3.3.3	Use of Physical Layer Approaches	34
3.3.4.	Using Trusted External Device	34
3.3.4.1.	Invasive Approaches	34
3.3.4.2.	Non-Invasive Approaches	37
3.3.5.	Emergency Access for IMDs	39
3.4.	Comparison of Security Models	39
3.5	Conclusion	41
CHAPTER – 4 A Buddy System for Securing Wireless IMDs		42
4.1.	Introduction	43
4.2.	Proposed solution: The Buddy System	43
4.3.	Features of Buddy Device	45

4.4.	Proposed Architecture using Buddy Device	46
4.4.1.	Buddy Device	46
4.4.2.	Implantable Medical Device	47
4.4.3.	Enhanced External Device (ED)	47
4.5.	Secure Communication Protocol	47
4.5.1.	MD-Buddy Device Pairing	48
4.5.2.	Reader Authentication	48
4.5.3.	Buddy Device-IMD Communication	48
4.5.4.	IMD-External Reader Communication	49
4.5.5.	Emergency Access	49
4.6.	Conclusion	50
CHAPTER – 5 Emergency Aware, Non-invasive, Personalized Access Control Framework for IMDs		51
5.1.	Introduction	51
5.2	Threat Model for Fail Open Security	53
5.2.1.	Assumptions	53
5.3.	Security Mechanisms proposed to be Installed on Proxy Device	53
5.3.1.	Authentication	53
5.3.2.	Access Control	54
5.3.2.1.	Traditional rule based model	54
5.3.2.2.	Role based access control model	54
5.3.2.3.	Context Aware Access Control Model	55
5.3.2.4.	Criticality Aware Access Control Model (CAAC)	56
5.4.	Proposed EAAC Architectural Framework	55
5.4.1.	Role Management	56
5.4.2.	Emergency State Management	56
5.4.3.	Emergency Management	57
5.5.	Conclusion	58

CHAPTER – 6 Detection of Active Attacks on wireless IMDs using Proxy Device and Localization Information		59
6.1.	Introduction	59
6.2.	RF based localization techniques	60
6.2.1.	Time of Arrival (ToA)	60
6.2.2.	Time Difference of Arrival (TDoA)	61
6.2.3.	Received Signal Strength Indicator (RSSI)	61
6.2.4.	Angle of Arrival (AoA)	61
6.3.	Overview of components	61
6.3.1.	System Configuration	61
6.3.2.	Assumption	61
6.2.3.	Proxy Device Overview	62
6.4.	Signature Generation and Verification	62
6.5.	Proposed Proxy based Protocol	63
6.6.	Conclusion	65
CHAPTER – 7 Two Tier Model for Securing Wireless IMDs		66
7.1.	Introduction	66
7.2.	Design Goals of Security Model	67
7.3.	Requirements of Two-tier Security Model	68
7.4.	Assumptions	68
7.5.	Overview of Proxy Based Two-tier Security System	69
7.6.	Profiling of Security Mechanisms for Tier-1: IMD and Proxy Device communication	70
7.6.1.	Security Service: Message Confidentiality	71
7.6.2.	Security Service: Message Integrity and Authentication	72
7.6.2.1.	Authenticated Encryption Mode- GCM	73
7.6.2.2.	Initial Vector Format for Tier -1	75
7.6.3.	Security Service: Replay Protection	76

7.6.3.1.	Counters	76
7.6.3.2.	Nonce	77
7.6.4.	Security Service: Mutual Authentication	78
7.6.5.	Security Service: Access Control	78
7.7.	Profiling of Security Mechanisms for Tier-2: Proxy Device and External Device communication	79
7.7.1.	Components of the Communication Model	79
7.7.2.	Design Choices for Proxy and ED communication	80
7.7.3.	Public Key Cryptography	80
7.7.4.	Security Service: Massage Confidentiality, Integrity and Authentication	81
7.7.5.	Security Service: Replay protection	81
7.7.6.	Security Service: Access Control	81
7.7.7.	Security Service: Mutual Authentication	81
7.8.	The Proposed Architecture and its Components	81
7.9.	Proxy Device and its role in the two-tier Security Model	83
7.10.	Description of proposed protocol for Tier 1: IMD and Proxy Communication	87
7.10.1.	Protocol : Proxy initiating communication	87
7.10.2.	Protocol: IMD initiating communication	89
7.10.3.	Message Formats for Tier One: Proxy-IMD communication	91
7.11.	Description of proposed protocol for Tier 2: Proxy and External Device Communication	91
7.11.1.	Protocol: Communication between Proxy and ED as Publisher	93
7.11.2.	Protocol: Communication between Proxy and ED as Subscriber	95
7.12.	Essential Functions Provided by Proxy	97
7.12.1.	Topic Management	97
7.12.2.	Device Management	98
7.12.3.	Access Management	98
7.12.4.	Key Management	99

7.12.5.	Emergency aware Access Management	99
7.13.	Deployment Model	99
CHAPTER – 8 Implementation and Analysis		102
8.1.	Implementation	102
8.2.	Security Analysis	106
8.3.	Conclusion	107
CHAPTER – 9 Conclusions, Major Contributions and Further Work		108
9.1.	Objective Achieved	108
9.2.	Major Contributions	109
9.3.	Comparison of proposed Security Model with Existing Solutions	110
9.4.	Possible further Work	112

List of Abbreviations

BCC: Body Coupled Communication

DoS: Denial of Service

DDoS: Distributed Denial of Service

ECG: Electrocardiogram

HIPAA: Health Insurance Portability and Accountability Act

ICD: Implantable Cardiac Defibrillators

IMD: Implantable Medical Device

AIMD: Active Implantable Medical Device

MAC: Message Authentication Code

MICS: Medical Implant Communication Service

MITM: Man In The Middle

NFC: Near Field Communication

PV: Physiological Value

RF: Radio Frequency

RFID: Radio Frequency Identification

RSSI: Received Signal Strength Indicator

WISP: Wireless Identification and Sensing Platform

RSSI: Received signal strength indicator

TOA: Time of arrival

DTOA differential time of arrival

AOA: Angle of arrival

AES: Advanced Encryption Standard.

CBC: Cipher Block Chaining

MAC: Message Authentication Code

TDEA: Triple Data Encryption Algorithm.

TLS: Transport Layer Security

WISP: Wireless Identification and Sensing Platform

PSV: Publisher Specific Value

ED: External Device

ECC: Elliptic Curve Cryptography

ECDSA: Elliptic Curve Digital Signature Algorithm

FDA: Food and Drug Administration

IDS: Intrusion Detection System

List of Figures

Figure No	Title	Page No
1.1	Position of Implantable Body Area Network	2
1.2	A range of IMDs (Photos: Medagadget)	2
1.3	Classifications of IMDs	3
1.4	Phases Covered in Research Work	16
2.1	A Hypothetical Attack Scenario	22
2.2	Types of Attackers	23
2.3	Context Level DFD for IMDs	26
2.4	Level One DFD for IMDs	26
3.1	Allowing reconfiguration from smaller distance and remote monitoring from longer distance [29]	31
3.2	ECG readings taken simultaneously by IMD and external device is matched to allow access [81]	36
3.3	Shield Jamming Unauthorized Communication [84]	37
4.1	Architecture of Proposed Security Scheme using Buddy Device	46
4.2	Sequence Diagram for Buddy Device based communication protocol	49
5.1	Block Diagram for Emergency Aware Access Control	52
5.2	State Transition Diagram for Emergency Aware Access Control using Proxy Device [124]	58
5.3	The Proposed Proxy based Architecture [124]	58
6.1	Signature Verification [122]	63
6.2	Sequence Diagram for Signature Verification Protocol [122]	65
7.1	Overall view of two-tier architecture	69
7.2	Structure of GCM [141]	73
7.3	Block Diagram of AES-GCM	74

7.4	Structures of IV	
(a)	Structure of IV for IMD	75
(b)	Structure of IV for Proxy	75
7.5	Architecture of Proxy based Two Tier solutions	82
7.6	Work Flow Diagram of Proxy Device	86
7.7	Sequence Diagram for Protocol: Proxy Initiating Communication	88
7.8	Sequence Diagram for Protocol: IMD Initiating Communication	90
7.9	Format of Messages	
(a)	Format of authentication request made by Proxy	91
(b)	Format of request and response messages	91
(c)	Format of authentication requests made by IMD	91
7.10	Sequence Diagram for communication between Proxy and External Device as Publisher	94
7.11	Sequence Diagram for communication between Proxy and External Device as Subscriber	96
7.12	Deployment Model	100
8.1	Network Switch Screen and Device Startup Screen	103
8.2	Mutual Authentications between IMD and Proxy.	104
8.3	External device sending join request to Proxy	105
8.4	Communications between Proxy, IMD and EDs	106

List of Tables

Table No	Title	Page No
1.1	IMD Characteristics	5
2.1	Vulnerabilities and Threats in Existing IMDs	21
2.2	Classification of Adversary	24
2.3	Threat Analysis Report	27
3.1	Comparisons of Surveyed Security Models	40
6.1	Table of Notation	64
7.1	Benchmark suite of symmetric ciphers	71
7.2	Summary of components adopted in communication protocol for Tier One: Proxy-IMD communication	79
7.3	Summary of components adopted in communication protocol for Tier Two: Proxy-ED communication	81
7.4	Notations used in Tier One: Proxy- IMD communication	87
7.5	Description of messages for Protocol: Proxy initiating communication	89
7.6	Description of messages for IMD initiating communication	90
7.7	Examples of Mapping of Biometric data to Topic	92
7.8	States of External Device maintained by Proxy	92
7.9	Description of notations used in Tier – two communications	93
7.10	Description of messages for Proxy and Publisher External Device communication	95
7.11	Description of messages for Proxy and Subscriber External Device communication	96
7.12	Topic Management Database	97
7.13	Device Information Database	98
7.14	Device Access Control Database	98

9.1	Comparison of proposed solution with [153]	111
9.2	Comparison of proposed solution with solutions proposing use of external device	112

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.

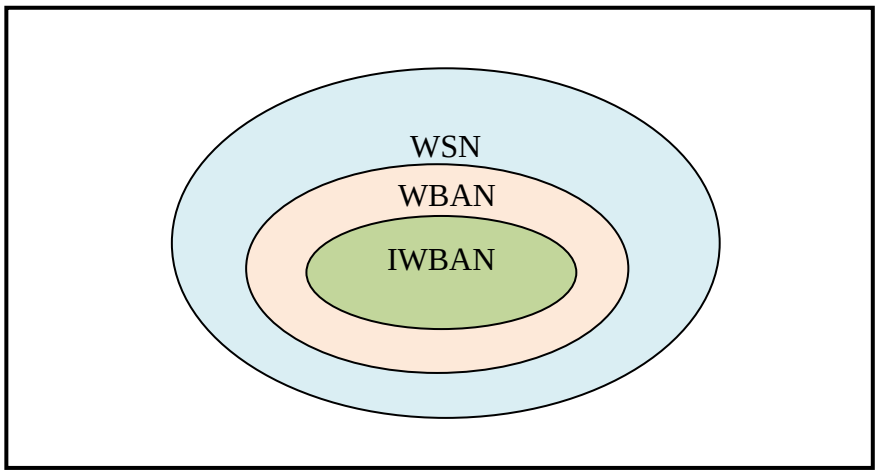

FIGURE 1.1 Position of Implantable Body Area Network

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.

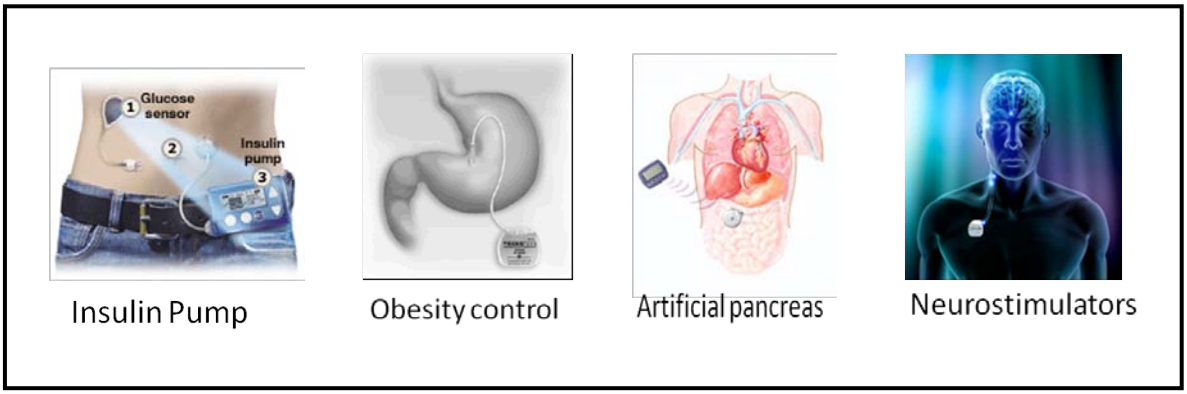

FIGURE 1.2 A range of IMDs (Photos: Medagadget)

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

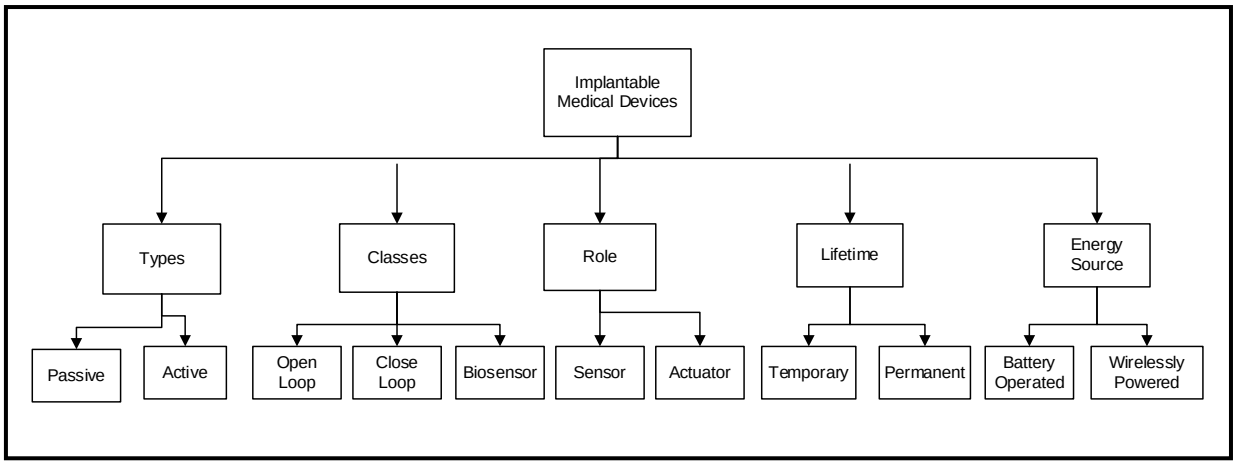

FIGURE 1.3 Classifications of IMDs

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.

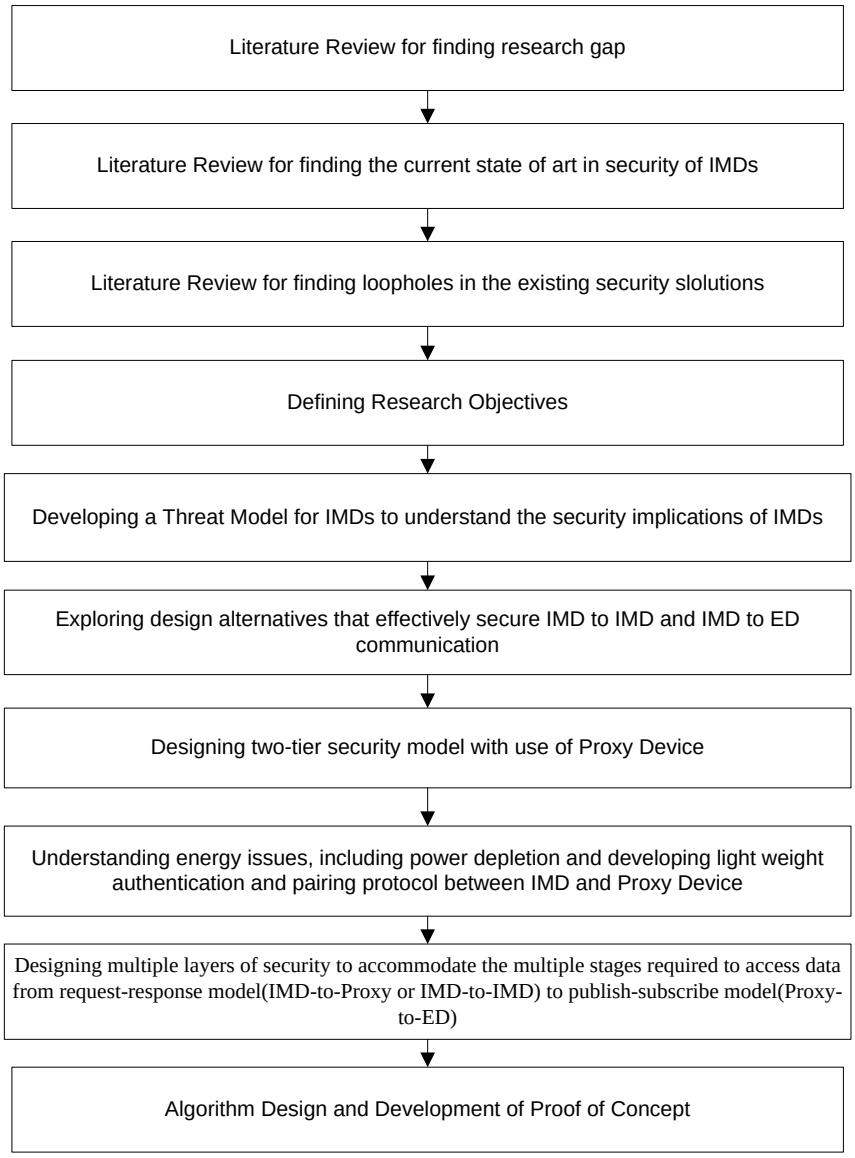

FIGURE 1.4 Phases Covered in Research Work

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.

CHAPTER – 2

Threat Modeling

2.1 Introduction

A literature survey of the existing body of work is essential during the entire process of doctoral work. The first phase of Literature survey was conducted to identify the broad research gap by referring to the research work that emphasizes on securing IMDs and also demonstrated attacks. This chapter is the outcome of the initial literature survey which helped us to derive a threat for IMDs as an outcome.

2.2 Threat Model

Recent security research has provided evidences that IMDs fail to meet the standard expectations of security for critically important systems. Ensuring security of wirelessly communicating IMDs is a critical issue as they perform life-critical or health-critical functions. Careful design of security technique either from scratch or by modifying existing techniques is the need of the hour. But before designing a security technique, the problem should first be clearly defined and the threats against which they will operate identified. A threat model is needed to adequately specify the security requirements. Our goal is to determine the threats that are of concern and should be defended against by proposing a comprehensive threat model for IMDs.

Threat modeling[35, 36] is the process of analyzing a software system for vulnerabilities, by examining the potential targets and sources of attack in the system. It has following benefits:

1. It prioritizes types of attacks to address.
2. It helps mitigating risks more effectively.
3. It helps identifying new potential attack vectors and vulnerabilities.

4. It adequately specifies security requirements

We find a lack of complete threat model for IMDs in literature. To address this gap, in this chapter we provide with a comprehensive threat model for IMDs which unifies previous work and discusses vulnerabilities and threats for wirelessly communicating inter-networked IMDs.

2.3 Related Work

There is a body of work which we referred and which identifies privacy and security vulnerabilities, threats and attacks and also indicates the mitigation steps. Following are the related work which emphasizes on security for IMDs:

In [16] tensions between design goals of wireless IMDs viz. security, safety, and utility is studied and it is stated that security and privacy goals of IMDs should to be in tandem with safety and utility.

In [14] attacks on confidentiality, integrity and availability of Implantable Cardiac Defibrillator (ICDs) are demonstrated and through reverse engineering it is shown that ICD discloses private information like patient name , hospital name and medical condition in plain. IMDs can be made to talk to unauthorized devices and commands may be replayed which may affect the functioning of these devices. These ICDs poses a risk of denial-of-service due to battery depletion when forced to communicate indefinitely with unauthorized party.

In [37] security issues of IMDs are described and major challenge of severe resource constraint is mentioned.

A survey [38] draws attention to technological approaches for improving IMD security and privacy including judicious use of cryptography and limiting unnecessary exposure to attackers. According to them premarket approval for IMDs should explicitly evaluate security and privacy and manufacturers should not rely on security through obscurity.

In [39] it is mentioned that networked IMDs have potential to communicate with other IMDs and establish complex feedback loops, such that attack on one IMD can affect others. It classifies vulnerabilities by their scope, level of access gained if exploited, cause (proximity, IMD activity, and patient state), result of exploitation (component affected, permanence). Also describes the protective, corrective, and detective countermeasures.

In [40] it is stated that along with security and safety, user acceptance, user environment, resource constraints, clinical effectiveness are also important factors for designing a security system. It categorizes security challenge through risk based analysis for Insulin Pump, Glucose Monitor and Continuous Glucose Monitor.

Work in [27] summarizes the recent work on IMD security. It identifies two classes of vulnerabilities. One is control vulnerability which includes unauthorized person gaining access and control of the IMD. Second is privacy vulnerability in which IMDs exposes the patient data to unauthorized person. It classifies the IMDs as open loop, closed loop and biosensors and enlists the threats for these classes. It classifies adversaries as passive having access to listening devices and active with the ability to generate radio transmissions. Such adversary may perform binary analysis by inspecting compiled code.

In [41], an overview of the trend of embedded devices is presented, with a case study of wearable and implantable medical devices and discussion on the vulnerabilities, security challenges and steps towards addressing them.

In [42] it is stated that security and privacy risks of medical device should be addressed at manufacturing phase itself to make them safe and effective. The risk of malware, use of old software versions and upgradability issues may lead to diminished integrity and availability.

It [43] shows possibility of subtle eavesdropping and injection attacks on sensor inputs which form the primary source of data for IMDs for making actuation decisions.

In [44] authors observed that poor security design can result in real vulnerabilities impacting the privacy, integrity and availability of the device.

In [45], author discusses the trustworthiness of medical devices and categorizes the solutions available for radio attacks as: (i) those proposing close-range communication to authorized devices, (ii) the introducing cryptography in IMDs and (iii) the use of external devices to support security processing for IMDs. [46] is a survey of security techniques relevant for IMDs.

A recent survey [47] enlists three categories viz. telemetry interface, software, and sensor interface layers in which security threats needs to be addressed.

In [48] author examines privacy related threats, and classifies them as identity threats (misuse of patient's identity), access threats (unauthorized access of patient health information) and disclosure threat (unauthorized disclosure of patient private health

information).Such is the seriousness of the issue that The U.S. Federal Drug Administration (FDA) has recently called for manufacturers to address cyber security issues relevant to medical devices [49].

In [50] access control approaches for IMD and three intra-body secret keys exchange techniques viz. acoustic, electric, and electromagnetic signals are surveyed.

2.4 Vulnerability and Threats in Existing IMDs

In absence of security association between IMD and external devices, we found multiple vulnerabilities that IMDs become exposed to. These vulnerabilities of IMDs are susceptible to exploitation by attackers leading to threats of different impact. A comprehensive list of vulnerabilities and resulting threats and demonstrated attacks by security researchers are presented in Table II.

TABLE 2.1 Vulnerabilities and Threats in IMDs

Vulnerability	Threat	Justification
Magnetic switch based access	Tampering with device settings;Unauthorized changing or disabling of therapies, continous wake-up calls to device	Attack on authentication using out-of band channels like audio, video or tactile is presented in [51]
Wireless mode of communication	Loss or disclosure of sensitive information; Traffic Analysis; Wireless Jamming ;Replay of older commands	An attack against an ICD using a software radio can deliver untimely defibrillation (shock) [14].
Networked IMDs	A compromise on one IMD may affect others; Distributed Denial of Service attack	Demonstrated theoritically in [41]
Limited or nonexistent authentication	Unauthorized telemetry access and commands; Denial of Service	Use of USB device to control the insulin pump's operations by intercepting wireless signals sent between the sensor device and the display device on BG monitors and to display inaccurate readings by knowing just the serial number [52].
Limited battery, storage and processing capacity	Battery Depletion; Inability of performing security related processing	Battery depletion demontrated in [48]
Wirelessly Programmable	Sophisticated attacks; Zero day attacks; reprogramming attacks without close proximity	Reprogramming attack demonstrated in [38]
Software and	Buffer overflow attack, Side Channel	Singnal injecton attack demontrated in

firmware design without considering security	Attack, Malwares ;Binary Analysis, Device Malfunction; Injection attacks	[43]
Telemetry without encryption	Harvesting Privacy Information	Eavesdropping demostrated in [28]
Granting access without authentication and authorization	Tampering with device settings;Unauthorized changing or disabling of therapies; MITM	Fatal attacks on Insulin Pump System like disabling the device alarm and delivering of a lethal dose were also demonstrated[52].
Tradeoff between security and safety	Inability to enforce stringent security measures to cater to immediate access during emergency.	Consequences demonstrated in [53][27[80]
Remote accessibility	Masquerade, MITM, DOS; Repudiation	Man-in-the-middle attack was demonstrated on a Bluetooth-enabled pulse-oximeter system in [54]

2.5 A Hypothetical Attack Scenario

To help visualize the security attacks on IMDs, we are taking a hypothetical scenario as shown on Fig 2.1.

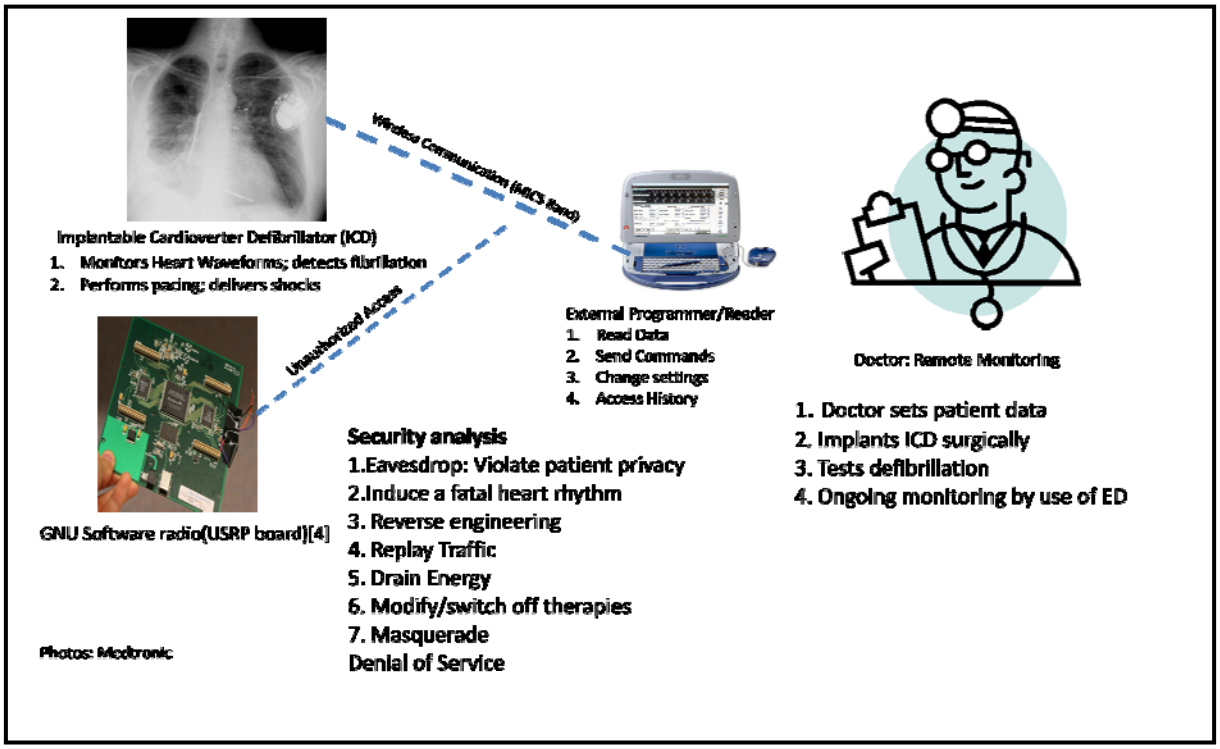

FIGURE 2.1 A Hypothetical Attack Scenario

A doctor sets patient data in the ICD during surgerical implantation into human body. He tests defibrillation to ensure that the device is working properly. Now onwards doctor performs monitoring by means of wireless channel by using an external programmer or reader. The external device reads data, sends commands to the device, changes settings to modify therapy and may also access the patient's history. An attacker may use GNU software radio or other off-the-shelf devices to perform unauthorized actions like eavesdropping to violate patient privacy. From the captured packets, attacker may reverse engineer the device ID and other information pertaining to patient [14], induce a fatal heart rhythm, replay recorded commands, drain energy of IMD battery, modify or switch off IMD therapies, masquerade or pose denial-of-service.

2.6 Adversarial Model

Threat modeling for IMDs presents significant challenges due to unavailability of these devices for security researchers to conduct experiments. In this section, we mention the attack sources, specify our assumptions, and present the threats that arise due to the insecure wireless communication and networking of IMDs. We provide a comprehensive listing of vulnerabilities and threats and then make use of Microsoft's threat modeling tool to generate threat model analysis report. As shown in Fig 2.2, adversaries are mainly classified as passive that perform a passive attack like eavesdropping or traffic analysis or active that has the capability of performing one or more active attacks.

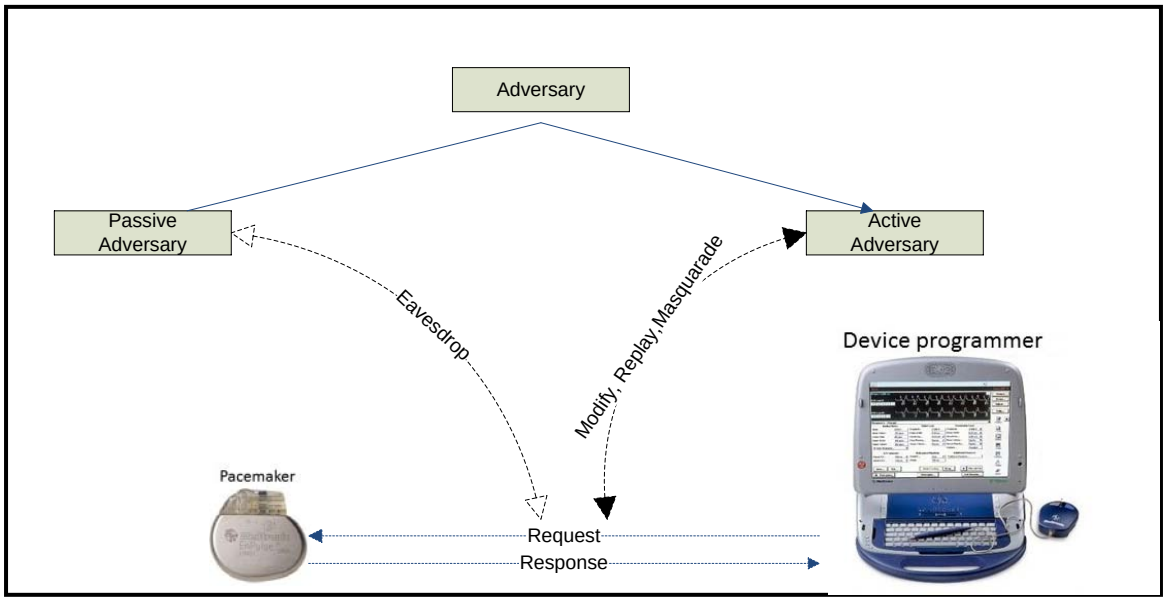

FIGURE 2.2 Types of Attackers

Different classes of Adversary that can be a passive or an active attacker and can harm the system are:

1. Insider: Such an adversary is a legitimate part of the system and therefore most difficult to identify. A patient himself my tamper with the data to fool insurance agencies.
2. Software Cracker: Such an adversary may gain control of IMD of similar make and reverse engineer the firmware to gain a lot of details.
3. Jammer: Such an adversary may perform jamming to hamper the wireless communication.
4. Rouge Device Owner: Such as adversary may own similar devices which communicate in MICS band and make the rouge device part of the network.

