

Doctoral theses at NTNU, 2020:136

Muhammad Faheem Awan

Physical Layer Security for In-Body Wireless Cardiac Sensor Network

ISBN 978-82-326-4620-3 (printed version)
ISBN 978-82-326-4621-0 (electronic version)
ISSN 1503-8181

Doctoral theses at NTNU, 2020:136

NTNU
Norwegian University of
Science and Technology
Faculty of Information Technology
and Electrical Engineering
Department of Electronic Systems



Muhammad Faheem Awan

Physical Layer Security for In-Body Wireless Cardiac Sensor Network

Thesis for the degree of Philosophiae Doctor

Trondheim, May 2020

Norwegian University of Science and Technology
Faculty of Information Technology
and Electrical Engineering
Department of Electronic Systems



Norwegian University of
Science and Technology

NTNU

Norwegian University of Science and Technology

Thesis for the degree of Philosophiae Doctor

Faculty of Information Technology
and Electrical Engineering
Department of Electronic Systems

© Muhammad Faheem Awan

ISBN 978-82-326-4620-3 (printed version)

ISBN 978-82-326-4621-0 (electronic version)

ISSN 1503-8181

Doctoral theses at NTNU, 2020:136



Printed by Skipnes Kommunikasjon as

Abstract

The thesis explores the physical layer security approaches for securing an in-body multi-nodal leadless cardiac pacemaker (LCP) communication system. Pacemakers are implanted medical devices, used to treat different types of cardiac arrhythmias. The widely used version of these pacemakers is implanted with intravascular leads. Due to lead related complications, the next generation of pacemaker systems are becoming wireless i.e., connecting multiple nodes wirelessly without intravascular leads.

Besides the unquestionable benefits of LCPs such as less invasive surgery, there are also some concerns associated with it. The wireless nature of these devices is a significant security risk and could lead to threats like eavesdropping, data tampering, and device modification.

This thesis deals with the problem of quantifying the severity of risks associated with the wireless nature of these next generation LCPs and the corresponding countermeasures by utilizing the physical layer security (PLS) techniques.

To evaluate the system eavesdropping risk without PLS, we use the concept of communication link outage probability. A link is said to be in an outage if the received signal to noise (SNR) ratio falls below the threshold required for error free decoding. We compute the eavesdropper (Eve) link outage probability for evaluation of eavesdropping risk with respect to the distance around the body. Similarly, for developing the corresponding countermeasures, we explore two different approaches of PLS for securing LCP. The first approach provides a secure communication strategy via channel modeling and offers data secrecy and reliability simultaneously, without use of data encryption. The second approach provides an alternative for symmetric key generation between legitimate nodes and avoids the use of key management and distribution servers as in the case of conventional cryptographic methods.

For channel modeling strategy, our hypothesis is on the availability of positive

secrecy capacity in the close proximity of the human body. Secrecy capacity is the performance metric that supports secrecy and reliability at the same time and is the maximum attainable secure communication rate without leakage of information to Eve. Secrecy capacity depends on the inherent noise within the wireless channels. To implement a channel modeling approach, prior knowledge about wireless channels is required and can only be implemented when the legitimate nodes have superior channel quality over Eve on the physical layer.

To evaluate the secrecy capacity, the methodology of electromagnetic simulations and experimental measurements is adopted for modeling the in-body to in-body (legitimate) and in-body to off-body (Eve) wireless channels. The results show that the positive secrecy capacity is achievable within the human personal space of 25 cm, with practical antenna realizations. Furthermore, to examine the effect of electromagnetic radiations through the human body across different angles in three dimensional space, the spatial secrecy capacity is also evaluated. The angle from which the maximum leakage of information takes place is found to the left from front, just above the heart and is termed as the “Eve sweet spot angle”. Eve’s sweet spot angle has the least secrecy capacity among all the eavesdropper spatial positions with the human heart as a reference position. The results proved our hypothesis that the human body as a lossy medium for electromagnetic propagation inherently provides high attenuation to off-body Eve link, thus offering legitimate nodes an advantage on the physical layer for implementation of channel modeling approach.

For solving the issues related to key management and distribution in case of traditional cryptographic algorithms, the dissertation also explores the source modeling approach to establish symmetric keys between legitimate nodes. The source modeling approach exploit the correlated information source between legitimate nodes for key generation. We hypothesized that the electromagnetic reflections experienced due to in-body transmissions provide enough randomness to generate a symmetric key from wireless parameters like received signal strength (RSS), phase, angle of arrival, etc. Therefore, we generated a symmetric key string between the in-body nodes by utilizing the randomness in the RSS measurements. Similarly, due to the availability of inherent physiological signals, the feasibility of symmetric group key establishment across multiple nodes of the leadless pacemaker system is also analyzed. Both methods provide viable alternatives with RSS based key generation method outperforming the other with a bit mismatch rate of approximately 1%.

Preface

The thesis is submitted to the Norwegian University of Science and Technology (NTNU) for the partial fulfillment of the requirements for the degree of Doctor of Philosophy.

The most of the doctoral work has been performed at the Department of Electronic Systems, NTNU, Trondheim, Norway. The work has been conducted under the supervision of Professor Kimmo Kansanen from September 2016 to November 2019.

Professor Narcís Cardona supervised me during my secondment at Universitat Politècnica de València, Spain from February 2018 to April 2018. Dr. Delphine Feuerstein supervised me from June 2018 to August 2018 during my work at Microport CRM, Pvt Limited, Paris, France. I was under the supervision of Professor Ilanko Balasingham from May 2019 to August 2019 during my secondment at Oslo University Hospital, Oslo, Norway. He is also a co-supervisor for my doctoral degree.

The work leading to these results has received funding from the EU Horizon 2020 (Marie Curie Actions - H2020), Project WiBEC (Wireless in Body Environment) under grant agreement no 675353.

Acknowledgments

I'd like to thank number of people for their continuous support who made this experience of work and life fascinating. Firstly, I express gratitude to my supervisor, Professor Kimmo Kansanen. He has been a constant source of encouragement and guiding light throughout my Ph.D. He not only shares his ideas and knowledge about the research but also provides valuable feedback and comments on other matters. I'd like to thank him for investing enormous time in my research activities and being a motivator in tough times, I am privileged to work with him.

Besides my supervisor, I would like to extend my wholehearted thanks to the rest of my dissertation committee members (Professor Pierluigi Salvo Rossi, Associate Professor Lorenzo Mucchi, Chief Scientist Habtamu Abie and Associate Professor Milica Orlandic) for their timely reviews and crucial remarks that shaped my final dissertation.

I enjoyed working at the Department of Electronic Systems at the Norwegian University of Science and Technology (NTNU). I made number of friends at the department who made my stay joyous. Moreover, I'd also like to thank the administration staff at the department, for their support and making administrative things easier and smooth from the beginning.

The research was conducted in Marie Curie Initial Training Network (ITN), in Wireless in-body Environment (WiBEC). I am honored to be a part of WiBEC network. I express my sincere gratitude to the entire WiBEC family who provided countless memories.

I am also grateful to my collaborators from academia and industry. More, specifically Sofia Perez Simbor, Concepcion Garcia-Pardo, and Prof. Narcís Cardona from Universitat Politècnica de València, Spain. Pritam Bose, Ali Khaleghi and Prof. Il-angko Balasingham from Oslo University Hospital, Oslo, Norway. Xiao Fang, Mehrab Ramzan, Niels Neumann, and Prof. Dirk Plettmeier from Technische Universität Dresden, Germany and finally Rafael Cordero Álvarez and Dr. Del-

phine Feuerstein from Microport CRM, Pvt Limited, Paris, France.

I owe many thanks to Muhammad Faisal Aftab and Sarmad Munir, for assisting me to settle in Trondheim. It would have been much harder without their support and kindness.

I want to thank all my friends for giving me the priceless company all these years and always willing to lend a helping hand.

Lastly, I owe my deepest gratitude to my family back home for their prayers and my wife Ayesha, and my son Zakariya for their patience and understanding of my busy schedule.

Muhammad Faheem Awan
Trondheim, May 2020

Contents

Abstract	iii
Preface	v
Acknowledgments	vii
List of Figures	xvii
List of Abbreviations	xvii
1 Introduction	1
1.1 Research Objective and Questions	3
1.1.1 Research Methods	3
1.2 Thesis Contributions	4
1.2.1 List of Publications	5
1.2.2 Papers Not Included in the Thesis	7
1.2.3 Project Deliverables	9
1.3 Thesis Organization	9

I	Background and Summary of Articles	11
2	Background	13
2.1	Wireless Body Area Network	13
2.2	Cardiac Pacemakers	15
2.2.1	Traditional Cardiac Pacemakers	15
2.2.2	Leadless Cardiac Pacemakers	17
2.2.3	Multinodal Leadless Cardiac Pacemakers	17
2.3	Information Security	18
2.3.1	Information Security and WBAN	19
2.3.2	Physical Layer Security	20
2.4	Research Methods and Approaches	21
2.4.1	Computational Modeling	23
2.4.2	Phantom Experiments	23
2.4.3	In-vivo Experiments	24
3	Eavesdropping Risk	25
3.1	Introduction	25
3.2	Background	25
3.3	Eavesdropping Risk	26
3.4	Limitations	28
3.5	Summary	28
4	Physical Layer Security — Channel Modeling Approach	31
4.1	Introduction	31
4.2	Background	31
4.3	Wiretap Channel	32
4.3.1	Secrecy Capacity	33

4.4	Evaluation of Secrecy Capacity for Leadless Cardiac Pacemakers	35
4.4.1	One-dimensional Secrecy Capacity	35
4.4.2	Spatial Secrecy Capacity	38
4.5	Summary	41
5	Physical Layer Security — Source Modeling Approach	43
5.1	Introduction	43
5.2	RSS-Based Key Generation	44
5.2.1	Limitations	46
5.3	Physiological Signals Based Key Generation	46
5.3.1	Limitations	48
5.4	Summary	50
6	Conclusions and Open Problems	51
	Bibliography	55
II	Articles	69
	Appendices	71
A	Estimating Eavesdropping Risk	71
	Paper A: Estimating Eavesdropping Risk for Next Generation Implants	71
B	Evaluation of Secrecy Capacity with Phantom Experiments in ISM 2.4 GHz	85
	Paper B: Experimental Phantom-based Evaluation of Physical Layer Security for Future Leadless Cardiac Pacemaker	85
C	Distance Based One-dimensional Evaluation of Secrecy Capacity	95

Paper C: Experimental Phantom-Based Security Analysis for Next-Generation Leadless Cardiac Pacemakers	95
D Simulation Based Secrecy Capacity for MICS, WMTS and ISM 868 MHz	121
Paper D: Evaluating Secrecy Capacity for In-body Wireless Channels	121
E Information Theoretic Analysis for IMDs	139
Paper E: Information Theoretic Analysis for Securing Next Generation Leadless Cardiac Pacemaker	139
F Evaluation of Spatial Secrecy Capacity	153
Paper F: Evaluation of Secrecy Capacity for Next-Generation Leadless Cardiac Pacemaker	153
G RSS-Based Secret Key Generation	167
Paper G: RSS-Based Secret Key Generation in Wireless In-body Networks	167
H Physiological Signals Based Secret Key Generation	175
Paper H: Securing Next Generation Multinodal Leadless Cardiac Pacemaker System: A Proof of Concept in a Single Animal	175

List of Figures

1.1	Link between research questions and publications	6
1.2	Overview of activities carried out by the author during Ph.D.	8
2.1	Wireless Body Area Network	14
2.2	Comparison between traditional (a) and a variant (b) of the next-generation CRT systems. IC-Subc. comm refers to intracardiac to subcutaneous communication and IC-IC. refers to intracardiac to intracardiac communication.	16
2.3	Information security paradigms	19
2.4	Multinodal leadless cardiac pacemaker system with an external eavesdropper	22
2.5	A sample computational model	23
2.6	Measurement setup for phantom experiments	24
3.1	A simple communication system with an Eve. P_e^R and P_e^E is the probability of error at legitimate receiver and Eve respectively.	26
3.2	Probability of bit error (P_e) vs SNR (legitimate receiver and Eve). Outage represents the region when Eve received SNR (SNR_E) is less than the threshold required for error-free communication.	26

3.3	A communication scenario between single leadless pacemaker in right ventricle and subcutaneous implant (Bob) in the presence of Eve.	27
3.4	Probability of successful eavesdropping at varying Eve distance	28
4.1	Shannon cipher system	32
4.2	Wiretap channel	32
4.3	Probability of error (P_e^E) at Eve with and without wiretap encoding, S represents the assumed P_e^E at Eve for confidentiality, R represents the point with no confidentiality, B represents Bob SNR (SNR_B)	34
4.4	Probability of positive secrecy capacity \mathcal{P}_{pc_s}	37
4.5	In-body communication link with human body as EM radiator	39
4.6	Eve placement in a sphere around the body	39
4.7	Secrecy capacity across all the spatial positions surrounding the body at a distance of 1 m. Front represents the frontal side. The cross (X) represents the approximate heart position inside the sphere	40
4.8	Boundary of in-secure volume around the body for fixed secrecy rate of 250 kbps	40
5.1	Phantom containers, containing blood, heart muscle and fat	44
5.2	RSS variations across mean for all the measurement positions during a single cardiac cycle	45
5.3	Cross correlation (a) between legitimate nodes (Alice-Bob) (b) between Alice and Eve outside the body within a distance of 10-27 cm	45
5.4	System model	47
5.5	(a) Evolution tachogram (b)(c)(d)(e) shows the correlation of single sample with other samples from a single source — before and after the difference operation	49
5.6	Block diagram of key generation process, DIFF represents the difference operator, TEO is Teager energy operator and PT is Pan-Tompkins algorithm	50

List of Abbreviations

AoA	angle of arrival
BMR	bit mismatch rate
bpcs	bits per complex symbol
bpm	beats per min
C1	leadless pacemaker in right atrium
C2	leadless pacemaker in right ventricle
C_s	secrecy capacity
CST	computer simulation technology
CDF	cumulative distributive function
CIR	channel impulse response
E1	link between C1 and Eve
ECC	elliptic curve cryptography
ECG	electrocardiography
EGM	electrogram
EM	electromagnetic
EMG	electromyogram
Eve	eavesdropper
Fig.	figure
HFSS	high frequency structure simulator
IB2IB	in-body to in-body
IB2OFF	in-body to off-body
ICD	implanted cardioverter defibrillator
ISM	industrial scientific and medical frequency band
ITU	international telecommunication union
KGR	key generation rate
L1	link between C1 and C2
L2	link between C1 and subcutaneous implant

LCP	leadless cardiac pacemaker
LDPC	low density parity check codes
MICS	medical implant communication systems
NIST	national institute of standards and technology
PL	path Loss
PLS	physical layer security
RF	radio frequency
R_s	fixed secure communication rate
RSS	received signal strength
RA	right atrium
RV	right ventricle
Rx	receiver
S-ECG	subcutaneous ECG
SNR	signal to noise ratio
TDD	time division duplexing
Tx	transmitter
UWB	ultrawide band
VNA	vector network analyzer
WAN	wide area network
WBAN	wireless body area network
WIBEC	wireless in-body environment
WMTS	wireless medical telemetry service

Chapter 1

Introduction

Technological advancements in wireless body area networks have led to the development of many implantable and wearable medical devices and systems. These developments also drove the transformation of decades old cardiac pacemakers and implantable cardioverter defibrillators (ICDs). Pacemakers are implanted in patients presenting abnormal heart rhythms.

Traditionally, pacemakers and similar systems consist of a device casing or ‘can’ that is implanted subcutaneously in a pectoral pocket below the left shoulder. The subcutaneous implantation refers to the placement of a device under the skin into the interior chest wall. The can is connected to transvenous wires or ‘leads’ that run down through veins and are fixed to the inner walls of the right atrium or right ventricle of the heart. Additionally, a third lead can be introduced above the left ventricle for cardiac resynchronization therapy (CRT). CRT is used to treat heart failure by coordinating the function of the left and right ventricles via a can [1]. The lead tips are equipped with sensors/electrodes to sense the electrical activity of the heart and provides actuation if an anomaly is detected.

Though the traditional pacemakers are quite effective, still one in every eight patients develops early complications. The lead related complications are deemed as the most critical ones because they may fracture, they may lead to infection and their explantation carries a significant risk of mortality [2].

To overcome these complications, the next generation of these pacemakers is expected to be wireless between implanted sensors/electrodes inside the heart chambers and the subcutaneous implant (can). These wireless electrodes/sensors implanted without transvenous leads are referred to as leadless cardiac pacemakers (LCP) [3]. The LCPs can be implanted as a single chamber device or multiple

chamber device communicating wirelessly between them and with subcutaneous implant. The project WiBEC¹[4] aims to introduce the multinodal leadless pacemaker technology with LCP in the right ventricle, right atrium, above the left ventricle and the wireless subcutaneous implant. This configuration is referred to as multinodal leadless cardiac pacemaker system and forms a wireless in-body cardiac sensor network.

Advantages of leadless pacemakers include less invasive surgery, avoidance of lead related complications and reduction in risk of infections as in the case of traditional pacemakers. With several advantages, there are also some issues related to leadless pacemakers [5]. One of the key issues is to protect a life saving device from eavesdroppers [6]. Successful eavesdropping may result in retrieval of a patient information (medical and non-medical) or performing attacks like denial of service and data altering. In addition, it may enable the modification of implant configuration without knowledge of the patient or physician. Thus, the wireless nature of these devices could be a significant security risk and must be efficiently secured.

These wireless implanted medical devices can be secured via utilizing traditional methods used in the case of conventional wireless networks. In conventional networks, information security is mainly implemented and studied via traditional cryptographic algorithms [7]. The cryptographic algorithms ensure security by encrypting data using secret keys. These keys help, encrypt and decrypt the information at a sender and a receiver respectively. They work on an assumption of limited eavesdropper's computational resources and requires a dedicated infrastructure for key management and distribution. However, it is challenging to implement key based infrastructure in the new emerging paradigms like wireless in-body sensor networks [8].

Another alternative could be the use of physical layer security (PLS), which relies on concepts of information theory. Security with information theoretic measures can be cryptanalytically unbreakable regardless of eavesdropper unlimited computational resources. The information-theoretic approach or PLS methods have several advantages; they *a*) solve the key distribution and management problem for power constrained devices, *b*) do not assume limited computational resources of an eavesdropper, *c*) can be stacked with traditional cryptosystems in order to add additional layer of security *d*) offers low complexity and resource saving since they eliminate key management servers [9]. There have been considerable efforts to secure wireless networks based on PLS methods. However, these methods mainly focus on free space wireless networks and cannot be directly applied to in-body wireless networks because of the completely different media for communication.

¹Wireless In-Body Environment

Based on the aforementioned advantages of PLS over traditional cryptographic methods, this thesis explores the PLS techniques to provide information security for next generation LCPs. The PLS techniques are exploited to provide information confidentiality and do not delve into other aspects like data integrity and nodes authorization. Information confidentiality mainly refers to the protection of information from un-authorized access whereas data integrity maintains and assures the accuracy of data. The authorization involves permitted access to the device.

In the following, we formalize our research objectives and questions for utilizing PLS methods and provide the relevant contributions based on our research methodologies.

1.1 Research Objective and Questions

In this thesis, first, we quantify the risks associated with the wireless nature of leadless cardiac pacemakers and then provide the countermeasures for information confidentiality using PLS methods. We mainly utilize the channel and source modeling approach of PLS. The objective is formulated in the following main question which is further subdivided into multiple research questions (RQ),

How next generation leadless cardiac pacemakers can be secured using PLS techniques?

RQ 1: What is the eavesdropping risk associated with next generation LCP?

RQ 2: What are the bounds on secure communication rate in case of utilizing channel modeling approach of PLS?

RQ 3: How source modeling approach of PLS can be utilized for key generation between legitimate nodes?

In order to answer the posted questions, we adopted the following research methodologies.

1.1.1 Research Methods

For effective implementation of PLS techniques, prior knowledge about wireless channels is required. In case of cardiac pacemakers, the wireless channels of concern are, in-body to in-body channel for legitimate transmissions and in-body to off-body for evaluation of Eve channel. To model the in-body and off-body wireless channels, the methodology of electromagnetic simulations and experimentation (phantom and in-vivo) is used. The electromagnetic simulations are performed

in CST² microwave studio whereas phantom experiments involve experiments on phantoms. Phantoms are liquid chemical solutions that depict the dielectric properties of human organs/tissues. In-vivo experiments involve experiments on animals. In case of experiments either the phantom or in-vivo, the transmit and receive antennas are submerged in a phantom or implanted in an animal for channel modeling. The modeling of wireless channels helps in evaluating the secure information rate in case of channel modeling approach of PLS whereas in case of source modeling approach, the wireless parameters from channel measurements are used to generate the secret key. The research methods are provided in detail in section 2.4.

1.2 Thesis Contributions

Our contribution to answer RQ 1 lies in the evaluation of eavesdropping risk by using the concept of link outage probability. The link outage probability is defined by computing the signal to noise (SNR) ratio at the input of the receiver chain when it falls below the threshold required for error free decoding. We complement the Eve link outage probability with the probability of successful eavesdropping. Lower the Eve link outage probability, higher the chances of successful eavesdropping. First, we utilized the channel models from literature which then are replaced with our own channel models developed in the later stage of the project.

Similarly, for answering RQ 2 in case of channel modeling approach, our contribution lies in the evaluation of the bounds on maximum secure transmission rates between legitimate nodes in the presence of an Eve. The performance parameter reflecting secure transmission rate is referred to as secrecy capacity. A positive secrecy capacity provides both data confidentiality and reliability. Our hypothesis is on the availability of positive secrecy capacity in the close proximity of the human body reflecting better legitimate channel over Eve on the physical layer. Simulations and experiments were performed to model the wireless channels for evaluation of secrecy capacity. In addition, the measurements were also performed in multiple frequency bands (MICS, WMTS, ISM, and UWB). Furthermore, the electromagnetic transmissions through human body involves heterogeneous medium that results in variation in electric field intensity across different angles outside the body. For the mentioned reason, we also evaluated the three-dimensional secrecy capacity on the spherical sphere around the body. Once the design limits in terms of secure transmission rates are known, one can choose among different wiretap codes for the transmission of confidential information without encryption.