Table 2.2 Classification of Adversary

Adversary Type	Action	Equipments Used	Impact	Security Service
Passive	Eavesdrops radio communication	Oscilloscope, software radio, directional antenna	Compromises Confidentiality	Data confidentiality
Active	Generates false radio transmission or manipulates, replays stale commands	Programmable Radios	Disabling of therapies, injecting excessive dosage, changing interpretation , shutting down or changing IMD behavior	Integrity Assurance, Authentication, Replay Resilience
Insider	Part of the system and holds legitimate information	Legitimate devices	Manipulation and tampering	Access Control
Software Cracker	Binary analysis	Source Code inspection and Analysis Tools	Analysis of the underlying cipher and protocol	Use of publicly studied cryptographic primitives
Jammer	Physical Jamming of communication	Jammer equipment	Communication is hampered	Anti-jamming Techniques
Rouge Device owner	A rouge sensor or rouge external device is	IMDs, Universal Software Radio Peripheral (USRP) [14] and external devices available in market	MITM attack, result manipulation	Continuous Authentication

Apart from simple passive and active attacks, more sophisticated attacks are possible. Some of them are given below:

1. **Binary Analysis:** By doing a binary analysis on the software of IMD an adversary may understand its operations and may also reverse engineer the communication protocol to break it.
2. **Reprogramming Attack:** By analyzing bugs in the software program of IMD, this attack forces the device to behave in an unpredictable manner. Attacks like buffer overflow or injection are also possible.
3. **Insecure software update:** The software in the IMDs are upgradable by patches to enhance functionality. An attacker may update the IMD software to make it behave in an unpredictable manner.
4. **Malware based Attack:** A malware is a program which masquerades or embeds itself in another program to get activated later to carry out harmful actions like erasing the device memory.
5. **Denial-of-Service:** Posing Denial-of-service (DOS) by blocking the communication between IMD and the external device or forcing IMD to communicate continuously thereby depleting its battery.
6. **Networking related Attack:** Multiple IMDs on a human body may be networked in an IWBAN. Security compromise on one device may adversely affect the other devices also leading to false diagnosis, treatment and actuation.
7. **Repudiation:** An attacker especially an insider may tamper the device or perform action that he may deny later.
8. **Elevation of Privilege:** Medical staffs who access the IMD may indulge in supplying commands of higher privilege and due to lack of access control may be successful in doing so.
9. **Spoofing:** A rouge device may be used to masquerade as another authorized device and gain illegitimate access.

The threats arising are by and large interrelated and interdependent on each other and need to be considered together for mitigation. For example if software does not implement proper input validation, forged packets can be injected through wireless medium [4].

2.7 Threat Modeling using SDL Tool

As a popular and free tool for threat enumeration we make use of Microsoft SDL Threat Modeling Tool [55] to perform threat modeling using a four-step process which helps in

identifying security objectives, creating the application overview, decomposing application to uncover threats, threat identification and vulnerability identification.

Step1: Creation of data flow diagrams that represents the flow of data through the system that is being modeled for threats. Fig. 2.3 shows the context level DFD for IMDs performing wireless communication with external devices.

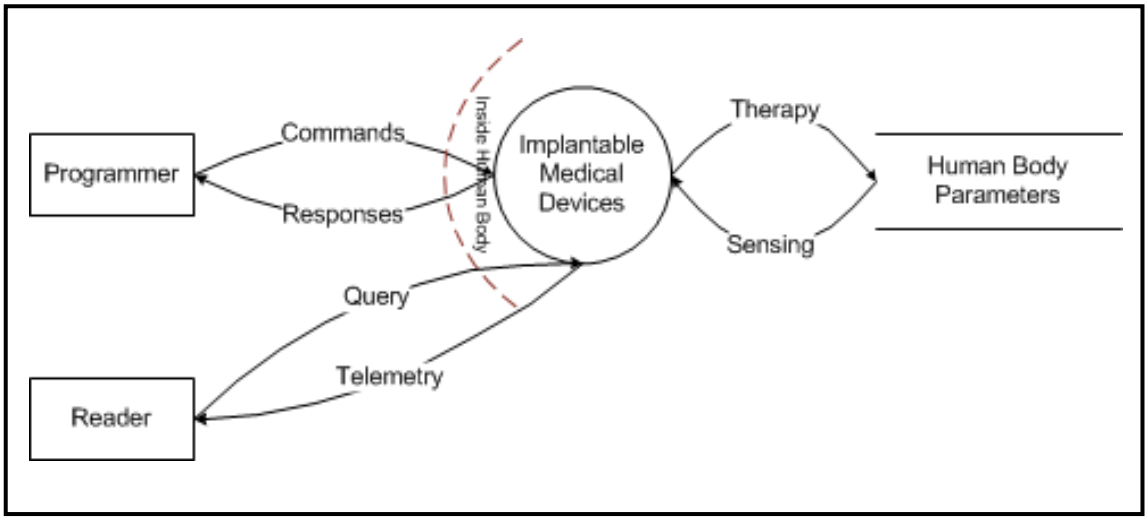

FIGURE 2.3 Context Level DFD for IMDs

In the next step, level one DFD is shown in FIGURE 2.4.It shows the IMDs which are networked using wireless medium to perform sensing and actuation.

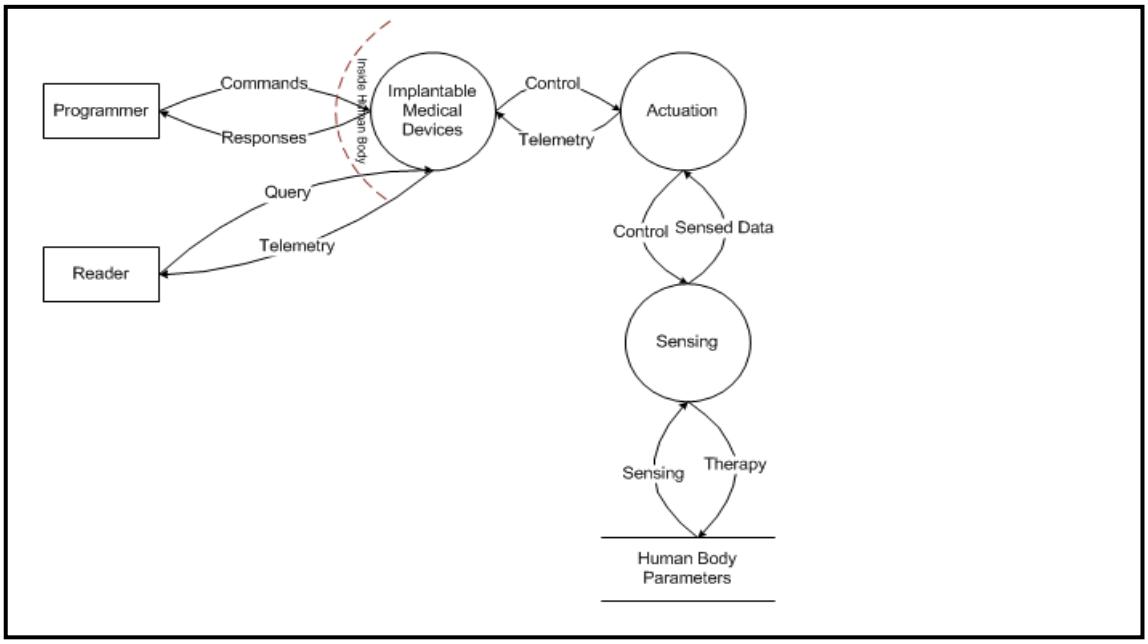

FIGURE 2.4 Level One DFD for IMDs

Step 2: Generation of a list of threats by running the tool. Table 2.3 shows the threat analysis report.

Step 3: Description of the environment in which the software will run. For example Wireless Environment and Implanted in Human Body.

Step 4: Report Generation. Finally we generate the threat model analysis report as shown in Figure 4 which shows a plethora of threats.

Table 2.3 : Threat Analysis Report

Threat Model Analysis Report:

Empty Threats

The following threats have no threat description:

Element Name	Threat Type
Commands	Tampering
Commands	InformationDisclosure
Commands	DenialOfService
Query	Tampering
Query	InformationDisclosure
Query	DenialOfService
Responses	Tampering
Responses	InformationDisclosure
Responses	DenialOfService
Sensing	Tampering
Sensing	InformationDisclosure
Sensing	DenialOfService
Telemetry	Tampering
Telemetry	InformationDisclosure
Telemetry	DenialOfService
Therapy	Tampering
Therapy	InformationDisclosure
Therapy	DenialOfService
Human Body Parameters	Tampering
Human Body Parameters	Repudiation
Human Body Parameters	InformationDisclosure
Human Body Parameters	DenialOfService
Programmer	Spoofing
Programmer	Repudiation
Reader	Spoofing
Reader	Repudiation
Implantable Medical Devices	Spoofing
Implantable Medical Devices	Tampering
Implantable Medical Devices	Repudiation
Implantable Medical Devices	InformationDisclosure
Implantable Medical Devices	DenialOfService
Implantable Medical Devices	ElevationOfPrivilege

2.8. Conclusion

The threat model shows it is necessary for IMDs to have an effective protection and/or detection mechanism for fighting against these attacks. Security services needs to be selected judiciously for securing such devices.

CHAPTER – 3

Literature Survey

In this chapter, we present a complete taxonomy and comparison of various communication security schemes proposed in literature on the basis of following security and design dimensions:

1.1. Security Dimensions

1. Key Management Provision: Whether the given scheme involves generation, distribution, and (periodic) replacement of keys used for securing the telemetry message to and fro the IMD.
2. Authentication Provision: Whether the given scheme verifies the identity of communicating devices and also that a message originates from the verifiable authenticated entity.
3. Message Integrity Provision: Whether the given scheme confirms that a message has been received correctly without unauthorized modification.
4. Confidentiality Provision: Whether the given scheme prevents disclosure of telemetry message to unauthorized entities.
5. Availability Provision: Whether the given scheme protects the IMD to ensure its availability and accessibility by authorized entities.
6. Access Control Provision: Whether the given scheme has the ability to limit and control the access to IMD and its application via a wireless communication link.
7. Non-repudiation: Whether the given scheme prevents communicating entity from denying transmission of a message or command.
8. Replay Attack Resilience: Whether the given scheme ensures message freshness to avoid a replay of stale packets.
9. Privacy Provision: Whether the given scheme satisfy privacy goals like IMD existence privacy; IMD type privacy; Specific IMD-Identification privacy; Measurement and log privacy; Bearer privacy and Tracking Privacy as explained in [16].

3.2 Design Dimensions

1. Protection Type: Whether the given scheme provides Detection of the attacks or Prevention from security attacks or both.
2. Target Device: Whether the given Scheme is applicable to all IMDs or to a specific type of IMD.
3. Invasiveness: Does the scheme require any modification in existing IMDs? If yes, is it a software modification (S/W) or a hardware modification (H/W) or both (BOTH).
4. Core Mechanism: What is the core mechanism on which this scheme is based on?
5. Access Pattern: Does the scheme secure communication during regular access (RA) or emergency access (EA) or in both the cases (BOTH)?
6. Energy Source: From where is the power required to do security related processing derived?
7. Flexibility: Does the scheme provide flexibility to change encryption algorithm and cipher if their security is compromised or a better one is available?
8. Applicability: Is the scheme applicable for IMD and external device communication (IMD↔ED) or for IMD to IMD communication (IMD↔IMD) or both for (BOTH).

3.3 Taxonomy of Security Models proposed in Literature

As these devices are evolving, the communication security schemes pertaining to them are also emerging. We discuss the communication security schemes provided in literature. Table 1 provides a complete summary of the classification scheme designed by us.

3.3.1 Inhibiting Long Range Communication

Inhibiting Long-Range Communication is a simple way of limiting access to IMD without making use of any security services and mechanisms. Even though it puts zero expense on IMDs resources, it is only effective against radio attacks launched from a certain distance. Problem remains if an attacker can pose an attack within a small distance from patient or make a physical contact. As in reality close-range communication schemes cannot defend against security and privacy attacks, we will not consider this category in our comparison oracle. Still they are worth a mention as they can be used in conjunction with security mechanisms. The proposed schemes are as under:

3.3.1.1 Use of small-range communication channel

Here, a wireless communication channel with limited range is chosen. The popular options are:

1. Radio frequency identification (RFID) based channel : RFID based channel between medical devices and external device is proposed in [56, 57]
2. Near Field Communication (NFC) : To improve privacy, Near Field Communication (NFC) with 3G smart phones is proposed in [58]. According to [59], NFC protocols currently do not provide an appropriate privacy properties for implanted medical applications.
3. Body Coupled Communication (BCC): Body Coupled Communication (BCC) which uses the human body as the transmission medium is proposed in [28]. BCC achieves very low data rates and the external device needs to be in vicinity of human skin.
4. Inductive coupled communication: Inductive coupled communication is used in [17]. Inductive coupled communication is not secure as presence of an eavesdropper may hamper communication by detuning the data transfer [60]. Moreover, an attacker with strong enough transmitters and a high-gain antenna can eavesdrop on the wireless channel even from up to ten meters away [61],[62].

3.3.1.2.Enforcing Proximity

These schemes allow external device to access IMD only if it is in close proximity.

1. **Ultrasonic distance-bounding**: An access control scheme based on ultrasonic distance-bounding is proposed in [29]. In this scheme, IMD grants access to only those devices that are close enough. IMD can operate in two different modes, in normal mode remote monitoring can be performed if reader is in possession of a shared key. During an emergency or for device reconfiguration, reader just needs to be within certain security range. Secret key is shared by Diffie-Hellman key exchange. Ultrasonic distance bounding requires RF shielding, moreover it is vulnerable to RF wormhole and distance-hijacking attacks as mentioned in [63]. This scheme also suffers from drawbacks like authentication using pre-shared keys which cannot be renewed, battery depletion attack by performing continuous authentication attempts and need for hardware modification in IMD.

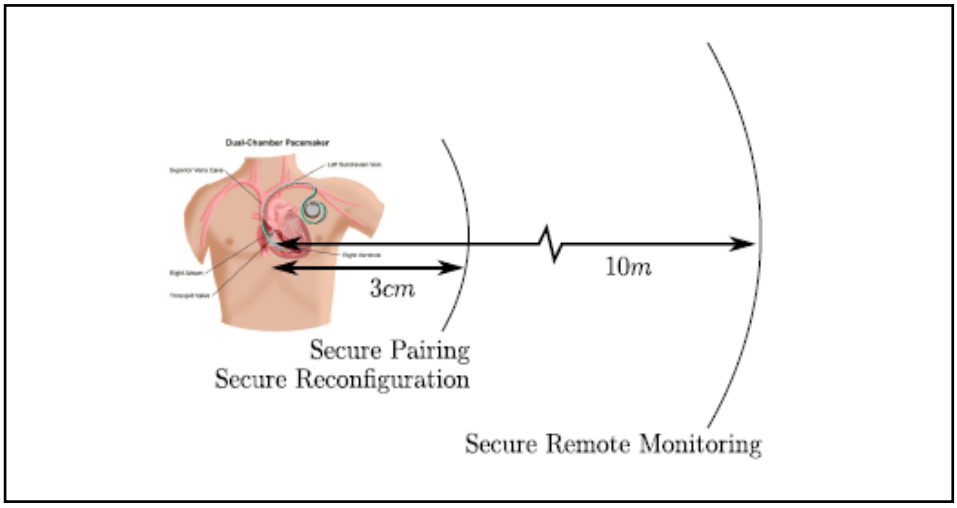

FIGURE 3.1Allowing reconfiguration from smaller distance and remote monitoring from longer distance [29]

2. **Location based service (LBS):** In order to prevent replay attacks, collusion attacks, and distance spoofing attacks, another scheme [64] is proposed based on the use of multiple location based service (LBS) devices by utilizing Bluetooth. Access is granted if the reader is located within a trusted area. The medical personnel's reader sends a broadcast message to nearby LBS devices which sends their partial key and signature to the medical personnel's reader. These keys are used by the reader to access nearby patient's medical data. Installation of LBS devices is a costly affair and key exchange between LBS devices and IMD is not explained. This scheme gives rise to a new vulnerability if one or more LBS devices are compromised.

3.3.2 Using Cryptography

As closed range schemes were incapable of addressing most of the challenges, as a matter of fact cryptography appeared as the most eligible approach. Cryptography can be classified as symmetric and asymmetric. Symmetric ciphers on one hand are considered to have lower computational complexity, power and energy requirements compared to asymmetric ones but on the other hand require each communicating party to access a unique key for maintaining communication confidentiality. Asymmetric systems feature simpler key management by investing more resources. Moreover use of cryptography prevents medical staff from accessing the patient's health data in case of an emergency if they do not have

credentials. Hence encryption scheme should be chosen considering the nature of the data, required security level and device constraints. As cryptography is a mere building block and needs to be complimented with a secure communication protocol, therefore we will not consider this category in our comparison oracle.

3.3.2.1 Using Symmetric Cryptography

In [28] Rolling Code Cryptography is proposed for encryption of telemetry data between IMD and external device. Authors in [65] propose a lightweight security protocol for ultra-low power ASIC Implementation to provide authentication, confidentiality and integrity that gives low-energy computation. But the secret key shared between IMD and base station is hard coded and cannot be renewed if compromised. Also it does not guarantee availability and is prone to DOS (Denial of Service) attacks. Hardware implementations of Hummingbird which is a combination of block and stream cipher is proposed in [66] and [67]. In [68] block cipher based security protocol based on Advanced Encryption Standard (AES) algorithm. The protocol works in stream mode for basic security and in session mode for strong security and uses role-based user authorization scheme. In [69] symmetric block ciphers are evaluated for average and peak power consumption, total energy budget, encryption rate and efficiency, program-code size and security level. According to them MISTY1[70] is superior as far as power consumption factor is considered.

3.3.2.2 Using Asymmetric Cryptography

Certificate-based approaches [59] require the IMD reader to be able to access the Internet for certificate verification, and presence of a global certifying authority (CA) is needed to maintain public key certificates. A reader may not always have online access, also it is costly to maintain and track Global Certification Authority for every IMD and such support may not be available all the time. The authors of [71] suggest use of elliptic-curve cryptography (ECC) algorithm to set up symmetric keys between sensor nodes and the base station. However, it is computation-inefficient and vulnerable to DoS attacks and thus unsuitable for IMDs.

3.3.3 Key Distribution and Management

Symmetric key cryptography is favorable in all aspects as explained above but the challenge it poses is of secret key exchange, management and renewal. Therefore literature of work in this area for Implantable Medical Devices is also worth a mention. To address the challenge of key distribution, initially a universal key was proposed to be preloaded in devices of the same model known to manufacturer and patient's doctor. It is it easy for an attacker to discover the secret key of a particular model as they devices can be bought online also. Therefore, secret keys specific to a patient's device were proposed. Such schemes are discussed below.

3.3.3.1 Putting Patient in the Loop

In [72], medical staff is allowed to access an IMD using an access token which can be a USB stick or bracelet configured with secret key, for secure data download and programming. These access tokens need to be protected from theft, if lost or stolen or forgotten, it creates a safety problem by rendering the IMD inaccessible. Moreover, keys in IMD are not reconfigurable once leaked. Authors in [73] propose password to be tattooed as ultraviolet-ink micro pigmentation which is invisible under normal light. Devices that interact with IMD must be equipped with reading mechanism to interpret the tattoo and an input mechanism for key entry. This technique itself mentions the risk of infection for patients from micro pigmentation and the risk that a tattoo could be rendered unreadable when needed. Moreover keys cannot be reconfigured in IMD one disclosed. As these solutions are naïve, therefore we will not consider this category in our comparison oracle.

3.3.3.2 Use of Patient Biometrics

In [74] author demonstrates possibility of using biometrics, specifically the inter-pulse interval (IPI), as a shared secret to securely share encryption keys among sensor nodes on the same body. In [75] author proposed use of Biometrics derived from patient body to secure the keying material for a network of implanted biosensors. Fuzzy commitment scheme with error correcting codes was used for error correction in different biometric readings taken independently. In [76] authors propose an algorithm for Physiological Value-based key-agreement, called OPFKA, that can also reduce the storage costs associated with fuzzy vaults. Emergency Access is provided in [77] by utilizing a patient's biometric information (iris recognition) to perform authentication. These schemes based on

biometrics lacks a rigorous security analysis as shown in [53] and also lacks possibility of utilization for a wide range of IMDs. The reader/programmer device needs to be brought sufficiently closer to the patient for biometric exchange to take place which is not a feasible solution for remote monitoring.

3.3.3.3 Use of Physical Layer Approaches

1. **Telemetry Data obfuscation:** In [78] instead of using cryptography, author uses a low cost multilevel key-based scrambling algorithm. It is stated that biological signals are bursty in nature and can be obfuscated to provide security. Two levels of encoding are performed. First part of key is used to determine the order of scrambling and second key is used change the order for each packet. By storing only the required permutations for a key, hardware overhead is minimized. This scheme requires strenuous security analysis.
2. **Physical Layer Approach:** Authors in[79] use Reciprocal Carrier-Phase Quantization for refreshing symmetric encryption keys in IMDs. They claim reciprocal quantization of the phase between local oscillators can be used without consuming IMD resources for key exchange. This can be further coupled with symmetric encryption for secure communication.

3.3.4 Using Trusted External Device

On one side when encryption and key exchange schemes were proposed, IMD resource constraint was still posing a challenge. To preserve IMD's resources (battery power), authentication of incoming requests was proposed to be offloaded to a trusted external device, which, unlike IMDs, can be easily recharged. This approach had potentials to even protect the IMD against battery-draining attacks. Therefore different schemes based on this avenue were proposed which can be classified as Invasive meaning one that require design or software changes in the current IMDs and Non-Invasive meaning the scheme can directly work with existing IMDs without any modifications. While non-invasive schemes provide great advantage for existing IMDs; invasive schemes are more robust.

3.3.4.1 Invasive Approaches

1. **Communication Cloaker:** A removable external device is proposed in [80] that provides fail-open defensive countermeasure. It controls access to the IMD by making it invisible to all unauthorized devices. It encrypts all communications to

and from the IMD and checks them for authenticity and integrity. It provides fail open access during emergency when removed and shifts power-intensive computation to the cloaker reduces battery consumption. Being chargeable, it can protect against battery draining attacks but no implementation is shown.

2. **WISPer:** Zero-power defenses [14] which means security at no cost to the IMD battery have been proposed for IMDs, in which the induced RF energy is harvested for notification, authentication, and key exchange. It uses RFID-style remote powering until the authentication process is completed, and then more general access to the implanted device and battery are enabled. External device (battery less proxy) is used by medical staff to negotiate a temporary key with the IMD through the patient's body by acoustic signaling to access the IMD. Zero-power notification harvests induced RF energy to wirelessly power a piezo-element that audibly alerts the patient of security-sensitive events at no cost to the battery. Zero-power authentication uses symmetric cryptographic techniques to prevent unauthorized access; it aims to protect against adversaries. Sensible key exchange combines techniques from both zero-power notification and zero-power authentication for vibration-based key exchange that a patient can sense. This scheme is susceptible to attacks on privacy and eavesdropping during key exchange.
3. ***Heart-to-heart (H2H) Authentication:*** Authors in [81] designed a security scheme which uses ECG (heartbeat data). Their scheme performs a cryptographic device pairing protocol that uses Physiological Values randomness to protect against attacks by active adversaries. It requires the IMD and external device to measure the PV simultaneously which requires physical proximity and therefore is not useful during remote monitoring. Moreover, they assume a Transport Layer Security (TLS) channel established between IMD and external device. TLS protocol is resource intensive therefore not advisable to be implemented in IMD.

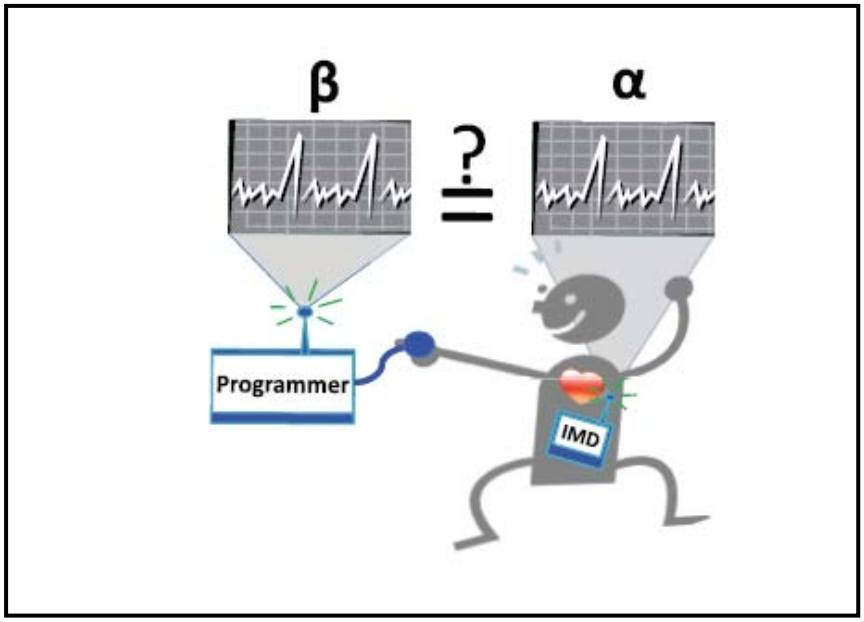

FIGURE 3.2 ECG readings taken simultaneously by IMD and external device is matched to allow access [81]

1. **SISC *for Secure Implants:*** In [82], a new implant system architecture is proposed where security and main-implant functionality are made completely decoupled by running the tasks onto two separate cores. The security core is powered by RF-harvested energy for it to perform external-reader authentication without fearing about Denial-of-Service (DoS) attack against battery. Authentication is performed without drawing energy from implant's battery by harvesting energy from requesting entity. The low-power security processor that executes the communication protocol is called Smart-Implant Security Core (SISC) and is designed to work independently from the primary implant module. It provides mutual authentication between IMD and external reader. It relies on offline key distribution and on fail open access in case of emergency.
2. ***Powerless Mutual Authentication:*** In [4] RF- energy harvesting is used to mitigate battery constraint and biometric key extracted from ECG signals is used for mutual authentication in regular and emergency access. It also protects the ICD against clogging attacks.
3. ***Trust Based Security:*** To meet the requirements on low computational complexity, N-th degree truncated polynomial ring (NTRU)-based encryption/decryption is used to secure IMD–sensor and sensor–sensor communications in [83]. This scheme is based on direct/indirect trust relationship among sensors.

3.3.4.2 Non-Invasive Approaches

1. **Shield**: Uses physical layer mechanism for secure communication with IMD and cryptographic channel to communicate with external devices. It deals with passive as well as active attacks. It works as a personal gateway which acts as a jammer-cum-receiver and jams the messages to make them and unauthorized commands IMDs preventing others from decoding them while itself being able to decode them [84]. It then encrypts the IMD message and sends it to the legitimate programmer. All commands must be encrypted and sent to the shield first, which is then relayed to the IMD. Being non-invasive for IMDs, it requires changes in all programmers. Here, confidentiality is not warranted for data exchange between shield and IMD. It is not effective for radio technology due to potential legal issues with jamming.

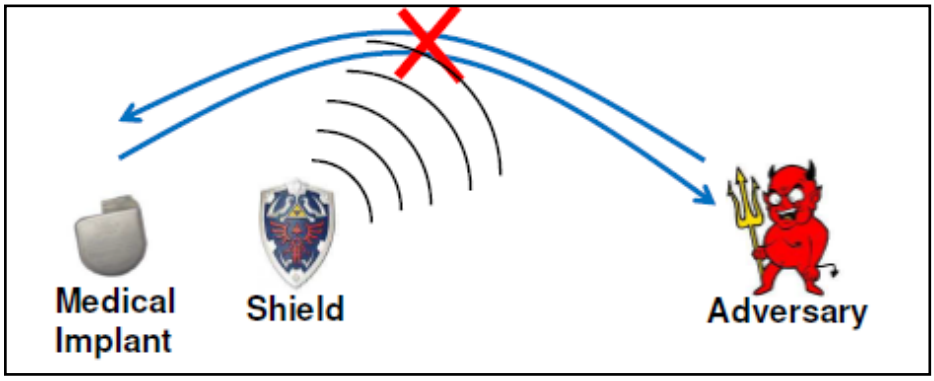

FIGURE 3.3 Shield Jamming Unauthorized Communication [84]

2. **MedMon:** Authors in [45] propose a medical security monitor (MedMon) for detection of active attacks by snooping (passive monitoring) on radio communication. It uses multi-layer anomaly detection. Physical anomalies are detected by observing received signal strength indicator (RSSI), time of arrival (TOA), differential time of arrival (DTOA), and angle of arrival (AOA). Behavioral anomalies are identified by checking with historical data and commands. On detecting malicious activity either audibly notifies the user or jams the communication. It requires to be trained to differentiate normal and malicious behavior. Like in other such systems, it may suffer from false positives and false negatives. Moreover this scheme does not protect from passive and replay attack.
3. **BodyDouble:** Authors in [85] employ a non-key based security scheme by use of external authentication proxy embedded in a gateway and paired with IMD. As in

[84] gateway transmits jamming signals to jam every incoming request to the IMD but itself receives the request and performs authentication using digital signals, for attacker it establishes a spoofed connection to thwart repeated attacks by same attacker. Here, communication is not encrypted (assumes a covert encryption channel) and authentication scheme cannot protect against identification frauds as IMD device ID and FCC ID are used for authentication.

4. **IMDGuard:** Authors in[86] secures Implantable Cardiac Devices(ICDs) by an external device that utilizes the patient's electrocardiography signals for key extraction. It is a device that would pair with an IMD and use radio jamming to defend against eavesdropping and unauthorized commands under non-emergency conditions. IMDGuard protocol is subjected to man-in-the-middle attack that reduces its effective key length as shown in [42].
5. **Statistical/Machine Learning:** Author in [37] proposes elliptic curve cryptography (ECC)-based key-management protocol to securely derive and update symmetric keys between medical sensors and collection devices. Protocol enables symmetric keys to be derived without the existence of any prior shared secrets, making it scalable to large systems. Collection device uses a two-tier authentication scheme to verify the source of incoming patient data. At the first tier, data from patient is accepted only if biometric signature matches. At the second tier, incoming physiological data is continually passed to a filter that assesses whether the data is consistent with prior data from that patient. The filter uses statistical or machine-learning techniques to learn a patient’s profile and then raises an alarm if incoming data deviates from that profile. An alarm could be triggered by falsified patient data or an acute change in the patient’s medical condition. This scheme does not consider the power constraint of IMD to a large extent.
6. ***PIPAC:*** Patient Infusion Pattern-based Access Control Scheme for Wireless Insulin Pump System [87]uses Smartphone to provide physical layer as well as application layer security. At physical layer Near Field Communication (NFC) based access control and at application layer it uses past glucose trends to detect anomalous insulin pump system behavior. This scheme can be used to defend against security attacks in particular (1) single acute overdose and (2) chronic overdose. It uses SVM based regression scheme and a supervised learning approach to learn normal patient infusions pattern with the dosage amount, rate, and time of infusion, which are

automatically recorded in insulin pump logs. The generated SVM based regression models are used to dynamically configure a safety infusion range for abnormal infusion identification. Abnormal infusions of bolus dosage, basal rate, and total daily insulin would send an alarm to the patient and can be deactivated during emergency to give fail open access. This scheme suffer from False Positive and False Negatives.

3.3.5 Emergency Access for IMDs

In Emergency State stringent security policies may pose a risk of inaccessibility for the IMD [80] [27] if authorized staff is unavailable threatening safety of patient. Therefore a viable solution is to disable security in case of an emergency. But this may turn out to become the weakest link for an unauthorized person to gain control of an IMD's operation or disable its therapeutic services, this may also motivate the attacker to induce false emergency. Therefore it is important to look into the solutions which work even during emergency.

1. **Biometric Based:** [77] provides biometric based two-level secure access control scheme for IMDs for use in emergency situation. The first level uses basic biometric information and second level requires iris recognition. This technique has limited use as it requires external devices to be equipped with features of biometric measurement.
2. Heart-to-heart (H2H): In [81] ICDs can be accessed in emergency by external device kept very close to patient's heart for matching of physiological values sensed by reader and ICD simultaneously.

3.4 Comparison of Security Models

In this section we discuss the merits and demerits of available security schemes. This field witnesses many state-of-art solutions for securing IMDs while considering the power management, emergency situations, and essential security properties as shown in Table 3.1. But there are certain loopholes. While none of the security scheme addresses IMD privacy and non-repudiation challenge, most of them also lack in Key Management front.

TABLE 3.1 Comparisons of Surveyed Security Models

	Proximity [29]	***IMDShield [84]***	**MedMon [45]**	**IMDGuard [86]**	**Cloaker [80]**	**H2H [81]**	**WISP [14]**
SECURITY DIMENSIONS							
Key Management	Yes	No	No	Yes	No	Yes	Yes
Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Message Integrity	No		Yes	No	Yes	Yes	No
Confidentiality	Partial	Yes	No	Yes	Yes	Yes	Yes
Availability	No	No	No	No	Yes	No	Yes
Access Control	No	No	No	No	No	No	No
Non-repudiation	No	No	No	No	No	No	No
Replay Resilience	No	No	No	No	No	Yes	No
Privacy	No	No	No	No	No	No	No
DESIGN DIMENSIONS							
Protection Type	PREV	PREV	DET	PREV	PREV	PREV	PREV
Target Device	All IMD	All IMD	All IMD	ICD	All IMD	ICD	All IMD
Invasive	Yes	No	No	Yes	Yes	Yes	Yes
Core Mechanism	Distance Bounding	Jamming	Anomaly Detection	Jamming	Secure Protocol	PV exchange and TLS	WISP
Access Pattern	Both	REG	REG	REG	REG	Both	REG
Energy Source	IMD battery	Shield Battery	External	External	External	IMD battery	Energy Harvesting
Flexibility	No	No	No	No	No	No	No
Applicability	IMD-ED	IMD-ED	IMD-ED	IMD-ED	IMD-ED	IMD-ED	IMD-ED

Most of the scheme uses a naïve technique of access control which is neither role based nor context aware. Quite a few schemes are device specific and cannot be used for all IMDs and do not address the heterogeneous nature of IMDs. These schemes secure wireless communication between an IMD and external device but fail to work for multiple IMDs implanted on a human body and internetworked with each other. The shortfalls are enumerated below:

1. Most of the schemes use pre-shared keys over a long period of time makes them vulnerable to cryptanalysis attacks.

2. Most of the schemes do not take IMD interoperability as design criteria.
3. Most of the schemes do not provision encipherment technique upgrade.
4. Above schemes do not address Privacy Issues.
5. Most of the schemes provide naïve access control which is neither role based (fine grained) nor context aware.
6. Above schemes do not provide non-repudiation.
7. Most of the schemes adopt fail-openness during emergency which leads to no security during emergency.
8. Most of the schemes are not scalable when more IMDs are added.
9. Many schemes are device specific thus not suitable for a wide range of IMDs.

3.5 Conclusion

In this chapter we have presented a complete taxonomy of security models designed in order to achieve communication security for IMDs. Our analysis shows that more emphasis has been given to securing IMD and External Device communication while paying less heed to IMD and IMD communication. We have identified several areas of future work such as need for a generalized and complete model for securing wireless communication of an IMD on a human body. Also the scheme needs to be autonomous for wide acceptability by patients who cannot afford to configure and maintain rigorous security schemes. Finally, as the IMD devices evolve to include interoperability the security scheme must evolve as well to cater to the increasing demands of security. As the external devices based approach is the most flexible and scalable option in which sophisticated security mechanism can added depending on the need of IMDs we use this model from development of a security solution.

CHAPTER – 4

A Buddy System for Securing Wireless IMDs

This chapter's contributions are:

1. A trusted external device called Buddy Device is used to authenticate external devices on behalf of IMDs to prevent resource-depletion. Buddy Device is a resource rich device supporting RSA based certificates for mutual authentication and temporary key exchange over wireless link.
2. Buddy Device allows IMD to emit a session key and performs friendly jamming to convey the session key only to an authenticated external device.
3. Following exchange of session key IMD and external device can indulge in secure wireless communication.
4. Allows Perfect Forward Security (PFS) as the session key is renewed for every session.
5. This solution can be explicitly use for IMD to external device communication as such communication is more vulnerable to attacks.

4.1. Introduction

As explained in Chapter 1, unauthenticated communication may force IMD to exhibit unpredictable behavior which may threaten a patient's life [38, 52, 88]. It is highly desirable to block unauthorized wireless communication attempts of an adversary while allowing seamless communication between IMD and authorized external device for immediate diagnosis and treatment. Typical IMDs are battery powered devices capable of running for five to seven years [48]. Their batteries cannot be charged unless surgerically removed from the body. Also due to miniaturized size and unique placement in human body, IMDs lack memory and computational skills unlike modern day wireless devices. Moreover putting stringent security policies may render the device inaccessible in case of an emergency for the healthcare personal who do not have the access credentials [89]. For a security scheme to work in presence of these limitations following requirements should be satisfied:

1. Energy, storage, computation, communication overhead induced should be minimized.
2. Support for real time generation and sharing of renewable and secure credentials should be provided.
3. Adherence to Perfect Forward Secrecy (PFS) requirement which means compromise of a session key will lead to disclosure of only the data encrypted by that key and not any subsequent data or key.
4. Support for security services viz. Confidentiality, Integrity and Availability for IMDs should be provided.
5. Support for rendering Authentication and Access Control for all communications with reader/programmer.
6. Access during emergency situations should also be controlled to a certain extent.
7. The scheme should provide security to any IMD in general and to a specific IMD in particular.
8. Support for scalability to cater to security requirements of multiple IMDs implanted for a patient.
9. The scheme should be minimally invasive requiring minor changes in existing IMDs.
10. The scheme should make use of standard algorithm rather than relying on security through obscurity.

4.2. Proposed Solution: The Buddy System

We provide a solution to this problem by introducing an external device called a Buddy Device which secures patient IMDs and enforces authenticated communication for the IMDs. It performs authentication of external devices on behalf of IMDs thus conserving scarce resources of IMD for critical therapeutic functions. Using our system, an external device obtains access to IMD provided it successfully passes the stringent authentication and access control policies rendered by the Buddy Device. When a reader seeks access to an IMD, Buddy Device initiates an authentication session which once successful leads to sharing of a temporary key between Buddy Device and authenticated external device. Buddy Device requests IMD to transmit the one time session key and simultaneously jams

the channel to bard other devices in vicinity from interpreting the key while allowing authenticated reader to interpret the key as it is in possession of the temporary key which can be used to cancel the jamming signal and derive the session key. The session key is renewed for every new session between IMD and external device. An important facet of our scheme is forward security and replay attack resilience as for every session a new session key is generated and used for encipherment of telemetry data. IMD supports session key generation by using time-varying biometric, known as physiological value (PV). Any PV can be used by an IMD to generate session key, one such example is use of the waveform produced by the heart, known as an ECG (electrocardiogram). MEMS Microcontrollers used for IMDs today allow it to perform only lightweight cryptography. Our scheme requires invocation of Ultra light weight cipher like PRESENT-80[90, 91] or MISTY1[70]. The Buddy Device performs following roles:

1. **Mutual authentication and temporary key generation:** The Buddy Device and external devices exchange RSA based Public Keys on prior basis. It authenticates external device (ED) on behalf of IMDs and a temporary key is generated.
2. **Access Control:** It provides a role based access control for IMD resources based on a configurable Access Control List (ACL) available with the Buddy Device.
3. **Jamming:** It requests IMD for one time session key generation and transmission to the external reader while simultaneously jamming the channel.

The proposed scheme is minimally invasive as the IMD only needs to generate session key and transmit it and later use it for encryption and decryption of telemetry data. The session key generation is lightweight procedure as IMD uses random bits from the sensed data to form a session key. This aims to provide a technique for sharing of secret session keys between implanted device and reader by use of friendly jamming which is controlled by temporary key in presence of adversary. This makes the session key unpredictable to adversary but as the authenticated reader is aware of the master key; it can remove the jamming signals and recover the key send by IMD. Once key is shared with authenticated external device, all communication between IMD and external device is encrypted by the session key ensuring message confidentiality and integrity. This scheme can also be used for securing multiple IMDs worn by a patient. To make session key generation light-weight, we propose use of Physiological values (PVs). PVs are sensed by IMDs as a part of their functionality. Therefore no extra overhead of pseudo random number generator (PRNG) or

Round Function is incurred. As described in [81], it is possible to extract four high-grade truly random and uncorrelated bits per IPI from processed ECG source. We propose use of such random bits for session key generation as they provide the required entropy.

From the literature survey in chapter 3, we found a lack of appropriate key sharing mechanisms, the use of pre-shared keys makes them vulnerable to cryptanalysis attacks, biometric [77] or physiological value (PV) [81] based key exchange requires closer assessment to be used in practical and also external device to be able to measure a PV. The solutions given in literature [84], [14, 29, 48] exhibit some or the other limitations like authentication using pre-shared keys which cannot be renewed even when compromised; use of invasive techniques which call for a major design change in current IMDs. Moreover encryption and authentication protocols used are vulnerable to battery depletion and denial-of-service attack. Fail-open access in case of emergency increases vulnerability; also the device specific nature of security solution makes them unusable for other implanted devices.

4.3 Features of Buddy Device

We propose the Buddy Device as trusted external device similar to shield [84] but differing in following aspects:

1. While the shield [84] act as a jammer-cum-receiver to jam the IMD messages and unauthorized commands, our Buddy Device uses jamming only for secure exchange of session key between IMD and external reader.
2. When present, our Buddy Device is also capable of using fast jamming techniques as shown in [6] to jam the frames which are directly addressed to IMD. This strategy prevents attacks like Denial-of-Service and battery depletion. No such attempt was made in [84].
3. When the shield [84] sends reader's commands to the IMD, confidentiality is not warranted. While in our case IMD and external reader communication is secured by use of session keys.
4. Shield [84] is vulnerable to attacks in presence of an adversary with two receiving antennas as shown in [50] we make an effort to mitigate this problem by use of temporay key as also proposed in ally friendly jamming [50].

4.4. Proposed Architecture using Buddy Device

Here we describe the proposed architecture which deviates from the from the normal communication pattern by introduction of a device called Buddy Devise. The Buddy Device based architecture is shown in Fig 4.1.

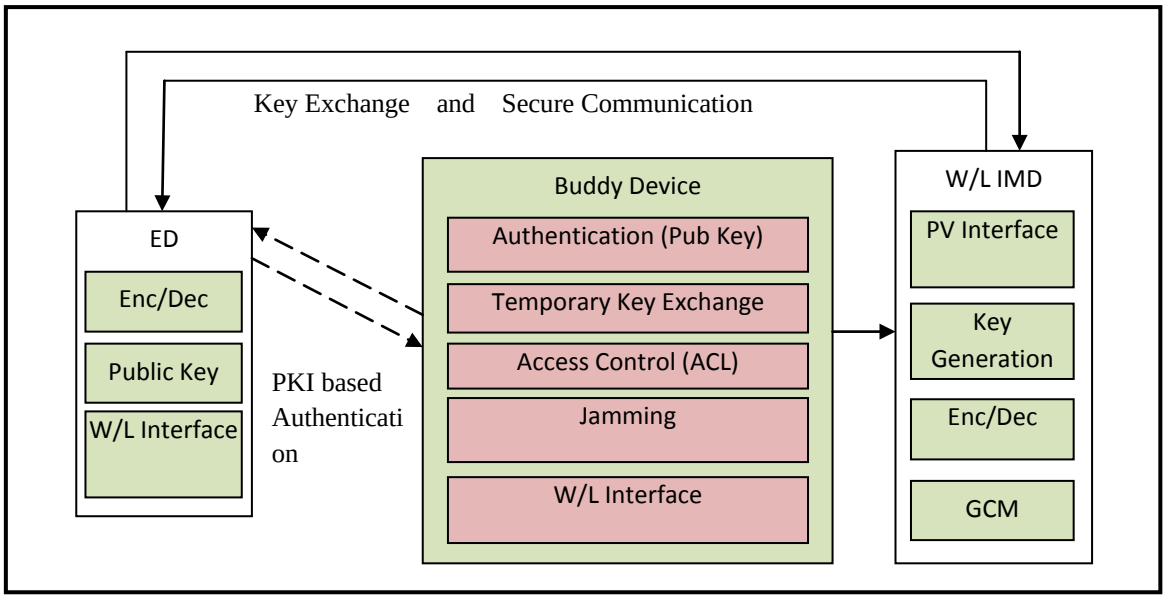

FIGURE 4.1 Architecture of Proposed Security Scheme using Buddy Device

The essential modules for working of the proposed solution are explained below

4.4.1 Buddy Device

Buddy Device is securely paired with IMD during IMD installation. This allows only the Buddy Device of the patient to request an IMD for session key generation and transmission while simultaneously jamming the channel. It contains following modules:

1. **Authentication:** By use of prestored RSA based Public Keys, Buddy Device and ED perform mutual authentication and a temporary key exchange. Buddy encrypts the generated temporary key by Public Key of ED and sends. ED decrypts the temporary key using its own Private Key.
2. **Access Control:** It uses a pre-configured access control list(ACL) to provide role based access control to IMD resources by the external devices.
3. **Jamming:** Three particular situations that require use of jamming are firstly when the session key is being transmitted by IMD to the external reader to avoid eavesdropping attempts of an attacker. Secondly, when an adversary bypasses the Buddy Device to communicate with IMD. Thirdly, when the proxy is unable to jam the adversary and finds IMD responding to the adversary.

4.4.2 Implantable Medical Device

This is a regular IMD which includes all the components that are already in existence like battery (provides power), memory (stores collected data and therapy settings), sensor (for sensing medical parameters), actuator (for giving therapy), microcontroller (which manages the IMD operation) and communication interface along with transreceiver. In addition for our scheme, IMD will have following components:

1. PV Interface:This is used to extract a PV and output random bits with sufficient entropy.
2. Session Key Generation: This is used for generation of random, unpredictable session keys by use of PV bits as seed.
3. Encryption/Decryption: Ultra light weight cipher called PRESENT-80[91] or MISTY 1[70] can be used for encryption. When used in combination with GCM, integrity is also assured.

4.4.3 Enhanced External Device (ED)

This is a regular external reader/programmer that is used for wireless communication with IMD. In the proposed work, we require such external device to undergo Public Key based authentication procedure at the end of which it tends to exchange a temporary key with Buddy Device. This key is used to cancel the jamming signals to derive the one time session key. It also makes use of symmetric encryption while communicating with IMD using a secure request-response communication protocol.

4.5 Secure Communication Protocol

In this section we discuss the communication protocol for securing IMD by use of Buddy Device. The sequence diagram of communication protocol which uses Buddy Device is illustrated in Fig. 2. The protocol is explained below:

4.5.1 MD-Buddy Device Pairing

The Buddy Device needs to be paired with one or more IMDs of a patient for the very first time. This pairing can be done in a restricted environment like hospital. Once the devices

are paired, the Buddy Device needs to be configured with the information about authenticated external readers and the Access Control List (ACL). As the Buddy Device is configurable, external device information like Public Key can be added or removed as per need.

4.5.2 Reader Authentication

The Buddy Device listens for a communication request by an external device, on receiving request; it first authenticates the reader and then authorizes the type of request according to the ACL. Since all the communication to IMD should pass through Buddy Device, if a communication request is directly addressed to IMD, it uses fast jamming technique [97] to jam the signal. If it is unsuccessful in jamming the readers signal and it somehow reaches the IMD to which IMD starts responding then it immediately jams the IMDs response signal using slow jamming technique[86] .

4.5.3 Buddy Device-IMD Communication

The buddy device sends a request to the IMD in response to which the IMD generates one time session key by using random bits of PVs. When session key, X_{IMD} is transmitted by IMD, buddy device jams the communication. For jamming, it makes use of a PRNG with temporary key K_{temp} as the seed to continuously emit jamming signals X_{Buddy}. In our technique, authenticated external device can employ proper signal processing techniques to cancel out the jamming signals from the received mixed signals with the help temporary key, K_{temp} to derive the session key XIMD. In contrast, the unauthorized device does not have the secret keys, and cannot remove the interference introduced by Buddy's jamming signals. For an unauthorized device E, the signals received will be the mixture of both X_{IMD} and some portion of X_{Buddy}. This results into distortion of the IMD signal, X_{IMD}. As a result, unauthorized device E is unable to receive the session key. However, since R has access to temporary key K_{temp}, it can regenerate the same jamming signals X_{Buddy}. Once it finds out which portion of X_{Buddy}. is mixed with X_{IMD}, it can subtract this portion of X_{Buddy} to get a clean copy of X_{IMD}.

4.5.4 IMD-External Reader Communication

Once X_{IMD} is shared, telemetry messages are encrypted using light weight schemes like PRESENT-80 [77] or MISTY 1 [55]. Once a session is over, one time session key is discarded and cannot be reused so as to avoid replay attacks.

4.5.5 Emergency Access

To tackle emergency access when an authenticated device is not around, access can be granted to a doctor or ambulance staff by switching off the Buddy Device so that no authentication or jamming is performed. When IMD senses the unavailability of Buddy Device, during emergency, it transmits the session key to which no jamming is performed by Buddy due to its absence. The external device can capture the session key and communicate with the IMD. But once the session is over the session keys will no more be usable and Buddy Device can again take control of the IMDs. Thus, our scheme provides a controlled access during emergency for a very short duration.

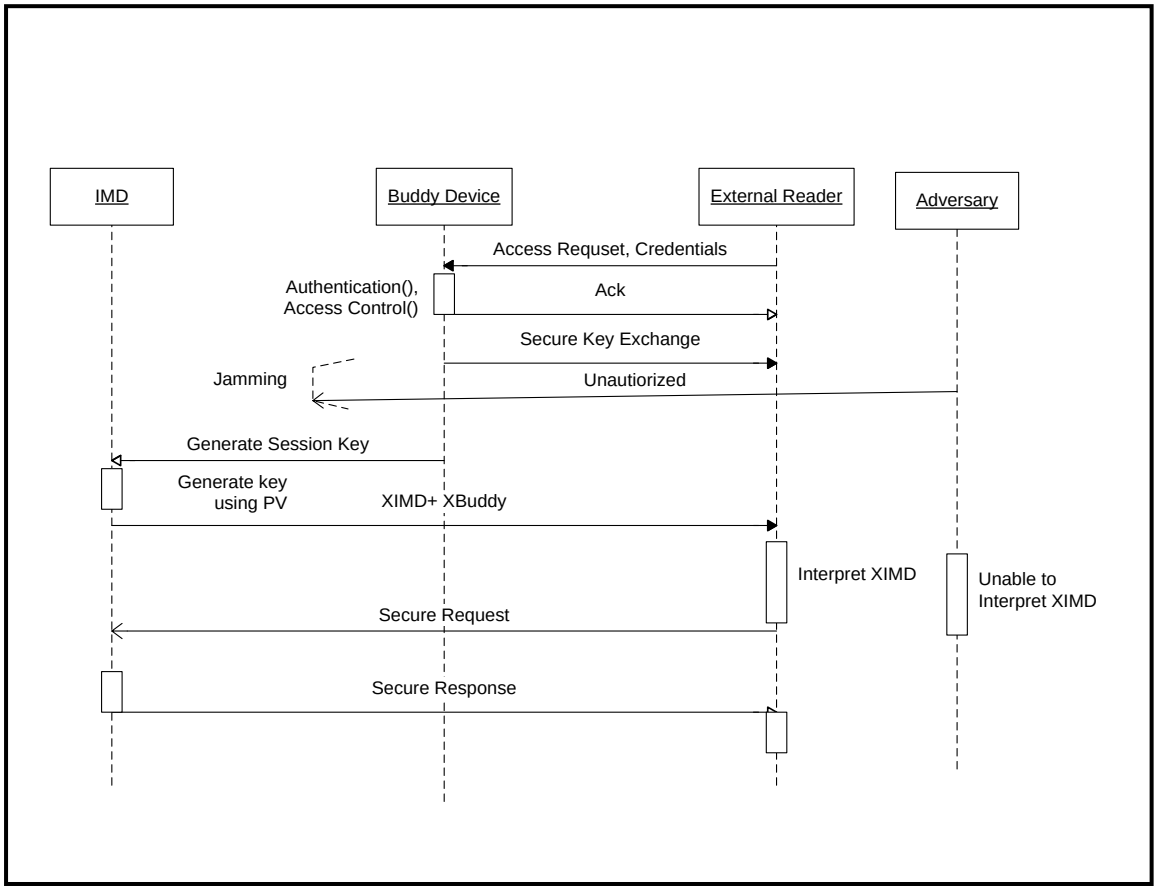

FIGURE 4.2 Sequence Diagram for Buddy Device based communication protocol

4.6 Conclusion

In this paper we proposed a Buddy Device which is used to grant secure access to IMD resources. Key based jamming technique is used to share session key at runtime. Our security protocol allows us to enforce Confidentiality, Integrity, Authentication and Access Control and also enforces Perfect Forward Secrecy (PFS). It protects the IMD against replay attacks. It is also successful in preventing resource depletion attack. As the jammer Buddy Device works as a mediatory it can be topped up with powerful access control policies, generation of audit logs and many other security features. Although this scheme enforces the patient to carry another device, these features can be integrated into the patients Smartphone itself. As a part of future work we explore the possibility of implementing the proposed security protocol on Android based Smart phones.

CHAPTER – 5

Emergency Aware, Non-invasive, Personalized Access Control Framework for IMDs

Contribution

This chapter provides justification for the belief that during emergency condition if fail-open security is provided, it increases the security risks. It extends the CAAC [98] Access Control model for providing controlled access to IMDs during emergency situation. The access control logic is placed on a trusted external device like PDA or cell phone which can be carried easily by the patient.

5.1. Introduction

Emergency medical staff may need immediate access to patient data [16]. The security solution requires a fail open access in order to make IMD accessible during emergencies to the health care providers who lack credentials. Fail Open access is granted bypassing all security techniques. This feature introduces a new vulnerability as the patient is feeble and complete removal of security may be dangerous for the safety of the patient. A solution is provided to provision fine grained Access Control which also incorporates emergency condition. Personalized Emergency Aware role based Access Control (EAAC) framework which can work in collaboration with Authentication and Encryption mechanisms to provide a strong security solution.

Access Control is a security mechanism which restricts the actions of a legitimate entity on a given resource object [99]. Due to resource constraints in IMD, we place the Access Control logic onto a handheld device like a cell phone or PDA belonging to the patient. Access Control in normal scenarios can follow standard pre-defined Access Control policies such as Role-Based Access Control defined in (or used in) [28]. However, during emergency scenarios, such Access Control policies may prevent an unregistered practitioner to access the patient's IMD for administering emergency treatment. In conditions of emergency, Access Control policies need to be modified dynamically to allow prompt access and quick treatment. But such changes should be temporary and

regular policies should be reinstated once the emergency is over. The Access Control framework should not only prevent unauthorized access to the IMD but should also be sensitive to critical cases which may run to an Emergency. Criticality Aware Access Control (CAAC) [98] framework for specifying Access Control policies is extended to control access to IMDs with automated operation during emergencies. Such framework requires continuous monitoring of context, authentication and application of Access Control policy. Therefore, instead of placing the service on the IMD itself, we propose to put it on an external proxy device. This is also useful when a patient has multiple IMDs installed, a centralized rechargeable proxy can manage secure access. PDA or cell phone which has an Internet access can be used as a proxy device. This helps in reducing resource consumption of IMD. During normal scenarios, Proxy Device performs Role Based Access Control and in emergency scenarios if registered practitioner is not available, Proxy device gets connected to its localized, Virtual Space to give emergency access to another medical practitioner by providing him with a temporary credential to access the Patient IMD for immediate treatment instead of failing open and giving access to everybody. During emergency this security scheme will provide Non-repudiation service which will ensure once an external device sends commands to IMD it cannot not deny doing so. A diagrammatic representation of the model is presented below:

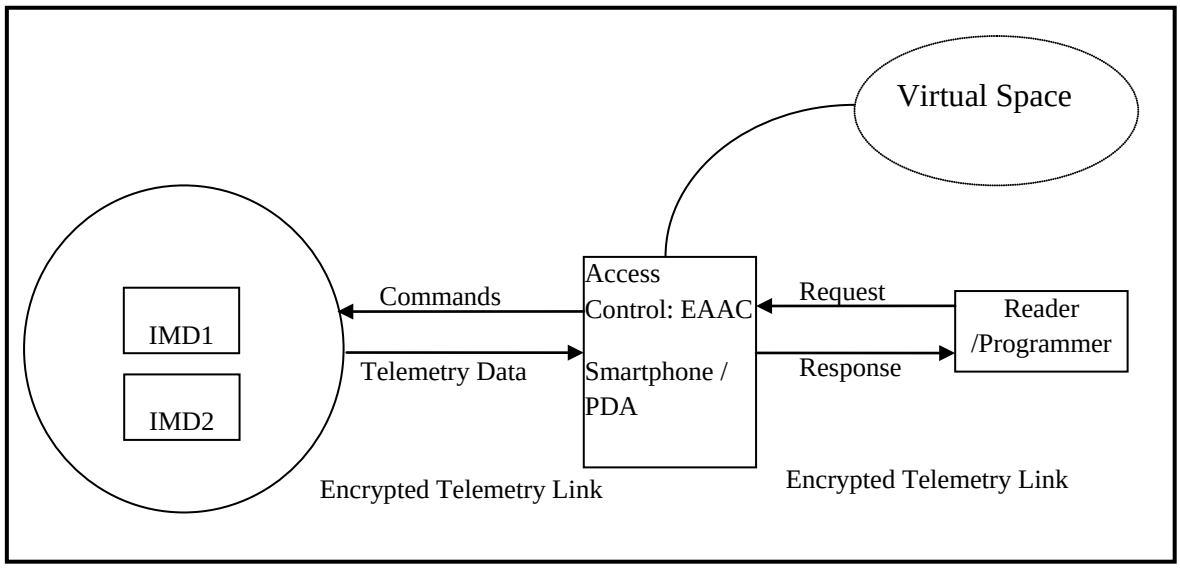

FIGURE 5.1 Block Diagram for Emergency Aware Access Control [124]

5.2. Threat Model for Fail Open Security

As discussed in [16], by bringing down the security to zero during emergencies means introducing vulnerability as IMD will communicate without using any cryptographic mechanism making the communication vulnerable to eavesdropping and alteration. This increases the risks of Insider and Outsider attacks like attacks on integrity, replay attacks, denial of service attacks. This can turn out to be a big loophole in the entire security framework and requires some amendment. This vulnerability may be exploited by an attacker by inducing false alarms to introduce a fake emergency situation and take control of the IMD.

5.2.1. Assumptions

As our concern is to provide Access Control, we assume a strong Authentication Mechanism available to authenticate user in Normal State similar to one suggested in chapter 7. We assume that Proxy device communicates with IMD via secure encrypted channel and it is capable of using an Internet connection to access Virtual Space which keeps a record of medical practitioners in proximity area of patient.

5.3. Security Mechanisms proposed to be Installed on Proxy Device

5.3.1. Authentication

For enforcing access control on IMD resources, external device needs to be authenticated first. During normal scenarios, authentication can be granted once authenticating party proves its legitimacy. This is typically brought into action by provisions like a password, or a physical key or biometrics like fingerprints, iris scan, signature and voice recognition or digital techniques (e-tokens, RFID, key fobs) [100]. Authentication is granted according to the principle of “least privilege”, which withholds privilege unless need is established by a specific request, for example, even if a doctor(provider) logs in he should not be unanimously allowed to stop IMD as he may accidently do so. A user needs to be re-authenticated with high reliability to gain a new trust credential with aggravated trust level [100]. Authentication Service must reliably identify the user and issue a credential which can be subsequently used with every request for access that an external device makes, which is used by the Access Control Service to identify the requester [101]. Once assured that credentials are not tampered with or stolen, the Access Control system can reliably identify the requester.

5.3.2 Access Control

To ensure secure communication, an Access Control mechanism for IMD is a crucial need. A typical Access Control system consists of following entities [98]:

1. **Subject:** An entity like External Device that seeks access to a resource object like an IMD.
2. **Object:** An entity that is protected by the Access Control system for example an IMD.
3. **Permission:** It is the access right of a subject to access an object in controlled manner.
4. **Credentials:** It is a proof that subject possesses to prove its authenticity.

An emergency-aware Access Control model uses contextual information to provide controlled access to sensitive data of IMDs. Here we rely on the fact that during emergencies if IMD detects a weak pulse, low blood glucose, or if the patient is unconscious, IMD informs the proxy device immediately. In such circumstances, if authorized staff is not available in the vicinity, the proxy may switch from Normal to Emergency State of Access Control for patient safety.

Below given are the popular Access Control mechanisms along with discussion on the suitability of their application in provision of Access Control for IMDs.

5.3.2.1 Traditional rule based model

Discretionary Access Control (DAC) model makes use of Access Control Matrix (ACM) to store the access rights of each subject over a set of resource object [99]. It is a static solution where subjects and objects need to be pre-defined. Therefore additional constraints cannot be imposed easily. In Mandatory Access Control (MAC) model, access rights are determined by a central authority. It labels each resource object with a sensitivity level and each subject with a clearance level. In order to access a resource, subject must possess a valid clearance level. These models lack the dynamism and flexibility required for providing Access Control for wireless access of IMDs.

5.3.2.2 Role based access control model

In Role based access control model [102], subjects are assigned a role and access right are assigned to such roles. Subjects in the system are assigned roles when they register to the

system, and are allowed to access resources, based on the privileges associated with the assigned roles. Given a set of roles and privileges, RBAC maps subjects to roles and the roles to different sets of privileges. Even if administration and modification of the policies is easily achieved, this model fails in incorporating dynamic assess control as the mappings are static and not context aware. An authorization model based on semantic web technologies [103] which uses Common Information Model (CIM). For managing the authorization of resources, an authorization system should implement its semantics in a manner that they match with semantics of underlying data and resources to be protected. In [104] the RBAC model is extended to support more complex privacy-related policies, while considering features like purposes and obligations.

5.3.2.3 Context Aware Access Control Model

Context Aware Access Control Model (CA-RBAC) [105] extends RBAC model to incorporate context related data for controlling access to sensitive resource objects. While providing flexibility and dynamism, this scheme depends on combination of role of the user, context information and state of the system. Similar to CA-RBAC, a dynamic context aware Access Control scheme for distributed healthcare applications was presented in [100].

5.3.2.4 Criticality Aware Access Control Model (CAAC)

Criticality Aware Access Control Model (CAAC): [98] responds to occurrences of critical event and changes Access Control policies autonomously. Criticality which is the measure of urgency required to handle a critical event. CAAC classify system context information into Critical and Noncritical. Critical context indicates the occurrence of a critical event which requires immediate action and noncritical contexts indicate normal operations and require no special action. Critical event allows adjustments in Access Control policies by including notification and logging, our Access Control draws inspiration from CAAC.