For source modeling approach in case of RQ 3, our contribution lies in the analysis of key generation methods for in-body implanted leadless pacemakers. An

²Computer Simulation Technology

encryption key can be generated between legitimate nodes if there is some common correlated source of randomness available between the nodes. The legitimate nodes access that common source directly and generate a common key from the source without sharing any information between them on the wireless link. The sources which we utilized are, *a*) received signal strength (RSS), *b*) physiological signals. In case of RSS based key generation method, we adopted the methodology of phantom experiments. The RSS measurements were taken simultaneously at both ends of the in-body wireless channel between legitimate nodes which are then used to generate a common key. Similarly, the physiological signals such as the electrocardiogram (ECG), electromyogram, electroencephalogram, or blood pressure may vary in morphology and amplitude depending on where they are recorded, but certain underlying physiological metrics, such as the heart rate, do not. The leadless pacemakers record the local physiological signal and use the underlying common parameter to generate the secret key without sharing of any information. The major contributions of this dissertation can be summarized as:

- Evaluation of eavesdropping risk for LCP.
- Development of phantoms for different human organs in multiple frequency bands to perform experiments.
- In-body to In-body and In-body to off-body channel modeling using electromagnetic simulations, phantom and in-vivo experiments in multiple frequency bands.
- Evaluation of one-dimensional secrecy capacity in multiple frequency bands.
- Evaluation of spatial secrecy capacity in the ISM 2.4 GHz frequency band.
- Evaluation of insecure volume around the body for a certain fixed secrecy rate.
- Analysis of RSS based key generation method for LCP using phantom experiments.
- Analysis of group key generation between multiple nodes of leadless pacemaker system using physiological signals.

1.2.1 List of Publications

All the papers listed below are outcomes of the research work carried out by the author of this dissertation. This includes 7 published and 1 submitted paper. The interconnection between research questions and publications is shown in Fig. 1.1

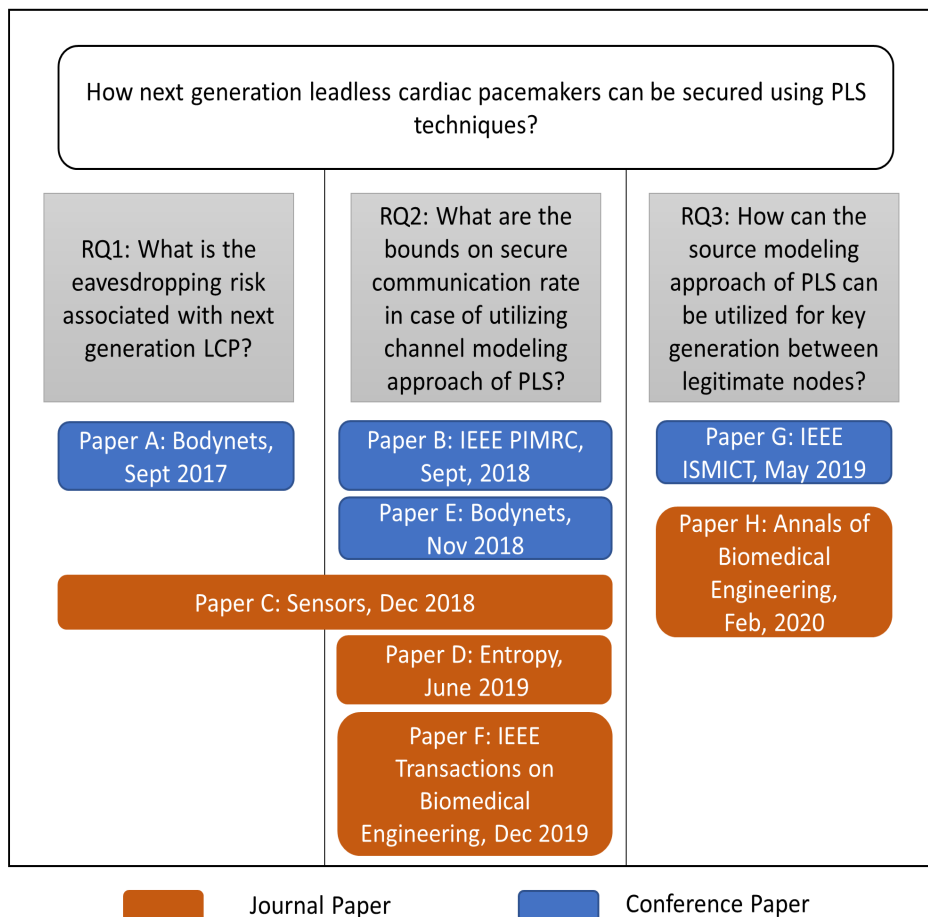


Figure 1.1: Link between research questions and publications

whereas Fig. 1.2 shows the overview of the activities carried by author during the Ph.D.

Paper A: [10] **Awan, Muhammad Faheem**; Kansanen, Kimmo. (2017) Estimating eavesdropping risk for next generation implants. *Advances in Body Area Networks I*. Springer, 2019. 387-398.

Paper B: [11] **Awan, Muhammad Faheem**; Perez-Simbor, Sofia; Garcia-Pardo, Concepcion; Kansanen, Kimmo; Bose, Pritam; Castelló-Palacios, Sergio and Cardona, Narcis. (2018) Experimental phantom-based evaluation of physical layer security for future leadless cardiac pacemaker.

2018 IEEE 29th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications, IEEE PIMRC, (pp. 333-339), IEEE.

- Paper C: [12] **Awan, Muhammad Faheem**; Perez-Simbor, Sofia; García-Pardo, Concepción; Kansanen, Kimmo; Cardona, Narcis. (2018) Experimental phantom-based security analysis for next-generation leadless cardiac pacemakers. *Sensors*. vol. 18 (12), 2018.
- Paper D: [13] **Awan, Muhammad Faheem**; Xiao, Fang; Mehrab, Ramzan; Niels, Neumann; Kimmo Kansanen; Qiong, Wang and Dirk Plettemeier. (2019) Evaluating secrecy capacity for in-body wireless channels, *Entropy* 2019, (21,858).
- Paper E: [14] **Awan, Muhammad Faheem**; Kansanen, Kimmo; Palaksha, Deepak. (2018) Information theoretic analysis for securing next generation leadless cardiac pacemaker. In 13th EAI International Conference on Body Area Networks, (pp. 407-418). Springer.
- Paper F: [15] **Awan, Muhammad Faheem**; Pritam Bose; Ali Khaleghi; Kimmo Kansanen; Ilangko balasingham. (2019) Evaluation of secrecy capacity for next-generation leadless cardiac pacemaker. Accepted for publication in *IEEE transactions on Biomedical Engineering* 2019 (in press, preprint version available online).
- Paper G: [16] **Awan, Muhammad Faheem**; Kansanen, Kimmo; Perez-Simbor S; Garcia-Pardo C; Castelló-Palacios S; Cardona N. (2019) RSS-based secret key generation in wireless in-body networks. In 2019, 13th IEEE international symposium on medical information and communication technology, IEEE ISMICT May 2019, Oslo, Norway.
- Paper H: [17] **Awan, Muhammad Faheem**; Rafael Cordero Alvarez; Kimmo Kansanen, and Delphine Feuerstein (2019) Securing next generation multinodal leadless cardiac pacemaker system: A proof of concept in a single animal. Submitted in *Annals of Biomedical Engineering* February 2020.

1.2.2 Papers Not Included in the Thesis

The author of the dissertation has also contributed to the following articles, as a co-author.

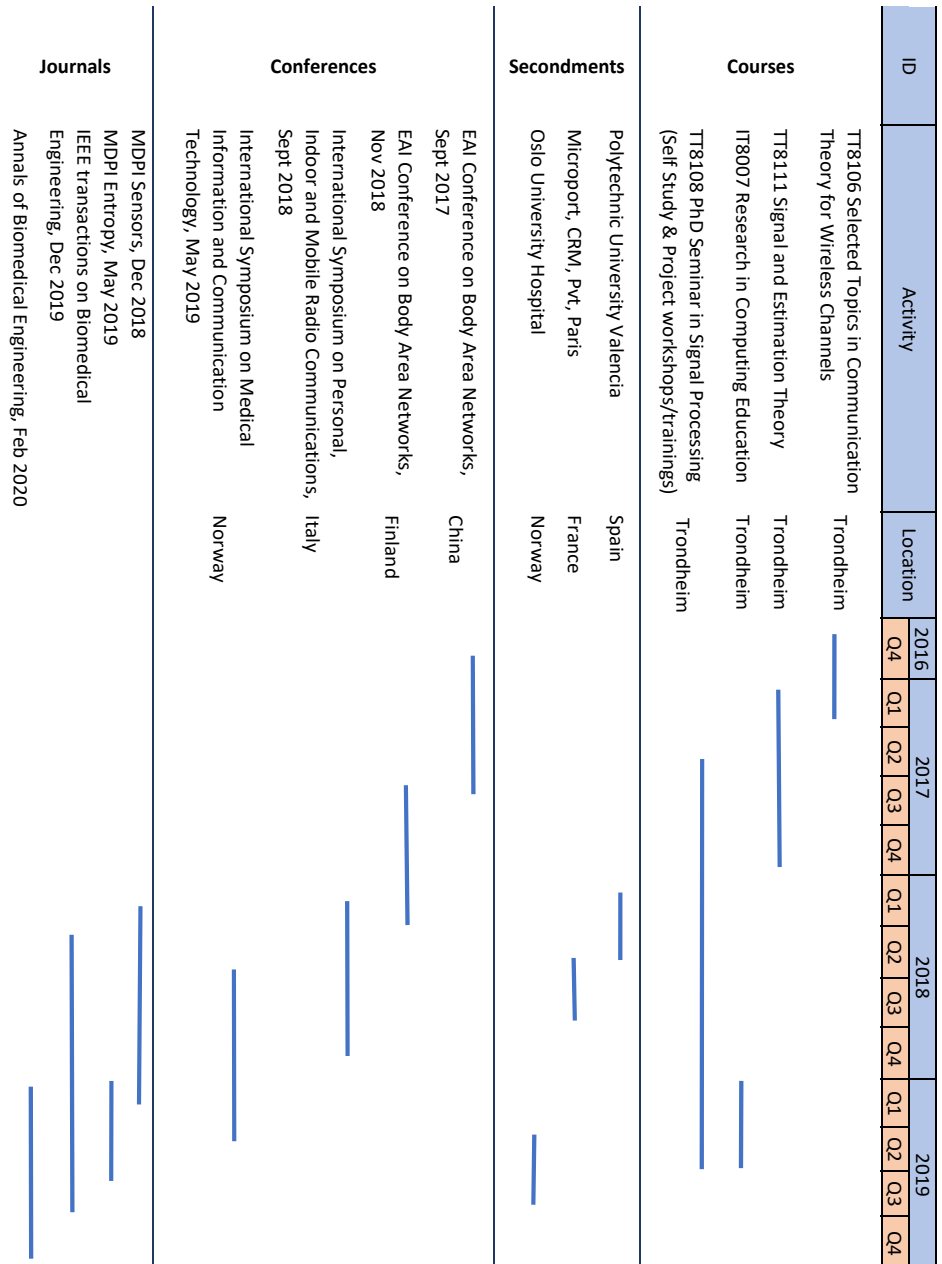


Figure 1.2: Overview of activities carried out by the author during Ph.D.

Paper 1: [18] Palaksha D; Kansanen K; **Awan MF**. Feasibility analysis for pulse based synchronization in a dual chamber leadless pacemaker system. In 13th EAI International Conference on Body Area Networks, (pp. 419-430). Springer.

Paper 2: [19] Mehrab Ramzan; Xiao Fang; Ali Khaleghi; **Muhammad Faheem Awan**; Qiong Wang; Niels Neumann; Dirk Plettemeier. Increasing the transmission efficiency of the miniaturized Implanted spiral antenna in the lossy medium in the MICS band. Submitted in IEEE transactions on antenna and propagation.

1.2.3 Project Deliverables

In project WiBEC, number of deliverables has been submitted to the European Commission that included inputs from different early stage researchers (ESR's). The following list of deliverables also contains author's contribution which is mainly doctoral work update, submitted in different phases of the project.

D1.10: Midterm review meeting/Final technical report (authors work update during halfway and end of the project).

D2.3 : Data rates and 50% improved operational time of the transceivers (author contributed in channel models leading to optimized energy utilization).

D2.4 : Ultra low power algorithms, software codes and evaluation of results (author contributed by reporting Paper G in the deliverable).

D4.1 : In-vitro test results (author reported performed phantom experiments from Paper C).

D4.2 : Final report on pre-clinical evaluation (author reported in-vivo experiment results from Paper F)

D5.1 : Local training activities (Ph.D. course work at NTNU and the trainings/workshops during the project)

1.3 Thesis Organization

The dissertation is a collection of eight technical articles. We structure the thesis in two parts, Part I provides the background and summary of articles and is divided into multiple chapters. The second chapter presents the background whereas the

rest of the chapters group together articles addressing similar topics. Each chapter conveys the basic problem, approach, methodology and descriptive summary of the research articles under the same theme. Part II provides the set of research articles and are scientific contributions of the dissertation. Part I follows the following structure.

- Chapter 2 provides background, clinical aspects of the cardiac pacemakers, and existing security methods for WBAN.
- Chapter 3 covers paper A and evolves from basic concepts to the approach used. Paper A estimates the eavesdropping risk for cardiac implants by considering the transmission of unencrypted information. (RQ: 1)
- Chapter 4 provides the channel modeling approach of PLS systems. First, it covers the basic idea of the approach and then summarizes Paper B, C, D, E, and F. (RQ: 2)
- Chapter 5 analyzes the PLS key generation approaches and summarizes paper G and H. (RQ: 3)
- Chapter 6 concludes and provides future directions.

Part II contains the research articles provided in the Appendix.

Part I

Background and Summary of Articles

Chapter 2

Background

2.1 Wireless Body Area Network

A network of wireless wearable computing devices is referred to as wireless body area network (WBAN) or medical body area network (MBAN) or body sensor network (BSN) [20–22]. The IEEE 802.15.6 is the latest international standard that defines short range, low power, and reliable wireless communication in the vicinity or inside the human body¹ [23]. The standard defines the approved frequency bands, power limitations, and required data rates for different applications along with required security measures to preserve the safety of the device. There are numerous applications of WBAN that are mainly characterized in two broader groups i.e., medical and non-medical applications. The non-medical applications include entertainment applications e.g., gaming, social networking, etc. The medical applications are basically classified into three different categories; wearable, ingestible, and implantable.

The wearable devices are worn, mounted or can be carried in a pocket. These devices contain sensors to monitor different physiological conditions e.g., glucose level, heart rate, temperature or biochemical properties [24–27]. Different sensors including electrocardiogram (ECG), electroencephalography (EEG), body temperature, pressure sensors, respiratory/heart rate monitors, spirometers, blood SpO₂ sensors, and fall detection sensors belong to on-body/wearable devices. The medical devices that can be swallowed are referred to as ingestible capsules and are mainly used for monitoring and diagnosis of gastro-intestinal tract [28, 29]. The most recent ingestible medical device is pillcam [30] which provides a thorough exam of the entire human colon via images. The patient swallows the pillcam

¹Not confined to humans only

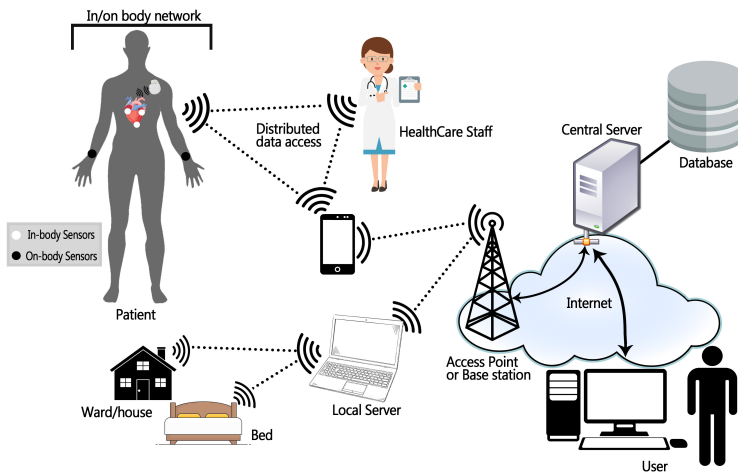


Figure 2.1: Wireless Body Area Network

capsule which takes images while traveling through the gastro-intestinal tract and transmit the images to a recorder which the patient wears on a belt. The procedure is performed under controlled conditions and last for 24 hours or even less.

The third category involves the implantation of medical devices inside the human body and is referred to as implanted medical devices. These devices are implanted using surgical or catheter-based procedures and contain sensors and actuators. Sensors are used for sensing the physiological conditions whereas the actuator performs appropriate therapy if needed. Notable among these implanted devices are neurostimulators, cochlear implants, retinal implants, biosensors with drug delivery systems and cardiac implants which include pacemakers and implantable cardioverter defibrillator (ICD). Moreover, the embedded devices implanted inside the body form an in-body network whereas the on body devices form an on-body network.

Fig. 2.1, shows a typical WBAN network, divided into different communication tiers. The communication of implanted nodes inside the body is referred to as an in-body network and is the first tier of communication. The second tier connects in-body nodes with the on-body nodes or can connect directly with the off-body node/hub. The on-body nodes may also be connected to each other via a central node which is then connected to the off-body hub. The off-body hub relays the data via a wide area network (WAN) to the cloud/storage databases. In this dissertation, the focus is mainly on the wireless in-body sensor network that contains multiple nodes of leadless cardiac pacemaker system.

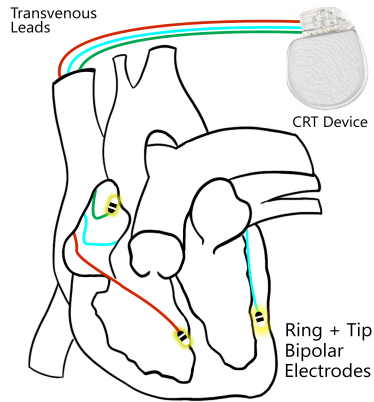
2.2 Cardiac Pacemakers

Cardiovascular diseases are considered to be one of the leading causes of death worldwide. These diseases include conditions that effect the structure or function of the heart such as, heart attack, narrowing of arteries, abnormal heart rhythms, heart failure, heart valve disease, blood vascular disease and many more.

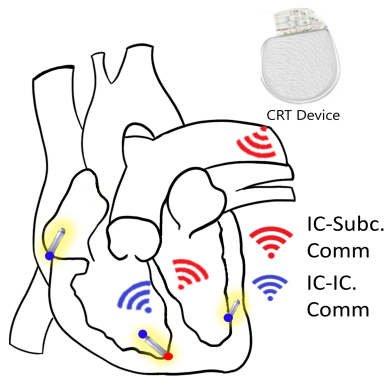
The human heart beats in steady, and even rhythm, about 60-100 beats per minute (bpm). That makes approximately 100,000 times a day. Due to the malfunction of the heart's cardiac function, the heart gets out of rhythm causing the abnormal heartbeats which are referred to as cardiac arrhythmias. The slow rhythm usually less than 60 bpm is referred to as bradycardia whereas the fast heart rhythms are called tachycardia. Cardiac pacemakers are the medically implanted devices designed to regulate abnormal cardiac rhythms. They monitor electrical activity regularly and stimulates when required. These cardiac devices are broadly divided into three categories, 1) pacemakers, used to treat bradycardia, 2) implantable cardioverter defibrillators (ICD), used as anti-tachycardia agent and delivers shock during critical conditions, 3) cardiac re-synchronization therapy devices (CRT), to synchronize the bi-ventricular contractions. There are approximately one million pacemaker implantations annually worldwide [31].

2.2.1 Traditional Cardiac Pacemakers

Conventionally, pacemakers and similar devices consist of a device casing or a 'can' that is implanted subcutaneously in the pectoral pocket and this exists since 1958 [32]. The 'can' is connected to wires or 'leads' that pierce into and run down the subclavian vein where they are ultimately fixed to the inner walls of the heart. Electrodes on the distal ends of these leads record cardiac electrophysiological signals known as electrograms (EGMs) and stimulate the heart accordingly. The electrodes lay in the right atrium, the right ventricle, and above the left ventricle, depending on the particular cardiopathology in question. Fig. 2.2a shows the traditional (i.e. transvenous) widely used cardiac re-synchronization therapy (CRT) system. The can contains a pulse generator, associated circuitry, and a battery. The conventional pacemakers are quite efficient but still there exist some complications and limitations. The complications include pocket infection or hematoma [33], cardiac perforation, pneumothorax, and lead dislodgement. The most critical complications are due to the system leads – they may fracture, they may lead to infection and their explantation is a highly morbid process, carrying a significant risk of mortality [34]. The leadless pacemakers have been seen as an efficient and reliable alternative to reduce the complications of conventional pacemakers.



(a) Traditional CRT system where electrodes are connected by leads to the subcutaneous can



(b) Next generation multi-nodal leadless CRT system

Figure 2.2: Comparison between traditional (a) and a variant (b) of the next-generation CRT systems. IC-Subc. comm refers to intracardiac to subcutaneous communication and IC-IC. refers to intracardiac to intracardiac communication.

2.2.2 Leadless Cardiac Pacemakers

The concept of leadless pacing was first introduced in 1970 [35]. The only leadless pacemaker currently available in the market is the single chamber Micra™ pacemaker distributed by Medtronic [36]. The Micra consists of an autonomous single chamber leadless pacemaker, implanted in the right ventricle and without a subcutaneous implant or a pocket under the skin. The Micra pacemaker is configured and programmed by placing a programmer head on the chest of a patient, above the implanted device. This allows establishing a wireless radio frequency communication between the programmer and the device. Micra only offers single chamber ventricular excitations which only covers less than 10 % of the patient's population. More than 50 % of cardiovascular patient's require multi-chamber pacing for which the ultimate solution is the CRT therapy consisting of multiple leadless pacemakers.