5.4 Proposed EAAC Architectural Framework

Our solution, Emergency Aware Access Control (EAAC) framework is designed for granting wireless access to one or more IMDs implanted on the Patient's body. Our proposal extends Criticality Aware Access Control [98] by incorporating a number of design choices specific to the IMD context and proposes its placement on a proxy device for personal security. Also we make use of virtual spaces to dynamically assign credentials

to medical practitioners to allow access of a patient's IMD during emergencies. Parts of our framework are as follows:

5.4.1 Role Management

Access rules for IMDs are delineated and assigned to a medical staff when he becomes a part of an IMD system of the patient by undergoing the process of registration and is established in his actual position and permissible activities. The primary task then is to assign well defined and unambiguous roles to subjects (medical staff) and providing them appropriate privileges based on their access rights.

Emergency aware role management is done by the help of a Web Service using which a medical practitioner can join a particular virtual space depending on his current location and can be contacted for providing emergency treatment to a patient bearing IMD is case of medical emergency when the registered medical practitioner with access privileges is unavailable. The privileges are, nevertheless, given to those who are authorized medical staff and are available within a limited distance from the place of exigency. Therefore system roles are a subset of space roles. The proxy on sensing a medical emergency, will access the virtual space by exhibiting the form of service required for the IMD and its placement to produce a list of doctors who are available in the vicinity. With a doctor's consent it will grant admittance to the IMD for a limited period as explained below to only a doctor and not to all. The physician will be provided credential and a complete access log will be stored in proxy for non-repudiation.

Context information [100] is helpful in modifying the Access Control policies to ensure IMD access and thus patient safety.

5.4.2 Emergency State Management

For Emergency State, following points are considered:

1. Emergency State requires autonomous changes in access policies if registered staff is unavailable.
2. All policy changes with respect to Emergency State are temporary and rolled back once emergency is over.

5.4.3 Emergency Management

Criticality is an amount of level of responsiveness required in taking corrective actions to curb the effects of a critical event and is used to find out the severity of critical events. To quantify this attribute, the term Window-of-Opportunity (Wo)[100] is introduced, which is defined as the maximum delay that is allowed to take corrective action after the IMD informs of a critical event and varies from application to application. Window-of-Opportunity = 0 indicates maximum criticality which leads to an emergency condition while a Window-of-Opportunity = ∞ indicates no criticality which means normal state of IMD and of patient Access Control policies.

Here, access policies are modified during the onset of a critical event in order to control the emergency in best possible manner. However completely diluting access control polities during critical events may introduce security concerns; therefore duration of relaxation of Access Control policies needs to be managed carefully. During a critical event, the Proxy implements a new set of access policies to facilitate prompt action. When the critical event is controlled and the patient is no longer in an emergency, the system restores to regular Access Control policies.

Criteria used for managing the Emergency mode: 1) the Window of opportunity Wo, 2) the time instant when the criticality is controlled T_{EOC} and 3) the time instant when all necessary actions to handle criticality has been taken (T_{EU}). The maximum duration for which the system can be in Emergency mode $T_{Emergency}$ is given by: $T_{Emergency}$ =min (Wo, T_{EU}, T_{EOC}). The Proxy determines the criticality level and on observing a critical event changes the access policies to Emergency-Aware and enters the Emergency State. It accesses the Virtual Space and provides credentials to one or more medical staff who are in the vicinity and agree to visit the patient, once emergency is over, then the system checks if it is in the EAAP - mode, if so, it returns the system to its Normal State and enforces the regular policies. Figure 2 below is a state transition diagram showing the Proxy States and Fig. 3 shows the Proxy architecture.

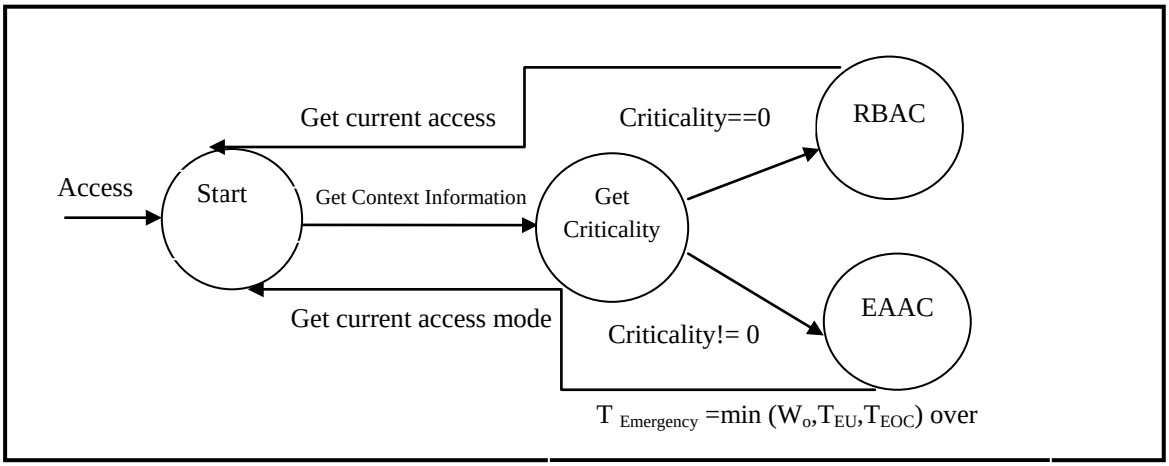

FIGURE 5.2 State Transition Diagram for Emergency Aware Access Control using Proxy Device [124]

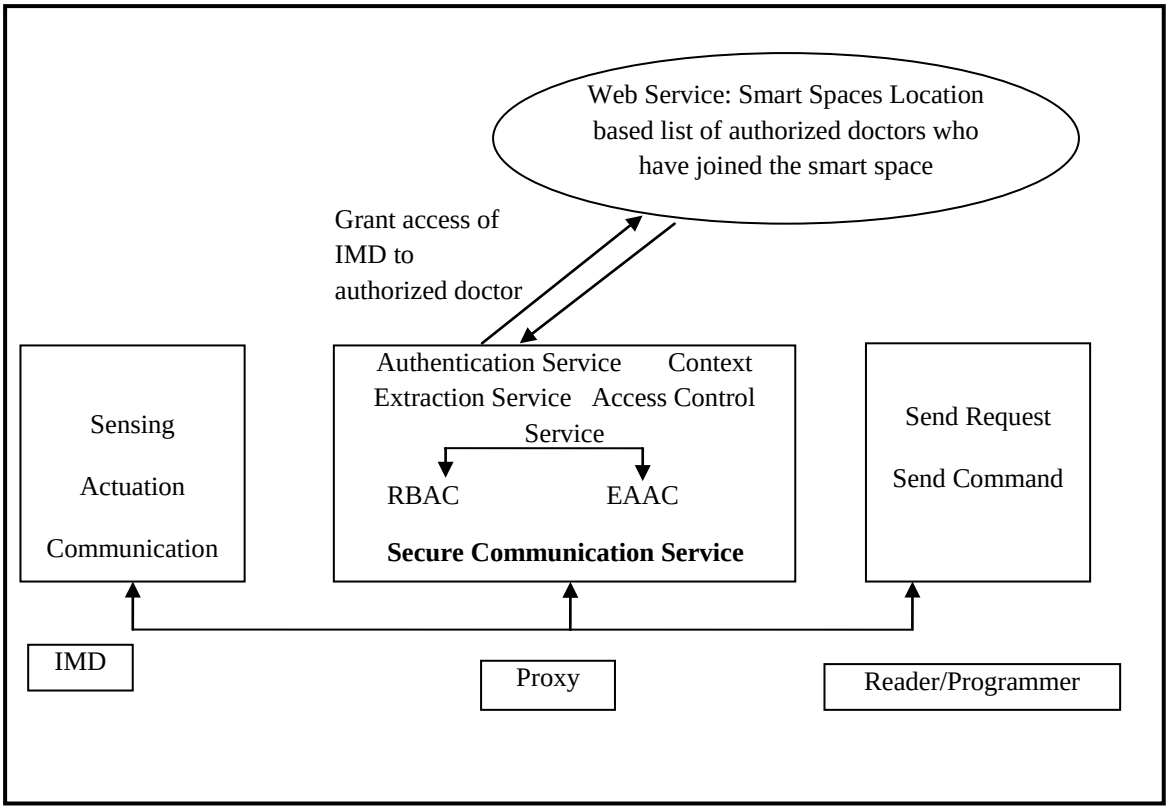

FIGURE 5.3 Proposed Proxy based Architecture [124]

The proxy implements RBAC [102] for Normal State and EAAC in Emergency State.

5.5 Conclusion

This system manages access control based on context information which allows it to provide controlled access during emergency which is beneficial for critical systems like IMDs.

CHAPTER – 6

Detection of Active Attacks on wireless IMDs using Proxy Device and Localization Information

6.1 Introduction

While passive attacks on IMD can be addressed using encryption techniques, active attacks like replay attacks, massage injection and MITM attacks needs more innovative techniques to be identified to handle with. To address the problem of Active Attacks, we advise the use of RF-signal based localization technique which leverages multi-antenna Proxy Device to profile the directions in which Reader/Programmer signal arrives and use the triangulation technique to generate a signature that uniquely identifies authorized external device. This technique is an extension of Secure Angle **[106]** which was proposed for wireless networks to improve security.

While security mechanisms like authentication and encryption is must, they alone are unable to fight active attacks like Man-in-the-Middle, Replay and Message Injection and require use of some extra technique. As IMDs are themselves resource constrained many researchers have proposed to shift the security related processing to an external proxy device which acts as an intermediary [80, 84, 86]. In this chapter, in order to prevent active attacks we propose to use a multi-antenna Proxy Device which securely pairs with IMD and relays messages from external device to and fro IMD.

In this model reader/programmer transmits an RF signal in order to communicate. The Proxy Device which is in listening mode, receives the transmitted signal and tries to estimate the Time Difference of Arrival (TDoA), Received time of flight (RTOF), phase of arrival (POA) and angle of arrival (AOA).These parameters depend on the location from which signal is being transmitted. We assume an authentication mechanism in place for differentiating an authorized reader from an unauthorized one. Once the authentication

stage is over, then in the second step, the accumulation of the estimated parameters is applied to bring forth a unique signature which is utilized to differentiate authorized external device from an un-authorized one by the Proxy Device. We assume that the proxy device is capable of deriving these values from the received signal.

Our work is different from the work proposed in [106] as they have used AoA signature in general wireless environment to prevent MAC spoofing attacks. Whereas we are using the AoA signature to prevent active attacks specific to Implantable Medical Devices using a Proxy Device. Information derived by use of Triangulation Techniques can be used by multi-antenna Proxy Device to drop frames from unauthorized reader/programmers by verifying its AoA signature. Thus, unauthorized requests will be refrained from being sent to IMDs hence saving its expensive resources. The techniques to mitigate active attacks on wireless telemetry between IMD and reader/programmer require extra energy, computation and bandwidth from the medical device Therefore we use a Proxy Device which mediates the communication.

6.2 RF based localization techniques

Wireless location based sensing systems for indoor applications are presented in [108] . Triangulation is one such technique that uses the geometric properties of triangles to estimate the target location. It has two derivatives: lateration and angulation. Lateration is used to estimate the position of an object by measuring its distance from multiple reference points by measuring Time of Arrival (ToA), Time Difference of Arrival (TDoA): and Received Signal Strength Indicator (RSSI). Angulation is used to locate an object by measuring the angles relative to multiple reference points and is called.Angle of Arrival(AoA). These techniques are described below:

6.2.1 Time of Arrival (ToA)

The ToA is the time taken by a signal to arrive at the receiver and is calculated as the sum of the transmitting time and the propagation delay. Once the one-way propagation time is measured, it is used to calculate the distance of the transmitter. It requires the devices to possess synchronized clocks and presence of a timestamp in transmitted signal for receiver to calculate the distance, signal has travelled. Its accuracy is affected by non-line of sight.

6.2.2 Time Difference of Arrival (TDoA)

In order to determine relative position of transmitter, the difference between several signal arriving times is used. The signal is received by multiple receivers are synchronized in time. Its accuracy is affected by non-line of sight.

6.2.3 Received Signal Strength Indicator (RSSI)

It is measured as voltage value representing the power present in radio signal of the receiver unit [109]. RF-signals are subject to multipath attenuations due to barriers.

6.2.4 Angle of Arrival (AoA):

Here the direction of a signal is used to calculate precise object locations. The result is obtained from the intersection of several pairs of angle direction lines, each formed by the circular radius from antennas of various devices [108]. Therefore the angle of the arriving signal is detected by using sensor arrays. At each sensor element a signal arrives with a path difference. These differences can be used to calculate the angle of arrival . The location estimate degrades as the mobile target moves farther from the measuring units. While in our proposed system, we make use of AoA, better results can be obtained by using a combination of techniques.

6.3 Overview of components

6.3.1 System Configuration

Our model consists of three components, the IMD, the multi-antenna Proxy Device and reader/programmer. The IMD is implemented in the body to perform therapeutic functions. The programmer/reader is interested in wireless communication IMD to read telemetry data or send commands. The Proxy Device is a multi-antenna device with more power and resources for security related transformations and is rechargeable. Proxy Device is tightly coupled with IMD. Proxy authenticates the reader/programmer on IMDs behalf. Once IMD and Proxy are paired, IMD acts only on those requests that are sent through the Proxy

6.3.2 Assumption

We use AoA technique not to find the exact location of a transmitting device, but to use AoA information to generate a unique signature to identify the communicating device. We

assume the authenticated reader / programmer is in close proximity to Proxy Device and that adversary does not possess information to get authenticated.

6.3.3 Proxy Device Overview

When an authorized reader starts communicating with Proxy device, it indirectly measures the distance between an incoming signal's arrival at each antenna and calculates the angle of arrival (AoA). It generates a signature from AOA that is unique to the reader/programmer. The proxy can recalculate the AOA at random intervals to identify forged devices. In order to forge the signature, the attacker needs to know the locations of the communicating devices and all obstacles in the vicinity The combined direct path and reflection path AoA unique signature can be generated as in [4]. This signature can be used in conjunction with other security techniques like encryption and authentication. When a reader moves or a barrier moves, the angle of arrival may change and therefore it needs to be recalculated. The proxy device is calibrated as mention in [106] to generate AoA signature.

6.4 Signature Generation and Verification

The proxy device authenticates the External Device, and measures TDOA, RTOF, POA and AOA. The resultant value is fed into a secure hash function, like SHA-256.

S= Hash (TDOA || RTOF POA|| AoA) ----------From [122]

This value easily verifies if the party transmitting is actual IMD or MIMT. Figure 6.1 shows the flowchart for Proxy Device performing signature verification.

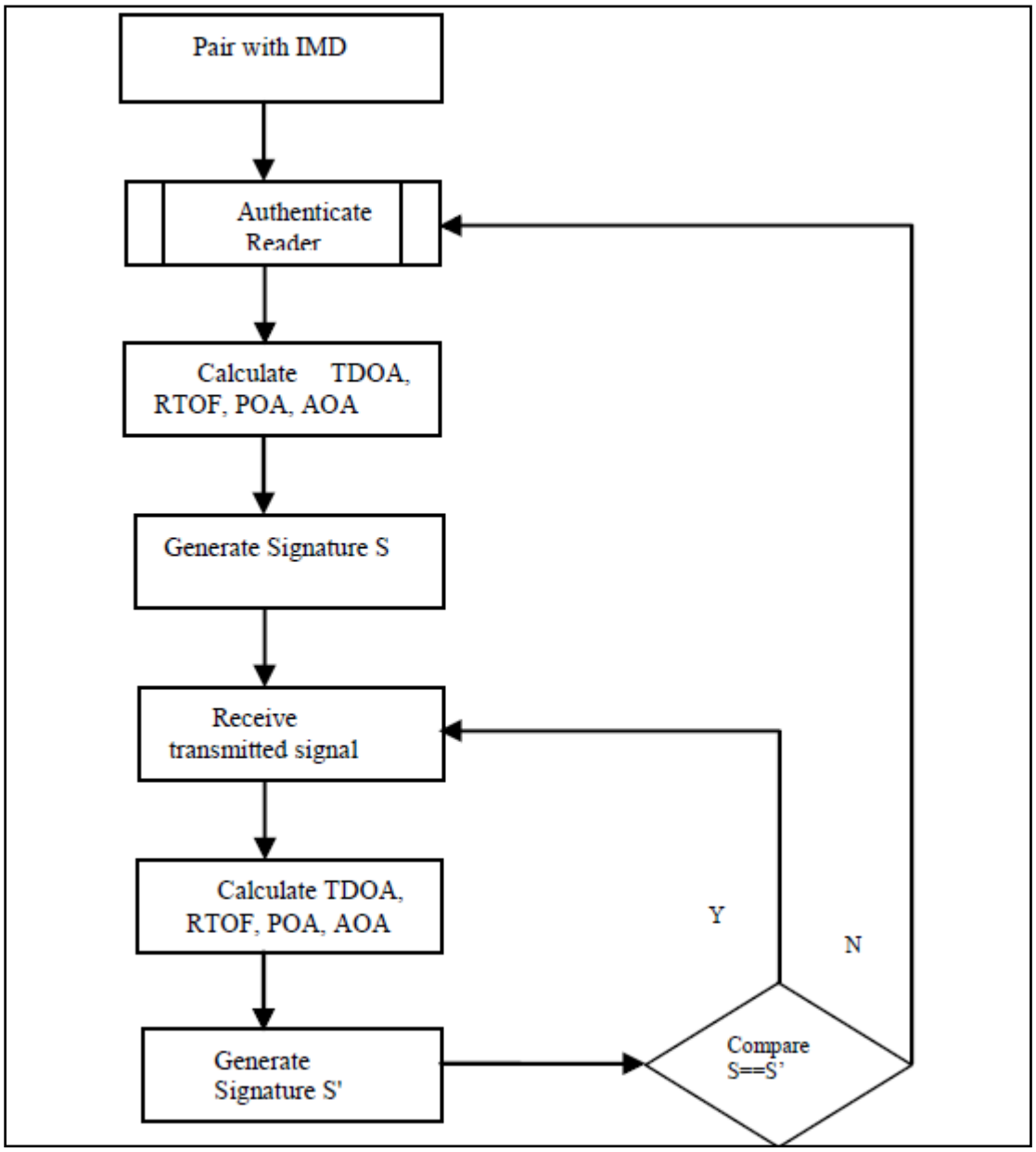

FIGURE 6.1 Signature Verification [122]

6.5 Proposed Proxy based Protocol

We assume that the IMD and Proxy Device are securely paired. Proxy Device (A) receives request from reader/programmer (B) for communication with IMD. Table 6.1 sums up the notations used. A after authenticating B, generates B's triangulation based signature S_B and stores it and grants access to the IMD. For every request from B or after random time intervals, A recalculates the AOA based signature and compares it with stored signature S_B. If there is a significant discrimination in the signature, A asks B to get authenticated (as either B or obstacle has changed position or a forged request is received). If B successfully

gets authenticated, it is granted access and its triangulation based signature is changed to the new value i.e. S_B'. Instead of B, if T sends a request to proxy the signature generated is S_T, which will not match with stored S_B and this will activate the authentication process during which T will be denied access. This technique is successful in preventing active attacks as any message from T will not get accepted unless either the device or the triangulation based signature is verified. As noted earlier, it is very difficult for T to spoof the triangulation based signature of B as T needs to induce the positioning data of both authorized reader/programmer and Proxy device, and also needs to forge the direct path AoA and all multipath AoA as an example. FIGURE 6.2 shows the sequence diagram for the signature verification based protocol.

TABLE 6.1 Table of Notation [122]

A	Proxy Device
B	Authenticated Reader/Programmer
T	Adversary Reader/Programmer
S_B	AoA Signature of B
S	AoA Signature calculated for each request
$S_{B'}$	Modified AoA Signature of B
S_T	AoA Signature of T

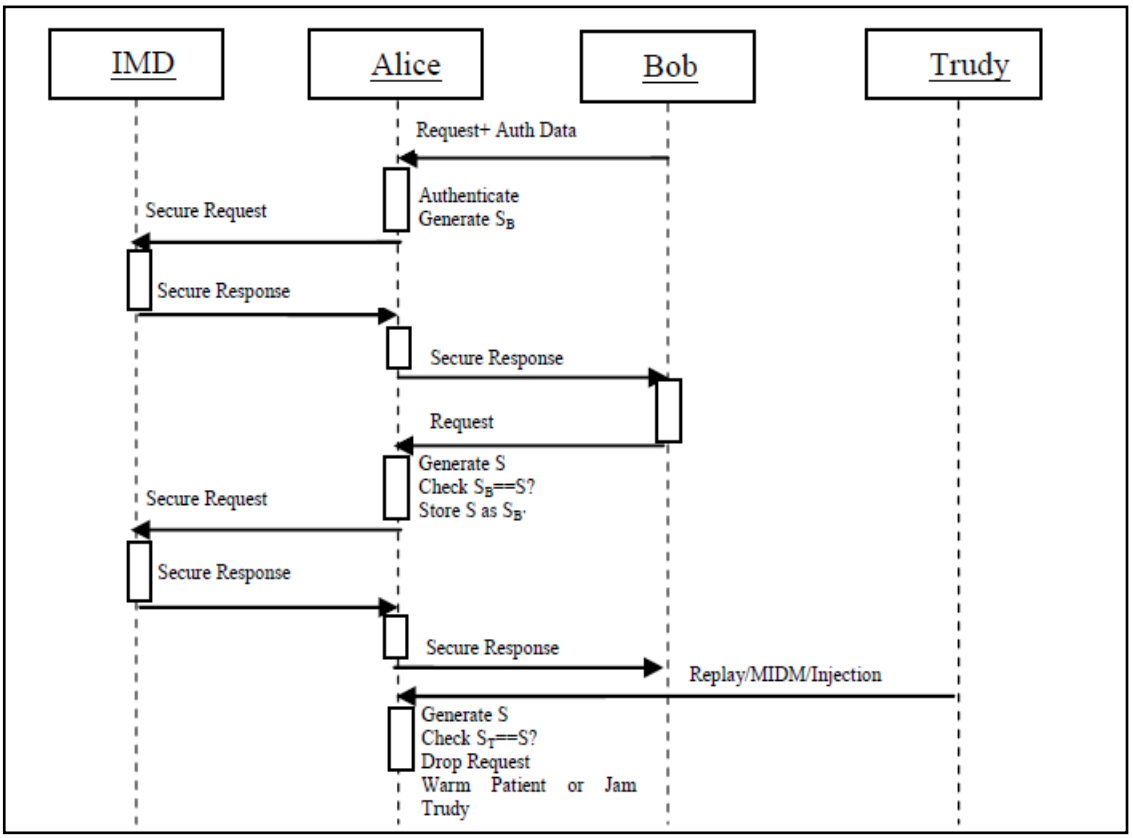

FIGURE 6.2 Sequence Diagram for Signature Verification Protocol [122]

6.6 Conclusion

In this chapter we made use of triangulation technique to generate a unique signature of the authorized external device and use it for detection of active attacks like MITM, Replay or Message Injection.

CHAPTER – 7

Two-Tier Model for Securing Wireless IMDs

Contribution

In this chapter we propose a secure IWBAN architecture based on two-tier model by making use of a proxy device. We use request-response messaging between IMD and Proxy and publish-subscribe messaging between Proxy and external devices. We analyze the available security mechanisms and justify our choices for Tier-1 and Tier-2. Based on the analysis, for tier-1, we present two protocols, first for Proxy initiating communication with IMD and second for IMD initiating communication with Proxy. For tier-2, we present two protocols, first for ED as publisher and second for ED as subscriber. We use a mapping engine in the Proxy which translates requests received from IMDs into subscribe message and response received from IMD into publish message for the external devices. The mapping engine converts Publish message received from ED to a response and Subscribe message received from ED to a request for IMDs. Two-tier proxy based communication model provides confidentiality, integrity, authentication, access control and replay resilience of sensitive information while ensuring availability of information during regular and emergency wireless telemetry access. The use of publish-subscribe allows timely delivery of critical health related information, reduces traffic on IMD thus saving its battery, allows IMDs and EDs to be decoupled and receive the required information without needing to know each other. Our security model is agnostic to underlying networking services. Any IMD that allows bidirectional communication can use the protocol.

7.1 Introduction

IMDs require end-to-end security solution therefore we provide a model for security which works at the application layer. To deduce a suitable security model, we are rethinking the way we store, transmit, process and access the telemetry data from IMDs. This will help us

to generalize the solution to provide security to a large range of IMDs. Our model uses a trusted external Proxy device to provide security. Proxy is a handheld device (like PDA or smartphone) acting as a mediator between external devices and different types of IMDs. This allows our defense system to shift security related transformations from IMD to the trusted Proxy device which in turn helps in reserving scarce resources of medical device exclusively for medical functions. The communication protocol is divided into two tiers to provide confidentiality, integrity, authentication, access control and replay resilience for IMD to IMD as well as IMD to External Device communication in an IWBAN. It provides availability of information during regular and emergency wireless telemetry access The first tier uses request-response model and the second tier uses asynchronous publish-subscribe [150] model. Due to selection of such communication model, the sender and receiver need not be synchronized and security mechanism can be selected based on the requirement and constraint of communicating parties.

7.2 Design Goals of Security Model

In this section, we present several criteria that represent desirable characteristics for a secure and lightweight communication system for IMDs which are mentioned below:

1. **Lightweight:** To match the low capabilities of the IMDs, it is important to minimize computation, communication, and storage overhead on the IMDs. Hence, cryptographic algorithms used with IMDs must satisfy these requirements to be resilient to DOS attacks.
2. **Access control:** Security framework should provide different privileges for different types of users. But, emergency situations require immediate medical action wherein access control must not pose a hurdle.
3. **Scalable:** The system should efficiently provide security even in a scenario where multiple IMDs are implanted and many EDs communicate with these IMDs.
4. **Flexible:** The security model should easily support addition or removal of external devices or IMDs.
5. **Minimize Invasiveness:** The security model should make minimal changes in the existing IMDs to increase acceptability by IMD manufacturers and patients**.**

6. **Support for Intrabody and Extracorporeal Communication:** The security model should be able to provide security for IMD-IMD communication as well as IMD-External Device communication.

7.3 Requirements of Two-Tier Security Model

1. All communication between External Device and IMD should pass through Proxy device.
2. The communication between the IMD and Proxy make use of the request response model, which must be supported by both IMD and Proxy.
3. The communication between the External Device and Proxy makes use of publish subscribe model, which must be supported by both External Device and Proxy.
4. The IMD is able to execute minimalist symmetric cryptographic operations for mutual authentication and authenticated encryption of messages and to store cryptographic key, counter and nonce for communicating with proxy.
5. The proxy is able to execute cryptographic operations and to store cryptographic keys for one or more IMDs and for one or more External Devices in tamper resistant manner.
6. The External Devices are able to execute symmetric and asymmetric cryptographic operations and to store cryptographic keys for communicating with proxy.
7. All IMDs constituting IWBAN of a single patient pair up with only one Proxy device

7.4 Assumptions

1. For developing a secure two-tier communication protocol for Implantable Medical Devices, we may assume typical IMD for our case.
2. The protocol assumes the presence of a no frills Transport Layer like UDP or any data transfer service like it to be available.
3. The external devices (ED) are operated by authorized medical staff.
4. One or more IMDs, Proxy Device and authorized external device follow the protocol as designed. IMD and the Proxy operate in Medical Implant Communication Service (MICS) band.
5. Proxy device is a patient's private device and only the patient or his doctor can have access to it.

6. The Proxy device is always present as it is an irreplaceable component of the security protocol.
7. The attacker does not try to physically harm the patient or remove the Proxy device.
8. We assume that the IMD and proxy have already been paired with a shared secret key after key establishment phase. This information can securely be installed when patient is in the hospital.
9. We recommend a different key for each IMD which is renewable, but our protocol imposes no such restriction.
10. We assume the Proxy has a list of legitimate programmers and their corresponding public keys. This information can securely be installed during device registration.

7.5 Overview of Proxy Based Two-Tier Security Model

The architecture of the proposed security system consists of three components: one or more IMDs, a Proxy device and one or more external devices all related to a single patient. The overall architecture is shown in FIGURE 7.1. It shows two-tier communication model for IMDs rendering secure wireless telemetry access. IMDs and Proxy device communicate in a secure manner by making use of request response protocol. Proxy device and External Devices communicate in a secure manner by making use of publish-subscribe protocol. The Proxy Device performs security related transformation on behalf of IMDs. A mapping engine in Proxy device is used to transform request-response messages to public-subscribe messages and vice-versa.

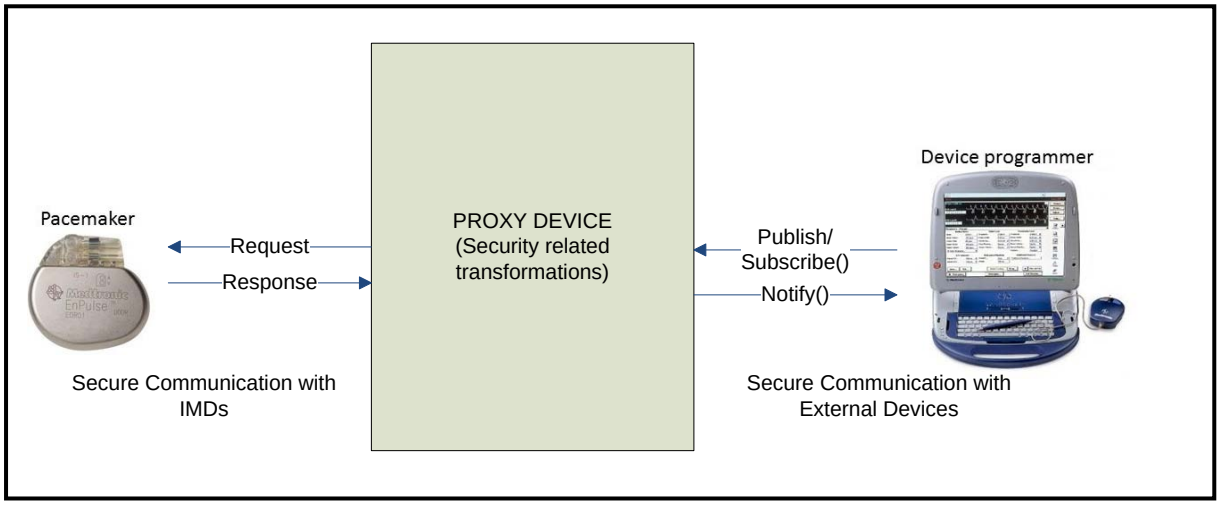

FIGURE 7.1 Overall view of two-tier architecture

Proxy device is responsible for converting the IMD request into a subscribe message and IMD response into a publish message. This allows interaction between the two communication models. Also do not require huge modifications in the IMD. We believe it is resource intensive for IMDs to support APIs provided by publish subscribe messaging middleware. This allows IMD to communicate in a light weight and secure manner. Publish-subscribe communication allows secure and seamless intercommunication of heterogeneous medical devices where one device can subscribe to data feed published by another device without need of knowing its identity.

7.6 Profiling of Security Mechanisms for Tier- 1: IMD and Proxy Device communication

We make use of request response model for communication between IMD and Proxy Device. In order to prevent adversaries from eavesdropping, injecting and tampering with data packets transmitted or received by IMDs, security services are necessary to be introduced into the communication protocol. Mutual authentication, data confidentiality and integrity, data origin authentication and replay protection are basic requirements which need implementation of cryptographic algorithms. Although cryptographic algorithms are already well established and are in use for wireless networks like WSN, the one to be used with IMDs needs to be chosen carefully due to its inevitable resource constraints. An IMD contains electronic circuits that perform data processing and control functions on an extremely small energy budget as explained in Chapter 1. On the other hand, using the security protocols always add additional overhead on the computational, storage and energy resources. Therefore, in order to design an energy efficient security model which suits the resource needs of these embedded devices it is critical to implement cryptography algorithms in a resource and computation efficient manner. The communication paradigm followed in IMDs is data-centric single-hop communication, instead of the route-centric multi-hop communication used in the conventional networks. Due to resource constraints and unique positioning, the use of conventional end-to-end security mechanisms like IPSec [134], TLS [135] SSL [136] in IMDs is obviated. Alternately, the necessary link layer security support may be provided by the underlying hardware based on IEEE 802.15.6 specification [137]. However, using a hardware based solution lacks flexibility and does not provide tailor made solutions to suit the need of recourse constrained IMD communication.

In the below text, we present the essential security services and the security mechanisms to be used in lieu and also the algorithm selected to meet its requirement in the proposed security model. We evaluate various aspects related to our model viz. selection of block ciphers, block cipher modes of operations, MAC sizes, IV generation, replay protection and mutual authentication scheme.

7.6.1 Security Service: Message Confidentiality

At the application layer, confidentiality can be achieved by use of encipherment techniques which is categorized as symmetric and asymmetric. Symmetric Cryptography is less resource intensive and therefore our choice for the communication protocol between IMD and Proxy. Symmetric ciphers are categorized as block cipher which processes plaintext in blocks or stream ciphers which processes plaintext as stream of data by making use of Pseudo Random Key Stream Generator. Available light weight block ciphers are AES, PRESENT, MISTY, XXTEA, BLOWFISH, IDEA and RC6 [128]. Table 7.1 lists some of the lightweight cipher and their parameters viz. the key-size, block-size and the number of rounds, security margin and program size in software. For choosing an appropriate block cipher we went through the published research work available in literature. Authors in [110] evaluates block and stream ciphers for their memory requirement and execution time. Authors in [111] analyses DES, AES and RC5 for energy expense during encryption, hashing and wireless transmission. In [112] author profiles block and stream ciphers for computational requirements and [113] profiles lightweight versions of block cipher for performance, power and memory requirements. In [3] author presents a comparative analysis of symmetric block ciphers for light weight encryption in implants.

Table 7.1 Benchmark suite of symmetric ciphers

Encryption Algorithm	Block Size (bits)	Key Size (bits)	Rounds (#)	Security Margin
3WAY [128]	96	96	11	2002
BLOWFISH [128]	128	128	16	2076
DES [128]	64	56	16	1982
GOST [128]	64	256	34	2243
IDEA [128]	64	128	8.5	2076
LOKI91 [129]	64	64	16	1992
RC5 [128]	64	128	12	2076
SKIPJACK [129]	64	80	32	2013
XXTEA [115]	64	128	32	2076
MISTY1 [114]	64	128	8	2076
RC6 [114]	18	128	20	2076
TWOFISH [114]	128	128	16	2076
RIJNDAEL [114]	128	128	12	2076

128-bits key size is essential for a cipher requiring security margin of 2076. We found the AES cipher Rijndael [132] was among the top five ciphers in all the performance metrics. For critical devices like IMDs we need to choose a stable algorithm which has been cryptanalyzed well. Therefore we use 128-bit key AES cipher Rijndael [132]. In fact, majority of research work [81] [68] [139] for securing implants have opted for the same. A message with multiple blocks can be encrypted in Electronic Codebook Mode (ECB) but as this method is vulnerable to cryptanalysis, therefore block cipher modes are used. Block modes of operation is the way of encrypting a message with a longer block size using algorithms like Cipher-Block Chaining (CBC), Cipher Feedback Mode (CFB), Output Feedback Mode (OFB) and Counter Mode (CTR). The choice of block cipher mode plays a significant role in determining the efficiency of secure communication protocols.

7.6.2 Security Service: Message Integrity and Authentication

A message authentication code (MAC), needs to be selected for assurance of message integrity and authentication. In security model of [69] encryption is done in ECB mode and then MAC is calculated using CMAC. Block cipher is used to encrypt n blocks first and then MAC algorithm is invoked for n blocks requiring a total of 2*n invocations. This overhead can be avoided by using Authenticated-encryption (AE) modes [92] which allow use of a single key to provide confidentiality and authenticity with significantly lower computational cost as compared to sequential encryption and authentication. Moreover it does not require use of the conventional block cipher modes. The popular AE modes are Offset Codebook mode (OCB) [93], Counter with Cipher Block Chaining (CCM) [94], Carter-Wegman + CTR mode (CWC) [121] and Galois Counter Mode (GCM) [95]. Out of these OCB [9] is covered with intellectual property rights. CCM [118] cannot be pipelined or parallelized. In CWC [121] message authentication is performed by 127-bit integer multiplication operation which increases the implementation cost as per [130]. GCM [119] is a two pass combined mode for authenticated encryption which not protected by intellectual property claims and gives high speed of processing. In [130] GCM mode is evaluated for implementation in link layer of wireless sensor network, their findings state that GCM mode can be selected for resource constrained applications that require message confidentiality as well as authentication. On comparing CPU usage cycle, throughput, and energy usage parameters with CBC-Skipjack and CBC-AES, it is shown that AES-GCM incurs overhead of 12% increase in energy and 28% increase in RAM usage, but at the

same time offers encryption as well as authentication [130]. Therefore, we make use of AES-GCM for authenticated encryption as explained below.

7.6.2.1 Authenticated Encryption Mode- GCM

Galois/Counter Mode (GCM) is a block cipher mode of operation which uses universal hashing operation over a binary Galois field for authenticated encryption [126]. It was proposed and recommended by NIST in 2007 [127]. As per [126], it is patent free, has high performance, and can be implemented in hardware as well as software; software implementations can make use of table driven field operations to achieve high efficiency. According to [15] GCM can act as a stand-alone MAC when encryption is not required, moreover it can act as an incremental MAC such that with computational cost is proportional to the number of bits that change. The structure of GCM mode is shown in Fig. 7.2.

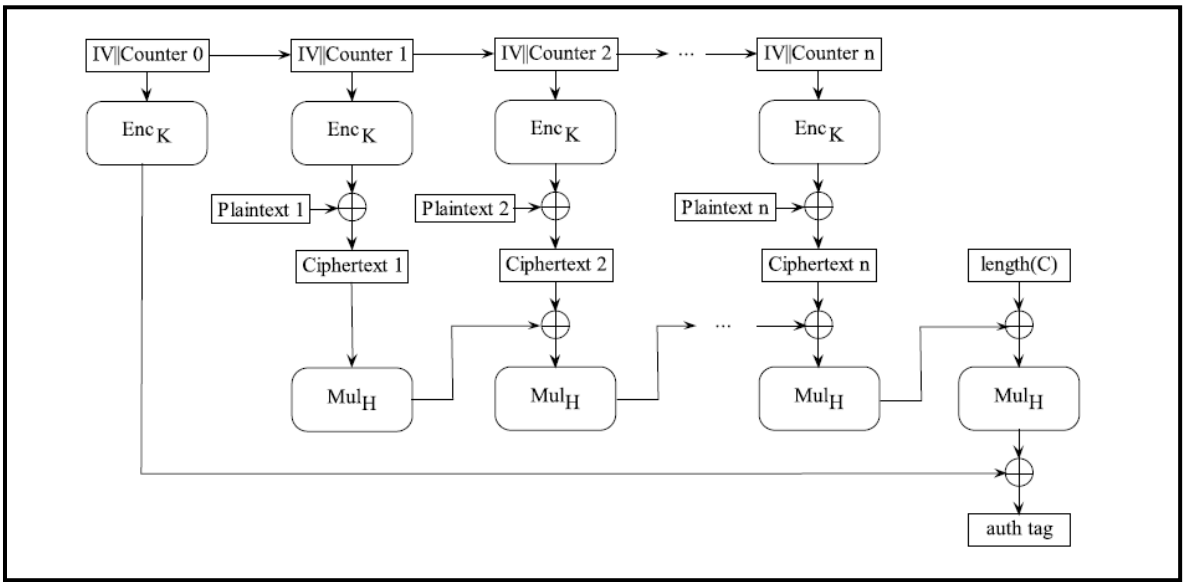

FIGURE 7.2 Structure of GCM [141]

GBM takes four inputs: a secret key, an initialization vector (IV), a plaintext, and additional authenticated data (AAD) which is authenticated but not encrypted. It produces two outputs, a cipher text of the same length as plaintext and an authentication tag as shown in FIGURE 7.2. The bit length of plaintext or cipher text is integer multiple of 128 bits [127]. The IV and Key are used to generate a key stream which is XORed with plaintext to get the cipher text. The Key stream must always have different values to avoid cryptanalytic attacks as XORing two ciphertexts will result into a value which is XOR of two plaintexts as shown below:

P1 ⊕ Encryption Key = C1

P2 ⊕ Encryption Key = C2

C1 ⊕ C2 = P1 ⊕ P2.

Therefore Encryption Key value should be different for each plaintext. The ciphertext generated for subsequent blocks is used to generate the authentication tag. The block diagram of AES-GCM is shown in Figure 7.3.

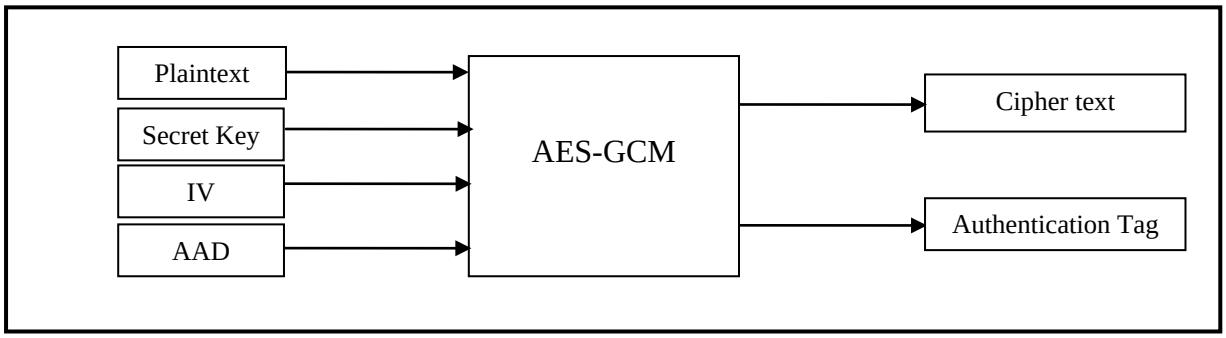

FIGURE 7.3 Block Diagram of AES-GCM

Description of the inputs required by AES-GCM and outputs generated are given below:

Plaintext

For an IMD, sensed physiometric data, patient related data, request for data from other IMDs and commands from external devices constitutes plaintext. For Proxy, it is a request for data or command that another authorized IMD or external device has issued. Plaintext is converted into blocks of 128-bits before encryption.

Secret Key

The IMD and Proxy shares pair wise secret key. According to [131], key size of 128-bits is a sufficiently long to defend against brute force attacks by a powerful adversary. Therefore 128-bit key is used.

AAD

Data like timestamp, device ID requires data integrity and data origin authentication but do not require confidentiality. Such data fields can be included in Additional Authenticated Data (AAD) field.

Initial Vector (IV)

Initial Vector (IV) is an essential component of block cipher mode. For AES-GCM, IV need not be a secret but must be unique for subsequent blocks of data. Instead of sending

the full length IV, in Minisec [133] a link layer security protocol of WSN, only few bits of IV are send to reduce transmission overhead. Instead of sending IV, we generate IV by use of the existing data header as explained in the next section.

Ciphertext

Ciphertext is of the same block size as that of plaintext. In order to decrypt the ciphertext generated by AES-GCM only encryption box needs to be installed as AES-GCM doesn't make use of a decryption box.

Authentication Tag

Size of the Message Authentication Code (MAC) employed must be chosen depending on the packet transmission rate of the device under consideration. According to [131], the appropriate MAC size is 8 bytes for embedded devices with transmission rate of 250 kbps in 2-3 meters. The Authentication Tag generated by AES-GCM by default is 12 bytes, which can be truncated to 8 bytes before sending to the peer device.

7.6.2.2 Initial Vector Format for Tier-1

As discussed above, we reduce communication overhead due to transmission of IV by deriving it from the data header of the application layer data. We generate IV by making use of nonce value and counter value which changes for every subsequent data block thus generating a unique IV. As IV need not be a secret it is generated by combining two 32-bit Nonces, one generated by IMD and one by Proxy and a 32-bit counter received from the communicating device to make a 96-bit IV as shown in Fig. 7 .4.

NonceIMD(32 bits)	NonceProxy(32bits)	CounterProxy(32 bits)

FIGURE 7.4 (a) Structure of IV for IMD

Nonce Proxy(32bits)	Nonce IMD(32 bits)	Counter IMD(32 bits)

FIGURE 7.4 (b) Structure of IV for Proxy.

7.6.3 Security Service: Replay Protection

Replay attack is performed by capturing packets of one communication session and replaying such packets later either to gain unauthorized access or to impersonate messages.

One of the areas where most of the security models proposed in literature fail is in provisioning replay resilience. In order to find an application layer replay scheme which can be used between IMD and Proxy, we studied the replay protection schemes given in [143] [144]. In [140] protection schemes are analyzed and categorized as synchronized counter based, nonce based, and bloom filter based.

7.6.3.1 Counters

For our scheme, we refer to [145] [143] and select counter based algorithm as it can be easily incorporated without much overhead. Use of a monotonously increasing counter guarantees semantic security. If a sender sends the same message, the resulting cipher text is different as different counter value and IV value are used. Also, once a receiver observes the counter value, it can rejects packets with an equal or smaller counter value. Therefore, an attacker cannot replay old packets without receiver detecting it. We make use of a 32-bit counter value which allows 2^{32} -1 counter values for a session. In [131] counter is used to drop stale packets. The use of such counter in our security model is twofold, one it is used for replay resilience and two it is used implicitly to construct the IV.
The algorithm [131] is modified for checking counter value at Proxy side and at IMD side as shown below:

Algorithm – 1: Executed by IMD to check the counter value of received message to detect replay of an older message.

```
CounterReplayDetect(CounterReceived,C_Proxy)
{
        if (CounterReceived <=C_Proxy)
                replayed = 1;
        else
        {
                replayed = 0;
                C_Proxy=CounterReceived;
        }
}
```

Algorithm – 2: Executed by Proxy to check the counter value for received message to detect replay of an older message.

```
CounterReplayDetect (Counter Received, IMD_ID)
{
        id = 0;
```

```
        for id = 1 to lastValidIMDId {
        if (id==IMD_ID) {
                if (CounterReceived <=LastCount[IMD_ID])
                        replayed = 1;
                Else
                {
                        replayed = 0;
                        LastCount[IMD_ID]=CounterReceived;
                }}}
}
```

7.6.3.2 Nonce

Nonce are random numbers are numbers that a sender associates with a message and receiver repeats in the response message to uniquely associate each message to its reply and ensures message freshness. Nonces are used only during first two exchanges for mutual authentication. They are generated on the fly during protocol execution and only the values associated with the current session are kept in memory, thus requiring minimal memory overhead. Nonce is also used in construction of IV at IMD and Proxy side.

1. **Nonce Generation for IMD**

   We make use of physiological value (PV) derived from the human body to generate nonce for the IMDs which in turn is used to secure the data communications against replay. The advantage is we do not require a Pseudo Random Number Generator at IMD side now. The level of randomness of biometric is determined by the amount of its entropy [146]. The required randomness can be obtained by simultaneous use of multiple biometrics or deriving a sequence from multiple instances of measurements. Thus random number generation overhead can be reduced by using a time-varying biometric, known as physiological value (PV). ECG (electrocardiogram) produced by cardiac IMDs such as ICDs and pacemakers are one of the popular and usable PV. Suitably processed ECG samples effectively constitute a low- bandwidth stream of random bits well suited for generation of random numbers. We use this entropy measure to generate Nonce at IMD side.

Algorithm – 3: Executed by IMD to generate random value Nonce.

```
Generate_Rand_IMD (Sensed_PV)
{
        bit_counter=1;
```

```
        for bit_counter=1 to n{
                extract_random_bits (Sensed_PV)
        }
        Combine random bits to generate 32 bit Nonce;
}
```

2. Nonce Generation for Proxy

In case of proxy device the pseudo-random number generator is used as it is a resource rich device. As specified in the [147], we use the block cipher AES in counter mode, called CTR. The algorithm is described here:

Algorithm – 4: Executed by Proxy to generate random value Nonce.

Block cipher-CTR mode (compliant with NIST 800-38A)

```
Generate_Rand_Proxy ( )
{
        Oj = AES-CTR(k, Ctrj )
        NProxy = |Oj |0···31
        Ctrj +1 = |Oj |32···64
}
```

7.6.4 Security Service: Mutual Authentication For mutual authentication, ISO/IEC 9798 Part 2 [148] specifies six schemes based on symmetric encryption algorithms [ISO 1999], which provides different degrees of authentication: unilateral authentication, mutual authentication, and authentication with key establishment using a third entity (server). Our proposed scheme is based on the fourth protocol of this standard, as we require mutual authentication between the Proxy and the IMD.

7.6.5 Security Service: Access Control

Although Access Control is implemented in the second tier, it is worth a mention here. IMD devices being resource constrained are incapable of handling Access Control. They trust the Proxy device completely which handles the access control in behalf of IMDs.

Table 7.2 Summary of components adopted in communication protocol for Tier 1: Proxy-IMD communication

Security Service	Adopted Security Mechanism
Key Management	Initial secret key distribution (during installation of IMD) Offline distribution and Offline Key Replacement
Message Authentication	AES-GCM
Message Integrity	AES-GCM
Freshness	Nonce and Counter
Confidentiality	Symmetric Encryption using AES
Mutual Authentication	Fourth protocol of ISO/IEC 9798 Part 2

7.7 Profiling of Security Mechanisms for Tier - 2: Proxy Device and External Device communication

We make use of topic based publish-subscribe model [150] for communication between IMD and Proxy Device. Essential security services are Confidentiality, Integrity, Authentication, Access Control and Replay protection [151].

7.7.1 Components of the Communication Model

1. **Publishers:** Publishers are either EDs that are capable of generating data for a specific topic or IMDs that are capable of sending a response when data related to the topic is requested by the proxy.
2. **Subscribers:** Subscribers are either EDs that express interest in a specific topic data or IMDs that have requested for a data from proxy which is related to a specific topic.
3. **Proxy:** Topics are registered with the proxy to whom publishers can send topic data after authentication and validation of its role for a topic. Subscribers can request for topic data after authentication and validation of its role for a topic. Proxy matches the two parties and store and forward topic data to subscribers. List of topics depend on the type of IMD, and may get modified for e.g. when an IMD is added or removed. Security services for mutual authentication, message confidentiality and authentication, replay resilience and access control needs to be provided.

7.7.2 Design Choices for Proxy and ED communication

Point-to-point security solutions like TLS/SSL or IPSec or Kerberos cannot be used here therefore we design a scheme for ensuring integrity and confidentiality of data. Unlike point-to-point communication which secures a stream of information, individual messages for Topics need to be secured. We make use of symmetric 128-bits Topic wise master key. Using shared secret key for publishers and subscribers would mean a group of parties sharing the keys which will increase vulnerability if even one of the parties is compromised. Therefore Topic master key is unique for every Topic. To provide forward and backward security, Topic master key is renewed whenever a subscriber leaves or joins the proxy. The advantage is that if the key for a specific Topic is compromised, still messages related to other Topics cannot be decrypted. For every publisher the topic encryption key is uniquely derived from the Topic master key by making use of Publisher Specific Value (PSV). The advantage is that one publisher cannot decrypt or modify the data send by another publisher on the same topic. For exchanging the symmetric keys and for mutual authentication between Proxy and ED we make use of Public Key cryptography.

7.7.3 Public Key Cryptography

A method for entity authentication and exchange of secret key is to use public key cryptography. Such algorithm uses a set of related keys known as Public and Private Keys. Public keys are exchanged and private keys are kept secret. Exchanged public key can be used for encryption and authentication. The keys used are large in size therefore instead of using them for data encryption; they are used to share secret keys which can then be used for Symmetric Encryption. The Algorithms can also be used to create digital signatures for entity authentication. As both Proxy Device and External Device are rechargeable and have the required computational power, therefore for mutual authentication and secret key exchange we propose use of public key cryptography. Algorithms for Public Key Cryptography are RSA [154] and Elliptic curve cryptography (ECC) [149]. ECC is being used by National Security Agency (NSA) for signature generation and key exchange [150] is preferred.

7.7.4 Security Service: Massage Confidentiality, Integrity and Authentication

Once secret key is shared between Proxy device and External Device using Public Key, Proxy and ED make use of AES-GCM for Message Confidentiality, Integrity and Authentication.

7.7.5 Security Service: Replay protection

Nonce are used for mutual authentication between Proxy and ED. Timestamps are used to ensure message freshness as there can be more that one device publishing to the same topic therefore use of counter will not be relevant.

7.7.6 Security Service: Access Control

An access control list is generated and stored in the Proxy device for granting access. It defines for which are the valid topics, for which topic which device can assume the role of a Publisher and which device can assume the role of a Subscriber.

7.7.7 Security Service: Mutual Authentication

By use of Digital Signatures on a random value nonce, Proxy and External device authenticates each other. Digital Signatures generation algorithm by use of ECC is proposed in [512].

Table 7.3 Summary of components adopted in communication protocol for Tier 2: Proxy-ED communication

Security Services	Devices	Security Mechanism
Source Authentication	Publisher Device, Subscriber Device and Proxy	Digital Signature
Topic Data Confidentiality	Publisher encrypts and Subscriber Decrypts	AES-GCM
Topic Data Integrity and authentication	Ensures Topic Data cannot be modified and source of origin can be proved.	AES-GCM
Anti-Replay	Ensures Topic Data cannot be replayed	Timestamp
Access Control	Ensures only authorized Publishers and Subscribers can communicate.	Access Control List maintained by proxy
Key Management	Publisher Device, Subscriber Device and Proxy	Proxy stores Public Key of devices during registration. Uses Public Key for sharing secret key.

7.8 The Two-Tier Proxy based Architecture and its Components

The secure dissemination of telemetry data between IMDs and external devices occurs with the proxy device as a mediator a shown in Fig. 7.5. IMD performs lightweight authentication and symmetric encryption and generation of random nonces. Rather than storing secret keys of various external devices, it only stores the secret key and counter for proxy device thus requiring less storage. IMD includes battery, sensing or actuation unit,

storage unit, processing unit and a wireless transceiver. The dashed line for skin shows that the IMDs are subcutaneous. For communication with IMDs, the proxy device supports secure request response protocol.

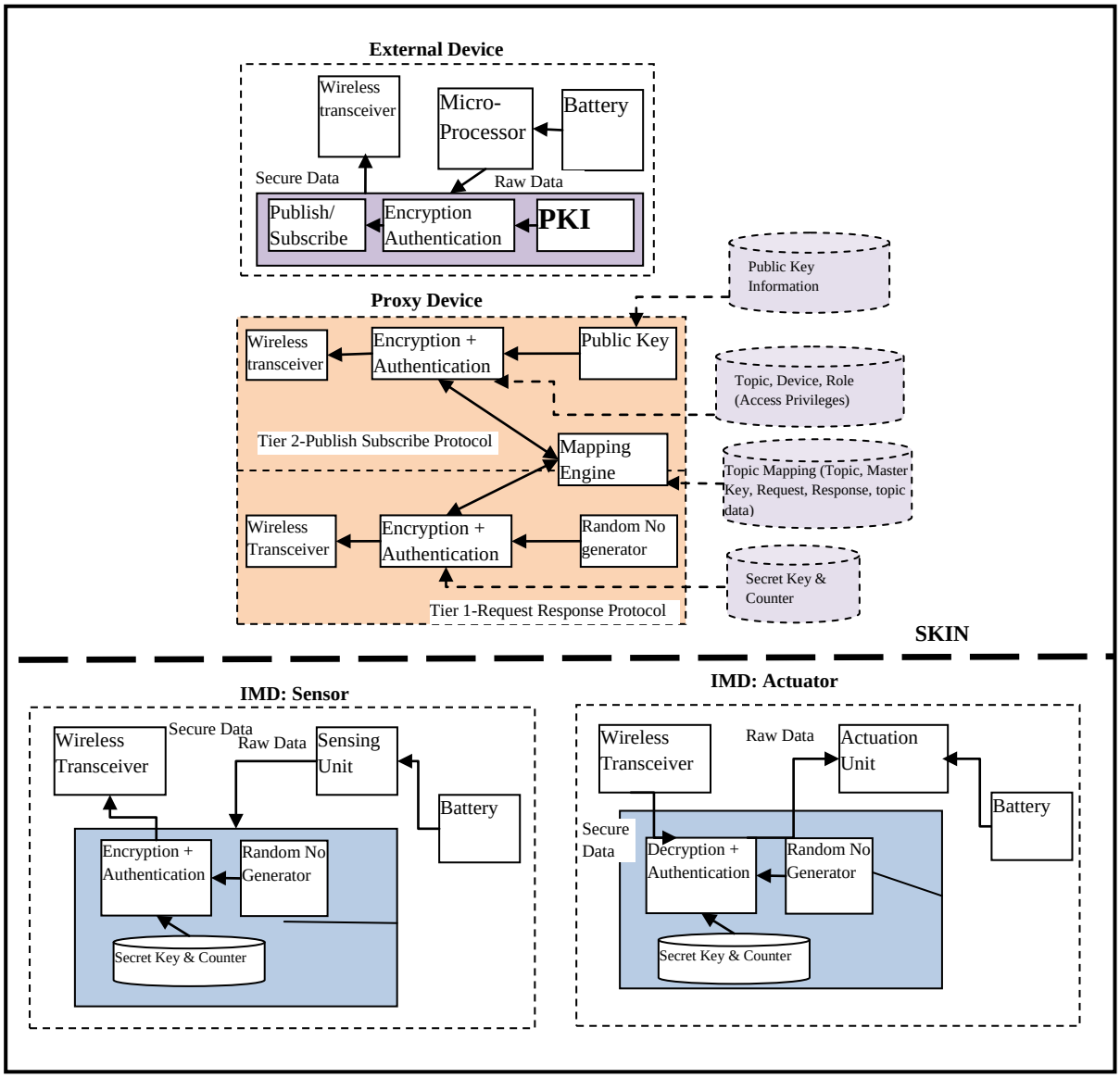

FIGURE 7.5 Architecture of Proxy based Two Tier solutions

Proxy device includes a wireless transceiver, supports lightweight authentication and symmetric encryption, and generation of random nonce. It stores the secret keys of all IMDs with which it is paired. It includes a mapping engine which transforms request-response messages to publish-subscribe messages. It stores Topic Mapping data like Topic Name, Master Key, Request format, Response format which is required by the mapping engine to perform the required conversion.

For secure communication with external devices, proxy device includes wireless transceiver, supports authentication and encryption with the use of Public key stored in

Public Key Information Database. Access Privileges are used by proxy for providing access control by defining specific roles for registered external devices for each topic. It also stores a list of topics, devices, their roles and validity period. It also stores the public key of the external devices which is used for mutual authentication and topic key exchange by use of public keys. For every topic, a list of authorized publisher and subscriber is maintained by the Proxy Device. The external devices are authenticated by the Proxy Device using mutual authentication protocol and for every topic their role of publisher or subscriber is verified. For example, if for a topic Blood Glucose, IMD is publisher and external device A is subscriber then only external device A will receive the notification for topic data and required topic key to decrypt the data. Even though adversary B can snoop over the wireless channel but it will not be able to decrypt the event. The topic data are encrypted using topic keys before disseminating the events in the wireless communication network.

The topic-driven communication is very advantageous for timely and real time information dissemination, for reducing traffic below the level typically required by resource-constrained wireless communication system of IMDs. Our security model functions with both multiple subscribers and multiple publishers which may have different roles for different telemetry event. Publish-subscribe entities operate asynchronously and are unaware of each other's existence.

The first tier constitutes the request-response communication between IMD and Proxy which has two protocols, one for Proxy initiating communication and second for IMD initiating communication. The second tier constitutes publish-subscribe communication with proxy as the mediator which supports two combinations; one with External Device as publisher and second with External Device as subscriber.

7.9 Proxy Device and its role in the two-tier Security Model

This section describes the proxy device and its role in the entire communication protocol. Fig. 7.7 is a flow diagram showing the working of Proxy device in a wireless communication network. One or more IMDs and one or more external medical devices are registered with the proxy device. At step (202), the Proxy device receives a communication request. At step (204), it checks the Device Type (IMD or External Device). At step (206) request-response mode is opted if the communicating device is an IMD. At step (208), light weight symmetric key based mutual authentication is performed for IMD by use of

secret key from (210). At (212) if the device is not found authentic, session is terminated at (214). Otherwise, encrypted request from IMD is received at (216). For the request, topic name is retrieved and role of the IMD as subscriber is verified at (218) from (226). At (220) if the device is not found authentic, session is terminated at (214).

The publisher device type for the topic is retrieved at (224) from (226). At (228), if the publisher device is an IMD, request is send to the IMD for data at (230). At (232) light weight symmetric key based mutual authentication is performed for IMD by use of secret key from (210). At step (234), if device authentication fails, session is terminated at (214). Otherwise at step (236), encrypted request is send to IMD and encrypted response is received at (238). At (240), data is decrypted; its integrity and freshness is checked. At step (242), if data is not found authentic it is discarded at (244) and information is logged. At step (246), data is encrypted and stored as published topic data in (226). At step (248), published topic data is send to all registered and available subscribers.

When the Publisher device is an external device, at step (250) the published topic data is converted to a response. At step (252) the data is encrypted and send to the IMD.

When the device sending connection request is an external device, publish-subscribe mode is used at (254). At step (256) public key based mutual authentication is carried out using public key from (258). At (260) if the device is not authentic, session is terminated at (262). Otherwise, at (264) topic name and device role is checked from (266). At step (268) if the topic and device role is valid, at (270) the role is checked for publisher or subscriber. If the device is subscriber for the topic, Topic Master Key is send to the device by encrypting it with subscriber device Public Key at (272). At step (274), request is send to corresponding IMD for data after retrieving IMD device name from (226). At step (276), encrypted response is received from IMD. At step (278), received data is decrypted and converted to topic data.

At (280) topic data is encrypted by a derived topic key. Topic master key generated by proxy, shared with registered subscriber of topic. This key is renewed when a subscriber joins or leaves the proxy. This provides forward and backward security. Topic master key is hashed to generate derived topic key using a Publisher Specific Value (PSV) specific to the publisher device. It is shared with authorized the publishers of topic by use of Public Key encryption. It is renewed when a subscriber joins or leaves the proxy. This provides forward and backward security. Publisher Specific Value (PSV) generated by Proxy for each Publisher Device for each topic. At (282) the encrypted data is notified to all

subscribers along with the specific value. At step (284), if the device is a publisher, derived topic key for that publisher is encrypted with Public key of the publisher and send. At (286) encrypted topic data is received from the publisher and stored at (226). At (282) the encrypted data is notified to all subscribers along with the Publisher Specific Value (PSV).