2.2.3 Multinodal Leadless Cardiac Pacemakers

The next generation of cardiac pacemaker system is becoming wireless i.e., connecting multiple nodes (electrodes) of the pacemaker system wirelessly without intravascular leads. Depending on the exact cardiopathology being treated, there will be different variants of future leadless cardiac pacemaker system and will exist as a single chamber pacemaker to a triple-chamber cardiac re-synchronization therapy (CRT) device. One possible configuration could consist of only multi-chamber leadless electrodes that would communicate with each other wirelessly and relay the data directly to an external programmer. Another possible configuration could also integrate a subcutaneous implant that could relay the data of leadless intracardiac electrodes to an external programmer (see Fig. 2.2b). Each intracardiac electrode will contain the sensor, RF communication module, and an actuation unit. The sensors will sense the physiological signals and proper actuation will be provided, if required. The subcutaneous implant will be considered as a hub or a master unit that will communicate wirelessly with intracardiac electrodes. It will act as a primarily processing unit that will take decisions and will store/relay the data to other peripheral devices (on-body or off-body). The subcutaneous implant will offload the burden from intracardiac electrodes to increase their lifetime.

As the pacemaker and similar systems become leadless, a wireless communication challenge arises between various nodes of the system. A few key challenges include power minimization, allocation of the frequency spectrum, data rate requirements and privacy/confidentiality of the implanted wireless devices. This dissertation focuses on information confidentiality related challenges of next generation leadless cardiac pacemakers.

The wireless nature of these pacemakers is a critical security concern as patient physiological information and therapy-related commands are communicated wirelessly. This makes communication more visible and thus facilitating eavesdropping and potential hacking. Due to the sensitive and often life-critical nature of these systems, it is essential to protect the communication between multiple cardiac nodes. Below we discuss the existing, most widely used approaches to provide information security in case of wireless communication networks along with the emerging security paradigms.

2.3 Information Security

Security is one of the most important issues in communication and plays a vital role in device reliability. The vital security concerns that arise in wireless communication network includes data integrity, data confidentiality, and authentication. Confidentiality ensures the reception of information to the legitimate receiver without leakage to an eavesdropper. Integrity proves that the received information is not being modified whereas authentication guarantees that information is sent by the legitimate source. Similarly, the attacks on communication networks can also be classified into two categories; active and passive attacks. The active attack involves disruption of the system whereas in the case of passive attacks the intruder only listens to the communication without any disruption. Usually, the passive attacks are mostly followed by active attacks. These concerns are even more critical for implanted medical devices because of application sensitivity. This dissertation mainly focuses on information confidentiality issues related to the next generation of leadless cardiac pacemakers and considers the passive eavesdropper outside the body.

Information confidentiality can be provided using traditional cryptographic methods which are based on data encryption and decryption [37]. In the process of encryption, the sender transforms the plain text into ciphertext using the encryption key whereas on the receiver side the reverse process is performed. Eavesdropper with no information about the key cannot decrypt the ciphertext. This process assumes the limited computational resources of an eavesdropper who cannot test the entire keyspace in a time span during which the information is considered being critical. The encryption based cryptographic algorithms are divided into symmetric and asymmetric algorithms [38]. The symmetric algorithms use the same key for encryption and decryption purposes whereas the asymmetric algorithms use separate keys for encryption and decryption purposes (mainly public and private key). Both methods put forward different challenges from key management and distribution to the requirement of high computational resources [39–41] in case of power constrained devices.

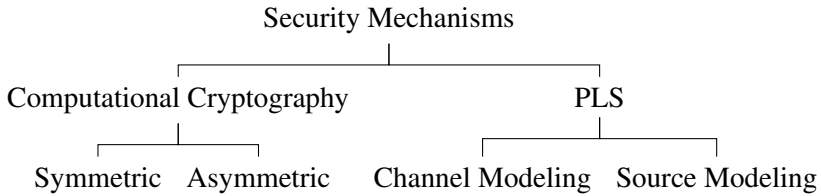


Figure 2.3: Information security paradigms

An alternative to traditional cryptographic methods is the information theoretic security or physical layer security (PLS) approach for securing wireless communication. The information theoretic security approaches the information confidentiality using the physical layer in a communication paradigm. It was pioneered by Shannon [42] in 1949 with an introduction to one-time pad, and was followed by Wyner [43] and Csiszár & Körner [44] with an introduction to wiretap channels in 1970s. The basic idea of PLS methods is to secure confidential information by utilizing physical medium (channel fluctuations, attenuations and noises). PLS methods provide a lightweight alternative for power constrained devices with several advantages over traditional methods. These are less complex and save resources by eliminating the use of key management and distribution servers. In addition, PLS systems do not assume the limited computational resources of an adversary/Eve and can also be stacked with traditional methods to provide an extra layer of security on the physical layer. Fig 2.3 shows the basic security paradigms, including conventional and PLS methods². In the following section, different types of threats are presented along with the existing security solutions in the context of WBAN.

2.3.1 Information Security and WBAN

Security for WBAN devices is considered as a very critical feature in the communication paradigm because of sensitive medical information [45]. Insecure medical devices and communication links can lead to severe consequences and could result in the loss of a patient's life [46]. To demonstrate the concern, Halperin et al. [47] performed software-based attacks on implanted cardioverter defibrillators (ICDs) using off-the-shelf programmer and directional antennas. It was shown that patient safety and privacy can be compromised due to insecure wireless communication links. The comprehensive survey on privacy and security issues related to implanted medical devices (IMDs) is provided in [6]. Similarly, [48] discusses the challenges, goals, and need for securing IMDs.

WBAN could be exposed to numerous threats like data tampering, jamming or

²PLS approaches used in this dissertation are only provided

denial of service. If any node in WBAN is compromised, then the availability of an entire network can be jeopardized. An adversary can also tamper the data, which can lead to inappropriate therapy. As WBANs are usually small networks, thus the operating frequencies can be jammed to make nodes unavailable. Similarly, nodes can be flooded with several broadcast requests to perform the denial of service attacks. In short, all the threats related to other computing devices are applicable to WBAN with severe consequences.

Several approaches have been reported in the literature to secure WBAN communication [49–51]. TinySec is a link-layer security solution for wireless sensor networks which was initially adapted for biomedical sensor networks [52, 53] in a way that the keys are manually programmed into the devices. Similarly, different modes of security are defined in IEEE 802.15.6, from no security to multiple levels of security [54]. In addition, some of the medical devices using Bluetooth or Zigbee utilizes the security algorithms implemented in these standards. Lee et al. [55] proposed a secure key management health care system using the elliptic curve cryptography (ECC). Likewise using ECC, an identity based authentication system was proposed by Zhao [56]. Similarly, [57–61] explores unique biometric features for identification purposes. A complete framework for anomaly detection using machine learning algorithms is provided by Saleem et al. [62]. Braua et al., Sun et al., and Saleem et al. in [63–65] respectively focus on patient’s data privacy. The targeted approaches mainly used traditional cryptographic algorithms for securing WBAN communication network and are mostly proposed for on-body to on-body or on-body to off-body WBAN networks.

2.3.2 Physical Layer Security

PLS methods provide several advantages over traditional methods, from low complexity to cryptanalytically unbreakable [66, 67]. In the following, we discuss the approaches utilized in this dissertation.

Source Modeling Approach

In the source modeling approach, secret keys can be generated between legitimate nodes by utilizing a correlated random source. A source could be among different wireless channel characteristics e.g. RSS, AoA, CIR, and Phase or physiological signals e.g. ECG, EGM, heart rate or blood pressure in case of WBAN.

Maurer et al. [68] were the first to introduce the methodology of generating secret keys from a common source. In recent years, extensive literature aims to utilize this approach for free space wireless networks [69–72]. The comprehensive survey is provided in [73], in which different techniques to generate secret keys are presented.

Similarly, Monroe et al [74], proposed the first biometric-based key generation method. These techniques were based on behavioral biometrics and are provided in [75, 76]. Biometric traits for key-generation can be divided into external and internal traits. The external traits refer to those that remain the same throughout the subject's life and include iris, fingerprints, hand geometry, DNA, and facial morphology [77–79]. The main drawback of external biometrics is that they can be easily forged (e.g we leave our fingerprints on all the objects we interact with on a daily basis). Conversely, internal biometrics are those that vary with time and typically represent internal physiological phenomena. Therefore, they are more resilient in this respect. These internal biometrics include the ECG, the photoplethysmogram (PPG), and the electroencephalogram (EEG) [80]. The use of inter-beat-intervals (IBIs) for a key generation was proposed in [81] where PPG and ECG were utilized to extract IBIs. Other similar works are also available in the literature, utilizing heart rate as a random source to generate the cryptographic keys [82–86].

Channel Modeling Approach

In contrast to the source model approach, the keyless approach or channel model approach, information theoretically secure the transmissions by utilizing the physical medium (channel fluctuations, attenuations, and noises). It makes use of the channel difference between the legitimate receiver and eavesdropper to benefit the legitimate party [87]. This approach does not require keys to secure the information. The channel modeling approach can only be utilized if the legitimate receiver has an advantage over eavesdropper on the physical layer. Different methods are proposed in the literature to secure standard wireless network transmissions using channel model approach with focus to degrade the Eve channel by making it noisier than legitimate channel. It can be achieved by using cooperative jamming with external helpers/relays, full-duplex receivers with multiple antennas or adding the artificial noise/jamming signal. Biao et al. in [88] secure the single antenna systems by introducing artificial noise. Similarly, in [89], different theoretical limits for practical design of PLS jamming in standard wireless networks are presented with introduction to transmit and receive jamming whereas [90, 91] explores different secrecy rate optimization techniques for multicast networks. A comprehensive survey on PLS channel model approaches is provided in [92, 93].

2.4 Research Methods and Approaches

In either case, the source model or channel model approach, PLS utilizes the communication channel between legitimate nodes in order to secure the confidential information. Thus, it necessitates some prior knowledge about wireless channels. Our application scenario of cardiac pacemaker involves the evaluation of wire-

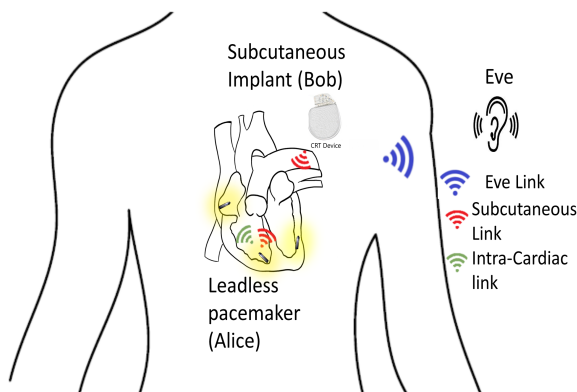


Figure 2.4: Multinodal leadless cardiac pacemaker system with an external eavesdropper

less channels inside and through the body. Fig 2.4 shows the considered system model in the thesis in which the in-body nodes are communicating with each other whereas Eve outside the body tries to eavesdrop the communication. There are two legitimate links, intracardiac and subcutaneous and one eavesdropper link. The intracardiac link is the link between intra-cardiac leadless pacemakers whereas the subcutaneous link is the link between the pacemaker in the right ventricle to the node (can) in the subcutaneous space. As the distance between intracardiac links is quite small as compared to the subcutaneous link, so we mainly consider subcutaneous link in most of the analysis in this dissertation. If the secrecy parameters are satisfied for the subcutaneous link, then it can easily be proved for intracardiac link.

To characterize the channels involving the human body, computational modeling, phantom, and in-vivo experiments are used. The ITU standard has recommended MICS (402-405 MHz) [94] frequency band for implant communication whereas ISM (433 MHz, 868 MHz, 2.4 GHz) [95], WMTS (608-614 MHz) [96], and UWB (3.1-5.1 GHz) [97] frequency bands are also utilized in implantable technologies. The choice of frequency band depends on multiple factors that include path loss to antenna size constraints. In addition, the dielectric properties of human organs also vary and depend upon the frequency band under observation.

Based on the suitability, availability, and appropriateness, we utilize all three methods to characterize the channels in the context of leadless cardiac pacemakers. In addition to different channel characterization methodologies, we also consider multiple frequency bands. In the following, our setup for each measurement methodology is presented.

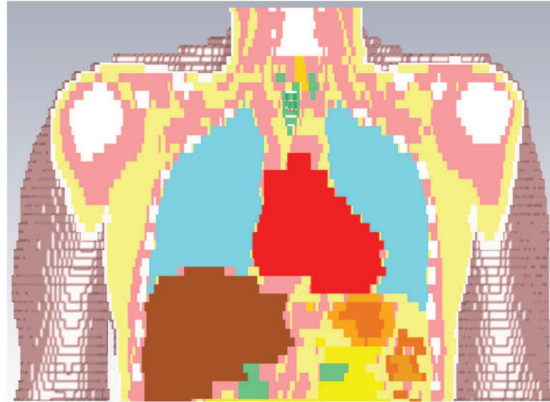


Figure 2.5: A sample computational model

2.4.1 Computational Modeling

Computational modeling is performed using electromagnetic (EM) simulation tools like CST (Computer Simulation Technology) [98], Ansoft HFSS (High Frequency Structure Simulator) [99], FEKO [100] and XFDTD [101]. In this dissertation, computational simulations are performed by using the 3D EM simulation tool CST that allows simulations both in time and frequency domains. CST evaluates the path loss for in-body transmissions by solving the Maxwell equations for a complex medium. We utilized the anatomical data set from CST voxel family [102] and visible human project [103, 104]. The Gustav model is used from a voxel family whereas Hugo model is used from a visible human project. In comparison to Gustav model, Hugo model is a highly complex and detailed model, developed from a dissected male corpse that is segmented into multiple layers. These layers are then sampled and interpolated to provide a highly efficient computational model of the human body. In addition, the frequency dependent dielectric properties of each individual biological tissue have also been considered in the model. We first utilized Gustav model in paper D, which was then replaced with Hugo model in paper F for detailed EM simulations.

For reduction in computational cost in our simulation's scenario, we only consider the upper torso of the human body, as the full body simulations are not required for cardiac application. Fig. 2.5 shows the sample computational model utilized for channel modeling.

2.4.2 Phantom Experiments

Phantoms are chemical solutions that mimic the dielectric properties of human organs/tissues. The phantoms are developed to emulate at room temperature (24°C),

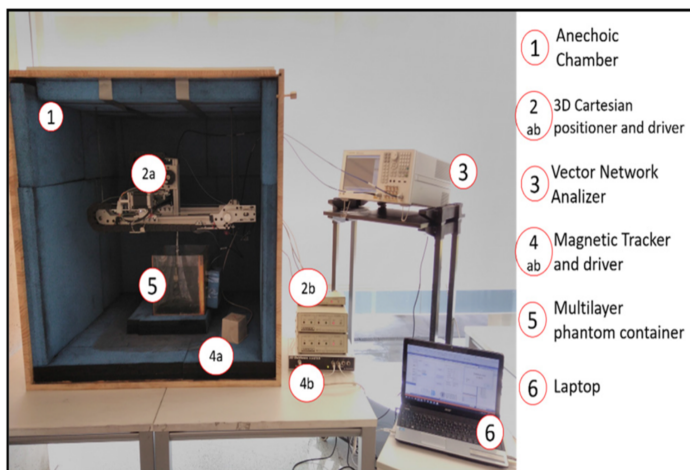


Figure 2.6: Measurement setup for phantom experiments

the electromagnetic properties of the human body at 37 °C provided by Gabriel [105]. In our work, the measurement setup of Fig. 2.6 has been utilized. Our measurement setup contained an anechoic chamber, a Vector Network Analyzer (VNA), a 3D spatial positioner, a phantom container, and a magnetic tracker. The anechoic chamber is used to reduce the surrounding environmental contributions, the magnetic tracker measures the distance between transmitter and receiver antenna at different measuring points, whereas the positioner is used to precisely move an antenna to different measuring points. The VNA is controlled via a laptop with software that performs initial calibration of components before measurement and configures all the devices. It is calibrated with *Rosenberger calibration kit RPC-3.50* to remove the losses due to coaxial cables. After defining the measurement parameters, including frequency range, measurement grid, resolution bandwidth, intermediate frequency, power and number of measurements per position, the measurement setup automatically evaluates the channel transfer function between in-body to in-body and in-body to off-body antennas at the specified grid points.

2.4.3 In-vivo Experiments

In-vivo experiments involve experiments on animals that represent an in-body environment close to that of the human body and are mostly performed to compare the results with the simulations and phantom experiments. In this dissertation, we mainly utilize the data from in-vivo experiments that were performed for other purposes. None of the in-vivo experiment presented in this dissertation was exclusively initiated by this work.

Chapter 3

Eavesdropping Risk

3.1 Introduction

In Paper A, we evaluate the eavesdropping risk, where we consider the transmission of unencrypted information between legitimate nodes, and measures the signal to noise ratio (SNR) outside the body to compute whether the SNR is high enough to decode the information by an eavesdropper (Eve). The eavesdropping risk is associated with the outage probability of a communication link [106].

3.2 Background

In a simple communication system, the source wants to transmit a message through a channel that the recipient wants to replicate as shown in Fig. 3.1. If the receiver signal to noise (SNR_R) is higher than the threshold (SNR_{th}) required, then the receiver can successfully decode the information with a small probability of error (P_e^R). The threshold SNR (SNR_{th}) required depends on an information rate (R) with which the source wants to communicate. Shannon in [107], quantified the information that one can reliably transmit with a relatively small probability of error and termed it as the capacity of the communication channel [108]. Capacity is the number of information bits per channel use. There exist coding techniques that can achieve the rate R equal to or close to the capacity of a communication channel e.g., LDPC codes, turbo codes. Our approach in Paper A utilizes the channel capacity as a measure to evaluate the eavesdropping risk. For a given information rate $R \leq C$, if the SNR_E is below the threshold required then the receiver (Eve) is not able to decode the information and we say that the communication link is in outage as shown in Fig. 3.2.

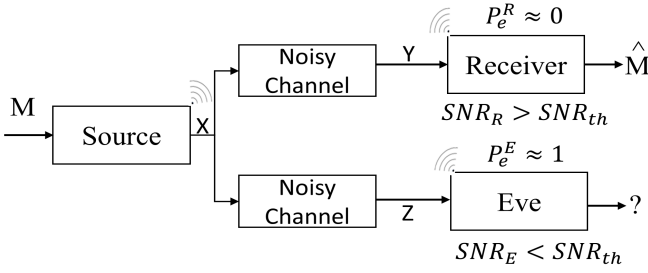


Figure 3.1: A simple communication system with an Eve. P_e^R and P_e^E is the probability of error at legitimate receiver and Eve respectively.

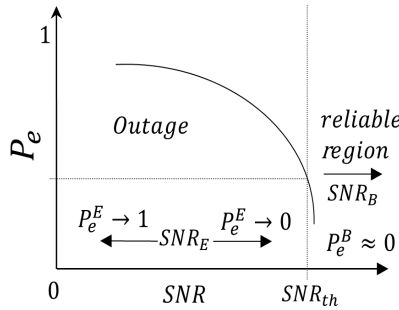


Figure 3.2: Probability of bit error (P_e) vs SNR (legitimate receiver and Eve). Outage represents the region when Eve received SNR (SNR_E) is less than the threshold required for error-free communication.

3.3 Eavesdropping Risk

Consider the system model of our cardiac application as shown in Fig. 3.3, where leadless pacemaker (Alice) is communicating unencrypted information to the subcutaneous implant (Bob) at a fixed distance of 15 cm and Eve outside the body is trying to eavesdrop. For reliable communication, the transmitter needs to communicate on a rate R , less than or equal to the capacity of the link which by Shannon's capacity formula can be expressed as,

$$C = B \times \log_2(1 + SNR_R), \quad (3.1)$$

where B is the channel bandwidth. If we assume the fixed information rate R then the threshold SNR required to achieve the rate R can be expressed as,

$$SNR_{th}(R) > 2^{\frac{R}{B}} - 1, \quad (3.2)$$

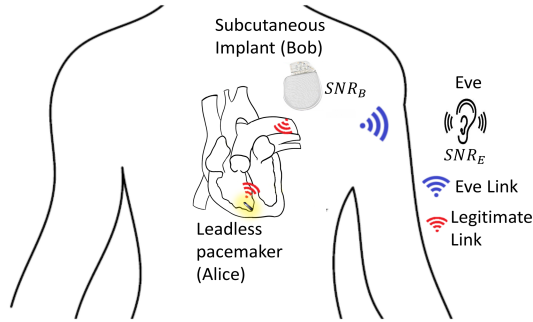


Figure 3.3: A communication scenario between single leadless pacemaker in right ventricle and subcutaneous implant (Bob) in the presence of Eve.

For our case scenario, we have two links, the legitimate link with received SNR represented as SNR_B and Eve link with SNR_E . We assume that the $SNR_B > SNR_{th}$ and Bob lies in the reliable region with probability of error $P_e^B \approx 0$ (see Fig. 3.2) whereas the SNR_E varies with respect to Eve distance. The Eve link is desired to be in an outage to minimize the risk of eavesdropping ($SNR_E < SNR_{th}$) (see Fig. 3.2). Based on Eve link outage probability, the eavesdropping risk can be expressed as,

$$\begin{aligned} \mathcal{P}_{out} &= \mathcal{P}_r(SNR_E < SNR_{th}) \\ \mathcal{P}_{SE} &= 1 - \mathcal{P}_{out} \end{aligned} \quad (3.3)$$

If we consider a constant transmit and noise power, the only parameter that effect the received SNR is the propagation loss. In Paper A, the statistical path loss model of [109] is utilized for in-body to in-body and in-body to off-body communication in the MICS frequency band. The path loss model is not for cardiac scenario and only provides an estimate¹. The model is log-normally distributed and can be expressed as,

$$PL(d)_{dB} = PL(d_o)_{dB} + 10 \times n \times \log_{10} \left(\frac{d}{d_o} \right) + S_h, \quad d \geq d_o \quad (3.4)$$

In (3.4), $PL(d)$ is the path loss/attenuation at a distance d between source and receiver, d_o is the reference distance and is equal to 5 cm. Path loss exponent is n and depends on an environment, for deep implant $n = 4.26$ [109]. Similarly, S_h is random scattering around the mean and can be represented as $\mathcal{N}(\mu, \sigma)$. Fig. 3.4 shows the eavesdropping risk with respect to Eve distance for different information rates. e.g., For ECG rate ($R=250$ kbps) and a MICS channel bandwidth of

¹In the later part of the dissertation, the channels are modeled specifically for cardiac scenario

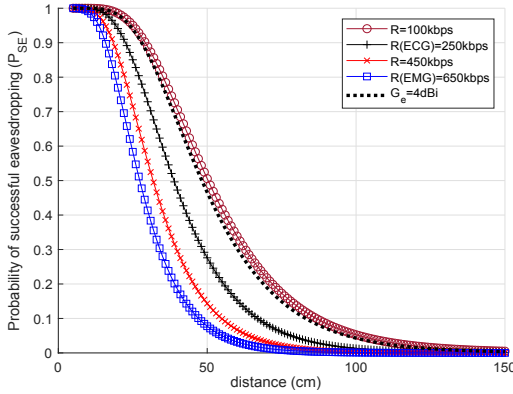


Figure 3.4: Probability of successful eavesdropping at varying Eve distance

300 kHz, the threshold SNR (SNR_{th}) required is -2.12 dB. For the mentioned rate (black line with plus mark), we found that the outage probability of Eve link at a distance of 15 cm is approximately 0%, resulting in an eavesdropping risk of about 100% ($SNR_E > SNR_{th}$, reliable region, Fig. 3.2). Thus, an Eve can decode the unencrypted information with a probability of error ($P_e^E \approx 0$). As Eve moves away from the body, SNR_E drops ($SNR_E < SNR_{th}$, outage region, Fig. 3.2), resulting in lower eavesdropping risk, which at a distance of 40 cm is about 50% and approaches to approximately 0% at a distance of about 100 cm.

3.4 Limitations

The statistical path loss model considered in this work doesn't correspond to cardiac scenario and new models need to be developed for the specific application (cardiac pacemakers). Also, the utilized path loss model is only for in-body to on-body or in-body to in-body communication. Thus, for modeling Eve link, we consider the free space path loss model from on-body to off-body device. These limitations have been addressed by developing our own channel models in the later phase of the project.

3.5 Summary

From Paper A, we have concluded that Eve can eavesdrop from a distance range of 1-2 m without any sophisticated setup that could include high gain antennas. Another important fact that opens the door for securing in-body network with the channel model approach of PLS methods, is the availability of degraded Eve link outside the body and will be explored further in the chapter to come.

The extended paper results including the eavesdropping risk against the outage probability of a legitimate link or the risk against different information rates with Eve high gain antenna are provided in Paper A (Appendix A).

Chapter 4

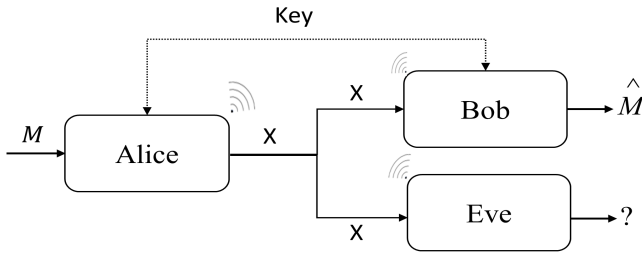
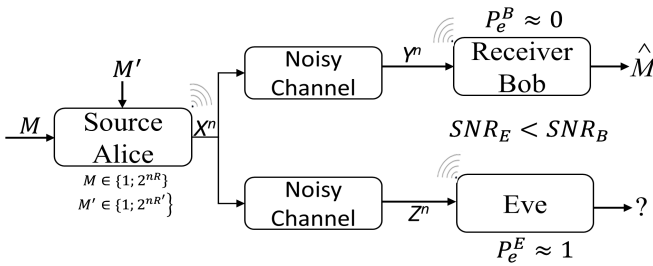
Physical Layer Security — Channel Modeling Approach

4.1 Introduction

In virtually all communication systems, the issues related to confidentiality, and privacy are implemented in upper layers of a protocol stack, utilizing different variants of public- or private-key cryptosystems. Traditional cryptosystems have proven effectiveness yet are impractical for emerging wireless paradigms like sensor or Adhoc networks. In contrast, physical layer security (PLS) or information-theoretic measures have the potential to address these security problems by taking an advantage of radio propagation at the physical layer.

4.2 Background

The problem of secure communication from an information theoretic perspective was pioneered by Shannon [42] in 1949. Shannon considered the noiseless cipher system which involves the transmission of message M to Bob in the presence of an Eve and assumes that both Alice and Bob share a common secret key as shown in Fig. 4.1. Eve doesn't have any knowledge about the shared key. Alice encrypts the message M with key K to a codeword X and transmits it to Bob. Bob on the receiver side utilizes the same Key to transform a codeword X back to M . The codeword X is also received by an Eve. Shannon showed that the system can achieve perfect secrecy if the received codeword X at Eve doesn't convey any information about the source message M i.e. the mutual information between M


Figure 4.1: Shannon cipher system

Figure 4.2: Wiretap channel

and X is zero ($I(M; X) = 0$)¹, which could only be possible if entropy of the key is as large as the entropy of the message. This means that X and M must be statistically independent. The only thing Eve can do is to make a random guess. Wyner [43] on the other hand showed that in the presence of a noisy channel, one can transmit the confidential messages even without the use of the shared keys.

4.3 Wiretap Channel

Recalling from chap. 3, which discussed that good code exists that can achieve the capacity of the channel with a small probability of error (P_e), thus guaranteeing the reliability. Wyner showed that if the Eve channel is degraded version of the Bob channel then messages can be encoded with two-fold advantages, one of reliability and the other of the secrecy as shown in Fig. 4.2.

The message M is encoded by Alice into a codeword X^n of length n , which is received by Bob as Y^n and Eve as Z^n through respective noisy channels. The length n code uses the channel for n times. The message is encoded in a way that

¹ $I(M; X) = H(M) - H(M|X)$, $H(M)$ is the entropy of M , and $H(M|X)$ is the entropy of M conditioned on X

Bob should recover M from a codeword Y^n with $P_e^B \rightarrow 0$ as $n \rightarrow \infty$ and it also ensures secrecy.

Wyner introduces secrecy by defining the equivocation rate or the conditional entropy² where the message received by Eve (Z^n) doesn't convey any information about the actual message M ($I(M; Z^n) \rightarrow 0$) as $n \rightarrow \infty$ and termed it as strong secrecy condition. $I(M; Z^n)$ defines the amount of confidential information leaked to the eavesdropper. It has been shown in [110] that strong secrecy ensures message confidentiality in a way that the decoding error at Eve exponentially approaches to one, no matter what decoding strategy Eve is using.

4.3.1 Secrecy Capacity

The notion of reliability and secrecy contradicts, the reliability requirement asks for the inclusion of redundancy in the encoder for combating the channel noise whereas the secrecy requirement necessitates limiting the redundancy for avoiding information leakage. The metric that simultaneously satisfies both conditions is termed as secrecy capacity which is the maximum transmission rate that can be achieved without any information leakage to Eve. The secrecy capacity of a wiretap channel defined by Wyner is expressed as,

$$C_S = \max_{V-X-(Y,Z)} (I(V; Y) - I(V; Z)) \quad (4.1)$$

The auxiliary random variable V introduces the artificial noise into the system and plays a role of making Eve channel noisier. The mutual information between Alice and Bob is represented by $I(V; Y)$ and depends on Bob's channel quality. It also characterizes the maximum transmission rate for reliable communication. Similarly, the information leaked to Eve is represented by $I(V; Z)$ and is the cost in terms of information rate one has to pay for introducing secrecy. Secrecy capacity is zero if Eve and Bob's channel qualities are identical. For secrecy capacity to be positive, Alice must have a better channel than Eve.

The codes used for this communication problem are referred to as wiretap codes [111–115]. In contrast to reliable channel codes, in wiretap codes, Alice instead of utilizing all resources for message transmission, has to utilize part of it in randomization by adding dummy messages. For each confidential message, the central idea is to select the randomization rate that corresponds to the Eve channel capacity/information rate i.e., $I(V; Z)$ also shown in Fig. 4.2 as R' where M' are the messages to confuse Eve. Ultimately Eve will be saturated with useless information in the form of dummy messages and will not be able to decode the confidential

² $\frac{1}{n} H(M|Z^n) \approx \frac{1}{n} H(M)$

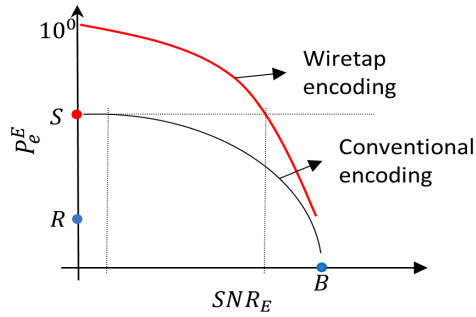


Figure 4.3: Probability of error (P_e^E) at Eve with and without wiretap encoding, S represents the assumed P_e^E at Eve for confidentiality, R represents the point with no confidentiality, B represents Bob SNR (SNR_B)

information [116]. As mentioned, the reliable transmission between Alice and Bob can be done on a rate $I(V;Y)$ but due to secrecy constraints, Alice is left with a rate C_S to transmit the confidential information, as shown in Fig. 4.2 as R with message M . Bob with superior channel quality can decode both the dummy and confidential messages.

Fig. 4.3 shows the probability of errors at Eve with and without wiretap encoding. The point S represents the threshold error rate at Eve to achieve confidentiality, whereas R represents the point with no confidentiality. It can be seen from Fig. 4.3 that the threshold error rate in case of conventional coding is achieved when SNR_E is almost zero, whereas with wiretap encoding the threshold error rate can be achieved even when Eve's SNR is close to the Bob's SNR. The advantage of wiretap encoding is that the bit error rates at Eve grow at a much faster rate with increasing SNR difference between Bob and Eve in comparison to conventional codes. For example, for Eve error probability of 0.4, 0.45, 0.49, the SNR difference required will be 0.6, 1.8, 4.1 dB by utilizing the wiretap encoding. However, for same Eve error rates with conventional encoding, the required SNR difference will be 14, 20, 34 dB respectively³.

Therefore via secure encoding, one can transmit the confidential messages even when there is low SNR difference but with a cost of compromising the legitimate transmission rate and accumulating more resources to transmit dummy messages for augmenting additional noise via dummy messages that leads to a high probability of errors at Eve.

³the numbers are provided as a reference from [66]

In the following, we will define our system model for secrecy capacity evaluation, followed by a brief summary of our articles that address the same problem.

4.4 Evaluation of Secrecy Capacity for Leadless Cardiac Pacemakers

The system model of our cardiac application is shown in Fig. 3.3 with an in-body legitimate channel and off-body Eve channel. Leadless pacemaker (Alice) in the right ventricle transmits a message U and subcutaneous implant (Bob) receives Y through the in-body channel. Similarly, Eve receives Z via a combination of in-body and off-body channels. Both the links are corrupted by additive white Gaussian noise N_B and N_E with zero mean μ and variance σ . Their input-output relation can be expressed as,

$$\begin{aligned} Y_i &= h_B X_i + N_{B,i} \\ Z_i &= h_E X_i + N_{E,i} \end{aligned} \quad (4.2)$$

where h_B and h_E are the Bob and Eve channel gains respectively at a channel use i . The input symbol is represented by X_i which is securely encoded using wiretap codes with two rate parameters, i.e., the codeword transmission rate, C_m , which is the capacity of a legitimate channel and the confidential information rate C_s . A length n wiretap code is constructed by generating 2^{nC_m} codewords $X^n(u, v)$, where $u = \{1, 2, \dots, 2^{nC_s}\}$ and $v = \{1, 2, \dots, 2^{n(C_m - C_s)}\}$. For each message index u , v is randomly selected from $\{1, 2, \dots, 2^{n(C_m - C_s)}\}$ with uniform probability and transmit the codeword $X^n(u, v)$. For average power constraint P and constant noise power σ , the confidential rate or secrecy capacity of a real-valued Gaussian wiretap channel can be expressed as,

$$\begin{aligned} C_s &= \frac{1}{2} \log_2 (1 + SNR_B) - \frac{1}{2} \log_2 (1 + SNR_E), \\ C_s &= \frac{1}{2} \log_2 \left(1 + \frac{P|h_B|^2}{\sigma^2} \right) - \frac{1}{2} \log_2 \left(1 + \frac{P|h_E|^2}{\sigma^2} \right) \end{aligned} \quad (4.3)$$

The dependence of secrecy capacity on the channel gains necessitates the requirement of some prior knowledge about communication channels for PLS systems. We utilized the methodologies presented in section 2.4 to model the in-body and off-body channels for evaluating channel gains.

4.4.1 One-dimensional Secrecy Capacity

A one-dimensional secrecy capacity is the secrecy capacity evaluated with respect to Eve distance. All the Eve measurement points are modeled as a distance irrespective of measuring angle from the body. In Paper C and D, the objective was

to evaluate the one-dimensional secrecy capacity for next generation leadless cardiac pacemaker in multiple frequency bands and to observe whether the positive secrecy capacity can be achievable in the close proximity of the human body or not.

Paper C and D

Paper C⁴ utilizes the methodology of phantom experiments with a measurement setup as shown in Fig. 2.6. The frequency bands under observation were ISM 2.4 GHz and the UWB frequency band (3.1-5.1 GHz). For in-body to in-body and in-body to off-body channel modeling the propagation channel consists of heterogeneous human organs/tissues. Thus, we developed the phantoms that reflect the dielectric properties of the heart muscle, blood, and fat. As the dielectric properties of human organs vary with respect to frequencies, different phantoms were developed for different frequency bands under investigation.

For in-body legitimate link, the transmitter antenna (leadless pacemaker) submerged inside the blood phantom was moved into different positions whereas the receiver antenna (subcutaneous implant) was mounted inside the fat layer. For Eve link, the transmitter was fixed inside the phantom with an implant depth of 10 cm whereas the Eve antenna was moved outside in different positions. The measurements were automatized via computer software that was interfaced with all the equipments. After defining the measurement points, the anechoic chamber was closed properly to avoid outside interference. The positioner automatically moved the antenna to each defined position in a grid and took multiple readings to avoid errors. In addition, the antennas were properly matched to have the maximum channel gain both for in-body legitimate link and off-body Eve link.

From measurements campaign, we develop the in-body and off-body channel models which are later fitted with log-normal distribution as in (3.4). From the developed channel models, we evaluate the probability of positive secrecy capacity with respect to eavesdropper distance which can be expressed as,

$$\mathcal{P}(C_s > 0) = \mathcal{P}(SNR_B > SNR_E) \quad (4.4)$$

In Paper D, the same performance metrics as in Paper C were evaluated but for different frequency bands i.e., (MICS (402-405 MHz), WMTS (608-614 MHz) and ISM 868 MHz frequency bands). Due to the unavailability of antennas in these frequency bands, instead of phantom experiments, electromagnetic simulations are performed for channel modeling in CST using Gustav model. Moreover, we consider three links, two legitimate links (i-e intracardiac (link b/w antenna in

⁴Paper B is the conference version of Paper C and is provided in Appendix B

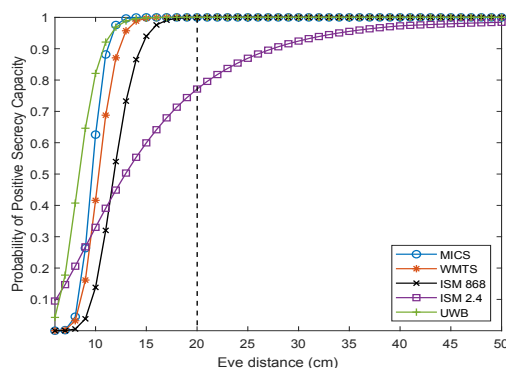


Figure 4.4: Probability of positive secrecy capacity \mathcal{P}_{pc_s} .

right ventricle and antenna in the right atrium), subcutaneous link) and the Eve link (see Fig. 2.4). Here we only consider the subcutaneous link as in Paper C.

Fig. 4.4 shows the probability of positive secrecy capacity for all the frequency bands under investigation. Though the results are not directly comparable, they prove our hypothesis of achieving approximately 100% positive secrecy capacity within the human personal space of 20 cm with exception in case of ISM 2.4 GHz. This could be attributed to the electrically small size of transmitter antenna⁵ which results in the flow of currents at the outer surface of the coaxial cable. These currents result in spurious radiations from the cable, causing lower propagation loss at this frequency.

The complete papers are provided in Appendix C and Appendix D which along with providing positive secrecy capacity, also contains, representation of dielectric properties of phantoms, phantoms preparation, reflection parameters of antennas in a phantom solution, evaluation and formulas derivation of eavesdropping risk and secrecy capacity based on computed log-normal channel models, outage probability of secrecy capacity for certain fixed secrecy rate and the effect of high gain Eve antenna.

Paper E

In addition to considering a Gaussian wiretap channel model for evaluation of secrecy capacity in Paper C and Paper D, Paper E utilizes the Gaussian broadcast channel model in which we consider the transmission of confidential information along with some common message. The confidential information is intended only for the legitimate receiver whereas common information is intended for both, the

⁵1 mm in radius, meander shaped, and 6 mm in length

legitimate receiver inside the body and the receiver/Eve outside the body. A statistical path loss model [109] for MICS frequency band is utilized. The corresponding secrecy rates R_0 for common information and R_1 for confidential information are evaluated by considering the in-body channel gains. The detailed results are provided in Paper E (Appendix E).

Summary/Limitations

To summarize the one-dimensional secrecy capacity results, we conclude that the positive secrecy capacity is achievable within human personal space of 20 cm. The phantom experiments do provide a good estimate, but coaxial cables also radiate in case of electrical small size of transmitter antenna. Similarly, the CST simulations consider less accurate in-body model (Gustav Model). Moreover, for the cases explained above, we only measure the Eve distance, irrespective of direction and angle from the pacemaker. To overcome these issues, in Paper F, we choose a single frequency band (ISM 2.4 GHz) based on recommendation in [117] and perform CST simulations with detailed and accurate Hugo model for heart scenario, Phantom experiments with standalone antenna and transmitter powered by a button cell battery, and an in-vivo experiment.

4.4.2 Spatial Secrecy Capacity

So far, we have explored the one-dimensional secrecy capacity. However, in-case of implanted medical devices, the entire human body radiates electromagnetic waves in three-dimensional space around it with the possibility of Eve at different angles in the space. This motivates us to evaluate the spatial secrecy capacity for examining the effect of electromagnetic radiations across different angles in three dimensional space.

Paper F evaluates the secrecy capacity of the space around the body, first by defining a spherical grid for Eve at a radius of 1 m, then using the free space path loss model to extrapolate over three dimensional space for different radial distances. The channels are modeled using EM simulations, phantom, and in-vivo experiments to provide a fair comparison between results. The tests and simulations are performed for the ISM frequency band (2.4 GHz). The frequency choice is based on the easy implementation of a very small antenna, providing sensible radiation efficiency and matching. Furthermore, in order to avoid EM radiations from coaxial cables, a small battery powered antenna with a transmitter was utilized.

The system model of Fig. 3.3 is considered without any prior assumption on Eve's position which can be located at different angles around the body. Fig. 4.5 shows the in-body positioning of the antennas and the human body torso radiating EM

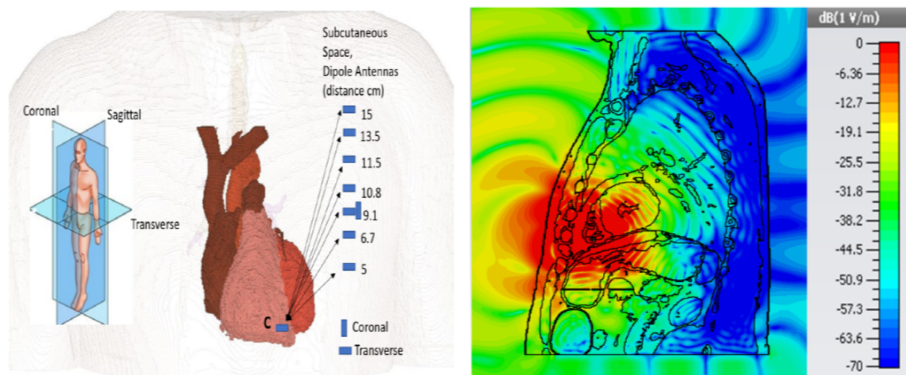


Figure 4.5: In-body communication link with human body as EM radiator

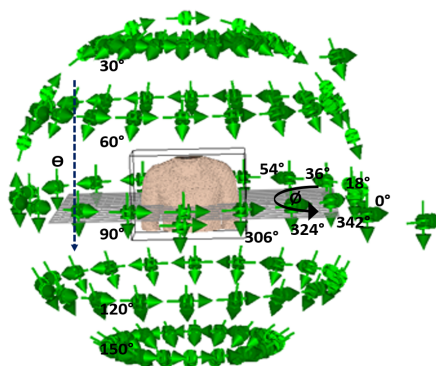


Figure 4.6: Eve placement in a sphere around the body

waves across different angles outside the body. Fig. 4.6 shows the spherical grid of Eve positions around the body. The secrecy capacity on the spherical surface around the body can be expressed as

$$C_S(r, \theta, \phi) = \begin{cases} \frac{1}{2} \left[\log_2 \left(\frac{1 + \frac{|h_{x,y}|^2 P}{\sigma^2}}{1 + \frac{|g_{r,\theta,\phi}|^2 P}{\sigma^2}} \right) \right]^+ & , |h_{x,y}|^2 < |g_{r,\theta,\phi}|^2 \\ 0, & \text{Otherwise} \end{cases} \quad (4.5)$$

After evaluating the secrecy capacity of all the AB-AE⁶ link channel attenuations in three dimensional space, we divide the space around the body into secure and insecure volumes for certain fixed secure communication rate. For fixed AB atten-

⁶AB is link b/w Alice in RV and Bob in subcutaneous space, whereas AE is b/w Alice and Eve

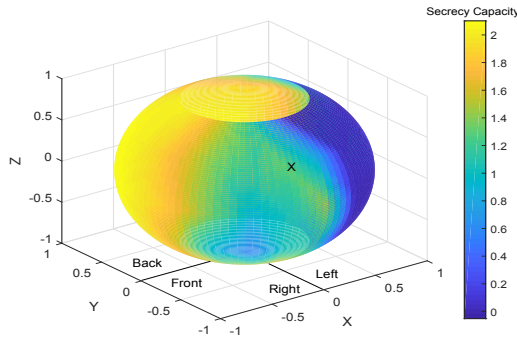


Figure 4.7: Secrecy capacity across all the spatial positions surrounding the body at a distance of 1 m. Front represents the frontal side. The cross (X) represents the approximate heart position inside the sphere

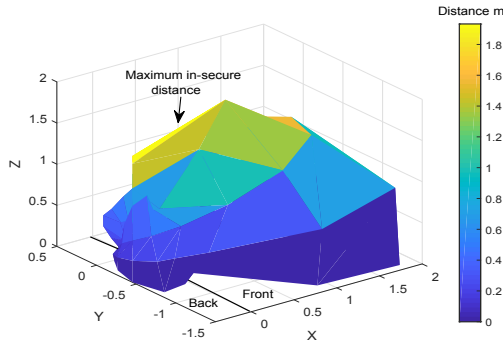


Figure 4.8: Boundary of in-secure volume around the body for fixed secrecy rate of 250 kbps

uation and communication rate, we solve for all the AE attenuations that lie in the secure and insecure volumes. The insecure volume defines all the Eve distances from which LCP can be eavesdropped and is expressed as,

$$d_{E(r,\theta,\phi)} \leq r \times 10^{\left(\frac{P - \beta - 10 \log_{10}(2^{(C_B - C_S) - 1}) - \sigma^2}{10n} \right)}. \quad (4.6)$$

$\forall (r, \theta, \phi)$

For a given power P , AB attenuation and secrecy rate, (4.6) holds for all (r, θ, ϕ) . Beyond the in-secure volume, communication is considered to be secure for a given secrecy rate. In (4.6), $d_{E(r,\theta,\phi)}$ is the eavesdropper distance at a specific angle from Alice, C_B is the capacity of the AB link, C_S is the fixed secrecy rate for communication, r is the reference eavesdropper distance and is equal to 1 m,

σ^2 is the noise power and β is the Eve channel attenuation at the reference Eve distance.