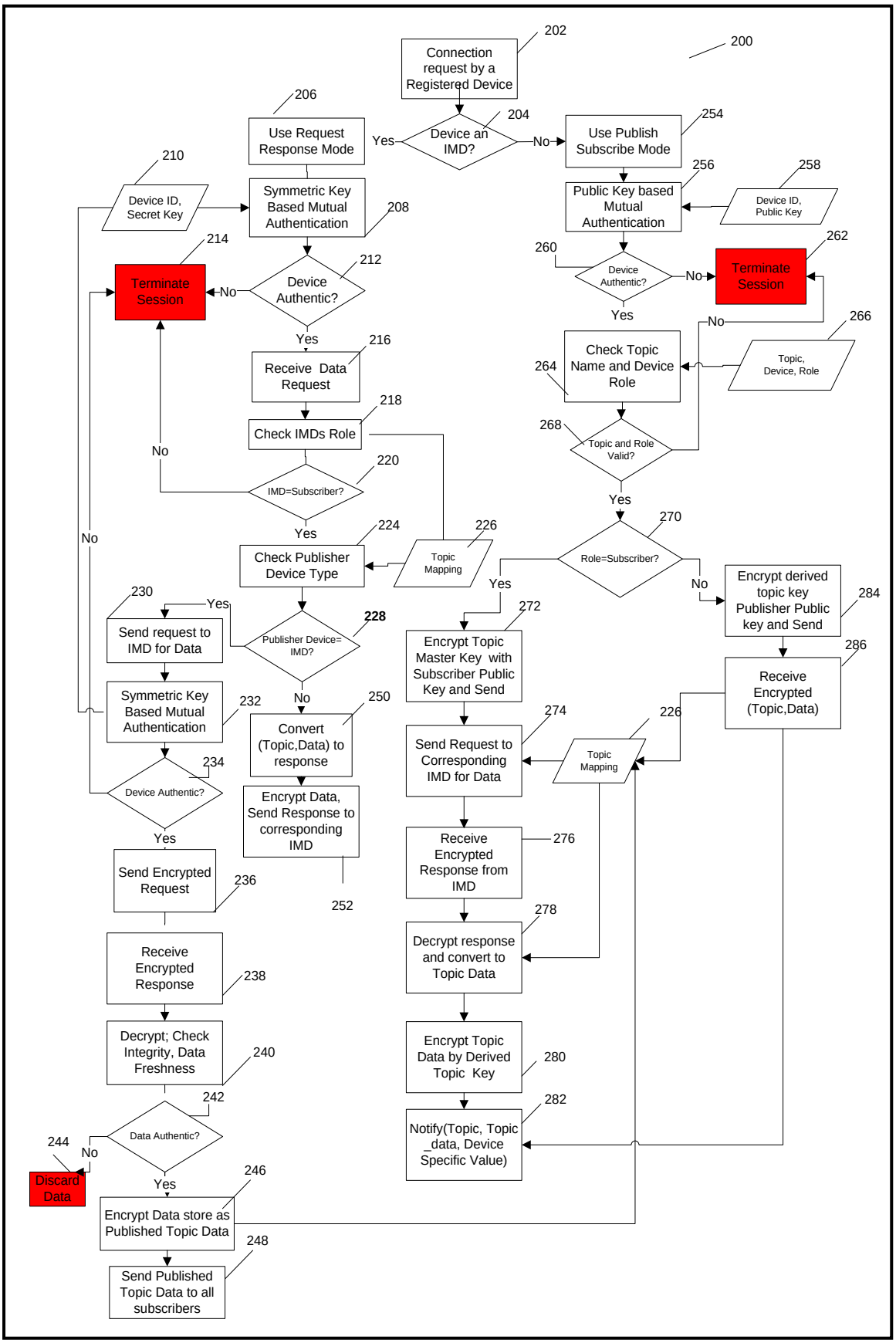

FIGURE 7.6 Work Flow Diagram of Proxy Device

7.10 Description of proposed protocol for Tier – 1: IMD and Proxy Communication

The communication protocols between IMD and Proxy is described in this section. Before commencement of the protocol, IMDs are registered with proxy during registration phase and shares secret keys with it.

The notations used by us for describing the protocols are shown in Table 7.4.

Table 7.4 Notations used in Tier 1: Proxy- IMD communication

Notation	Size	Meaning
IMD	-	Medical Device implanted inside human body
Proxy	-	External Device that provides secure communication with one or more IMDs for a patient.
ID_{Proxy}	32-bits	Identifier of Proxy
ID_{IMD}	32-bits	Identifier of IMD
N_{IMD}	32-bits	Nonce generated by IMD
N_{Proxy}	32-bits	Nonce generated by Proxy
$K_{IMD,Proxy}$	128-bits	AES-GCM encryption Key for secure communication from IMD to Proxy. Stored by IMD and Proxy.
$K_{Proxy, IMD}$	128-bits	AES-GCM encryption Key for secure communication from Proxy to IMD. Stored by IMD and Proxy
C_{IMD}	32 bits	Counter of IMD to avoid replay attack
C_{Proxy}	32 bits	Counter of Proxy to avoid replay attack
IV_{IMD}	96 bits	IV used by IMD for AES-GCM encryption. $IV_{IMD}= N_{IMD}\| N_{Proxy}\| C_{Proxy}$
IV_{Proxy}	96 bits	IV used by Proxy for AES- GCM encryption. $IV_{IMD}= N_{Proxy}\| N_{IMD}\| C_{IMD}$
REQ	32 bits	Request in plaintext
RESP	N*32 bits	Response of Request in plaintext; multiples of 32 bits
(C,Tag)	-	(C,Tag)=GCM_K(IV,P,AAD) K=Encryption Key ($K_{Proxy, IMD}$ or $K_{IMD,Proxy}$) IV=Initialization Vector P=Plaintext message to be encrypted and authenticated AAD=Additional Authenticated Data; This data is authenticated, but not encrypted C=Ciphertext Tag= Authentication Tag
Tag	64 bits	Authentication Tag

The communication between IMD and Proxy can occur in two scenarios. The proposed protocol for, Proxy initiating communication and IMD initiating communication are given below:

7.10.1 Protocol 1: Proxy initiating communication

When an external device or another IMD requires telemetry data they subscribe to the corresponding Topic with the Proxy. For every Topic and related request-response

sequences needed are preconfigured in Proxy. The proxy wakes up the respective IMD associated with that topic as a publisher.

In this scenario, Proxy initiates communication with the IMD. Before communicating, proxy is authenticated by IMD using a light weight challenge handshake protocol as shown in the sequence diagram in Figure 7.7.

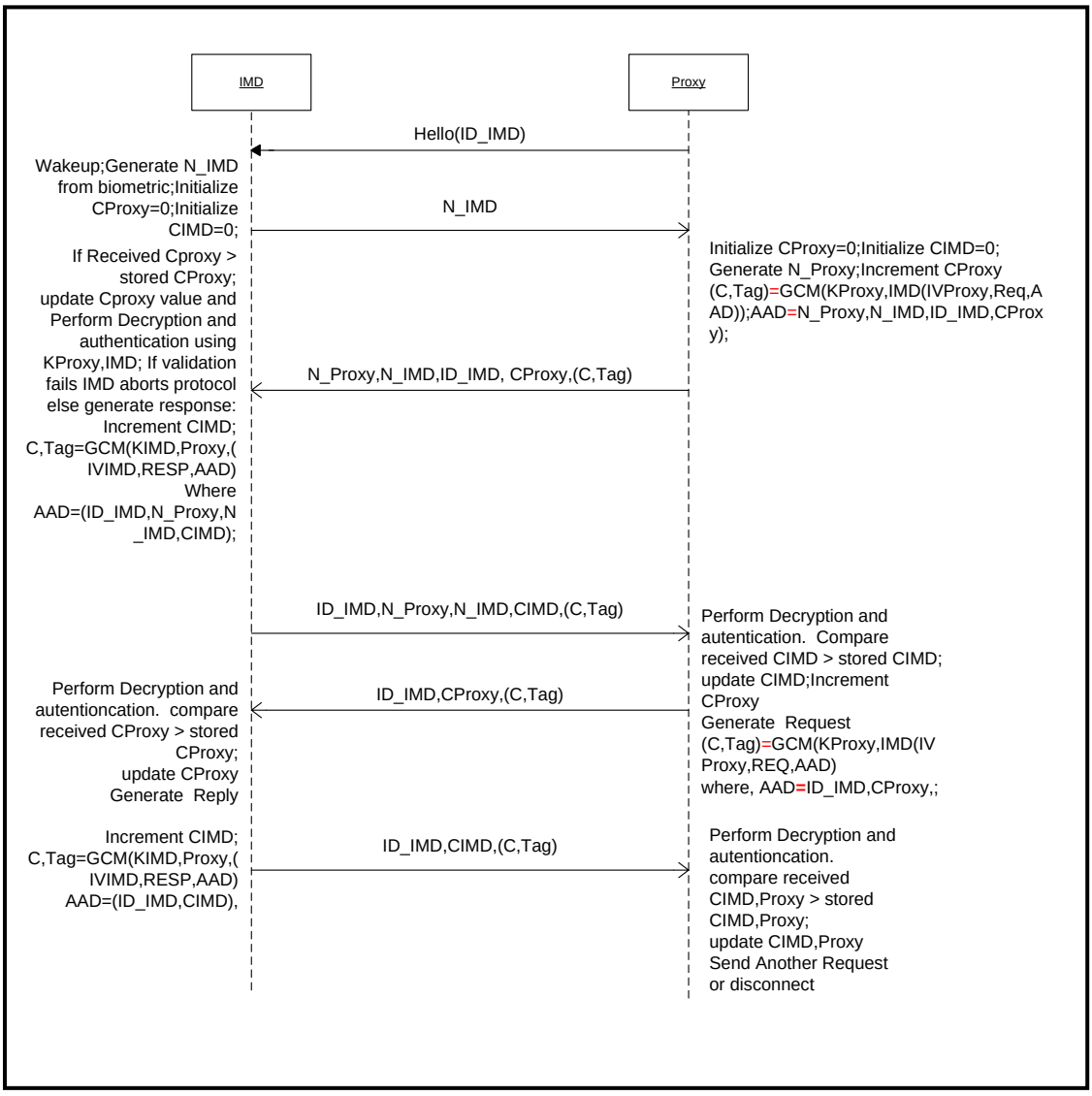

Figure 7.7: Sequence Diagram for Protocol: Proxy Initiating Communication

The message exchanges related to this protocol and their interpretations are given in Table 7.5. The table shows the sender and the receiver of the message, the message transmitted and also what action is taken by the receiver after receiving the message.

Table 7.5 Description of messages for Protocol: Proxy initiating communication

Sender→Receiver	Message	Interpretation
Proxy→ IMD	hello(ID_{IMD})	The proxy sends Hello to wake up the implant.
IMD → Proxy	N_{IMD}	The IMD generates a nonce by use of Physiological Value and sends it to the proxy
Proxy→ IMD	N_{Proxy}, N_{IMD},ID_{IMD},C_{Proxy} ,(C,Tag)	The proxy generates a random number and computes an Authentication Tag. It includes the random number received and the one generated by Proxy, the identifier of the target IMD (ID_{IMD}), Counter of Proxy(C_{Proxy}). Additionally, a command field (REQ) is included as a part of this message. Finally, these two random numbers together with the Authentication Tag and an encrypted version of the command are sent to the implant.
IMD → Proxy	ID_{IMD}, N_{Proxy}, N_{IMD}, C_{IMD} ,(C,Tag)	The implant decrypts the REQ received, computes a local version of the Authentication Tag, and checks its equality with the received value. Note that only the target implant knows the identifier (ID_{IMD}) used and the two nonces associated with the session. If this authentication fails, the implant aborts the protocol. Otherwise, the IMD generates a response and sends an Authentication Tag, which includes the two nonces and the response command (RESP). It also includes the response in encrypted form.
Proxy→IMD	ID_{IMD},C_{Proxy},(C,Tag)	The proxy decrypts the response. Then, knowing the RESP and the two nonces linked to the current session, the proxy calculates a local version of the Authentication Tag. If the received values and the computed values are equal, the reader and the implant are mutually authenticated and can perform request response. If not, the proxy disconnects and generates log. Proxy sends request which contains Identifier of IMD, Counter, encrypted data and authentication tag.
IMD → Proxy	ID_{IMD},C_{IMD},(C,Tag)	IMD decrypts the request, checks its authentication and sends response in encrypted form. If this authentication fails, the implant aborts the protocol.

Once the mutual authentication between IMD and proxy is over, Nonce is no longer used. To counter Replay Attacks, counters are used at IMD side and Proxy side.

7.10.2 Protocol 2: IMD initiating communication

IMD initiates communication when it requires some telemetry data from sensor IMD. Once an IMD has subscribed for the data for actuation purpose, Proxy is responsible for delivering the data after predefined time intervals. IMD also initiates communication in case of an emergency sensed by IMD. In this protocol, Proxy at random periods broadcasts Nonce. If an IMD wants to communicate with Proxy, it listens for the broadcasted nonce and then executes the protocol shown in Figure 7.8. Once mutual authentication is over, both may communicate further by sending request and receiving response.

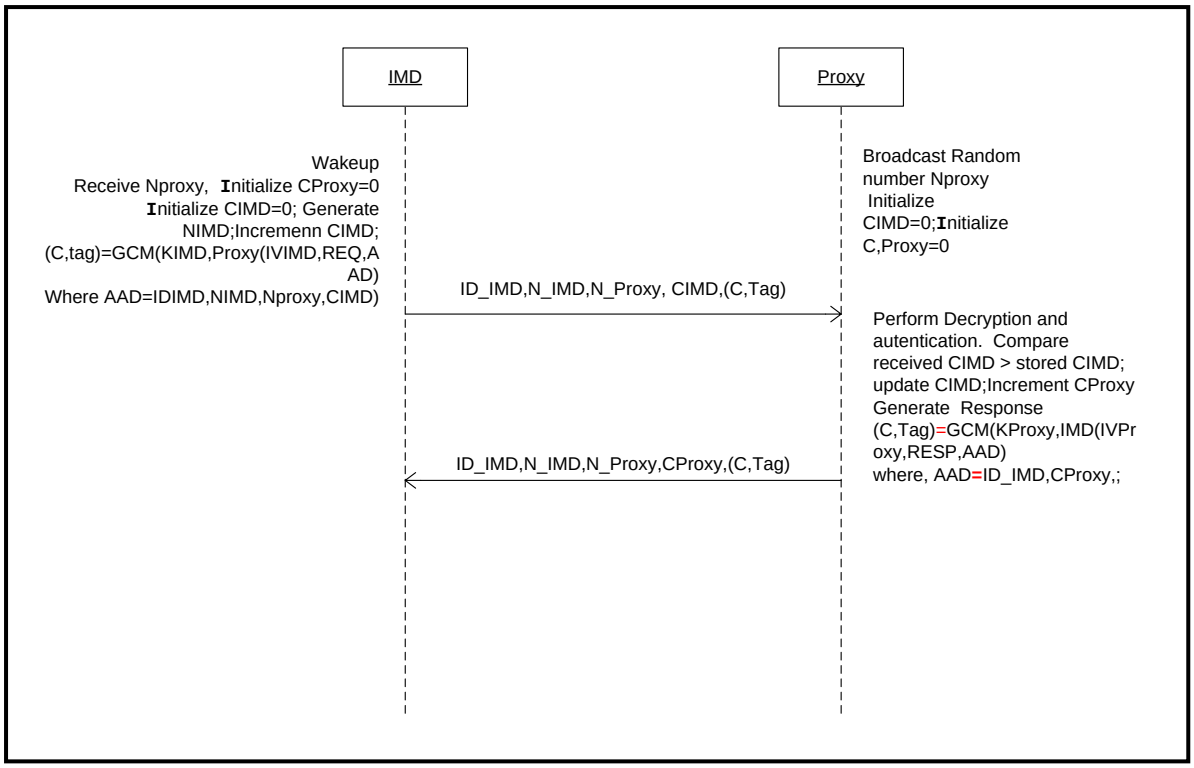

Figure 7.8: Sequence Diagram for Protocol: IMD Initiating Communication

The message exchanges related to this protocol and their interpretations are given in Table 7.6. It shows the sender and the receiver of the message, the message transmitted and also what action is taken by receiver after receiving the message.

Table 7.6 Description of messages for IMD initiating communication

Sender → Receiver	**Message**	**Interpretation**
Proxy → IMD	Broadcast N_{Proxy}	IMD broadcasts an nonce at random periods, when IMD wants to communicate with proxy, it listens for the broadcast and reads the N_{Proxy}
IMD → Proxy	ID_{IMD},N_{IMD},N_{Proxy}, C_{IMD},(C,Tag)	The IMD generates a nonce by use of Physiological Value and computes an Authentication Tag. It includes the random number received and the one generated by Proxy, its identifier (ID_{IMD}), Counter of IMD(C_{IMD}). Additionally, a command field (REQ) is included as a part of this message. Finally, these two random numbers together with the Authentication Tag and an encrypted version of the command are sent to the proxy.
Proxy → IMD	ID_{IMD},N_{IMD},N_{Proxy}, C_{Proxy},(C,Tag)	The proxy decrypts the response. Then, knowing the RESP and two nonces linked to the current session, the proxy calculates a local version of the Authentication Tag. If the received values and the computed values are equal, the reader and the implant are mutually authenticated and can perform request response. If not, the proxy disconnects and generates log. Proxy sends request which contains Identifier of IMD, Counter, encrypted response and authentication tag.

7.10.3. Message Formats for Tier 1: Proxy-IMD communication

In the communication protocols, it is desired that the overhead of additional data fields due to introduction of security transformations should be minimized as far as possible. The message formats that we have designed for the above described sequence of messages between IMD and Proxy are shown in Figure 7.9.

1) Authentication request message send by Proxy to IMD

ID_{IMD} [32-bits]	N_{IMD} [32-bits]	N_{Proxy} [32-bits]	C_{Proxy} [32-bits]	Encrypted Data [N*128 bits]	Authentication Tag [64-bits]

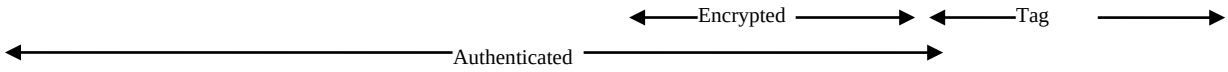

FIGURE 7.9 (a) Format of authentication request made by Proxy

2) Request and Response message between Proxy and IMD

ID_{IMD} [32-bits]	Counter [32-bits]	Encrypted Data [N*128 bits]	Authentication Tag [64 bits]

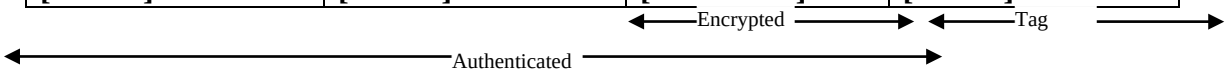

FIGURE 7.9 (b) Format of request and response messages

3) Authentication Message: IMD to Proxy

ID_{IMD} [32-bits]	N_{IMD} [32-bits]	N_{Proxy} [32-bits]	C_{IMD} [32-bits]	Encrypted Data [N*128 bits]	Authentication Tag [64 bits]

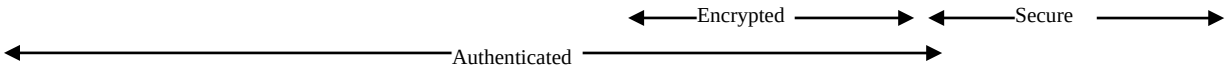

FIGURE 7.9 (c) Format of authentication requests made by IMD

7.11 Description of proposed protocol for Tier 2: Proxy and External Device Communication

The protocols for topic based publish-subscribe communications via the Proxy for External Devices is described in this section. Before commencement of the protocol, EDs are registered with proxy during registration phase and store each other's public key.

Tier II uses publish-subscribe communication model [150] with proxy as the mediator between IMDs and EDs. The Proxy performs conversion of IMD response to Publish Message and IMD request to Subscribe Message. Communication may not only be one-to-one, but can also be many-to-one, one-to-many, or many-to-many. Data (telemetry messages and commands) to be communicated or requested is organized into topics which are uniquely identified by a name and stored in the proxy during device registration. Proxy receives topic-data from publisher device and in turn forwards it to the intended subscriber device. Proxy is aware of Publisher's and Subscriber's identity, and authenticates them on behalf of IMD. In a topic based Publish-Subscribe paradigm, instead of addressing messages to actual recipient, sender application puts the name of a topic and delivers it to the proxy. The proxy then sends the message to all the devices that have subscribed to messages on that topic and are currently available (active).

Some Examples of Mapping of Biometric data to Topics are shown in TABLE 7.7.

Table 7.7 Examples of Mapping of Biometric data to Topics

Request Messages	Topic
Hemoglobin	HMB
Blood Glucose	BG
Blood Pressure	BP
Temperature	TEMP
Blood Flow	BF
Emergency	EMER

The states of External Device are given in Table 7.8.

Table 7.8 States of External Device maintained by Proxy

State	Description
Registered	A device for which information is available with the proxy. IMDs are registered and paired with proxy using secret key. EDs are registered using their public key.
Active	A registered device when sends join request to the proxy to Publish or Subscribe data. The mutual authentication between Proxy and IMD occur using Digital Signature. For IMDs the state is always active.
Unregistered	A device which wants to communicate with IMD but is not registered. It needs to be registered with the proxy in case of Normal Condition. But in case of an Emergency Condition when the patient's life is at stake, ED can directly start communicating with the proxy bypassing registration.
Inactive	A device which is registered with the proxy but is not currently associated with the proxy for Publishing or Subscribing to Telemetry Data. EDs can be inactive but IMDs are always active.

The notations used by us for describing the protocols are shown in Table 7.9.

Table 7.9 Description of notations used in Tier – 2 communications

Notations	Generation Technique	Description
PU_{Proxy}	ECC	Public Key of Proxy
PR_{Proxy}	ECC	Private Key of Proxy
PU_{Dev}	ECC	Public Key of Device
PR_{Dev}	ECC	Private Key of Device
K_{Topic_Master}	AES-CTR	Topic wise Master Secret Key generated by proxy, shared with registered subscriber of topic when they are active. Renewed when a subscriber joins or leaves the proxy. This provides forward and backward security.
K_{Topic_Pub}	K_{Topic_Pub} =Hash(PSV_{Pub},K_{Topic_Master})	Publisher Key, K_{Topic_Pub} is generated by proxy from master key K_{Topic_Master} by using PSV_{Pub} for a publisher for each Topic. It is shared with registered publisher of topic when they are active. It is renewed when a subscriber joins or leaves the proxy as Topic Master Key for the topic changes.
PSV_{Pub}	AES-CTR	Publisher Specific Value (PSV) generated by Proxy for each Publisher Device for each topic. This PSV is used to generate K_{Topic_Pub} for each publisher.
Id_{Device}	-	Unique Id of External Device
N_{Device}	-	Nonce generated by External Device
N_{Proxy}	-	Nonce generated by Proxy
DS_{Device}	DS_{Device}=E(PR_{Device},H(Id_{Proxy} ,$Id_{Device,}$ N_{Device}))	Digital Signature generated by External Device for authentication [152]
DS_{Proxy}	DS_{Device}=E(PR_{Proxy},H(Id_{Proxy} ,$Id_{Device,}$ $N_{Device,}$ N_{Proxy}))	Digital Signature generated by Proxy for authentication [152]
Id_{Topic}		This Identifier value is mapped with Topic name
TS	By device publishing data	Timestamp for Data to check for message freshness.

7.11.1. Protocol: Communication between Proxy and ED as Publisher

When an external device (ED) wants to publish data for a Topic registered with Proxy, initial message exchange occurs prior to topic data publication for mutual authentication. When the publisher wants to publish topic data, it first sends a join message to the Proxy using the device identifier, nonce and digital signature for publisher authentication and authorization. When the authentication and authorization is successful, proxy sends a join acknowledgment message to the publisher along with its digital signature for mutual authentication. The publisher requests for the topic key for a particular Topic which is send to it after encrypting with Publisher's Public Key along with the Publisher Specific Value (PSV) allocated to the Publisher. The publisher can encrypt the data and send data to proxy which stores the topic data for forwarding it to the subscribers. The sequence diagram for

communication between Proxy and External Device acting as Publisher is shown in Fig. 7.10.

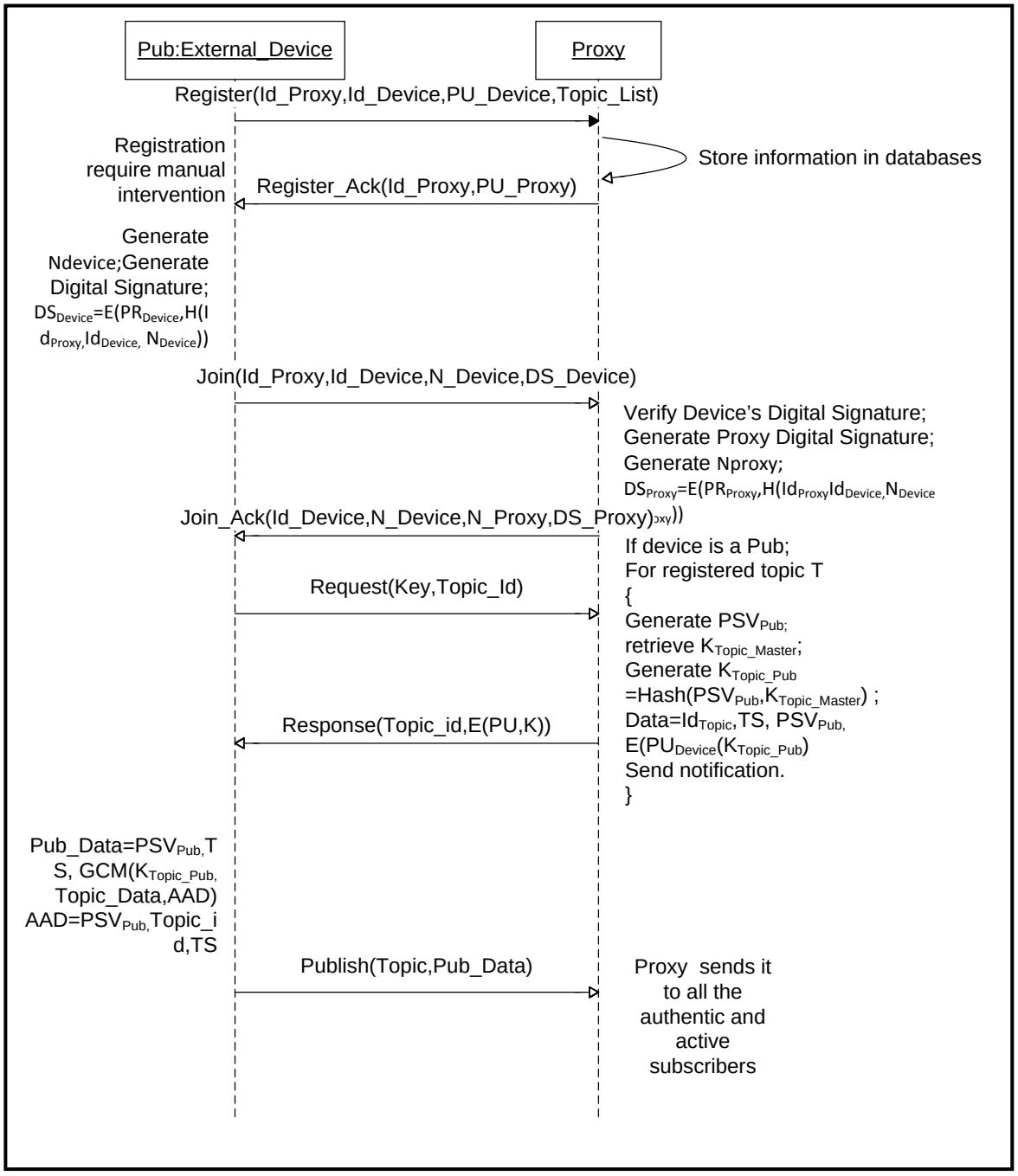

Figure 7.10: Sequence Diagram for communication between Proxy and External Device as Publisher

The message exchanges related to this protocol and their interpretations are given in Table 7.10. The table shows the sender and the receiver of the message, the message transmitted and also what action is taken by receiver after receiving the message.

Table 7.10 Description of messages for Proxy and Publisher External Device communication

Sender→Receiver	Message	Interpretation
Publisher ED → Proxy	Join(Id_{Proxy},Id_{Device},N_{Device},DS_{Device})	Join request is sent by a registered ED along with its Nonce and Digital Signature
Proxy→ Publisher ED	Join_Ack(Id_{Device},N_{Device},N_{Proxy},DS_{Proxy})	Proxy verifies the Digital Signature of ED, generates its Nonce value, generated a digital signature and sends to the ED.
Publisher ED → Proxy	Request(Key,Topic Id)	Before publishing Topic data, Publisher ED requests the Proxy to send the Topic Publish Key and Publisher Specific Value (PSV). The proxy on receiving this request verifies the role of the device for the Topic. It generates PSV_{Pub} and retrieves Topic Master Key retrieve K_{Topic_Master}. Generation of Publisher Key K_{Topic_Pub} =Hash(PSV_{Pub},K_{Topic_Master}) ;
Proxy→ Publisher ED	Response(Topic_id, E(PU,K))	The Publisher receives Id_{Topic},TS,$PSV_{Pub,}$,E(PU_{Device}(K_{Topic_Pub}) From which it decrypts the Publisher Key, K_{Topic_Pub} and uses it to encrypt the Topic data using AES-GCM. Pub_Data: TS,PSV_{Pub} ,(C,Tag) (C,Tag)=GCM(K_{Topic_Pub},Topic_Data, AAD) AAD= PSV_{Pub},Topic_id,TS
Publisher ED → Proxy	Publish(Topic_id,Pub_Data)	When proxy receives Topic data from publisher it mediates the data to all the authentic and active subscribers for that topic.

7.11.2. Protocol: Communication between Proxy and ED as Subscriber

When the subscriber wants to receive topic data, it first sends a join message containing digital signature to the Proxy for authentication and authorization. When the authentication and authorization of the subscriber is successful, proxy sends a join acknowledgment message to the subscriber along with its own digital signature for mutual authentication. When subscriber requests topic master key, Proxy encrypts the key with public key of subscriber and sends it. When data is available for the topic, the proxy notifies the subscribers that are active. The sequence diagram for communication between Proxy and External Device acting as Subscriber is shown in Figure 7.11.

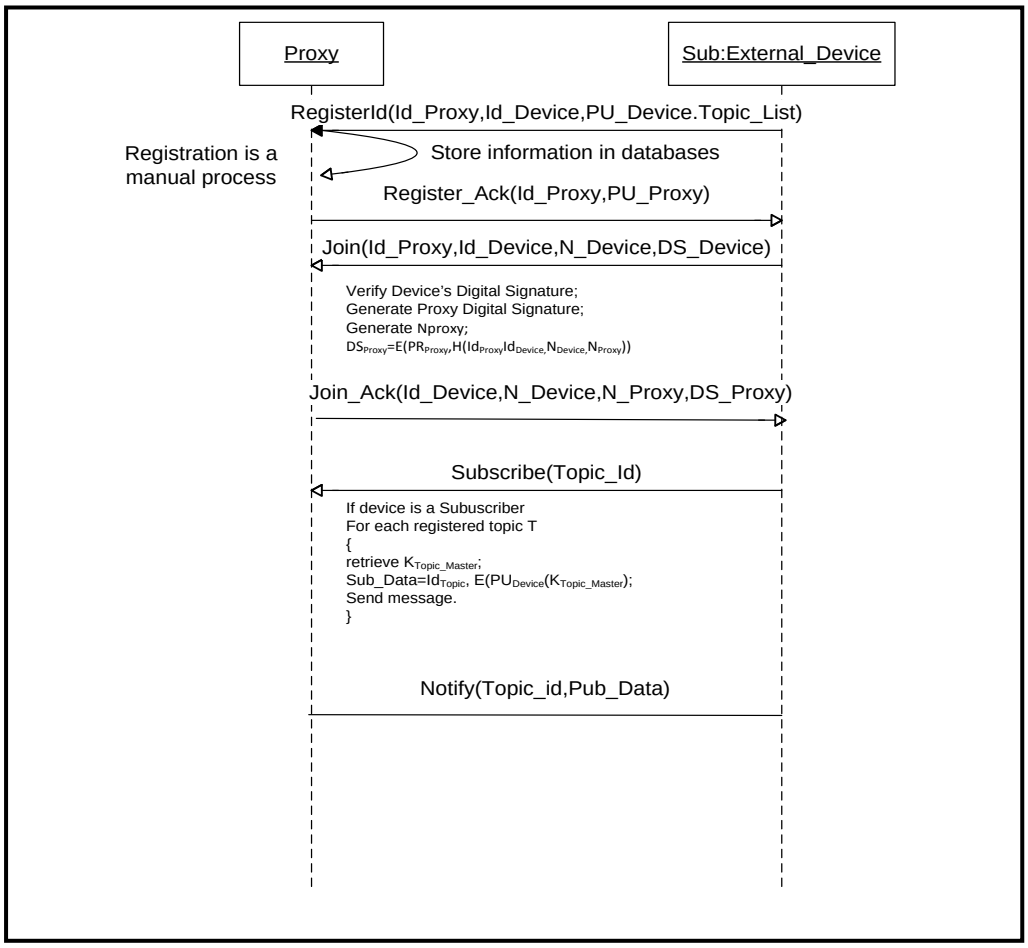

Figure 7.11: Sequence Diagram for communication between Proxy and External Device as Subscriber

The message exchanges related to this protocol and their interpretations are given in Table 7.11. The table shows the sender and the receiver of the message, the message transmitted and also what action is taken by receiver after receiving the message.