Our results from EM simulations show that the angle where Eve has the minimum channel attenuation is found to the left from front, just above the heart and is termed as the “Eve sweet spot angle”. Eve’s sweet spot angle has the least secrecy capacity among all the eavesdropper spatial positions with the human heart as the reference position as shown in Fig. 4.7 (shaded blue region). Similarly, an insecure volume for a fixed secrecy rate of 250 kbps is shown in Fig. 4.8. The volume is irregular because of different attenuation values across different angles through the body. Moreover, we found that by considering an ideal antenna for EM simulations, the insecure volume has a maximum distance of 2.5 m at an Eve sweet spot angle whereas the experimental results show the maximum distance of about 14 cm, contradicting with EM results. However, in case of EM simulations, if we consider a realistic scenario with practical implant antenna effects, the secrecy distance reduces to 15 cm which is in correlation with the experimental measurements (phantom and in-vivo).

For extended results, Paper F is provided in Appendix F which contains, evaluation of channel models from EM simulations, phantom, and in-vivo experiments, evaluation of 3-dimensional secrecy capacity along with a comparison between different measurement methodologies. Similarly, a comparison is also drawn for insecure volume by considering the best case scenario for Eve.

Limitations

In case of in-vivo experiment, a single posture was examined and we consider that the movement of off-body antenna does compensates for animal postures, but still, different animal postures might have different measurements. Also, the experimental results correspond to specific utilized antennas and results might vary with different antennas. In addition, the effect of Eve antenna gain has not be analyzed in this work, which could also effect the results. The work is also not applicable to any other in-body medical application except cardiac pacemakers but however can be utilized as an estimate.

4.5 Summary

For wireless in-body cardiac sensor network, our findings show that the channel modeling approach of physical layer security methods can be an efficient alternative to secure the implanted medical devices on a physical layer. This is because the human body being a lossy medium for electromagnetic propagation, inherently provides high channel attenuation to off-body links e.g., the eavesdropper link, thus naturally assuring a degraded wiretap scenario for off-body links.

Chapter 5

Physical Layer Security — Source Modeling Approach

5.1 Introduction

In traditional cryptographic systems, the legitimate nodes share a secret in the form of a key which is distributed among all the nodes. The sender encrypts the data with a key and transmits it over a channel, the receiver on the other side decrypts the information with the same key (see Fig. 4.1). The storing, managing and distribution of the keys require dedicated infrastructure. It is challenging to implement key based infrastructure in the new emerging paradigm like wireless in-body sensor network.

PLS systems provide an alternative for key distribution, solving the key management and distribution issues. By using the source model approach, PLS systems establish the cryptographic keys between legitimate nodes by exploiting correlated information sources. The correlated source could be the wireless channel or any third-party source. Different wireless channel characteristics e.g. RSS, AoA, Phase, etc. can be exploited based on channel reciprocity [118]. The channel serves as a random source for key generation. Similarly, a third-party source like physiological signals can also be utilized in case of WBAN [119, 120].

In Paper G, we utilize RSS between the legitimate nodes for key generation whereas Paper H focuses on physiological signals (EGM/S-ECG) for symmetric key generation.

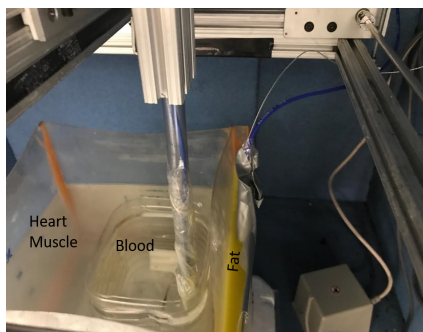


Figure 5.1: Phantom containers, containing blood, heart muscle and fat

5.2 RSS-Based Key Generation

For key generation, the wireless channel can be exploited by utilizing the three basic principles i.e., temporal variation, channel reciprocity, and spatial decorrelation [121]. The movement of a transmitter/receiver/environment introduces temporal variations because of reflection, scattering, or refraction in the channel path. Similarly, multipath and fading is also considered to be the same at both ends of the link because of the channel reciprocity in the same frequency band. Furthermore, Eve located outside the body will experience decorrelated channel measurements.

The in-body wireless cardiac channel experience reflections, scattering, or refraction of electromagnetic waves due to heart movement, change of blood volume and difference in dielectric properties of organs/tissues along the channel path [122]. We consider a system model of Fig. 3.3, with a pacemaker unit (Alice) in right ventricle, and a receiver subcutaneously implanted (Bob). These units probe the wireless channel during the cardiac cycle to extract the RSS measurements for key generation. Phantom experiments were adapted to emulate the cardiac cycle with a measurement setup as shown in Fig. 2.6. In the practical application scenario of a cardiac pacemaker, the transmitter inside the right ventricle will experience back and forth rotational cardiac displacement along with different proportions of blood volume during a single cardiac cycle. As it was not possible to mimic the real time dynamic pumping of the blood, therefore we approximated the dynamics by measuring the two extremes, one with blood phantom and one without blood phantom. In addition, the movement of a transmitter antenna inside the phantom emulates the cardiac displacement during a single cycle. Fig. 5.1 shows different phantoms with transmitter antenna submerged in a blood phantom and subcutaneous antenna inside the fat layer.

The variations in RSS measurements for the in-body wireless channel during a

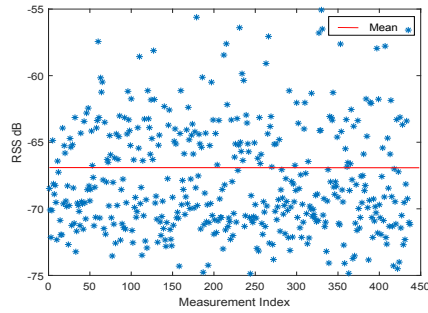


Figure 5.2: RSS variations across mean for all the measurement positions during a single cardiac cycle

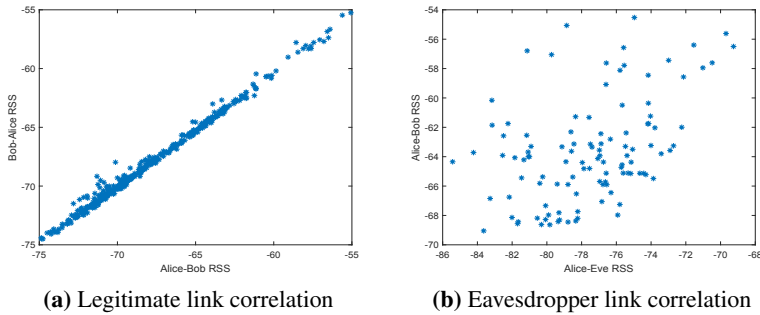


Figure 5.3: Cross correlation (a) between legitimate nodes (Alice-Bob) (b) between Alice and Eve outside the body within a distance of 10-27 cm

single cardiac cycle can be seen in Fig. 5.2. The measurements are tested to be independent identical distributed (i.i.d) in time and can be fitted with log-normal distribution having the standard deviation of approximately 4.04 dB. The number of random bits extracted during a single cardiac cycle can be provided by the entropy of the source which in case of a log-normal i.i.d. source is expressed as,

$$\mathbb{H} = 1.44 \times \frac{1}{2} \times \log(2\pi\sigma^2 e) \approx 2.7 \text{ bits}, \quad (5.1)$$

Equation (5.1) shows that during a single cardiac cycle, 2.7 random bits can be extracted. We model the quantization algorithm in a way that it extracts only 2 bits from each RSS measurement in order to reduce the bit mismatch at both ends. Fig. 5.3 shows the correlation between RSS measurements between Alice and Bob and Alice and Eve. We found a high correlation between AB measurements whereas a strong decorrelation was observed in AE measurements.

From Paper G, we concluded that for a normal heart rate of 64 bpm, the RSS based key generation approach takes about 60 seconds to generate a key string of 128-bits with an average bit mismatch rate of about 1%.

More insights on phantoms, channel measurements, utilized antennas, region segregation based on a log-normal distribution and quantization algorithm is provided in Paper G (Appendix G).

5.2.1 Limitations

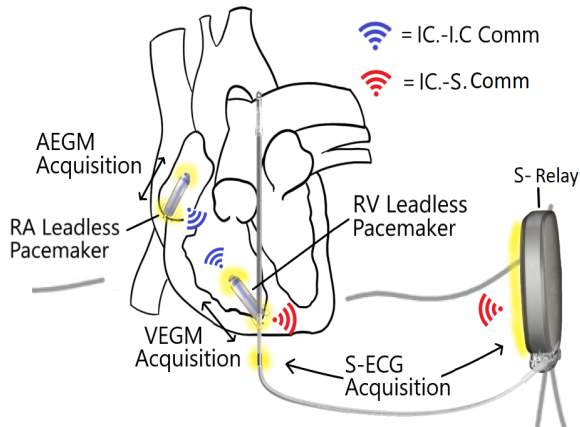
The results from phantom experiments are encouraging, though the method needs to be tested by an in-vivo experiment. Also, the RSS measurements were antenna dependent and could vary due to the change in antennas. Furthermore, the approach also needs to be tested in multiple frequency bands. The hardware implementation of the algorithm is also required to completely evaluate the system complexity.

5.3 Physiological Signals Based Key Generation

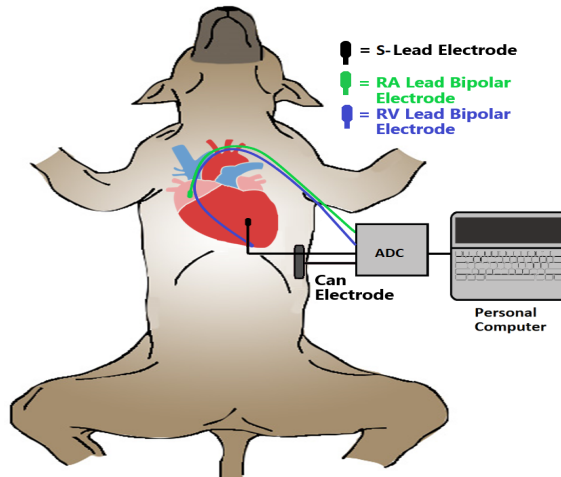
In case of WBAN, the inherent physiological signals can also provide an alternative to generate symmetric keys across multiple nodes, in or on the body. Although physiological signals such as the electrocardiogram (ECG), electromyogram, electroencephalogram, or blood pressure vary in morphology and amplitude depending on where they are recorded, but certain underlying physiological metrics, such as the heart rate, do not, and can be determined from the ECG, electrogram (EGM) or even blood pressure signals.

In paper H, we utilize an inter beat interval (IBI) as a random source to generate the symmetric keys across multiple nodes of a leadless cardiac pacemaker system. The IBI is the time elapsed between contiguous heart cycles and varies with time, depending on different physiological factors. A system model of Fig. 5.4a is considered which was mimicked by performing an in-vivo experiment using the conventional cardiac pacing leads in the right atrium, the right ventricle and the subcutaneous space of the animal (Fig. 5.4b). A metallic dummy pacemaker casing or ‘can’ was also implanted subcutaneously. The implantation of these sensors allowed for the acquisition of EGM and subcutaneous ECG (S-ECG) signals in order to extract IBIs from their respective channels. To extract the IBIs from EGM signals, we used the Teager Energy Operator (TEO) [123] to detect the local depolarization. For IBI extraction from S-ECG, we utilize Pan & Tompkins algorithm [124]. Fig. 5.5a shows the extracted IBIs from respected signals. The IBI sequences across all the nodes of a pacemaker system are highly correlated. The observed cross correlation is about 0.9937 between the IBI sequences. In order to generate a completely random sequence of bits from a given source, the correla-

tion within each of the time series IBI sequence samples should be approximately zero. Fig. 5.5b shows the autocorrelation between the time series IBI samples generated from the node in the right atrium. A high correlation is observed between the adjacent IBI samples, which is not considered as a favorable scenario to generate completely random bits from each sample. This adjacent sample correlation is also reflected on the bits generated, specifically on most significant bits (MSBs)



(a) Dual-chamber leadless pacemaker system with S-relay. IC-IC is intracardia-intracardiac communication, IC-S. is intracardiac to subcutaneous communications.



(b) Dual-chamber leadless pacemaker system with S-relay using transvenous pacemaker leads and inactive 'can' in a dog. ADC is an analog to digital converter.

Figure 5.4: System model

as shown in Fig. 5.5c. In order to reduce the autocorrelation between the adjacent samples, the strategy of difference sequence is applied. The difference sequence is evaluated by taking the difference between adjacent IBI sample values. The difference operator doesn't transform the IBI sequence samples to be completely independent but reduces the autocorrelation to an extent that it can be treated as an i.i.d source. Fig. 5.5d and Fig. 5.5e shows the independence achieved within the IBI time series samples after the difference operation.

The generated IBI sequences are then fitted with a normal distribution. The evaluated fitting parameters are transformed to zero mean with a standard deviation of 0.015 seconds. The number of bits extracted from normally distributed independent identical (i.i.d.) source can be expressed as

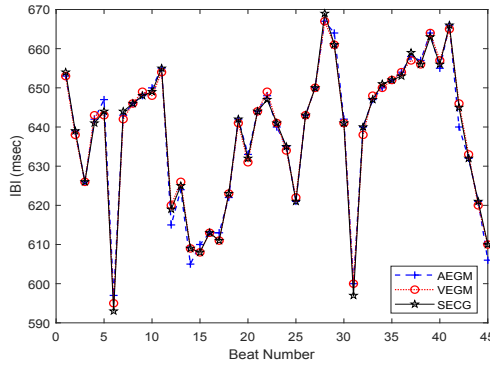
$$\mathbb{H} = 1.44 \times \frac{1}{2} \times \log(2\pi\sigma^2e) \approx 4 \text{ bits}, \quad (5.2)$$

where σ is the standard deviation. Equation (5.2) shows that approximately four random bits can be generated per IBI sample. In this work, the utilized quantization algorithm is modeled in a way that it generates only 3 bits per IBI sample. This is to reduce the potential mismatches between generated bits across the nodes. Fig. 5.6 shows the block diagram of an entire key generation process.

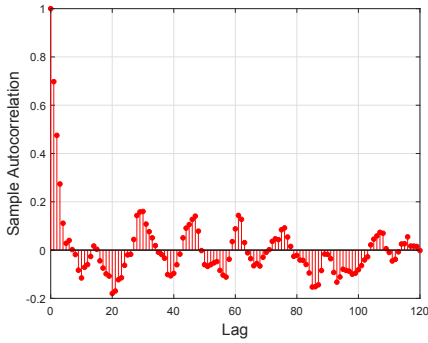
In Paper H, we concluded that by utilizing the physiological signals, PLS systems can generate a 128-bit key string between multiple nodes of a leadless pacemaker system with a key generation rate of 3.56 bits per sec and an average bit mismatch rate of approximately 3%. The extended results containing experiment procedure, signals acquisition, quantization algorithm, gray coding, keys reconciliation, National Institute of Standards and Technology (NIST) based key randomness tests, and correlation tests between keys generated from patient history are provided in Paper H (Appendix H).

5.3.1 Limitations

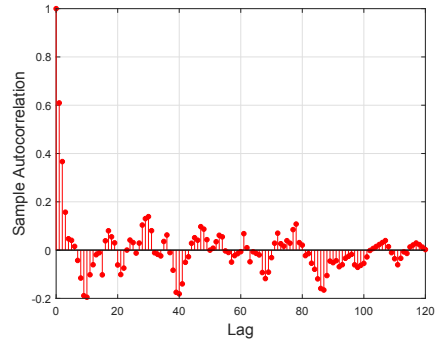
The results from animal experiment are encouraging and supports the process of effective cryptographic key generation from IBIs for next-generation multinodal leadless cardiac pacemaker but there are also some limitations to the current encryption method. The described method fails, if Eve have knowledge about key-generation method and can collect the IBIs at the same instance as of legitimate nodes of the system, as the Eve would be able to generate the same symmetric key. Also, the conditions in which we perform the test were normal, resting sinus rhythm. The method is not tested on different conditions that could include elevated heart rate, atrial fibrillation, or desynchronized ventricles.



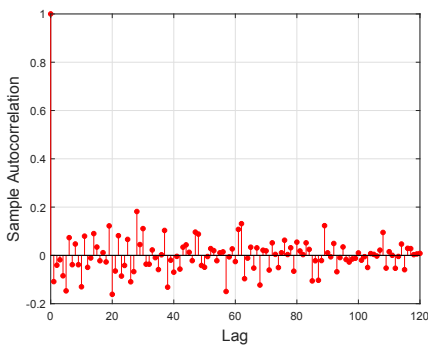
(a) IBI at each node



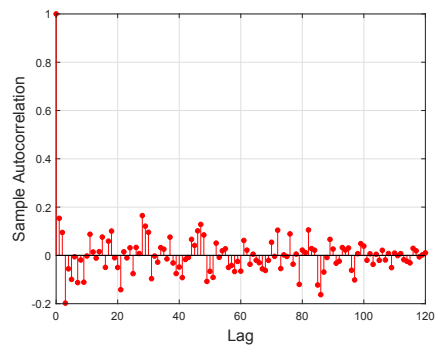
(b) Sample (Before)



(c) MSB (Before)



(d) Sample (After)



(e) MSB (After)

Figure 5.5: (a) Evolution tachogram (b)(c)(d)(e) shows the correlation of single sample with other samples from a single source — before and after the difference operation

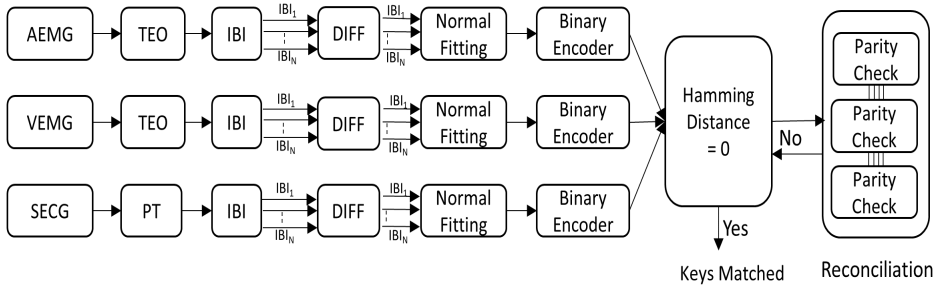


Figure 5.6: Block diagram of key generation process, DIFF represents the difference operator, TEO is Teager energy operator and PT is Pan-Tompkins algorithm

5.4 Summary

Though the key generation rate by using the physiological signals is almost twice as that from RSS based key generation method, but with a higher key mismatch rate. We concluded that the RSS based key generation method has potentially lower complexity than methods based on physiological signals and can be considered as a more viable solution for wireless in-body cardiac sensor network.

Chapter 6

Conclusions and Open Problems

The thesis is aimed to analyze and test the physical layer security (PLS) approaches for securing in-body wireless sensor networks with an application to the next generation of leadless cardiac pacemakers. It primarily focuses on utilization of channel and source model approaches for information confidentiality. The core work can be divided into three parts, namely *a)* eavesdropping risk analysis, *b)* channel modeling or keyless approach for data confidentiality and *c)* source modeling or key based approaches for data encryption.

The risk analysis part is covered by using the concept of the outage probability of the in-body wireless communication link. Initially, the in-body channel models from the literature are utilized which afterwards are replaced by developing the channel models for the used case scenario of a leadless cardiac pacemaker. Based on the Eve link outage probability, it has been observed that for unencrypted information the eavesdropping risk spans between 1-2 m around the body.

For the data confidentiality part using the channel modeling approach, the methodology of electromagnetic simulations (EM), phantom and in-vivo experiments is utilized. We investigate multiple frequency bands and evaluates the bound on maximum secure transmission rate for communicating confidential information. The performance parameter that defines a secure transmission rate is referred to as secrecy capacity. Along with evaluation of one-dimensional secrecy capacity, which is the secrecy capacity with respect to Eve distance, we also evaluate the spatial secrecy capacity which is the secrecy capacity on the spherical surface around the body. The angle where Eve outside the body has the minimum channel attenuation is found to the left from front, just above the heart and is termed as the “Eve sweet spot angle”. Eve’s sweet spot angle has the least secrecy capacity among

all the eavesdropper spatial positions with human heart as the reference position. Moreover, the insecure volume is also evaluated around the human body for a secure cardiac transmission rate of 250 kbps. The insecure volume reflects all Eve positions from where the pacemaker can be eavesdropped. The volume is irregular with a maximum stretch of 15 cm at Eve sweet spot angle after realization of the practical antennas. The experimental measurements support the EM simulation results and prove that the inherently lossy human body medium provides high attenuation to off-body links e.g. the eavesdropper link, due to which the pacemakers can be secured using the channel model approach of PLS on the physical layer.

For the source modeling approach, two different methods are tested, one based on channel reciprocity, second based on physiological signals. For channel reciprocity, received signal strength (RSS) is utilized for symmetric key generation between in-body legitimate nodes by adapting the methodology of phantom experiments. The automatized measurement setup estimates the bidirectional RSS measurements, based on which the secret keys are generated. The reflections due to in-body organs/tissues create enough randomness to generate 2 bits per RSS measurement with a bit mismatch rate of approximately 1% for a key length of 128-bits.

Similarly, by using the inherent physiological signals, the symmetric keys can be generated across multiple nodes of a pacemaker system. For our application scenario, the intra-cardiac pacemaker nodes sense EGM signals, whereas a subcutaneous implant senses ECG signal to extract the interbeat interval (IBI). The IBI remains same irrespective of sensing locations. The inherent randomness in IBI's sequence allows to generate 3 bits per IBI with an average mismatch rate of approximately 3% for a 128-bit key length. A pre-clinical proof of concept is provided by performing an in-vivo experiment in a single animal. Both key generation approaches are considered as a viable solution to overcome the key management and distribution problem for power constrained medical devices. RSS approach outperforms the physiological signals approach in-terms of complexity and bit mismatch rate.

The simulations and experimental measurements prove that the PLS methods for wireless in-body networks could be tenable and efficient alternative for securing in-body networks like a multi-nodal leadless cardiac pacemaker system. However, these approaches still require validity by prototyping the algorithms for pacemakers and testing the complexity of the entire security paradigm. Moreover, the off-body communication link between a subcutaneous implant and an external programmer also needs to be tested using PLS approaches. Integrating the PLS approaches with conventional cryptographic algorithms could also be a good direc-

tion in order to provide an extra layer of security for critically sensitive applications like implanted medical devices.

Bibliography

- [1] Geoffrey F Lewis and Michael R Gold. Developments in cardiac resynchronisation therapy. *Arrhythmia & electrophysiology review*, 4(2):122, 2015.
- [2] Rikke Esberg Kirkfeldt, Jens Brock Johansen, Ellen Aagaard Nohr, Ole Dan Jørgensen, and Jens Cosedis Nielsen. Complications after cardiac implantable electronic device implantations: an analysis of a complete, nationwide cohort in denmark. *European heart journal*, 35(18):1186–1194, Dec, 2013.
- [3] Matthias Merkel, Philipp Grotherr, Andrea Radzewitz, and Claus Schmitt. Leadless pacing: current state and future direction. *Cardiology and therapy*, 6(2):175–181, 2017.
- [4] Eu horizon 2020 project wibec. <https://www.ntnu.edu/wibec>, 2016. Accessed: 20-11-2018.
- [5] Johannes Sperzel, Haran Burri, Daniel Gras, Fleur VY Tjong, Reinoud E Knops, Gerhard Hindricks, Clemens Steinwender, and Pascal Defaye. State of the art of leadless pacing. *Ep Europace*, 17(10):1508–1513, 2015.
- [6] Carmen Camara, Pedro Peris-Lopez, and Juan E Tapiador. Security and privacy issues in implantable medical devices: A comprehensive survey. *Journal of biomedical informatics*, 55:272–289, Jun, 2015.
- [7] Jonathan Katz, Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 1996.
- [8] Shahnaz Saleem, Sana Ullah, and Hyeong Seon Yoo. On the security issues in wireless body area networks. *International Journal of Digital Content Technology and its Applications*, 3(3):178–184, 2009.

- [9] Yiliang Liu, Hsiao-Hwa Chen, and Liangmin Wang. Physical layer security for next generation wireless networks: Theories, technologies, and challenges. *IEEE Communications Surveys & Tutorials*, 19(1):347–376, 2016.
- [10] Muhammad Faheem Awan and Kimmo Kansanen. Estimating eavesdropping risk for next generation implants. In *Advances in Body Area Networks I*, pages 387–398. Springer, 2019.
- [11] Muhammad Faheem Awan, Sofia Perez-Simbor, Concepcion Garcia-Pardo, Kimmo Kansanen, Pritam Bose, Sergio Castelló-Palacios, and Narcis Cardona. Experimental phantom-based evaluation of physical layer security for future leadless cardiac pacemaker. In *2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pages 333–339. IEEE, Sep, 2018.
- [12] Muhammad Awan, Sofia Perez-Simbor, Concepcion Garcia-Pardo, Kimmo Kansanen, and Narcis Cardona. Experimental phantom-based security analysis for next-generation leadless cardiac pacemakers. *Sensors*, 18(12):4327, Dec, 2018.
- [13] Muhammad Faheem Awan, Xiao Fang, Mehrab Ramzan, Niels Neumann, Qiong Wang, Dirk Plettmeier, and Kimmo Kansanen. Evaluating secrecy capacity for in-body wireless channels. *Entropy*, 21(9):858, Sep, 2019.
- [14] Muhammad Faheem Awan, Kimmo Kansanen, and Deepak Palaksha. Information theoretic analysis for securing next generation leadless cardiac pacemaker. In *13th EAI International Conference on Body Area Networks*. Springer, 2020.
- [15] Muhammad Faheem Awan, Pritam Bose, Ali Khaleghi, Kimmo kansanen, and Ilanko Balasingham. Evaluation of secrecy capacity for next-generation leadless cardiac pacemaker. *Accepted for publication in IEEE Transactions on Biomedical Engineering*, 2019.
- [16] Muhammad Faheem Awan, Kimmo Kansanen, Sofia Perez-Simbor, Concepcion Garcia-Pardo, Sergio Castelló-Palacios, and Narcis Cardona. Rss-based secret key generation in wireless in-body networks. In *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*, pages 1–6. IEEE, May, 2019.
- [17] Muhammad Faheem Awan, Rafael Cordero Alvarez, Kimmo Kansanen, and Delphine Feuerstein. Securing next generation multinodal leadless cardiac pacemaker system: A proof of concept in single animal. *Submitted to Annals of Biomedical Engineering, Feb 2020*, 2020.

-
- [18] Deepak Palaksha, Kimmo Kansanen, and Muhammad Faheem Awan. Feasibility analysis for pulse based synchronization in a dual chamber leadless pacemaker system. In *13th EAI International Conference on Body Area Networks*. Springer, 2019.
- [19] Mehrab Ramzan; Xiao Fang; Ali Khaleghi; Muhammad Faheem Awan; Qiong Wang; Niels Neumann; Dirk Plettemeier. Increasing the transmission efficiency of the miniaturized implanted spiral antenna in the lossy medium in the mics band. *Submitted to IEEE transactions on antenna and propagation, Feb 2020*, 2020.
- [20] Sana Ullah, Henry Higgins, Bart Braem, Benoit Latre, Chris Blondia, Ingrid Moerman, Shahnaz Saleem, Ziaur Rahman, and Kyung Sup Kwak. A comprehensive survey of wireless body area networks. *Journal of medical systems*, 36(3):1065–1094, 2012.
- [21] Min Chen, Sergio Gonzalez, Athanasios Vasilakos, Huasong Cao, and Victor C Leung. Body area networks: A survey. *Mobile networks and applications*, 16(2):171–193, 2011.
- [22] Samaneh Movassaghi, Mehran Abolhasan, Justin Lipman, David Smith, and Abbas Jamalipour. Wireless body area networks: A survey. *IEEE Communications surveys & tutorials*, 16(3):1658–1686, 2014.
- [23] IEEE Standards Association et al. 802.15. 6-2012 iee standards for local and metropolitan area networks—part 15.6: Wireless body area networks, 2012.
- [24] Hyunjae Lee, Changyeong Song, Yong Seok Hong, Min Sung Kim, Hye Rim Cho, Taegyu Kang, Kwangsoo Shin, Seung Hong Choi, Taeghwan Hyeon, and Dae-Hyeong Kim. Wearable/disposable sweat-based glucose monitoring device with multistage transdermal drug delivery module. *Science Advances*, 3(3):e1601314, 2017.
- [25] Tran Quang Trung, Subramaniyan Ramasundaram, Byeong-Ung Hwang, and Nae-Eung Lee. An all-elastomeric transparent and stretchable temperature sensor for body-attachable wearable electronics. *Advanced materials*, 28(3):502–509, 2016.
- [26] Fatema El-Amrawy and Mohamed Ismail Nounou. Are currently available wearable devices for activity tracking and heart rate monitoring accurate, precise, and medically beneficial? *Healthcare informatics research*, 21(4):315–320, 2015.

- [27] Kevin Hung, Yuan-Ting Zhang, and B Tai. Wearable medical devices for tele-home healthcare. In *The 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, volume 2, pages 5384–5387. IEEE, 2004.
- [28] Gavriel Iddan, Gavriel Meron, Arkady Glukhovsky, and Paul Swain. Wireless capsule endoscopy. *Nature*, 405(6785):417, 2000.
- [29] Asimina Kiourti, Konstantinos A Psathas, and Konstantina S Nikita. Implantable and ingestible medical devices with wireless telemetry functionalities: A review of current status and challenges. *Bioelectromagnetics*, 35(1):1–15, 2014.
- [30] Medtronic. Capsule endoscopy. <http://pillcamcolon.com/patients.html>, October 2017.
- [31] Harry G Mond and Alessandro Proclemer. The 11th world survey of cardiac pacing and implantable cardioverter-defibrillators: calendar year 2009—a world society of arrhythmia’s project. *Pacing and clinical electrophysiology*, 34(8):1013–1027, Aug, 2011.
- [32] Oscar Aquilina. A brief history of cardiac pacing. *Images in paediatric cardiology*, 8(2):17, 2006.
- [33] Sami Pakarinen, Lasse Oikarinen, and Lauri Toivonen. Short-term implantation-related complications of cardiac rhythm management device therapy: a retrospective single-centre 1-year survey. *Europace*, 12(1):103–108, 2009.
- [34] Robert G Hauser, William T Katsiyannis, Charles C Gornick, Adrian K Almquist, and Linda M Kallinen. Deaths and cardiovascular injuries due to device-assisted implantable cardioverter-defibrillator and pacemaker lead extraction. *Europace*, 12(3):395–401, Nov, 2009.
- [35] J William Spickler, Ned S Rasor, Paul Kezdi, SN Misra, KE Robins, and Charles LeBoeuf. Totally self-contained intracardiac pacemaker. *Journal of electrocardiology*, 3(3-4):325–331, 1970.
- [36] Medtronic micra leadless pacemaker. <https://www.medtronic.com/us-en/patients/treatments-therapies/pacemakers/our/micra.html>, 2012. Accessed: 20-11-2018.
- [37] Naveen Sastry and David Wagner. Security considerations for ieee 802.15.4 networks. In *Proceedings of the 3rd ACM workshop on Wireless security*, pages 32–42. ACM, 2004.

-
- [38] Gustavus J Simmons. Symmetric and asymmetric encryption. *ACM Computing Surveys (CSUR)*, 11(4):305–330, 1979.
- [39] N Asokan and Philip Ginzboorg. Key agreement in ad hoc networks. *Computer communications*, 23(17):1627–1637, 2000.
- [40] Haowen Chan, Adrian Perrig, and Dawn Song. Random key predistribution schemes for sensor networks. 2003.
- [41] Laurent Eschenauer and Virgil D Gligor. A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM conference on Computer and communications security*, pages 41–47. ACM, 2002.
- [42] Claude E Shannon. Communication theory of secrecy systems. *Bell system technical journal*, 28(4):656–715, 1949.
- [43] Aaron D Wyner. The wire-tap channel. *Bell system technical journal*, 54(8):1355–1387, Oct, 1975.
- [44] Imre Csiszár and Janos Korner. Broadcast channels with confidential messages. *IEEE transactions on information theory*, 24(3):339–348, May, 1978.
- [45] Juha Partala, Niina Keränen, Mariella Särestöniemi, Matti Hämäläinen, Jari Iinatti, Timo Jämsä, Jarmo Reponen, and Tapio Seppänen. Security threats against the transmission chain of a medical health monitoring system. In *2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013)*, pages 243–248. IEEE, 2013.
- [46] T Kavitha and D Sridharan. Security vulnerabilities in wireless sensor networks: A survey. *Journal of information Assurance and Security*, 5(1):31–44, 2010.
- [47] Daniel Halperin, Thomas S Heydt-Benjamin, Benjamin Ransford, Shane S Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pages 129–142. IEEE, May, 2008.
- [48] Daniel Halperin, Thomas S Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, and William H Maisel. Security and privacy for implantable medical devices. *IEEE pervasive computing*, 7(1):30–39, Jan, 2008.

- [49] Michael Rushanan, Aviel D Rubin, Denis Foo Kune, and Colleen M Swanson. Sok: Security and privacy in implantable medical devices and body area networks. In *2014 IEEE Symposium on Security and Privacy*, pages 524–539. IEEE, May, 2014.
- [50] Samaher Al-Janabi, Ibrahim Al-Shourbaji, Mohammad Shojafar, and Shahaboddin Shamshirband. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egyptian Informatics Journal*, 18(2):113–122, 2017.
- [51] James Kang and Sasan Adibi. A review of security protocols in mhealth wireless body area networks (wban). In *International Conference on Future Network Systems and Security*, pages 61–83. Springer, 2015.
- [52] Chris Karlof, Naveen Sastry, and David Wagner. Tinysec: a link layer security architecture for wireless sensor networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 162–175. ACM, 2004.
- [53] D Sharma et al. Wireless health care monitoring system with data security and privacy. *Int J Res Comput Eng Electron*, 2(2):1–2, 2013.
- [54] Sana Ullah, Manar Mohaisen, and Mohammed A Alnuem. A review of ieee 802.15. 6 mac, phy, and security specifications. *International Journal of Distributed Sensor Networks*, 9(4):950704, 2013.
- [55] Young Sil Lee, Esko Alasaarela, and HoonJae Lee. Secure key management scheme based on ecc algorithm for patient’s medical information in health-care system. In *The International Conference on Information Networking 2014 (ICOIN2014)*, pages 453–457. IEEE, 2014.
- [56] Zhenguo Zhao. An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. *Journal of medical systems*, 38(2):13, 2014.
- [57] André Leier, Christoph Richter, Wolfgang Banzhaf, and Hilmar Rauhe. Cryptography with dna binary strands. *Biosystems*, 57(1):13–22, 2000.
- [58] Alwyn Goh and David CL Ngo. Computation of cryptographic keys from face biometrics. In *IFIP International Conference on Communications and Multimedia Security*, pages 1–13. Springer, 2003.
- [59] Krishna K Venkatasubramanian, Ayan Banerjee, and Sandeep KS Gupta. Plethysmogram-based secure inter-sensor communication in body area networks. In *Military communications conference*, pages 1–7, 2008.

-
- [60] Nima Karimian, Zimu Guo, Mark Tehranipoor, and Domenic Forte. Highly reliable key generation from electrocardiogram (ecg). *IEEE Transactions on Biomedical Engineering*, 64(6):1400–1411, 2017.
- [61] Carmen Camara, Pedro Peris-Lopez, Honorio Martín, Mu’awya Aldalaien, et al. Ecg-rng: A random number generator based on ecg signals and suitable for securing wireless sensor networks. *Sensors*, 18(9):2747, Aug, 2018.
- [62] Osman Salem, Alexey Guerassimov, Ahmed Mehaoua, Anthony Marcus, and Borko Furht. Anomaly detection in medical wireless sensor networks using svm and linear regression models. *International Journal of E-Health and Medical Communications (IJEHMC)*, 5(1):20–45, 2014.
- [63] Mrinmoy Barua, Xiaohui Liang, Rongxing Lu, and Xuemin Shen. Peace: An efficient and secure patient-centric access control scheme for ehealth care system. In *2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 970–975. IEEE, 2011.
- [64] Jinyuan Sun, Xiaoyan Zhu, and Yuguang Fang. Preserving privacy in emergency response based on wireless body sensor networks. In *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, pages 1–6. IEEE, 2010.
- [65] Shahnaz Saleem, Sana Ullah, and Kyung Sup Kwak. Towards security issues and solutions in wireless body area networks. In *INC2010: 6th International Conference on Networked Computing*, pages 1–4. IEEE, 2010.
- [66] Xiangyun Zhou, Lingyang Song, and Yan Zhang. *Physical layer security in wireless communications*. Crc Press, Apr, 2016.
- [67] Yingbin Liang, H Vincent Poor, Shlomo Shamai, et al. Information theoretic security. *Foundations and Trends® in Communications and Information Theory*, 5(4–5):355–580, Jun, 2009.
- [68] Ueli M Maurer. Secret key agreement by public discussion from common information. *IEEE transactions on information theory*, 39(3):733–742, May, 1993.
- [69] Peng Xu, Kanapathippillai Cumanan, Zhiguo Ding, Xuchu Dai, and Kin K Leung. Group secret key generation in wireless networks: algorithms and rate optimization. *IEEE Transactions on Information Forensics and Security*, 11(8):1831–1846, Apr, 2016.

- [70] Kemedi Moara-Nkwe, Qi Shi, Gyu Myoung Lee, and Mahmoud Hashem Eiza. A novel physical layer secure key generation and refreshment scheme for wireless sensor networks. *IEEE Access*, 6:11374–11387, Feb, 2018.
- [71] Xiaohui Shang, Aijun Liu, Hao Yin, Yida Wang, and Yong Wang. Rss-aoa-based physical layer secret key generation for mobile wireless nodes. In *Journal of Physics: Conference Series*, volume 1169, page 012067. IOP Publishing, Feb, 2019.
- [72] Zhouzhou Li, Honggang Wang, and Hua Fang. Group-based cooperation on symmetric key generation for wireless body area networks. *IEEE Internet of Things Journal*, 4(6):1955–1963, Oct, 2017.
- [73] Youssef El Hajj Shehadeh and Dieter Hogrefe. A survey on secret key generation mechanisms on the physical layer in wireless networks. *Security and Communication Networks*, 8(2):332–341, Jan, 2015.
- [74] Fabian Monrose, Michael K Reiter, and Susanne Wetzel. Password hardening based on keystroke dynamics. *International Journal of Information Security*, 1(2):69–83, 2002.
- [75] Hao Feng and Chan Choong Wah. Private key generation from on-line handwritten signatures. *Information Management & Computer Security*, 10(4):159–164, 2002.
- [76] M Freire-Santos, J Fierrez-Aguilar, and J Ortega-Garcia. Cryptographic key generation using handwritten signature. In *Biometric Technology for Human Identification III*, volume 6202, page 62020N. International Society for Optics and Photonics, 2006.
- [77] Youn Joo Lee, Kwanghyuk Bae, Sung Joo Lee, Kang Ryoung Park, and Jaihie Kim. Biometric key binding: Fuzzy vault based on iris images. In *International Conference on Biometrics*, pages 800–808. Springer, 2007.
- [78] Zhe Jin, Andrew Beng Jin Teoh, Bok-Min Goi, and Yong-Haur Tay. Biometric cryptosystems: a new biometric key binding and its implementation for fingerprint minutiae-based representation. *Pattern Recognition*, 56:50–62, 2016.
- [79] Nalini K Ratha, Sharat Chikkerur, Jonathan H Connell, and Ruud M Bolle. Generating cancelable fingerprint templates. *IEEE Transactions on pattern analysis and machine intelligence*, 29(4):561–572, 2007.

-
- [80] KVR Ravi, Ramaswamy Palaniappan, C Eswaran, and S Phon-Amnuaisuk. Data encryption using event-related brain signals. In *International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007)*, volume 1, pages 540–544. IEEE, 2007.
- [81] Carmen CY Poon, Yuan-Ting Zhang, and Shu-Di Bao. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine*, 44(4):73–81, 2006.
- [82] Sandeep Pirbhulal, Heye Zhang, Wanqing Wu, Subhas Chandra Mukhopadhyay, and Yuan-Ting Zhang. Heartbeats based biometric random binary sequences generation to secure wireless body sensor networks. *IEEE Transactions on Biomedical Engineering*, 65(12):2751–2759, Mar, 2018.
- [83] HA Garcia-Baleon and V Alarcon-Aquino. Cryptographic key generation from biometric data using wavelets. In *2009 Electronics, Robotics and Automotive Mechanics Conference (CERMA)*, pages 15–20. IEEE, 2009.
- [84] Hassan Chizari and Emil C Lupu. Extracting randomness from the trend of ipi for cryptographic operators in implantable medical devices. *IEEE Transactions on Dependable and Secure Computing*, Jun, 2019.
- [85] Masoud Rostami, Ari Juels, and Farinaz Koushanfar. Heart-to-heart (h2h): authentication for implanted medical devices. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 1099–1112. ACM, Nov, 2013.
- [86] Nima Karimian, Zimu Guo, Mark Tehranipoor, and Domenic Forte. Highly reliable key generation from electrocardiogram (ecg). *IEEE Transactions on Biomedical Engineering*, 64(6):1400–1411, Sep, 2016.
- [87] Joao Barros and Miguel RD Rodrigues. Secrecy capacity of wireless channels. In *Information Theory, 2006 IEEE International Symposium on*, pages 356–360. IEEE, Jul, 2006.
- [88] Biao He, Yechao She, and Vincent KN Lau. Artificial noise injection for securing single-antenna systems. *IEEE Transactions on Vehicular Technology*, 66(10):9577–9581, May, 2017.
- [89] Kanapathippillai Cumanan, Hong Xing, Peng Xu, Gan Zheng, Xuchu Dai, Arumugam Nallanathan, Zhiguo Ding, and George K Karagiannidis. Physical layer security jamming: Theoretical limits and practical designs in wireless networks. *IEEE Access*, 5:3603–3611, Dec, 2016.