Table 7.11 Description of messages for Proxy and Subscriber External Device communication

Sender→Receiver	**Message**	**Interpretation**
Subscriber ED → Proxy	Join(Id_{Proxy},Id_{Device},N_{Device},DS_{Device})	Join request is sent by a registered ED along with its Nonce and Digital Signature
Proxy→ Subscriber ED	Join_Ack(IdDevice,NDevice,NProxy,DSProxy)	Proxy verifies the Digital Signature of ED, generates its own Nonce value, generates a digital signature and sends to the ED.
Subscriber ED → Proxy	Subscribe(TopicList)	Proxy validates the role of ED as a subscriber for a particular Topic and retrieves the Topic Master Key. It encrypts the Topic Master Key by Public Key of subscriber and sends it to the ED.
Proxy→ Subscriber ED	Notify(Topic_id,Pub_Data)	If Published data is available, Proxy notifies the Publisher Specific Value (PSV) and the Encrypted data to the ED. ED at its end generates the Key to decrypt data by

		performing one way hash on the Topic Master Key using PSV send with the encrypted message. Subscriber checks timestamp to ensure data is not replayed. The recipient subscriber uses receive PSV_{Pub} to check for data authentication. Uses the topic master key K_{Topic_Master} to generate the Publisher Key to decrypt the Topic data. K_{Topic_Pub} =Hash(PSV_{Pub},K_{Topic_Master}) Plaintext Topic_Data= GCM(K_{Topic_Pub},Topic_Data)

7.12 Essential Functions Provided by Proxy

Proxy device is the heart of our protocol and performs many essential functions to support the proposed security model. We provide a list of such functions and the data structures used for that.

7.12.1. Topic Management

The topics need to be defined and preregistered with the proxy when an IMD is registered. For every topic defined with the proxy, either publisher or subscriber or both are IMD devices. Therefore for every topic proxy that maintains, the corresponding request message and response message for communicating with the IMD is also stored. The format of Data Structure for Topic management is shown in Table 7.12.

Table 7.12 Topic Management Database

Field	Description
Topic Identifier	This field uniquely identifies the topics.
Topic Name	This is a user defined name given to the topic
Description	This is the additional information stored for the topic.
Topic Flag	This flag is used by Proxy to check if the topic is Active or Inactive. If the topic is active it means that for this topic there are IMDs associated with proxy.
Topic Master Key(K_{Topic_Master})	This is the master key related to the topic which is shared with the subscribers. It is also used to generate the Publisher key by using Publisher Specific Value (PSV).
Request Message (REQ)	This stores the format of request message to be sent to the IMD for requesting data for this topic. This is required if Publisher is IMD.
Response Message (RESP)	This stores the format of response message to be sent to the IMD when data is available on this topic. This is required if the Subscriber is an IMD.
Probe Time Interval	With the topic we also keep a probe time interval after which a new request is send to IMD by proxy if there are active subscribers for that topic. This allows the IMD to remain in sleep state this saving battery power.

If no active subscribers are present no data request goes to the IMD in order to save IMD battery power. If a new subscriber joins during the time interval for which response is already received from proxy, the same response is sent to the subscriber without generating a new request for the IMD. For a single Topic if there are two or more IMDs publishing

data, Proxy may adopt any cast wherein request may be send to any one of the IMD in general or to a specific IMD by taking into consideration the amount of battery available with IMD. If publisher and subscriber both for a particular Topic are IMDs then proxy can implement a timer which when fires, proxy requests data from Publisher IMD (by request-response) and then delivers the data to subscriber IMD (by request-response).

7.12.2. Device Management

All external devices including proxy have a set of public and private keys. During registration of an ED, information like its Identifier, Topic Identifier, Role of the ED for the topic, and Public key are stored as shown in Table 7.13.

Table 7.13 Device Information Database

Field	Description
Device Id	This field uniquely identifies the device.
Device Name	This is a user defined name given to the device.
Device Type	This field is used to store the type of registered device which can be an either IMD or ED.
Device Flag	For an ED, this flag is true, it means that the device is currently active and is associated with proxy by sending a join message. By default for all IMDs currently installed, the flag is true.
Device Description	This is the additional information about the device.
Public Key	If the device is an ED, this field stores the RSA or ECC Public key of the device.

7.12.3. Access Management

ED that is a Subscriber for a topic when registered with proxy can only receive messages that they are authorized for. Publisher when registered with proxy can publish to one or more topics only if are authorized for the topic. For every topic the role and validity period for a device is stored as shown in Table 7.14.

Table 7.14 Device Access Control Database

Field	Description
Topic Id	This field uniquely identifies a topic.
Device Id	This field uniquely identifies the device associated with the topic.
Role	This field stores the role of the device which can be either publisher or subscriber.
Valid From	This stores the validity period start date and time.
Valid To	This stores the validity period end date and time.

7.12.4. Key Management

The Topic Master key needs to be renewed from time to time. Especially when an ED subscriber joins or leaves the proxy, the master key needs to renewed in order to render forward and backward security. In order to do this, Proxy generates new Topic master key (K_{Topic_Master}) and notifies all the subscribers who are active for a specific topic. For each active publisher of the topic, it uses the Publisher Specific Value (PSV_{Pub}) and to derive a new Topic Publish Key(K_{Topic_Pub}) and notifies it to the corresponding publisher.

7.12.5. Emergency aware Access Management

When an IMD initiates communication with the proxy device in case of a patient emergency condition the Proxy notifies all the active external devices by publishing on emergency topic. This enables the health provider to take an immediate action for patient health restoration. In case none of the registered ED are available in the vicinity, the proxy may allow unregistered external device to access the IMD for a specific period of time which can be calculated with the help of solution given in [124].

7.13 Deployment Model

The proposed security model can be deployed by use of an additional handheld device like PDA or smartphone which is readily available. It may provide a user interface for registration of IMD and EDs and also for defining topics. Figure 7.12 show the deployment model with IMDs implanted in human body and registered with proxy device, EDs registered with proxy device and proxy device providing the functionalities for Tier-1 and Tier-2. To keep it simple we do not show the data that is being passed along with the methods.

Methods used for Tier-1 Request-response protocols between IMD and Proxy are mentioned below:

2.1 Registration: This method allows registration of an IMD with the proxy device. A pair of secret key is shared and the IMD related information is stored.

2.2 Mutual Authentication: This method allows IMD and Proxy to authenticate each other before requesting for data or generating response.

2.3 Request: This method allows proxy device or the IMD to generate a request and send it in a secure manner.

2.4 Response: This method allows proxy device or the IMD to generate a response and send it in a secure manner.

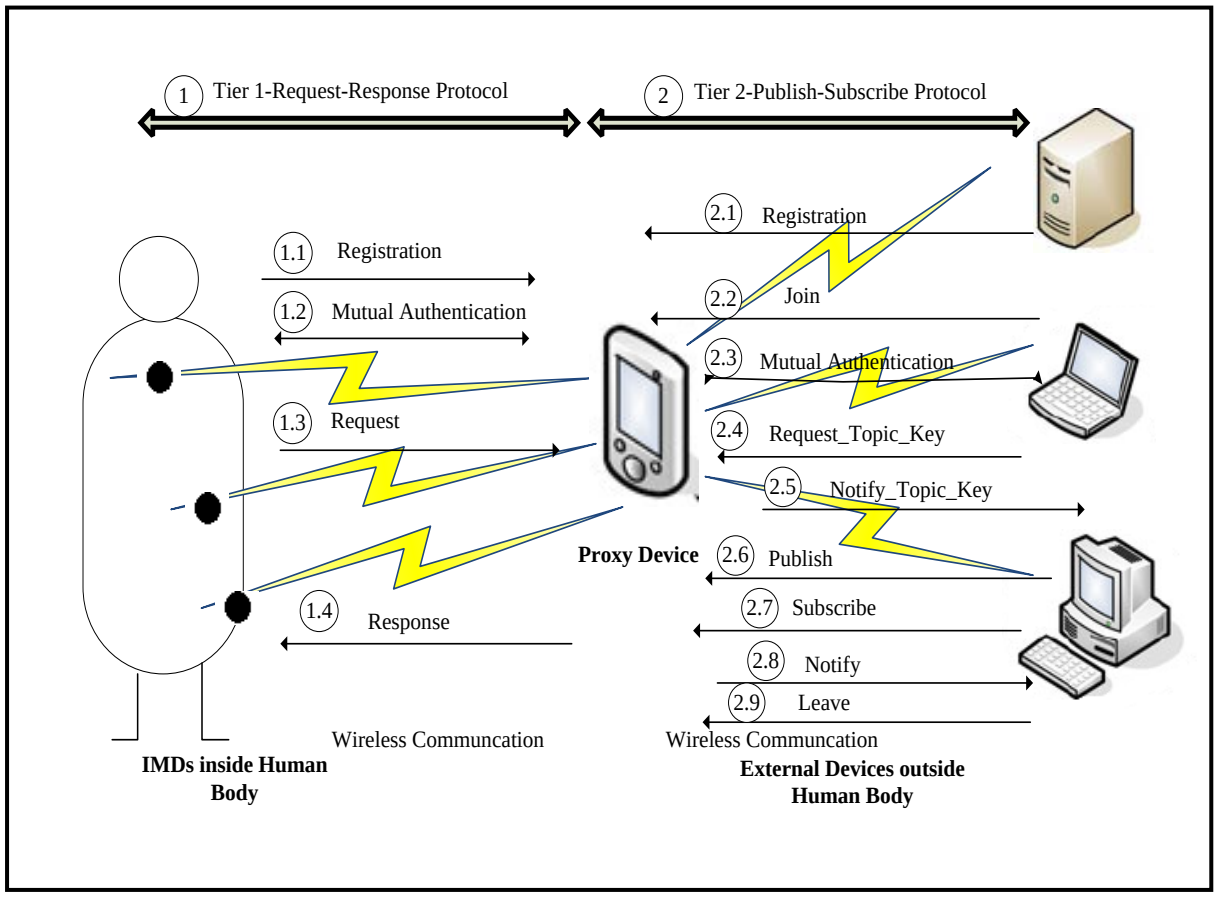

Figure 7.12 Deployment Model

The Methods used for Tier-1 Request-response protocols between Proxy and External Device are mentioned below:

2.1 Registration: This method allows use of User Interface for input of the device information like public key, a set of topics and the role of the device for that topic.

2.2 Join: This method allows a registered external device to get associated with the proxy device.

2.3 Mutual Authentication: This method allows ED and Proxy to authenticate each other before requesting for data or generating response.

2.4 Request_Topic_Key: This method allows ED to request for a symmetric key related to a topic either for encrypting data to be published for the topic of for decrypting the received topic data.

2.5 Notify_Topic_Key: This method allows Proxy to notify the Topic related key to the active EDs.

2.6 Publish: This method allows Publisher ED to publish data related to a topic in secure manner. It also allows proxy to publish data on behalf of IMD.

2.7 Subscribe: This method allows Subscriber ED to subscribe to data feed related to a topic. It also allows proxy to subscribe to data feed on behalf of IMD.

2.8 Notify: This method allows Proxy to send available data for a topic to a subscriber.

2.9 Leave: This method allows EDs to get disassociated from the proxy device when they no longer want to receive data.

CHAPTER – 8

Implementation and Analysis

8.1. Implementation

We implemented the entire protocol to provide a proof of concept using C# programming language and XML. The prototype implementation demonstrated the suitability of our proposed solution. We have developed the prototype which is explained below:

Network Switch that simulates a wireless environment and broadcasts the received data to all the devices present in the network. The UI for the Network Switch is shown in Fig. 8.1.

Device Selection Screen which can be used to select a number of IMDs and a number of ED which are registered with the Proxy. It is compulsory to start the Proxy as the Proxy Device is heart of the proposed security model. The screen shot shown in Fig. 8.1 shows the UI for device selection. It shows the Device ID, Device Type, Name, Description, configuration file.

The configuration file is an XML file storing the details of the device. The Topic Management, device management and role management is implemented as XML files.

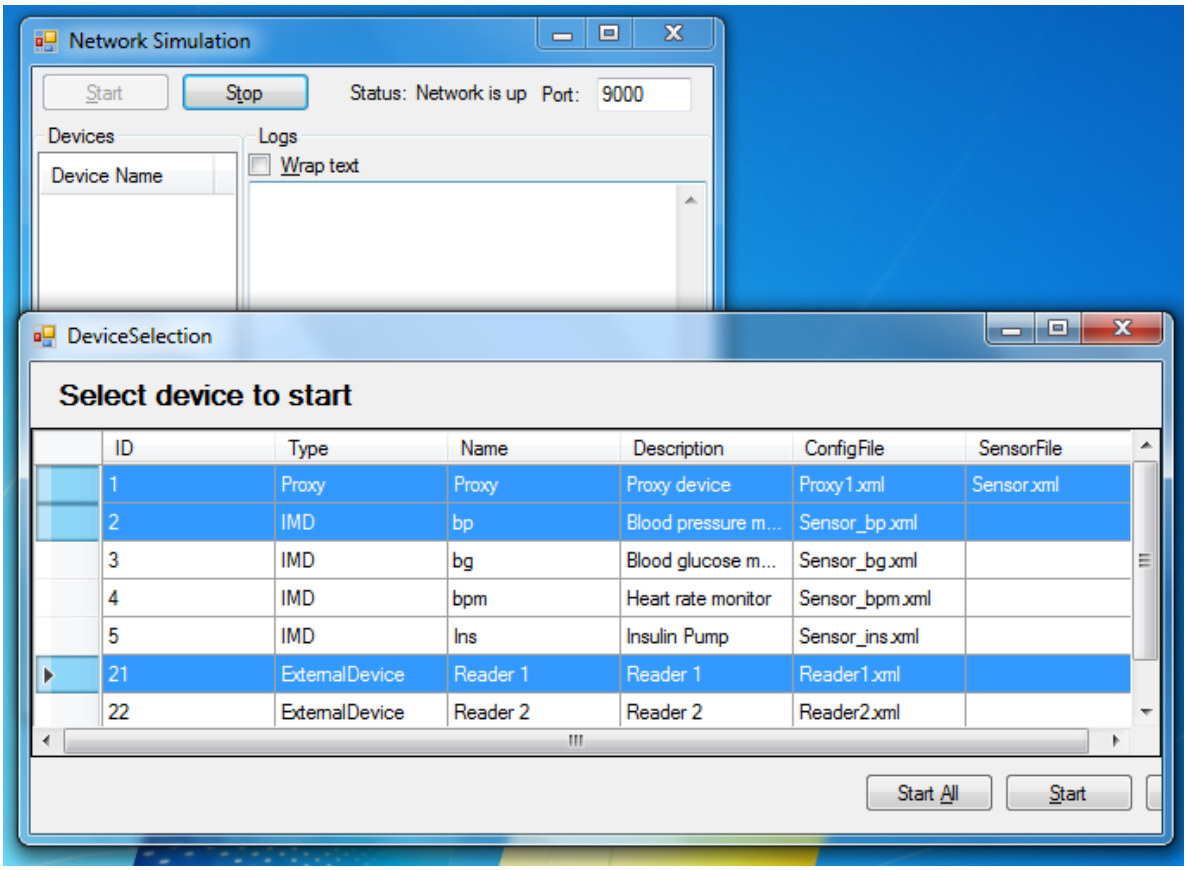

Figure 8.1 Network Switch Screen and Device Startup Screen

Once the Proxy device has started, secure request-response protocol is executed on click of Connect button of Proxy Device. The request-response protocol for Proxy initiating communication is described in Chapter 7. Mutual authentication between IMD and Proxy is shown in Fig 8.2. If one or more EDs are available, secure publish-subscribe communication protocol as described in Chapter 7 is executed by the Proxy.

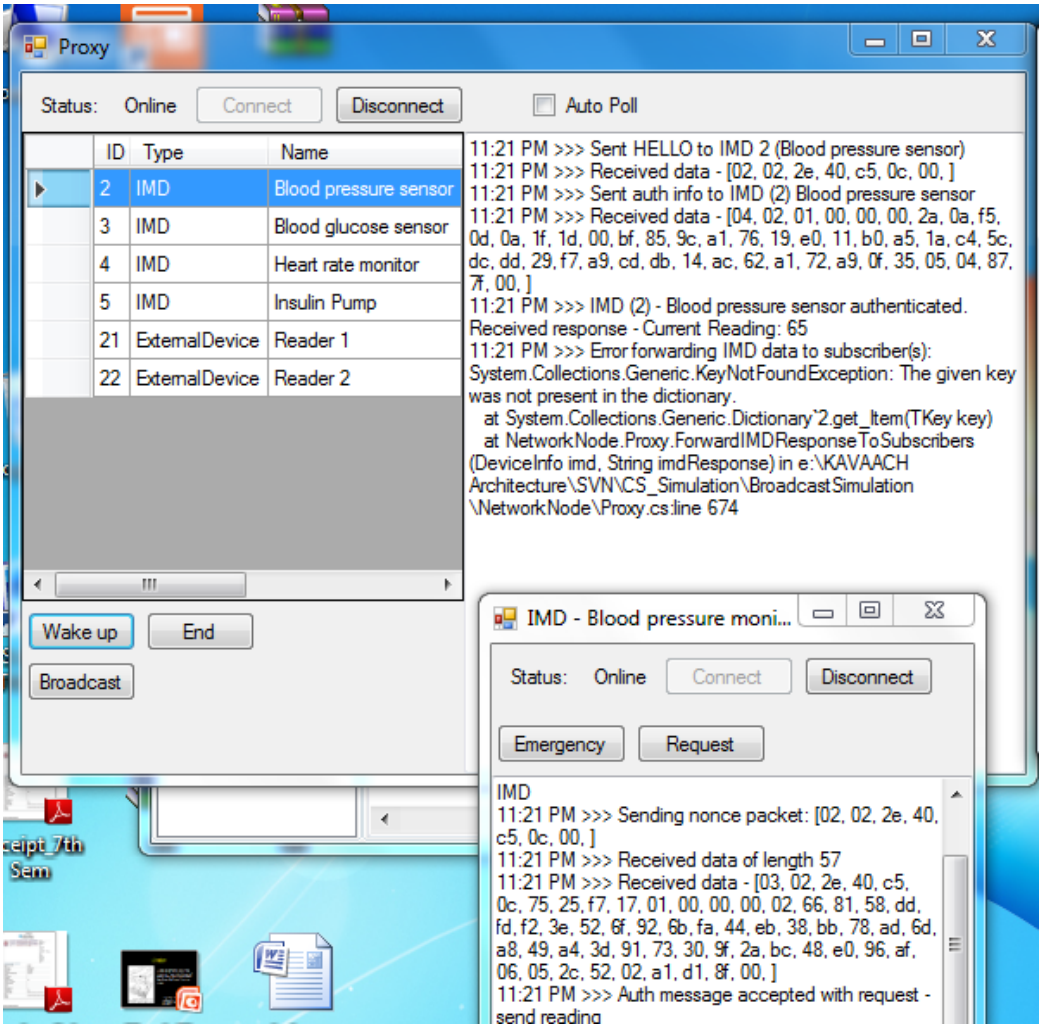

Figure 8.2 Mutual Authentications between IMD and Proxy.

A Registered External device can send a join request to the Proxy following which a mutual authentication protocol is executed by the Proxy and ED. The screenshot of External device sending join request to the proxy is given in Fig. 8.3.

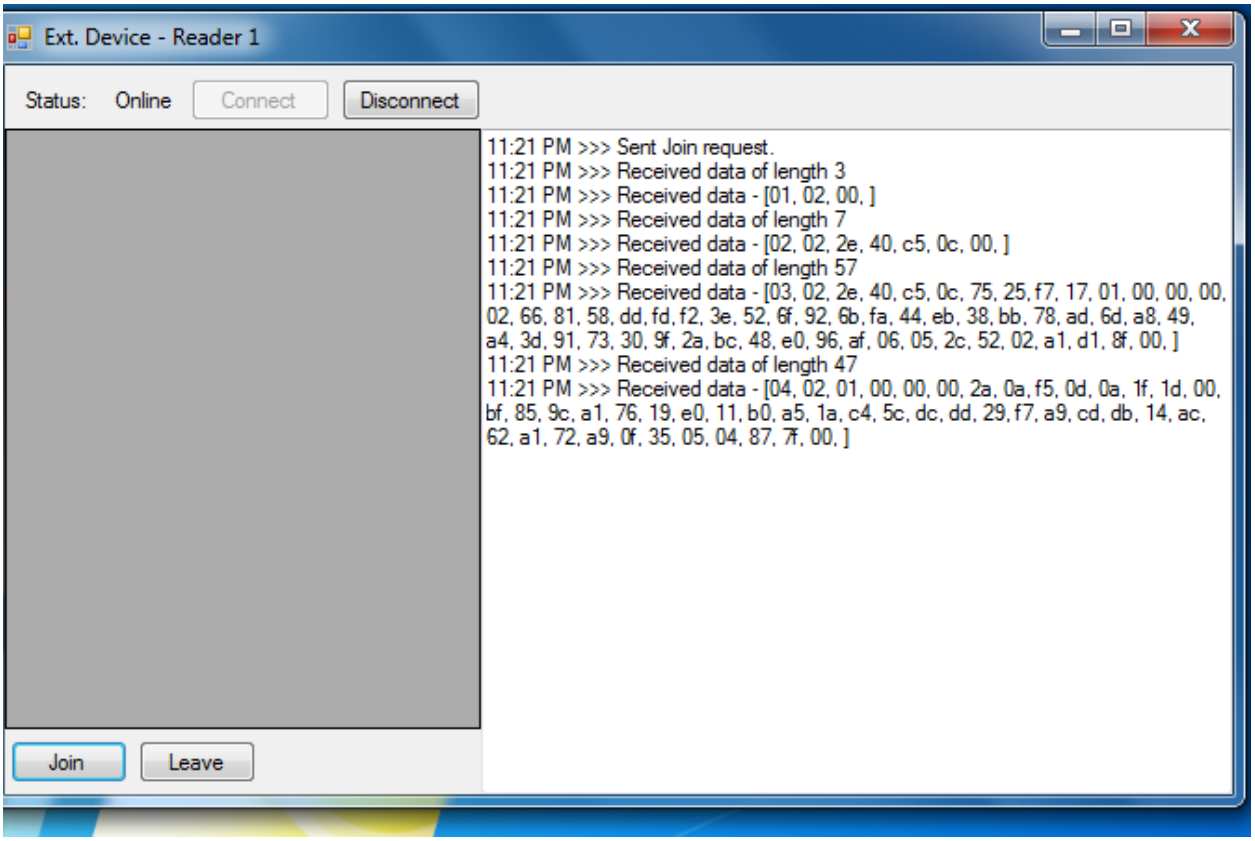

Figure 8.3 External device sending join request to Proxy

One the devices have started and mutual authentication phase is over. IMD and ED can communicate securely via the proxy device. A subscribe message from an external device for which IMD is the publisher is send by the proxy to the corresponding IMD as a request for data, The response obtained from the IMD is transformed into a publish message and a notified to the subscriber device. Similarly, when an external device or IMD publishes data for a topic, the subscriber IMD or external device is notified. The proxy communicates simultaneously with the IMDs and also with the EDs as shown in Fig. 8.4**.**

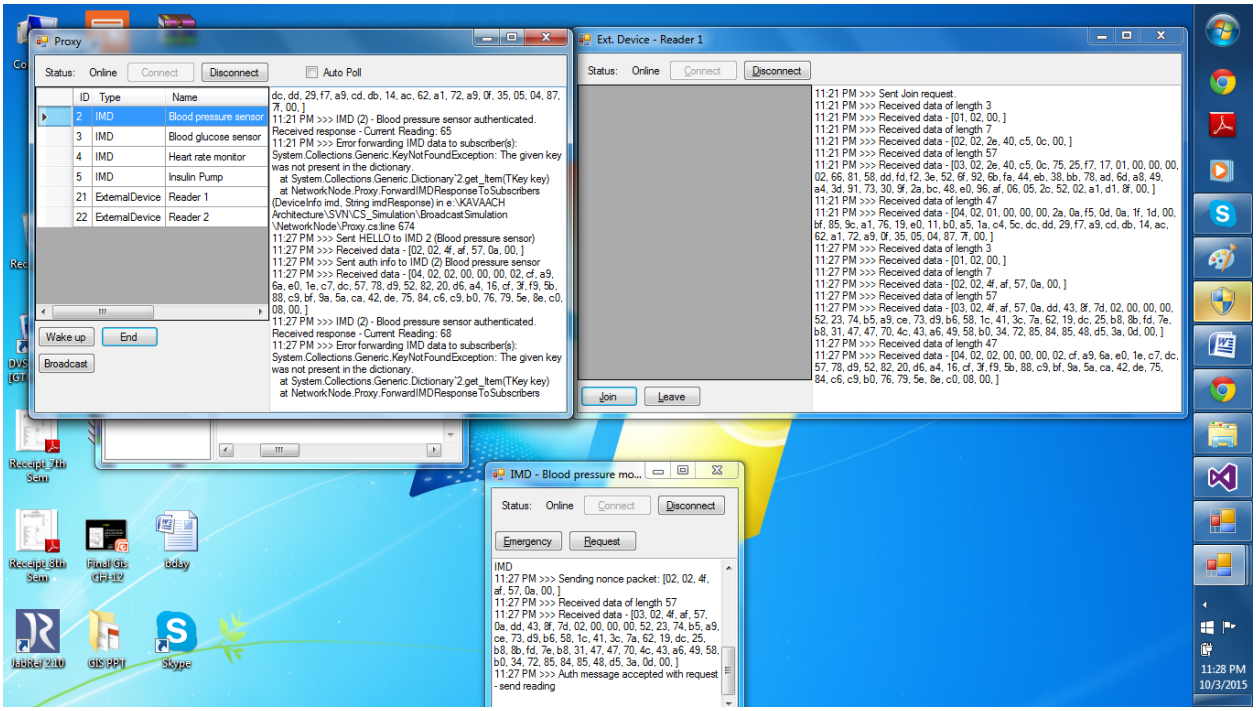

Figure 8.4 Communications between Proxy, IMD and EDs.

The data related to the topics, devices and access control policies is maintained by the proxy device in XML files. Thus all required information is present in the XML files. The Proxy communicated with the IMD using request response protocol in a secure manner. We have implemented the mutual authentication protocol proposed in chapter 7 which also required generation of nonce. For message encryption and decryption AES-GCM is used. We have implemented the formation of IV, and algorithm for incrementing the counter to check for message freshness.

8.1. Security Analysis

In this section we measure the security strength of the proposed model explained in chapter 7 with respect to some well know attacks:

1. **Denial of Service Attack:** The proposed security model has highly resistant to denial of service attack. The use of an additional Proxy device minimizes the load of performing security transformations. Use of symmetric cryptography for mutual authentication, and for data confidentiality between IMD and Proxy reduces energy consumption. Use of authenticated mode of encryption provides data integrity and authentication. The packets are designed in a manner to reduce the transmission overhead.

2. **Man in the Middle Attack (MITM):** The proposed security model uses a mutual authentication protocol which helps to thwart the man in the middle attacks.

3. **Replay Attack:** Involves passive capture of data messages or commands and then their retransmission. As we are making use of counter to detect packet freshness such attack can be detected.

4. **Masquerade Attack:** A rouge device can pretend to be an IMD or a proxy by capturing authentication sequences and replaying. Such attacks can be thwarted by the mutual authentication by making use of nonce.

5. **Message Modification:** Alteration in message can be detected by the recipients due to use of authenticated mode of encryption.

6. **Known-Ciphertext Attack:** In this attack adversary tries to deduce a plaintext or key from a set of known ciphertexts. GCM uses a pseudo random function to generate a unique key before performing encryption therefore adversary cannot deduce any information about the key or plaintext from the ciphertext.

7. **Known-Plaintext Attack:** In this attack adversary has one or more plaintext-ciphertext pairs formed with the secret key from which it tries to deduce the key of the plaintext. The encryption scheme chosen is resilient to such attack. The secret key shared between IMD and Proxy is not known to external device therefore our model is secure.

8.3. Conclusion

Through our prototype implementation we developed a proof of concept which confirms that the proposed two tier based security framework is possible to be implemented with wireless IMDs which are networked in and IWBAN. The security analysis with respect to various attacks shows that our scheme is resilient to security attacks which are most critical for IMDs.

CHAPTER – 9

Conclusion, Major Contributions and Further Work

9.1 Objectives Achieved

This thesis addressed several challenging issues related to secure wireless communication of Implantable Medical Devices (IMDs). Solutions provided make use of an additional proxy device.

The contributions of our work, while trying to achieve the main goal of providing two-tier solution, are the following:

1. Firstly we performed a thorough Literature survey and threat modeling for security issues prevalent in wirelessly communication IMDs.
2. Secondly, we surveyed and analyzed all the available security solutions proposed by researchers.
3. Thirdly, we worked on providing a solution to detect active attacks for IMDs and also worked on providing emergency aware access control.
4. Fourthly, we proposed Buddy system solution for IMDs communicating with external devices.
5. Finally, we proposed a two tier based security model and designed communication protocol for various scenarios. We also implemented the protocol to provide a proof of concept.
6. Our solution based on two-tier model is intended to support heterogeneous co-existing IMDs on a human body and external devices like reader and programmer with widely varying capabilities when it comes to communication and computation

speeds and resource availability. The senders and receivers of data are decoupled. This allows the IMD to go back to sleep state once information has been relayed to proxy which can cache the data and save IMDs battery power.

7. The solution supports adjustments of frequency of probes that are performed on the IMD depending on the battery power, patient health condition etc.
8. The solution proposed is flexible and scalable providing a balance by using light-weight request-response protocols at one end and asynchronous publish-subscribe protocol at the other end.

9.2. Major Contributions

1. We proposed an IWBAN framework for securing wireless access of IMDs by providing end-to-end security at the application layer for intra-body as well as extracorporeal communication.
2. In the proposed security framework, we use an additional hand held proxy device (like PDA) as a mediator between external devices and different types of IMDs. This allows our defence system to offload security related processing and storage from the medical device thus conserving IMDs energy and memory. This offloading helps in reserving medical device resources only for medical functions.
3. In the proposed security framework we use secure and light-weight request-response communication protocol between IMD and proxy to provide mutual authentication, confidentiality, integrity and message freshness, for to and fro communication. These security services are provided by use of symmetric encryption and message authentication technique using 128-bit secret key, random nonces and counters. The secret keys required for symmetric encryption is exchanged between proxy and IMD during registration. For each IMD, a set of requests/response messages are defined and a list of Topics is defined with respect to the requests and responses, role (Publisher/Subscriber) of the IMD for each Topic is defined.
4. In the proposed security framework we use Publish-Subscribe communication protocol between proxy and external devices (readers and programmers) that are registered with the proxy and their public keys are stored for future authentication. A user interface is provided for selecting the available Topics and role

(Publisher/Subscriber) of the external device for each topic which further constitutes the access control list. Once external devices are registered with Proxy, they can securely publish or subscribe to the topics. Such communication provides mutual authentication, confidentiality, integrity, message freshness, and access control.