- [90] Kanapathippillai Cumanan, Zhiguo Ding, Bayan Sharif, Gui Yun Tian, and Kin K Leung. Secrecy rate optimizations for a mimo secrecy channel with a multiple-antenna eavesdropper. *IEEE Transactions on Vehicular Technology*, 63(4):1678–1690, Oct, 2013.
- [91] Kanapathippillai Cumanan, Zhiguo Ding, Mai Xu, and H Vincent Poor. Secrecy rate optimization for secure multicast communications. *IEEE Journal of Selected Topics in Signal Processing*, 10(8):1417–1432, Aug, 2016.
- [92] Amitav Mukherjee, S Ali A Fakoorian, Jing Huang, and A Lee Swindlehurst. Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Communications Surveys & Tutorials*, 16(3):1550–1573, Feb, 2014.
- [93] Matthieu Bloch, João Barros, Miguel RD Rodrigues, and Steven W McLaughlin. Wireless information-theoretic security. *IEEE Transactions on Information Theory*, 54(6):2515–2534, May, 2008.
- [94] Huseyin S Savci, Ahmet Sula, Zheng Wang, Numan S Dogan, and Ercument Arvas. Mics transceivers: regulatory standards and applications [medical implant communications service]. In *Proceedings. IEEE SoutheastCon, 2005.*, pages 179–182. IEEE, 2005.
- [95] Antonietta Stango, Kamyā Yekeh Yazdandoost, Francesco Negro, and Dario Farina. Characterization of in-body to on-body wireless radio frequency link for upper limb prostheses. *PloS one*, 11(10):e0164987, 2016.
- [96] Mehmet R Yuce and Chee Keong Ho. Implementation of body area networks based on mics/wmts medical bands for healthcare systems. In *2008 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 3417–3421. IEEE, 2008.
- [97] Ashutosh Ghildiyal, Karima Amara, Renzo Dal Molin, Balwant Godara, Amara Amara, and RK Shevgaonkar. Uwb for in-body medical implants: A viable option. In *2010 IEEE International Conference on Ultra-Wideband*, volume 2, pages 1–4. IEEE, 2010.
- [98] Microwave Studio. Cst-computer simulation technology. *Bad Nuheimer Str*, 19:64289, 2008.
- [99] ANSYS. HFSS Electromagnetic Simulation Software. <https://www.ansys.com/products/electronics/ansys-hfss>, 1994. [Online; accessed 20-11-2018].

-
- [100] Feko electromagnetic simulation software. <https://altairhyperworks.com/product/FEKO>, 2005. Accessed: 20-11-2018.
- [101] Xfdtd electromagnetic simulation software. <https://www.remcom.com/xfdd-3d-em-simulation-software>, 2000. Accessed: 20-11-2018.
- [102] Nina Petoussi-Henss, Maria Zankl, Ute Fill, and Dieter Regulla. The gs family of voxel phantoms. *Physics in Medicine & Biology*, 47(1):89, 2001.
- [103] Victor Spitzer, Michael J Ackerman, Ann L Scherzinger, and David Whitlock. The visible human male: a technical report. *Journal of the American Medical Informatics Association*, 3(2):118–130, Mar, 1996.
- [104] Michael J Ackerman. The visible human project. *Proceedings of the IEEE*, 86(3):504–511, Mar, 1998.
- [105] Camelia Gabriel. Compilation of the dielectric properties of body tissues at rf and microwave frequencies. Technical report, KING’S COLL LONDON (UNITED KINGDOM) DEPT OF PHYSICS, Jun, 1996.
- [106] David Tse and Pramod Viswanath. *Fundamentals of wireless communication*. Cambridge university press, 2005.
- [107] Claude E Shannon. A mathematical theory of communication. *Bell system technical journal*, 27(3):379–423, 1948.
- [108] David JC MacKay and David JC Mac Kay. *Information theory, inference and learning algorithms*. Cambridge university press, 2003.
- [109] Kamran Sayrafian-Pour, Wen-Bin Yang, John Hagedorn, Judith Terrill, and Kamy Yekeh Yazdandoost. A statistical path loss model for medical implant communication channels. In *2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, pages 2995–2999. IEEE, Sep, 2009.
- [110] Igor Bjelaković, Holger Boche, and Jochen Sommerfeld. Secrecy results for compound wiretap channels. *Problems of Information Transmission*, 49(1):73–98, 2013.
- [111] Himanshu Tyagi and Alexander Vardy. Explicit capacity-achieving coding scheme for the gaussian wiretap channel. In *2014 IEEE International Symposium on Information Theory*, pages 956–960. IEEE, 2014.

- [112] Li Huguét. Coding scheme for a wire-tap channel using regular codes. *Discrete mathematics*, 56(2-3):191–201, 1985.
- [113] Demijan Klinc, Jeongseok Ha, Steven W McLaughlin, Joao Barros, and Byung-Jae Kwak. Ldpc codes for the gaussian wiretap channel. *IEEE Transactions on Information Forensics and Security*, 6(3):532–540, 2011.
- [114] Yi-Peng Wei and Sennur Ulukus. Polar coding for the general wiretap channel. In *2015 IEEE Information Theory Workshop (ITW)*, pages 1–5. IEEE, 2015.
- [115] Frédérique Oggier, Patrick Solé, and Jean-Claude Belfiore. Lattice codes for the wiretap gaussian channel: Construction and analysis. *IEEE Transactions on Information Theory*, 62(10):5690–5708, 2015.
- [116] James L Massey. A simplified treatment on wyner’s wiretap channel. In *Proc. 21st Allerton Conf. on Comm., Control and Computing, 1983*, pages 268–276, 1983.
- [117] Pritam Bose, Ali Khaleghi, Mohammad Albatat, Jacob Bergsland, and Ilanko Balasingham. Rf channel modeling for implant to implant communication and implant to sub-cutaneous implant communication for future leadless cardiac pacemakers. *IEEE Transactions on Biomedical Engineering*, Mar, 2018.
- [118] Tao Wang, Yao Liu, and Athanasios V Vasilakos. Survey on channel reciprocity based key establishment techniques for wireless systems. *Wireless Networks*, 21(6):1835–1846, 2015.
- [119] Duygu Karaođlan Altop, Albert Levi, and Volkan Tuzcu. Towards using physiological signals as cryptographic keys in body area networks. In *2015 9th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth)*, pages 92–99. IEEE, 2015.
- [120] Duygu Karaođlan Altop, Albert Levi, and Volkan Tuzcu. Deriving cryptographic keys from physiological signals. *Pervasive and Mobile Computing*, 39:65–79, 2017.
- [121] Theodore S Rappaport et al. *Wireless communications: principles and practice*, volume 2. prentice hall PTR New Jersey, 1996.
- [122] Pål Anders Floor, Raúl Chávez-Santiago, Anna N Kim, Kimmo Kansanen, Tor A Ramstad, and Ilanko Balasingham. Communication aspects for a measurement based uwb in-body to on-body channel. *IEEE Access*, 7:29425–29440, 2019.

- [123] Hooman Sedghamiz and Daniele Santonocito. Unsupervised detection and classification of motor unit action potentials in intramuscular electromyography signals. In *2015 e-health and bioengineering conference (ehb)*, pages 1–6. IEEE, 2015.
- [124] Jiapu Pan and Willis J Tompkins. A real-time qrs detection algorithm. *IEEE Trans. Biomed. Eng.*, 32(3):230–236, 1985.

Part II

Articles

Appendix A

Estimating Eavesdropping Risk

Paper A: Estimating Eavesdropping Risk for Next Generation
Implants

Muhammad Faheem Awan and Kimmo Kansanen

Advances in Body Area Networks I

This article is not included due to copyright

Appendix B

Evaluation of Secrecy Capacity with Phantom Experiments in ISM 2.4 GHz

Paper B: Experimental Phantom-based Evaluation of Physical
Layer Security for Future Leadless Cardiac Pacemaker
Muhammad Faheem Awan, Sofia Perez-Simbor, Concepcion Garcia-Pardo,
Kimmo Kansanen, Pritam Bose, Sergio Castello-Palacios and Narcis Cardona
*2018 IEEE 29th Annual International Symposium on Personal, Indoor and
Mobile Radio Communications (PIMRC)*

This article is not included due to copyright

Appendix C

Distance Based One-dimensional Evaluation of Secrecy Capacity

Paper C: Experimental Phantom-Based Security Analysis for





Next-Generation Leadless Cardiac Pacemakers

Muhammad Faheem Awan, Sofia Perez-Simbor, Concepcion Garcia-Pardo,
Kimmo Kansanen, and Narcis Cardona

Sensors 2018

Article

Experimental Phantom-Based Security Analysis for Next-Generation Leadless Cardiac Pacemakers

Muhammad Faheem Awan ^{1,*}, Sofia Perez-Simbor ², Concepcion Garcia-Pardo ²,
Kimmo Kansanen ¹ and Narcis Cardona ²

¹ Department of Electronic Systems, Norwegian University of Science and Technology, NTNU, NO-7491 Trondheim, Norway; kimmo.kansanen@ntnu.no

² iTEAM, Universitat Politècnica de València, 46022 Valencia, Spain; sopresim@iteam.upv.es (S.P.-S.); cgpardo@iteam.upv.es (C.G.-P.); ncardona@iteam.upv.es (N.C.)

* Correspondence: faheem.awan@ntnu.no

Received: 31 October 2018; Accepted: 5 December 2018; Published: 7 December 2018



Abstract: With technological advancement, implanted medical devices can treat a wide range of chronic diseases such as cardiac arrhythmia, deafness, diabetes, etc. Cardiac pacemakers are used to maintain normal heart rhythms. The next generation of these pacemakers is expected to be completely wireless, providing new security threats. Thus, it is critical to secure pacemaker transmissions between legitimate nodes from a third party or an eavesdropper. This work estimates the eavesdropping risk and explores the potential of securing transmissions between leadless capsules inside the heart and the subcutaneous implant under the skin against external eavesdroppers by using physical-layer security methods. In this work, we perform phantom experiments to replicate the dielectric properties of the human heart, blood, and fat for channel modeling between in-body-to-in-body devices and from in-body-to-off-body scenario. These scenarios reflect the channel between legitimate nodes and that between a legitimate node and an eavesdropper. In our case, a legitimate node is a leadless cardiac pacemaker implanted in the right ventricle of a human heart transmitting to a legitimate receiver, which is a subcutaneous implant beneath the collar bone under the skin. In addition, a third party outside the body is trying to eavesdrop the communication. The measurements are performed for ultrawide band (UWB) and industrial, scientific, and medical (ISM) frequency bands. By using these channel models, we analyzed the risk of using the concept of outage probability and determine the eavesdropping range in the case of using UWB and ISM frequency bands. Furthermore, the probability of positive secrecy capacity is also determined, along with outage probability of a secrecy rate, which are the fundamental parameters in depicting the physical-layer security methods. Here, we show that path loss follows a log-normal distribution. In addition, for the ISM frequency band, the probability of successful eavesdropping for a data rate of 600 kbps (Electromyogram (EMG)) is about 97.68% at an eavesdropper distance of 1.3 m and approaches 28.13% at an eavesdropper distance of 4.2 m, whereas for UWB frequency band the eavesdropping risk approaches 0.2847% at an eavesdropper distance of 0.22 m. Furthermore, the probability of positive secrecy capacity is about 44.88% at eavesdropper distance of 0.12 m and approaches approximately 97% at an eavesdropper distance of 0.4 m for ISM frequency band, whereas for UWB, the same statistics are 96.84% at 0.12 m and 100% at 0.4 m. Moreover, the outage probability of secrecy capacity is also determined by using a fixed secrecy rate.

Keywords: implanted medical devices; wireless leadless cardiac pacemaker; WBAN; security and privacy; physical-layer security; phantom experiments; channel modeling

1. Introduction

Rapid development in personal health systems due to wireless body area networks (WBAN) has resulted in a number of implantable and wearable medical devices. These on-body and in-body wireless medical devices continuously monitor different physiological conditions and provide proper diagnosis and treatment. Notable among these devices are cardiac pacemakers and implanted cardiac defibrillators (ICDs).

Pacemakers are used to treat different types of cardiac arrhythmias. Annually, there are about 0.7 million pacemaker implantations worldwide [1]. A pacemaker senses irregularities between heartbeats and provides proper actuation via electrodes, thus facilitating the proper functioning of human heart. Currently these pacemakers are mostly implanted with wired connection between subcutaneous implants and electrodes in right ventricle and right atrium of the human heart. The next generation of these pacemakers is expected to be wireless between subcutaneous implants and electrodes (EU Horizon 2020 Project WiBEC'' Wireless In-Body Environment) [2]. The only currently available leadless pacemaker on the market is Medtronic's Micra [3], which is an autonomous leadless pacemaker implanted in the right ventricle of a human heart, whereas our project focuses on multi-nodal leadless pacemakers with subcutaneous implant. Our work focuses on the analysis of the eavesdropping risk and secrecy rate between a node implanted in the right ventricle and another node as subcutaneous implanted, but it can be applicable to other scenarios for in-body communications. These scenarios may include communication between nodes within a heart.

The wireless nature of modern implanted medical devices (IMDs) is a significant source of security risks. It makes an IMD more visible and can allow an eavesdropper to listen. Thus, an insecure communication channel makes it easier for an eavesdropper to perform attacks on an implant similar to attacks on other computing devices. Successful eavesdropping may result in the retrieval of patient information (medical and non-medical) or performing attacks such as data forging or altering. In addition, it may enable the modification of the implant configuration without the knowledge of the patient or physician.

The aim of this work is to estimate the channel models for legitimate and eavesdropper links by phantom experiments. Estimated channel models are then used to determine the eavesdropping risk in respective bands along with providing information regarding theoretical secrecy analysis i.e., the availability of the secure channel based on secrecy capacity, which can be directly applied, without any leakage of information to the eavesdropper. We focus on the communication between the leadless cardiac pacemaker (LCP) and subcutaneous implant in frequencies from 1.7–2.5 GHz (ISM band) and 3.1–5.1 GHz (UWB). We develop path-loss models for an in-body-to-in-body (IB2IB) scenario (a legitimate link between the leadless pacemaker in the right ventricle of the human heart and the subcutaneous implant under the skin below the shoulder) and an in-body-to-off-body (IB2OFF) scenario (eavesdropper link between the leadless pacemaker and the eavesdropper outside the body). All results are provided for ultrawide band (UWB) and industrial, scientific, and medical (ISM) frequency bands, and comparison is provided where applicable. Our key contributions in this paper are:

- Single and multilayer phantoms for heart muscle, fat, and blood are developed for respective frequency bands.
- Channel modeling of both legitimate link (IB2IB) and eavesdropper link (IB2OFF).
- Comparison of channel models obtained from measurements performed with different phantoms.
- Probability of successful eavesdropping with respect to eavesdropper distance.
- Secrecy capacity analysis and evaluation of the probability of positive secrecy capacity.
- Design principles or privacy by design where outage probability of a secure rate is determined.

The rest of the paper is organized as follows. Section 2 provides background and problem description, followed by measurement setup in Section 3. Section 4 provides channel models based

on measurements. Secrecy analysis including eavesdropping risk and positive secrecy capacity is provided in Sections 5 and 6. Section 7 discusses the results and Section 8 concludes the work.

2. Background & Problem Description

2.1. Background

The work of Halperin et al. [4] is considered to be the pioneer work in security analysis of IMDs, followed by different research activities providing security for IMD devices [5]. Most of the research is focused on mitigating the security risks via providing different encryption mechanisms to protect data between a sender and legitimate nodes [6–8]. In conventional wireless networks, security is considered to be an independent feature with no or little connection to other tasks of a communication network. State-of-the-art encryption algorithms are developed for such purposes and are implemented and studied via cryptographic algorithms (e.g., RSA, AES, DES etc.) [9,10]. These methods rely on the limited computational power of an eavesdropper and require proper key management servers for implementation, which cannot be the case for tiny IMDs. In addition, the computational complexity is also higher because of data encryption with the key.

An alternative could be to offer secure communication via information theoretic measures or physical-layer security. The concept of information theoretic security was first introduced by Shannon [11], which was further extended by Wyner [12] with introduction to the wiretap channel. The idea behind information theoretic security is to limit the leakage of information to an eavesdropper. A secure communication channel by information theoretic measures can be achieved in two different ways: one is to secure communication without keys, and can be referred to as keyless security, whereas the other is to secure communication with keys. Keyless security can be achieved using appropriate coding schemes with the aid of secrecy capacity [13,14]. Secrecy capacity is the maximum attainable communication rate without leakage of information to an eavesdropper. The second method uses random channel characteristics, e.g., received signal strength (RSS), phase or channel state information (CSI), to generate a key on the physical layer for data encryption. The key-generation methods rely on channel reciprocity. A good deal of research is devoted to key generation using channel reciprocity [15–19].

The focal point of information theoretic security or physical-layer security is using the characteristics of wireless channels. If one can estimate the wireless channels between legitimate nodes and eavesdropper, then the secure rate for communication can be determined. Thus, to provide physical-layer security using the keyless security method, the essential part is to predict the legitimate and eavesdropper channels. The channel characteristics can be achieved by measuring the channel transfer functions of the legitimate and eavesdropper link. In addition, it can help determine the channel capacities, respectively. If the eavesdropper channel's signal-to-noise ratio (SNR) is lower than that of the legitimate channel, then the difference between the link capacities provides the secrecy capacity for communication. Furthermore, secrecy capacity is the maximum achievable transmission rate keeping eavesdropper uncertainty about the source message to maximum. To determine the secrecy capacity of a system, the knowledge about channels between the legitimate link and the eavesdropper link is required.

Channel characterizations are usually done by software simulations and experimental measurements that include in vivo and phantom experiments. It is difficult to simulate these channels in practice using in vivo experiments because of moral, ethical, and physical integrity reasons. Similarly, software simulations are computationally very costly and requires a good deal of time. A cheap and better alternative is to characterize human body channels via phantom experiments [20]. Phantoms are chemical mixtures that can be used to mimic the electromagnetic behavior of different human body parts provided by Gabriel [21]. From phantom experiments, the amount of data gathered is of considerable size compared to that of in vivo and software simulations, and can lead to better estimation of channels.

In Wireless Body Area Network (WBAN) standard IEEE 802.15.6, Medical Implant Communication System (MICS) frequency band is allocated for implant-to-implant communication that spans 402–405 MHz. Literature is also available on channel modelling in other frequency bands using phantom experiments for in-body nodes [22–26]. In [27], the off-body-to-in-body mathematical model based on software simulations is also provided for the propagation of electromagnetic waves through various tissues/layers by considering reflections from different layers. In our work, we opt for phantom experiments to measure the channels because of less complexity and ease of use, considering the random angles of both the receivers (legitimate receiver and eavesdropper). We focus on ISM and UWB. These frequency bands are under study for implant communications due to prospects such as high data rate and smaller antenna dimensions.

2.2. Problem Description

The real-world scenario which we want to replicate using phantom experiments is shown in Figure 1. Our system includes a LCP inside the right ventricle of a human heart that communicates with a subcutaneous implant whereas an eavesdropper wants to eavesdrop the communication outside the body. Thus, for security analysis, first we determine the channel models for legitimate and eavesdropper links using phantom experiments in both ISM and UWB frequency bands. We consider a transmission of a sounding signal in the respective bands using vector analyzer (VNA), through different mediums that constitute heart muscle, blood, and fat, emulated as phantoms. Different antennas are used to replicate a leadless pacemaker in right ventricle, a subcutaneous implant, and an eavesdropper. Moreover, the antennas used for ISM and UWB frequency bands are also different. Afterwards these channel models are used to predict the eavesdropping risk and secrecy capacity analysis. In this paper, the link between a pacemaker and the subcutaneous implant is referred to as a legitimate link or in-body-to-in-body (IB2IB) link, whereas the link between pacemaker and eavesdropper is referred as the eavesdropper link or in-body-to-off-body (IB2OFF) link. In addition, we assume that the eavesdropper is of a passive nature and the legitimate nodes are authenticated by some authentication protocol.

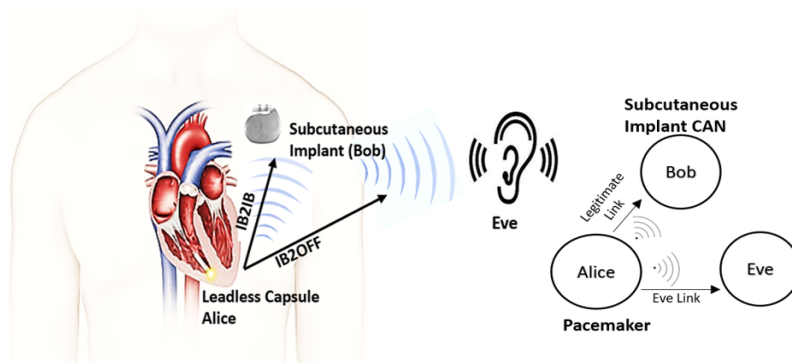


Figure 1. System Model.

3. Measurement Setup

The setup used for measuring the legitimate and eavesdropper channel is shown in Figure 2. It contains an anechoic chamber, a Vector Network Analyzer (VNA), a 3D spatial positioner, a phantom container, and a magnetic tracker. The anechoic chamber is used to reduce the surrounding environmental contributions, the magnetic tracker measures the distance between transmitter and receiver antenna at different measuring points, whereas the positioner is used to precisely move an antenna to different measuring points. The VNA is controlled via a laptop with software that performs initial calibration of components before measurement and configures all the devices.

First, it is calibrated with *Rosenberger calibration kit RPC-3.50* to remove the losses due to coaxial cables. Afterwards, it automatically measures the coupling between antennas at the specified grid points. The phantom temperature is maintained at 24 °C because of the variation in permittivity due to temperature change. The phantoms are developed to emulate at room temperature (24 °C), the electromagnetic properties of the human body at 37 °C provided by Gabriel in [21]. More details about the anechoic chamber and measurement setup can be found in [26]. Table 1, shows the set of parameters used for ISM and UWB frequency-band measurements. When everything is in place, before starting automatic measurements across different grid points, the anechoic chamber is closed from the front to keep it completely concealed from outdoor surroundings.

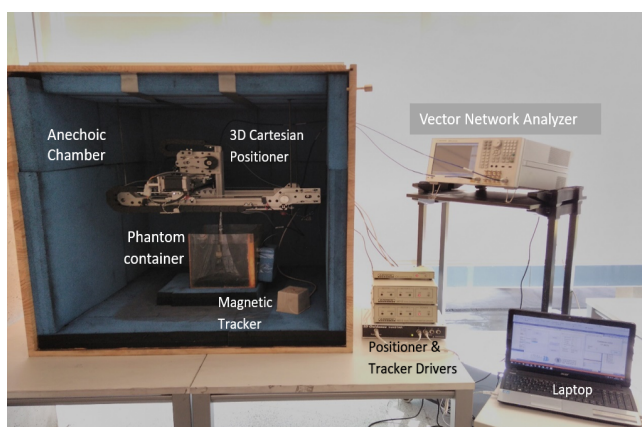


Figure 2. Measurement Setup.

Table 1. Setup parameters.