5. In the proposed security framework we use Proxy Device for secure dissemination of received telemetry data from IMDs to other IMDs or external devices which are registered as subscribers for the topic pertaining to the telemetry data.
6. In the proposed security framework we use Publish-Subscribe paradigm in the Proxy Device for secure collection of Published telemetry data for a specific Topic by IMDs or external devices which are registered as publishers and forward it to the relevant subscribers for that topic.
7. In the proposed security framework we provide a centralized security solution to communication pertaining to heterogeneous IMDs and other external medical devices which may either act as publisher or subscriber for a particular topic.
8. In the proposed security framework we use symmetric encryption techniques to secure communication between IMD and Proxy Device.
9. In the proposed security framework we use both symmetric encryption and asymmetric encryption techniques to secure communication between Proxy Device and other external device.
10. In the proposed security framework we provide a mechanism for peer-to-peer, end-to-end, multicast and broadcast wireless communication in a secure manner.
11. In the proposed security framework we provide a mechanism for asynchronous communication between IMDs and other external devices.
12. In the proposed security framework we provide resilience to Denial of Service attacks by using light-weight authentication and external proxy device.

9.3 Comparison of proposed Security Model with Existing Solutions

Our solution described in chapter 7 can be compared with [153] in which secure architecture is proposed based on publish-subscribe paradigm to guarantee confidentiality and access control.

Table 9.1 Comparison of proposed solution with [153]

Parameters	**[153]**	**Our Approach**
Use of Additional Device	Message Bus	Proxy Device
Communication model	Publish-subscribe	Request-response between IMD and Proxy Publish-subscribe between Proxy and ED
Confidentiality	Ciphertext policy attribute-based encryption (CP-ABE)	AES-GCM for authenticated encryption.
Access Control	Lattice-based access control (LBAC). Access control policies managed by IMD.	Device Role and Topic based. Access Control policies managed by proxy.
Access Control policies	Set on the IMDs therefore cannot be modified later.	Managed by Proxy device, therefore can be managed easily.
Perfect Forward Security (PFS)	No assurance of forward and backward security	Assurance for forward and backward security.
Support for Authentication	No	Yes
Overhead	Use of CP-Abe for encryption of symmetric key. Use of another algorithm for data encryption	IMD require use of AES-GCM encryption.
Usability	Secure Communication amongst IMDs	Secure Communication amongst IMDs and also with external devices.
Replay resilience	Not provided	Provided
DOS resilience	Not provided	Provided
Paradigm	Publish-Subscribe	Request-response and Publish-subscribe

The other available work with which our proposed solution can be compared are the ones which also make use of an external device to provide security. A comparison with such security schemes are given the table 9.2

Table 9.2 Comparison of proposed solution with solutions proposing use of external device

Comparison Parameters	**H2H [81]**	**Cloaker [80]**	**IMD Shield [84]**	**IMD Guard [86]**	**Medmon [45]**	**Our Approach**
Design Approach	Use of PVs	Trusted External Device	Trusted External Device	Trusted External Device (PVs)	Trusted External Device	Trusted External Device
Invasive Approach	Y	Y	N	Y	N	Y
Confidentiality	Y	Y	Y	Y	N	Y
Data Integrity	Y	Y	Y	Y	N	Y
Authentication	Y	Y	Y	Y	Y	Y
Message Freshness	N	N	N	N	N	Y
Replay Resilience	N	N	N	N	N	Y
Access Control	N	N	N	Y	Y	Y
Fail-open system?	N	Y	Y	Y	N	N
Secure IMD-IMD communication?	N	N	N	N	N	Y
Secure IMD-ED communication?	Y	Y	Y	Y	Y	Y

9.4 Possible Further Work

1. More investigation is required regarding the commands the IMD receives from a valid device or from other IMDs.
2. Secure software upgrades for IMDs needs to be analyzed further.
3. More complex access control policies can be derived for our security model.
4. Key exchange techniques between IMDs and external devices have a scope of further analysis. Cross layer security solutions need to be studied.
5. Implementation in simulators and analysis of energy expense and efficiency of the communication protocol for IMDs required to be studied further.
6. The current work on access control can be enhanced by including context awareness in the security model.

References

[1] Schmidt, R., et al., *Body Area Network BAN–a key infrastructure element for patient-centered medical applications.* Biomedizinische Technik/Biomedical Engineering, 2002. **47**(s1a): p. 365-368.

[2] Yazdandoost, K.Y. and R. Kohno, *Body implanted medical device communications.* IEICE transactions on communications, 2009. **92**(2): p. 410-417.

[3] Strydis, C., G. Gaydadjiev, and S. Vassiliadis, *Implantable microelectronic devices: A comprehensive review*. Computer Engineering, Delft University of Technology," CE-TR-2006-01, 2006.

[4] Ellouze, N., et al. *Securing implantable cardiac medical devices: use of radio frequency energy harvesting*. in *Proceedings of the 3rd international workshop on Trustworthy embedded devices*. 2013. ACM.

[5] Pope, A., et al., *Innovation and Invention in Medical Devices:: Workshop Summary*. 2001: National Academies Press.

[6] Maisel, W.H., et al., *Pacemaker and ICD generator malfunctions: analysis of Food and Drug Administration annual reports.* Jama, 2006. **295**(16): p. 1901-1906.

[7] Flick, B.B. and R. Orglmeister, *A portable microsystem-based telemetric pressure and temperature measurement unit.* Biomedical Engineering, IEEE Transactions on, 2000. **47**(1): p. 12-16.

[8] Shults, M.C., et al., *A telemetry-instrumentation system for monitoring multiple subcutaneously implanted glucose sensors.* Biomedical Engineering, IEEE Transactions on, 1994. **41**(10): p. 937-942.

[9] Valdastri, P., et al., *An implantable telemetry platform system for in vivo monitoring of physiological parameters.* Information Technology in Biomedicine, IEEE Transactions on, 2004. **8**(3): p. 271-278.

[10] Min, M., et al., *An implantable analyzer of bio-impedance dynamics: mixed signal approach [telemetric monitors]*. Instrumentation and Measurement, IEEE Transactions on, 2002. **51**(4): p. 674-678.

[11] Smith, B., et al., *An externally powered, multichannel, implantable stimulator-telemeter for control of paralyzed muscle.* Biomedical Engineering, IEEE Transactions on, 1998. **45**(4): p. 463-475.

[12] Sawan, M., et al. *A wireless implantable electrical stimulator based on two FPGAs*. in *Electronics, Circuits, and Systems, 1996. ICECS'96., Proceedings of the Third IEEE International Conference on*. 1996. IEEE.

[13] Schwarz, M., et al., *Single chip CMOS imagers and flexible microelectronic stimulators for a retina implant system.* Sensors and Actuators A: Physical, 2000. **83**(1): p. 40-46.

[14] Halperin, D., et al. *Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses*. in *Security and Privacy, 2008. SP 2008. IEEE Symposium on*. 2008. IEEE.

[15] Bigger Jr, J.T., *Prophylactic use of implanted cardiac defibrillators in patients at high risk for ventricular arrhythmias after coronary-artery bypass graft surgery.* New England Journal of Medicine, 1997. **337**(22): p. 1569-1575.

[16] Halperin, D., et al., *Security and privacy for implantable medical devices.* Pervasive Computing, IEEE, 2008. **7**(1): p. 30-39.

[17] Carrara, S., et al., *Fully integrated biochip platforms for advanced healthcare.* Sensors, 2012. **12**(8): p. 11013-11060.

[18] Commission, F.C., *MICS Medical Implant Communication Services.* FCC 47CFR95: p. 601-95.673.

[19] Astrin, A.W., L. Huan-Bang, and R. Kohno, *Standardization for body area networks.* IEICE transactions on communications, 2009. **92**(2): p. 366-372.

[20] Bradley, P.D., *Implantable ultralow-power radio chip facilitates in-body communications.* RF DESIGN, 2007. **30**(6): p. 20.

[21] Maisel, W.H., *Safety issues involving medical devices: implications of recent implantable cardioverter-defibrillator malfunctions.* JAMA, 2005. **294**(8): p. 955-958.

[22] Holmes, C.F. and B.B. Owens, *Batteries for implantable biomedical applications.* Wiley Encyclopedia of Biomedical Engineering, 2006.

[23] Semiconductor, Z., *ZL70101 medical implantable RF transceiver data sheet*. 2007, May.

[24] Olivo, J., S. Carrara, and G. De Micheli, *Energy harvesting and remote powering for implantable biosensors.* IEEE Sensors Journal, 2011. **11**(EPFL-ARTICLE-152140): p. 1573-1586.

[25] Lee, I., et al., *High-confidence medical device software and systems.* Computer, 2006. **39**(4): p. 33-38.

[26] Fang, Q., et al., *Developing a wireless implantable body sensor network in MICS band.* Information Technology in Biomedicine, IEEE Transactions on, 2011. **15**(4): p. 567-576.

[27] Burleson, W., et al. *Design challenges for secure implantable medical devices*. in *Proceedings of the 49th Annual Design Automation Conference*. 2012. ACM.

[28] Li, C., A. Raghunathan, and N.K. Jha. *Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system*. in *e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on*. 2011. IEEE.

[29] Rasmussen, K.B., et al. *Proximity-based access control for implantable medical devices*. in *Proceedings of the 16th ACM conference on Computer and communications security*. 2009. ACM.

[30] Recommendation, X., *800, Security Architecture for Open Systems Interconnection for CCITT Applications.* International Telecommunication Union (ITU), 1991.

[31] Gerrish, P., et al., *Challenges and constraints in designing implantable medical ICs.* Device and Materials Reliability, IEEE Transactions on, 2005. **5**(3): p. 435-444.

[32] Bruen, A.A., et al., *Applied cryptography: protocols, algorithms, and source code in C.* 1996.

[33] Carollo, K., *Can Your Insulin Pump Be Hacked.* ABC News: Medical Unit, 2012.

[34] Zhan, C., et al., *Cardiac device implantation in the United States from 1997 through 2004: a population-based analysis.* Journal of General Internal Medicine, 2008. **23**(1): p. 13-19.

[35] Myagmar, S., A.J. Lee, and W. Yurcik. *Threat modeling as a basis for security requirements*. in *Symposium on requirements engineering for information security (SREIS)*. 2005.

[36] Steven, J., *Threat Modeling-Perhaps It's Time.* Security & Privacy, IEEE, 2010. **8**(3): p. 83-86.

[37] Malasri, K. and L. Wang, *Securing wireless implantable devices for healthcare: Ideas and challenges.* Communications Magazine, IEEE, 2009. **47**(7): p. 74-80.

[38] Fu, K., *Inside risks Reducing risks of implantable medical devices.* Communications of the ACM, 2009. **52**(6): p. 25-27.

[39] Hansen, J.A. and N.M. Hansen. *A taxonomy of vulnerabilities in implantable medical devices*. in *Proceedings of the second annual workshop on Security and privacy in medical and home-care systems*. 2010. ACM.

[40] Paul, N., T. Kohno, and D.C. Klonoff, *A review of the security of insulin pump infusion systems.* Journal of diabetes science and technology, 2011. **5**(6): p. 1557-1562.

[41] Kermani, M.M., et al., *Emerging Frontiers in Embedded Security*. 2013: p. 203-208.

[42] Fu, K. and J. Blum, *Controlling for cybersecurity risks of medical device software.* Communications of the ACM, 2013. **56**(10): p. 35-37.

[43] Kune, D.F., et al. *Ghost talk: Mitigating EMI signal injection attacks against analog sensors*. in *Security and Privacy (SP), 2013 IEEE Symposium on*. 2013. IEEE.

[44] Fu, K. and J. Blum, *Controlling for Cybersecurity Risks of Medical Device Software.* Biomedical Instrumentation & Technology, 2014. **48**(s1): p. 38-41.

[45] Zhang, M., A. Raghunathan, and N.K. Jha. *Towards trustworthy medical devices and body area networks*. in *Proceedings of the 50th Annual Design Automation Conference*. 2013. ACM.

[46] Clark, S.S. and K. Fu, *Recent results in computer security for medical devices*, in *Wireless Mobile Communication and Healthcare*. 2012, Springer. p. 111-118.

[47] Rushanan, M., et al. *SoK: Security and privacy in implantable medical devices and body area networks*. in *Security and Privacy (SP), 2014 IEEE Symposium on*. 2014. IEEE.

[48] Hei, X., et al. *Defending resource depletion attacks on implantable medical devices*. in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*. 2010. IEEE.

[49] Food, U. and D. Administration, *Content of premarket submissions for management of cybersecurity in medical devices: draft guidance for industry and food and drug administration staff*. 2013.

[50] Shen, W., et al. *Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time*. in *Security and Privacy (SP), 2013 IEEE Symposium on*. 2013. IEEE.

[51] 51. Halevi, T. and N. Saxena. *On pairing constrained wireless devices based on secrecy of auxiliary channels: The case of acoustic eavesdropping*. in *Proceedings*

of the 17th ACM conference on Computer and communications security. 2010. ACM.

[52] Radcliffe, J. *Hacking medical devices for fun and insulin: Breaking the human SCADA system*. in *Black Hat Conference presentation slides*. 2011.

[53] Rostami, M., et al. *Balancing security and utility in medical devices?* in *Proceedings of the 50th Annual Design Automation Conference*. 2013. ACM.

[54] Pournaghshband, V., M. Sarrafzadeh, and P. Reiher, *Securing legacy mobile medical devices*, in *Wireless Mobile Communication and Healthcare*. 2013, Springer. p. 163-172.

[55] Shostack, A. *Experiences threat modeling at microsoft*. in *Modeling Security Workshop. Dept. of Computing, Lancaster University, UK*. 2008.

[56] Israel, C.W. and S.S. Barold, *Pacemaker systems as implantable cardiac rhythm monitors.* The American journal of cardiology, 2001. **88**(4): p. 442-445.

[57] Jebali, N., S. Beldi, and A. Gharsallah, *An RFID Antenna Implanted In The Human Arm For Medical Applications.* Skin, 2015. **41**: p. 0.874705.

[58] Kim, B., J. Yu, and H. Kim. *In-vivo NFC: remote monitoring of implanted medical devices with improved privacy*. in *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems*. 2012. ACM.

[59] Freudenthal, E., et al. *Suitability of nfc for medical device communication and power delivery*. in *Engineering in Medicine and Biology Workshop, 2007 IEEE Dallas*. 2007. IEEE.

[60] Varshney, L.R., P. Grover, and A. Sahai. *Securing inductively-coupled communication*. in *Information Theory and Applications Workshop (ITA), 2012*. 2012. IEEE.

[61] Hancke, G. *Eavesdropping attacks on high-frequency RFID tokens*. in *4th Workshop on RFID Security (RFIDSec)*. 2008.

[62] Haselsteiner, E. and K. Breitfuß. *Security in near field communication (NFC)*. in *Workshop on RFID Security RFIDSec*. 2006.

[63] Cremers, C., et al. *Distance hijacking attacks on distance bounding protocols*. in *Security and Privacy (SP), 2012 IEEE Symposium on*. 2012. IEEE.

[64] Choi, S., et al. *Secure and resilient proximity-based access control*. in *Proceedings of the 2013 international workshop on Data management & analytics for healthcare*. 2013. ACM.

[65] Hosseini-Khayat, S. *A lightweight security protocol for ultra-low power ASIC implementation for wireless implantable medical devices*. in *Medical Information & Communication Technology (ISMICT), 2011 5th International Symposium on*. 2011. IEEE.

[66] Fan, X., et al. *FPGA implementations of the Hummingbird cryptographic algorithm*. in *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on*. 2010. IEEE.

[67] Fan, X., et al. *Lightweight implementation of Hummingbird cryptographic algorithm on 4-bit microcontrollers*. in *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*. 2009. IEEE.

[68] Beck, C., et al. *Block cipher based security for severely resource-constrained implantable medical devices*. in *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies*. 2011. ACM.

[69] Strydis, C., D. Zhu, and G.N. Gaydadjiev. *Profiling of symmetric-encryption algorithms for a novel biomedical-implant architecture*. in *Proceedings of the 5th conference on Computing frontiers*. 2008. ACM.

[70] Ohta, H. and M. Matsui, *A description of the misty1 encryption algorithm.* RFC2994, November, 2000.

[71] Malasri, K. and L. Wang, *Design and implementation of a securewireless mote-based medical sensor network.* Sensors, 2009. **9**(8): p. 6273-6297.

[72] Bergamasco, S., M. Bon, and P. Inchingolo. *Medical data protection with a new generation of hardware authentication tokens*. in *Mediterranean Conference on Medical and Biological Engineering and Computing*. 2001. Citeseer.

[73] Schechter, S., *Security that is Meant to be Skin Deep Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices.* 2010.

[74] Poon, C.C., Y.-T. Zhang, and S.-D. Bao, *A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health.* Communications Magazine, IEEE, 2006. **44**(4): p. 73-81.

[75] Cherukuri, S., K.K. Venkatasubramanian, and S.K. Gupta. *BioSec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body*. in *Parallel Processing Workshops, 2003. Proceedings. 2003 International Conference on*. 2003. IEEE.

[76] Hu, C., et al. *OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks*. in *INFOCOM, 2013 Proceedings IEEE*. 2013. IEEE.

[77] Hei, X. and X. Du. *Biometric-based two-level secure access control for implantable medical devices during emergencies*. in *INFOCOM, 2011 Proceedings IEEE*. 2011. IEEE.

[78] Narasimhan, S., X. Wang, and S. Bhunia. *Implantable electronics: emerging design issues and an ultra light-weight security solution*. in *Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE*. 2010. IEEE.

[79] Tsouri, G.R. *Securing wireless communication with implanted medical devices using reciprocal carrier-phase quantization*. in *World of Wireless, Mobile and Multimedia Networks & Workshops, 2009. WoWMoM 2009. IEEE International Symposium on a*. 2009. IEEE.

[80] Denning, T., K. Fu, and T. Kohno. *Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security*. in *HotSec*. 2008.

[81] Rostami, M., A. Juels, and F. Koushanfar. *Heart-to-heart (H2H): authentication for implanted medical devices*. in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. 2013. ACM.

[82] Strydis, C., et al., *A system architecture, processor, and communication protocol for secure implants.* ACM Transactions on Architecture and Code Optimization (TACO), 2013. **10**(4): p. 57.

[83] Hu, F., et al., *Trustworthy data collection from implantable medical devices via high-speed security implementation based on IEEE 1363.* Information Technology in Biomedicine, IEEE Transactions on, 2010. **14**(6): p. 1397-1404.

[84] Gollakota, S., et al., *They can hear your heartbeats: non-invasive security for implantable medical devices.* ACM SIGCOMM Computer Communication Review, 2011. **41**(4): p. 2-13.

[85] Zheng, G., et al. *A Non-key based security scheme supporting emergency treatment of wireless implants*. in *Communications (ICC), 2014 IEEE International Conference on*. 2014. IEEE.

[86] Xu, F., et al. *IMDGuard: Securing implantable medical devices with the external wearable guardian*. in *INFOCOM, 2011 Proceedings IEEE*. 2011. IEEE.

[87] Hei, X., et al. *PIPAC: patient infusion pattern based access control scheme for wireless insulin pump system*. in *INFOCOM, 2013 Proceedings IEEE*. 2013. IEEE.

[88] Panescu, D., *Emerging Technologies [wireless communication systems for implantable medical devices]*. Engineering in Medicine and Biology Magazine, IEEE, 2008. **27**(2): p. 96-101.

[89] Fu, K., *Inside risksReducing risks of implantable medical devices.* Communications of the ACM, 2009. **52**(6): p. 25.

[90] St Denis, T., *Cryptography for developers*. 2006: Syngress.

[91] Bogdanov, A., et al., *PRESENT: An ultra-lightweight block cipher*. 2007: Springer.

[92] Bellare, M., P. Rogaway, and D. Wagner, *A conventional authenticated-encryption mode.* manuscript, April, 2003.

[93] Rogaway, P., M. Bellare, and J. Black, *OCB: A block-cipher mode of operation for efficient authenticated encryption.* ACM Transactions on Information and System Security (TISSEC), 2003. **6**(3): p. 365-403.

[94] Dworkin, M., *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004.* NIST Special Publication.

[95] Dworkin, M. *Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) for confidentiality and authentication*. in *Federal Information Processing Standard Publication FIPS*. 2006. Citeseer.

[96] Dworkin, M., *NIST Special Publication 800-38A," Recommendation for Block Cipher Modes of Operation: Methods and Techniques", 2001*.

[97] Martinovic, I., P. Pichota, and J.B. Schmitt. *Jamming for good: a fresh approach to authentic communication in WSNs*. in *Proceedings of the second ACM conference on Wireless network security*. 2009. ACM.

[98] Gupta, S.K., T. Mukherjee, and K. Venkatasubramanian. *Criticality aware access control model for pervasive applications*. in *Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications (PERCOM '06).* 2006. IEEE.

[99] Sandhu, R.S. and P. Samarati, *Access control: principle and practice.* Communications Magazine, IEEE, 1994. **32**(9): p. 40-48.

[100] Hu, J. and A.C. Weaver. *A dynamic, context-aware security infrastructure for distributed healthcare applications*. in *Proceedings of the first workshop on pervasive privacy security, privacy, and trust*. 2004. Citeseer.

[101] 101. Al-Muhtadi, J., et al. *Cerberus: a context-aware security scheme for smart spaces*. in *Pervasive Computing and Communications, 2003.(PerCom 2003). Proceedings of the First IEEE International Conference on*. 2003. IEEE.

[102] Sandhu, R.S., et al., *Role-based access control models.* Computer, 1996(2): p. 38-47.

[103] Alcaraz Calero, J.M., G. Martinez Perez, and A.F. Gomez Skarmeta, *Towards an authorisation model for distributed systems based on the Semantic Web.* Information Security, IET, 2010. **4**(4): p. 411-421.

[104] Ni, Q., et al., *Privacy-aware role-based access control.* ACM Transactions on Information and System Security (TISSEC), 2010. **13**(3): p. 24.

[105] Covington, M.J., et al. *Securing context-aware applications using environment roles*. in *Proceedings of the sixth ACM symposium on Access control models and technologies*. 2001. ACM.

[106] Xiong, J. and K. Jamieson. *SecureAngle: improving wireless security using angle-of-arrival information*. in *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*. 2010. ACM.

[107] Garcia-Morchon, O., et al., *Security Considerations in the IP-based Internet of Things.* 2013.

[108] Liu, H., et al., *Survey of wireless indoor positioning techniques and systems.* Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, 2007. **37**(6): p. 1067-1080.

[109] Lieckfeldt, D., *Efficient Localization of Users and Devices in Smart Environments*. 2010, Dissertation, University of Rostock.

[110] Luo, X., et al. *Encryption algorithms comparisons for wireless networked sensors*. in *Systems, Man and Cybernetics, 2004 IEEE International Conference on*. 2004. IEEE.

[111] Chang, C.-C., S. Muftic, and D.J. Nagel. *Measurement of energy costs of security in wireless sensor nodes*. in *Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference on*. 2007. IEEE.

[112] Venugopalan, R., et al. *Encryption overhead in embedded systems and sensor network nodes: Modeling and analysis*. in *Proceedings of the 2003 international conference on Compilers, architecture and synthesis for embedded systems*. 2003. ACM.

[113] Großschädl, J., et al. *Energy evaluation of software implementations of block ciphers under memory constraints*. in *Proceedings of the conference on Design, automation and test in Europe*. 2007. EDA Consortium.

[114] Law, Y.W., J. Doumen, and P. Hartel, *Survey and benchmark of block ciphers for wireless sensor networks.* ACM Transactions on Sensor Networks (TOSN), 2006. **2**(1): p. 65-93.

[115] Needham, R.M. and D.J. Wheeler, *Correction to xtea*. 1998.

[116] Bellare, M., P. Rogaway, and D. Wagner, *A conventional authenticated-encryption mode.* manuscript, April, 2003.

[117] Rogaway, P., M. Bellare, and J. Black, *OCB: A block-cipher mode of operation for efficient authenticated encryption.* ACM Transactions on Information and System Security (TISSEC), 2003. **6**(3): p. 365-403.

[118] Dworkin, M.J., *Sp 800-38c. recommendation for block cipher modes of operation: the ccm mode for authentication and confidentiality*. 2004.

[119] McGrew, D.A. and J. Viega, *The security and performance of the Galois/Counter Mode (GCM) of operation (full version).* URL: http://csrc. nist. gov/CryptoToolkit/modes/proposedmodes/gcmgcm-ad. pdf, 2008.

[120] McGrew, D. and J. Viega, *The Galois/counter mode of operation (GCM).* Submission to NIST. http://csrc. nist. gov/CryptoToolkit/modes/proposedmodes/gcm/gcm-spec. pdf, 2004.

[121] Kohno, T., J. Viega, and D. Whiting, *The CWC-AES dual-use mode.* Submission to NIST Modes of Operation Process, 2003.

[122] Darji, M. and B.H. Trivedi, *Detection of active attacks on wireless IMDs using proxy device and localization information*, in *Security in Computing and Communications*. 2014, Springer. p. 353-362.

[123] Darji, M. and B. Trivedi, *Imd-ids a specification based intrusion detection system for wireless imds.* International Journal of Applied Information Systems, 2013. **5**(6): p. 19-23.

[124] Darji, M. and B.H. Trivedi, *Emergency Aware, Non-invasive, Personalized Access Control Framework for IMDs*, in *Recent Trends in Computer Networks and Distributed Systems Security*. 2014, Springer. p. 370-381.

[125] Eugster, P.T., et al., *The many faces of publish/subscribe*. ACM Computing Surveys (CSUR), 2003. **35**(2): p. 114-131.

[126] 126. Costa, P., G.P. Picco, and S. Rossetto. *Publish-subscribe on sensor networks: A semi-probabilistic approach*. in *Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on*. 2005. IEEE.

[127] Dworkin, M., *Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC*. 2007.

[128] 3-WAY, BLOWFISH, DES, GOST, IDEA, RC5 source code. www.cis.udel.edu/~mills/database/schneier/.

[129] SKIPJACK, LOKI91 source code. www.mirrors.wiretapped.net/security/

[130] Jariwala, Vivaksha, and D. C. Jinwala., *Evaluating Galois Counter mode in link layer security architecture for wireless sensor networks.* In *International Journal of Network Security & Its Applications* 2.4 (2010): 55-65.

[131] Jinwala, Devesh, Dhiren Patel, and Kankar Dasgupta., *FlexiSec: a configurable link layer security architecture for wireless sensor networks*, *arXiv preprint arXiv:1203.4697* (2012).

[132] Joan Daemen, Vincent Rijmen. *The Design of Rijndael AES - The Advanced Encryption Standard.* In *Springer Series on Information Security and Cryptography*, Springer-Verlag, 2002.

[133] Luk, Mark, et al. MiniSec: a secure sensor network communication architecture. In p*roceedings of the 6th international conference on Information processing in sensor networks*. ACM, 2007.

[134] IPSec: Requests For Comments. RFC 2401, RFC 2402, RFC 2406, RFC 2408. [Online]. Available:http://www.ietf.org/rfc/rfc240n.txt.

[135] Transport Layer Security. Requests For Comments:RFC 4346. [Online]. Available http://tools.ietf.org/html/rfc5246

[136] D. Wagner and B. Schneier. Analysis of the SSL 3.0 protocol. In *proceedings of the 2nd USENIX Workshop on Electronic Commerce (EC-96)*, pp. 29-40, USENIX Association, Berkeley, 1996.

[137] Kwak, Kyung Sup, Sana Ullah, and Niamat Ullah. An overview of IEEE 802.15. 6 standard. In *3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on*. IEEE, 2010.

[138] Moteiv Telos Motes. [Online]. Available :http://www.moteiv.com.

[139] T. Wollinger, M. Wang, J. Guajardo, and C. Paar. How well are high-end DSPs suited for the AES algorithms? In *proceedings of 3rd AES conference*, New York, pp. 94-105, 2000

[140] Devesh Jinwala, Dhiren Patel, K S Dasgupta. *Optimizing the Replay Protection at the Link Layer Security Framework in Wireless Sensor Networks. In* IAENG International Journal of Computer Science,International Association of Engineers Publication,Hong Kong. 2009

[141] David A. McGrew and John Viega. The Security and Performance of the Galois/Counter Mode (GCM) of Operation. In *proceedings of the INDOCRYPT*, LNCS Book Series, Vol. 9743, pp. 343- 355, Springer-Verlag, 2004.

[142] B. Bloom. "Space/time trade-offs in hash coding with allowable errors." *Communications of the ACM*, 13(7),pp. 422-426, July 1970.

[143] Paul Syverson. A Taxonomy of Replay Attacks. In *CSFW'94: Proceedings of the Seventh Computer Security Foundations Workshop*, pp. 187-191, IEEE Computer Society Press, 1994.

[144] T. Aura. Strategies against replay attacks. In *Proceedings of the 10th IEEE Computer SocietyFoundations Workshop*, pp. 59–68, IEEE Computer Society Press, MA, June 1997.

[145] Cryptographic Random Numbers Standard P1363: Appendix E, November, 1995

[146] Dworkin, Morris. Recommendation for block cipher modes of operation: methods and techniques. No. NIST-SP-800-38A. NATIONAL INST OF STANDARDS AND TECHNOLOGY GAITHERSBURG MD COMPUTER SECURITY DIV, 2001.

[147] International Organization for Standardization. ISO/IEC 9798-2: Information Technology - Security techniques — Entity Authentication Mechanisms Part 2: Entity authentication using symmetric techniques. ISO/IEC, 1993

[148] Hankerson, Darrel, Alfred J. Menezes, and Scott Vanstone. *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[149] Lauter, Kristin. The advantages of elliptic curve cryptography for wireless security. In *IEEE Wireless communications*, 2004

[150] Eugster, P. T., Felber, P. A., Guerraoui, R., & Kermarrec. The many faces of publish/subscribe. *ACM Computing Surveys (CSUR)*,2005.

[151] Pallickara, S., Pierce, M., Gadgil, H., Fox, G., Yan, Y., & Huang, Y. A framework for secure end-to-end delivery of messages in publish/subscribe systems.

In *Proceedings of the 7th IEEE/ACM International Conference on Grid Computing* (pp. 215-222). IEEE Computer Society, 2006.

[152] Johnson, D., Menezes, A., & Vanstone. The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security,1*(1), 36-63, 2001.

[153] Picazo-Sanchez, P., Tapiador, J. E., Peris-Lopez, P., & Suarez-Tangil. Secure publish-subscribe protocols for heterogeneous medical wireless body area networks. *Sensors*, 2014

[154] Kaliski, B., & Staddon. *PKCS# 1: RSA cryptography specifications version 2.0.* RFC 2437, October 1998.

List of Publications

Patent Filed:

1. **An Improved System for Securing Implantable Medical Devices. Application Number: 92/MUM/2015**

Paper Presented or Published:

1 Darji, M. and B. Trivedi, *Secure leader election algorithm optimized for power saving using mobile agents for intrusion detection in MANET*, in *Recent Trends in Computer Networks and Distributed Systems Security*. 2012, Springer. p. 54-63.

2 Darji, M. and B. Trivedi, *Survey of intrusion detection and prevention system in MANETs based on data gathering techniques.* IJAIS, 2012. **1**: p. 38-43.

3 Darji, M. and B.H. Trivedi, *Detection of active attacks on wireless IMDs using proxy device and localization information*, in *Security in Computing and Communications*. 2014, Springer. p. 353-362.

4 Darji, M. and B. Trivedi, *Imd-ids a specification based intrusion detection system for wireless imds.* International Journal of Applied Information Systems, 2013. **5**(6): p. 19-23.

5 Darji, M. and B.H. Trivedi, *Emergency Aware, Non-invasive, Personalized Access Control Framework for IMDs*, in *Recent Trends in Computer Networks and Distributed Systems Security*. 2014, Springer. p. 370-381.