Band	ISM	UWB
Phantom	Heart muscle, blood & Fat	Heart muscle, blood & Fat
Frequency range	1.7–2.5 GHz	3.1–5.1 GHz
Resolution points	1601	1601
Resolution Frequency	0.5 MHz	1.25 MHz
Intermediate Frequency	3 KHz	3 KHz
Output power	8 dBm	8 dBm
Snapshots per position	Ns = 5	Ns = 5

3.1. Phantom Composition and Antenna Description

In phantom-based experiments, a container is filled with liquid phantom that mimics the dielectric properties of a required human tissue/body organ. Considering our real-world scenario, the phantoms that depict the dielectric properties of a human heart, fat, and blood are developed. The dielectric properties of a human body vary in frequency, resulting in different compositions of phantoms for different frequency bands. First, the phantom formation for the ISM frequency band is presented along with antennas used. Then, the UWB frequency band will follow.

3.1.1. ISM Band

ISM band is a common band to be employed in medical environments due to being license free. We develop phantoms with dielectric properties of a human heart, fat, and blood. Figure 3 shows the dielectric properties of a replicated phantom with its counterpart reported in [21], widely used in literature. A good approximation of dielectric properties of heart muscle, fat, and blood is observed

around 2 GHz. A single-layer phantom consists of only heart muscle which is composed of 39.2% sugar with the remainder water [28]. Multilayer phantom includes heart muscle, blood, and fat. The fat phantom is composed of 86% of oil in water where 1% of TX-100 was used as surfactant [29]. The blood phantom is composed of 40% acetonitrile and 1.25% NaCl [30] in water.

For ISM band measurements, we used three sets of antennas to perform our measurement campaign. An in-body antenna (transmitter) that replicates the leadless pacemaker transmission, a subcutaneous antenna (legitimate receiver) that is used as a subcutaneous implant, and an external antenna (eve antenna) that replicates an eavesdropper link. Figure 4 shows reflection coefficients of the antennas. The reflection coefficients show good matching among all the antennas around 2 GHz. The antennas used are directional and provided in Figure 5. More details on antennas can be found in [31].

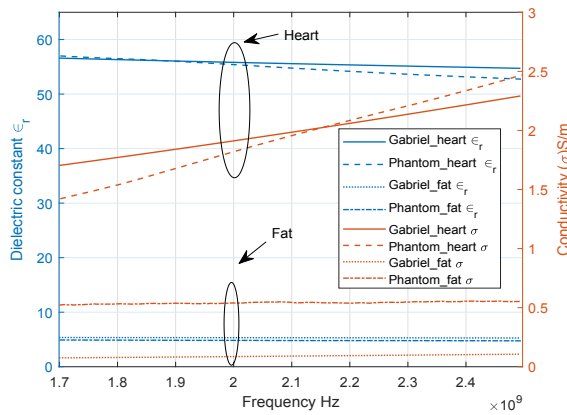


Figure 3. Dielectric Properties of ISM Phantom.

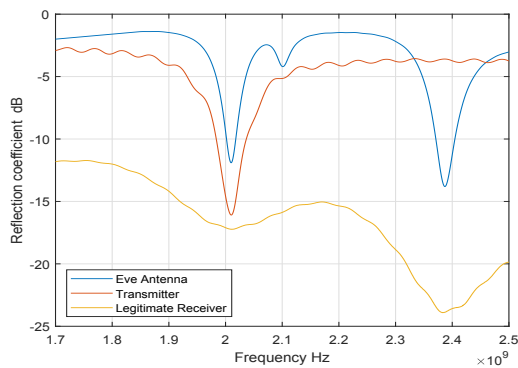


Figure 4. Reflection coefficients for Legitimate and Eavesdropper antennas (ISM).

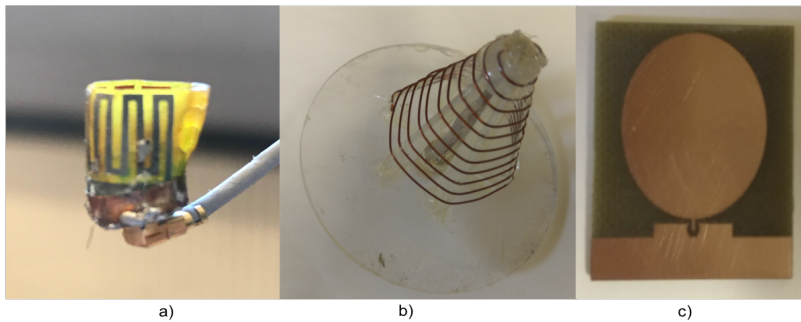


Figure 5. ISM band antennas (a) Transmitter (b) Eve antenna (c) legitimate Receiver.

3.1.2. UWB Frequency Band

We develop phantoms that mimic the dielectric properties of human heart muscle, blood, and fat in the UWB frequency band. Figure 6, shows the dielectric properties of the replicated phantoms. For the UWB band, the heart phantom is composed of 54.2% acetonitrile and 1.07% salt in water [32]. Similarly, fat and blood phantom is altered to fit for UWB frequency band.

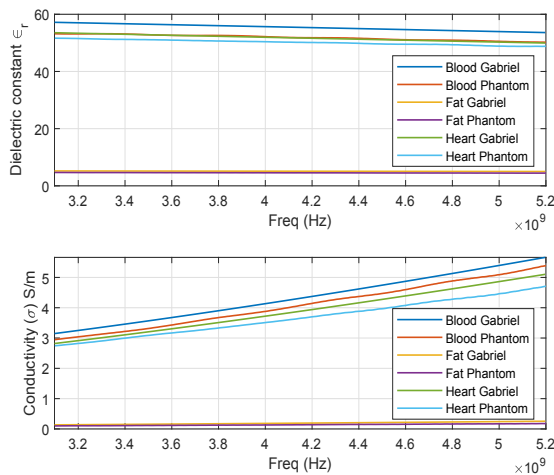


Figure 6. Dielectric Properties of UWB Phantom.

Three sets of UWB antennas are used, similar to the ISM band, one implanted (Transmitter), one subcutaneous (legitimate receiver) and one external antenna (eve antenna). Figure 7 shows the antennas used. Figure 7b is the transmitter antenna and a similar antenna is used as the legitimate receiver. The transmitter and legitimate receiver have dimensions of 2.3×2 cm² whereas the eve antenna dimensions are 5×4.4 cm². All the antennas have a quasi-omnidirectional radiation pattern. More details on the antennas are provided in [33,34]. Figure 8 shows the S-parameters of the antennas. All the antennas have transmission parameters of less than -10 dB, which is considered to be a very efficient transmission parameter.

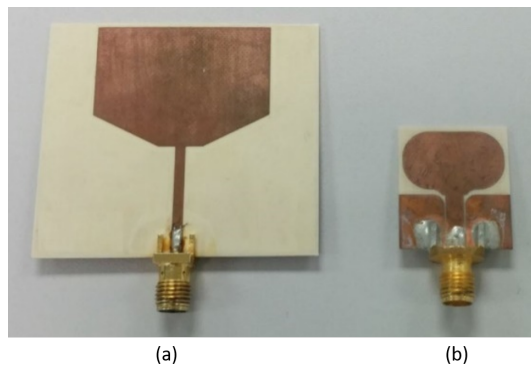


Figure 7. UWB antennas (a) Eve Antenna (b) Transmitter and Legitimate receiver.

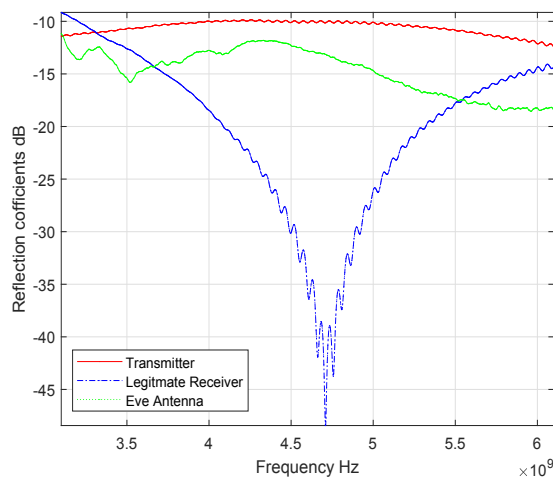


Figure 8. S-parameters of UWB antennas.

4. Measured Channel Models

In this section, using the measurement setup, the IB2IB and IB2OFF channel models are determined for the ISM and UWB frequency bands.

As mentioned earlier, the phantoms prepared are different for different frequency bands. Therefore, while conducting the experiments for ISM and UWB frequency band, phantoms and antennas are replaced. First, we used a single-layer phantom that contains only heart muscle for ISM and perform the IB2IB and IB2OFF measurements. Then we added the fat layer and repeated the measurements. Once the results are analyzed, a small difference in results with and without fat is observed. Considering this fact, for UWB frequency band instead of using only heart muscle, we performed experiments directly with heart muscle and fat layer for IB2IB and IB2OFF measurements and afterwards the blood layer is added (We wanted to use blood for ISM experiments as well, but the antenna was broken while performing that experiment due to which the path loss containing blood phantom for ISM band is not presented).

The measurements for legitimate link (IB2IB) are performed by implanting a transmitter antenna inside the liquid phantom, whereas the subcutaneous antenna or legitimate receiver is mounted on the wall of the container (subcutaneous). In the case of the fat layer, the subcutaneous antenna is placed inside the fat layer as shown in Figure 9. Furthermore, for legitimate link measurements, the implanted

antenna (transmitter) is moved in different grid points along the x, y and z axis with a step size of $\Delta x, \Delta y$ & Δz with total grid points of (N_x, N_y, N_z) as shown in Figure 10. For eavesdropper link measurement, the implanted antenna (transmitter) is fixed at a certain implant depth and eve antenna is moved across different grid points outside the phantom container to replicate different eavesdropper positions. In addition, for each measuring point, five snapshots are taken and then averaged to enhance the SNR. We would like to highlight the fact that the entire experiment takes around three weeks.

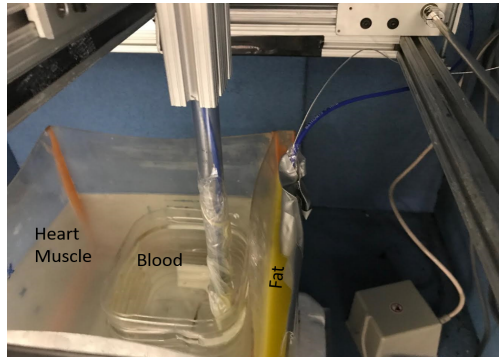


Figure 9. Multilayer phantom container inside anechoic chamber.

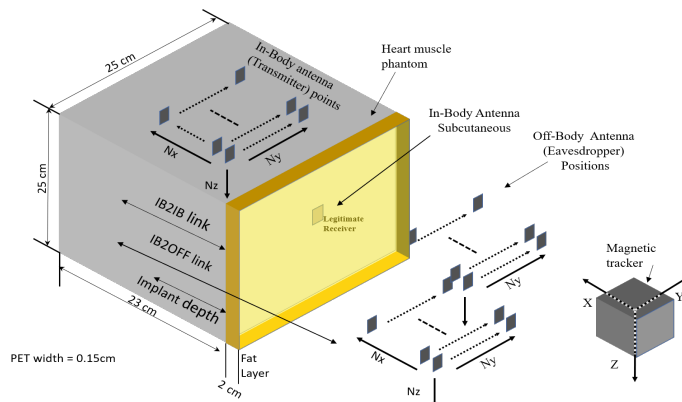


Figure 10. Measurement Grid points.

4.1. Path-Loss Models

From the measurements, we obtain the channel transfer functions, which help in determining the path loss for single-layer (heart muscle) and multilayer phantoms (fat + heart + blood) in both frequency bands. We measured the forward transmission coefficient S_{21} for N resolution points (see Table 1); the path loss per spatial position can be expressed as,

$$PL_i(dB) = |h_i|^2 = 10 \times \log_{10} \left(\sum_{k=N} \frac{|H(f_j)_k|^2}{N} \right), \quad (1)$$

$i \in (r, e)$
 $j \in (ISM, UWB)$

$H(f_j) = |S_{21}|e^{-j\angle S_{21}}$, where $|S_{21}|$ and $\angle S_{21}$ are module and phase of transmission coefficient. “ i ” represents legitimate link (r) and eavesdropper link (e). Similarly, “ j ” represents the frequency band ($j = \text{ISM or UWB}$).

4.1.1. ISM Band

4.1.1.1. IB2IB or Legitimate Link

For the legitimate link, the receiver antenna is mounted on the inner surface of the container’s wall for a single-layer phantom that contains only heart muscle, and the transmitting antenna is moved in different grid points inside the phantom (Figure 10). A leadless pacemaker is considered to be an implanted antenna whereas an antenna fixed on the wall of a container is considered to be a subcutaneous implant. The measured frequency band is 1.7 GHz to 2.5 GHz for the ISM band, but we only take the narrowband part in which the transmitter’s S_{11} is below -6 dB. Thus, only those measurements of S_{21} , for which the S_{11} reflection coefficient is below -6 dB, are taken into account. The resulting measured frequency band is 1.946–2.072 GHz as can be seen in Figure 4. The obtained path loss can be modeled as a distance-dependent logarithmic function and can be expressed as

$$PL_{dB} = PL_{d_0} + 10 \times n \times \log_{10}\left(\frac{d}{d_0}\right) + \mathcal{N}(\mu, \sigma) \quad (2)$$

where, $d_0 = 4$ cm, $PL_{d_0} = 22.9284$ dB, $n = 4.12$ and $\mathcal{N}(\mu, \sigma) = (-3.42 \times 10^{-15}, 7.3002) \approx (0, 7.3002)$. This model is valid for legitimate link distances from 2.7–12 cm. The observed randomness is because of measurements at different angles from the transmitting antenna. For a 2-layer phantom, we fill the portion of the container with a fat layer (Figure 9 except blood layer) and mounted the subcutaneous antenna in the fat layer. We determined the path-loss model, similar to (2). The parameters are $d_0 = 4$ cm, $PL_{d_0} = 21.85$ dB, $n = 4.12$ and $\mathcal{N}(\mu, \sigma) = (-4.6 \times 10^{-16}, 4.5) \approx (0, 4.5)$. Figure 11 shows the path-loss models both for single-layer and multilayer phantoms together, in which dots are path-loss measurements and the lines are the fitted model. It can be seen that because of the low value of fat dielectric constant, it does not greatly change the path loss model.

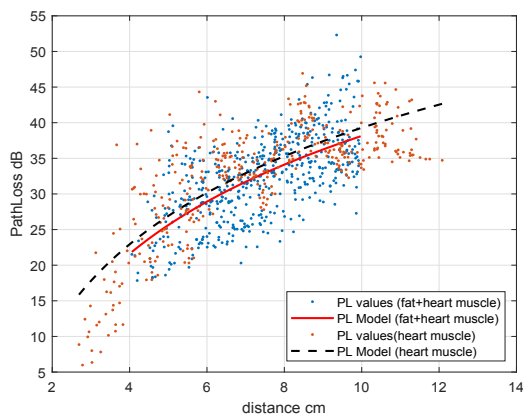


Figure 11. Path-loss legitimate link (IB2IB, ISM).

4.1.1.2. IB2OFF or Eavesdropper Link

As we noticed a slight difference in path-loss model with and without fat layer for IB2OFF measurements, we used the single-layer phantom (heart muscle). To find the path loss for the off-body link, we fixed the implanted antenna inside the heart phantom at an implant depth of 11.5 cm and moved the external antenna along the grid points as shown in Figure 10. This replicates the scenario

where the leadless pacemaker is implanted at a depth of 11.5 cm inside the body, transmitting to a subcutaneous implant and an eavesdropper outside the body trying to eavesdrop the communication. Similarly to IB2IB, we take S_{21} measurements for narrowband where matching occurs. The path-loss model obtained can be expressed in terms of distance-dependent logarithmic function (2) and the parameters are $d_0 = 17.45$ cm, $PL_{d_0} = 46.97$ dB, $n = 3.352$ and $\mathcal{N}(\mu, \sigma) = (-1.17 \times 10^{-15}, 4.40235) \approx (0, 4.40235)$. Figure 12 shows the path-loss model for mentioned implant depth. This path-loss model is valid for a distance range of 17.5–40 cm. After 40 cm, a free-space path-loss model can be applied.

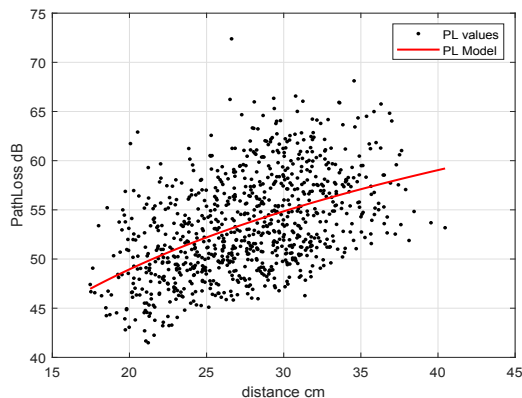


Figure 12. Path-loss eavesdropper link (IB2OFF, ISM).

4.1.2. UWB Band

4.1.2.1. IB2IB or Legitimate Link

For the UWB frequency band, first, an experiment with a heart muscle and fat layer is performed which is then followed by the blood phantom. To find the IB2IB path-loss model, we fixed an in-body antenna (subcutaneous) in the fat layer and move another in-body antenna to different grid points. Figure 9 shows the placement scenario inside an anechoic chamber. The path-loss model parameters for the IB2IB scenario containing all three phantom layers (heart muscle, blood, and fat) are $d_0 = 4$ cm, $PL_{d_0} = 59.54$ dB, $n = 3.7284$ and $\mathcal{N}(\mu, \sigma) = (-1.445 \times 10^{-14}, 1.9675) \approx (0, 1.9675)$. This path-loss model is valid for distances of 1 cm–10 cm. Similarly the parameters for 2-layer phantom (heart muscle and fat), $d_0 = 4$ cm, $PL_{d_0} = 54.1830$ dB, $n = 3.37$ and $\mathcal{N}(\mu, \sigma) = (-2.8442 \times 10^{-16}, 1.5301) \approx (0, 1.5301)$. Figure 13 shows the path-loss model with and without blood. A difference of about 5 dB is observed in experiments with and without blood.

4.1.2.2. IB2OFF or Eavesdropper Link

For IB2OFF, we measured the channel only by considering fat and heart muscle. This is because from an eavesdropping perspective the path loss without blood will be the best-case scenario and worst-case scenario for the leadless capsule. However, if we want to have path loss with blood, at each measuring point 5 dB of loss must be added.

We fixed an in-body antenna at an implant depth of 7 cm and then moved the off-body antenna to different points. Figure 14 shows the path-loss model of the off-body scenario. The parameters in terms of log distance model are $d_0 = 10$ cm, $PL_{d_0} = 72.24$ dB, $n = 2.67$ and $\mathcal{N}(\mu, \sigma) = (-1.1627 \times 10^{-15}, 1.6328) \approx (0, 1.6328)$. In the case of UWB, the IB2OFF path-loss model is valid for 10–27 cm, whereas beyond 27 cm the free-space path-loss model can be applied.

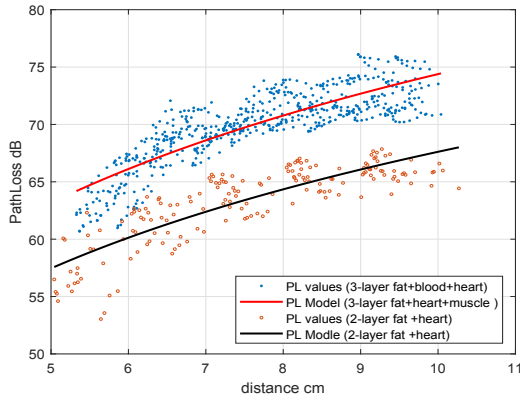


Figure 13. Path-loss legitimate link with and without blood (IB2IB, UWB).

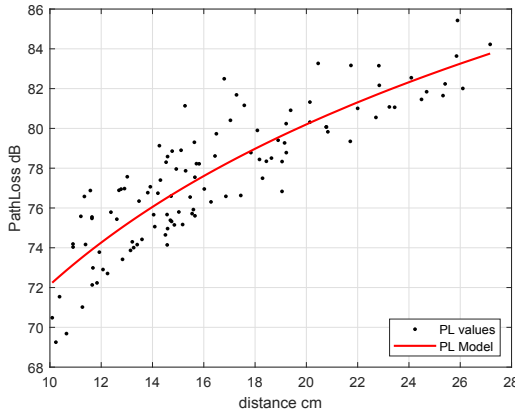


Figure 14. Path-loss Eve link without blood (IB2OFF UWB).

Table 2 provides summary and comparison of path-loss models for ISM and UWB frequency band.

Table 2. Summary of path-loss models.

Parameters	ISM Band			UWB Band		
	Legitimate Link (IB2IB)	Legitimate Link (IB2IB)	Eve Link (IB2OFF)	Legitimate Link (IB2IB)	Legitimate Link (IB2IB)	Eve Link (IB2OFF)
Layers	1	2	1	3	2	2
PL_{d_0} (dB)	22.92	21.85	46.97	59.54	54.138	72.24
n	4.12	4.12	3.352	3.7284	3.37	2.67
σ	7.3002	4.5	4.4023	1.9675	1.5301	1.6328
μ	0	0	0	0	0	0
d_0 (cm)	4	4	17.45	4	4	10
Distance Range (cm)	2.7–12	2.7–12	17.5–40	1–10	1–10	10–27

5. Estimating Eavesdropping Risk (Risk Analysis)

This section focuses on estimating eavesdropping risk for next-generation leadless pacemakers in the case of using ISM and UWB band for RF communication. As mentioned earlier, our system consists of an eavesdropper, an IMD and a subcutaneous node as shown in Figure 1. We consider implanted leadless capsules inside the right ventricle of a human heart. This leadless capsule transmits

un-encrypted data to the subcutaneous implant, where the eavesdropper tries to eavesdrop the communication. In case of IMDs, Eve can be categorized as

- An eavesdropper, where eavesdropping legitimate transmission can be an active or passive node.
- A possibility of single eavesdropper, or part of a well-organized group.
- An external intruder, but there can be the case where an eavesdropper is from inside the system e.g., physician, hospital administration, equipment manufacturers etc., because they have the benefit of being close to patient.

It can be seen that each eavesdropper may have different intentions or goals. There may be the possibility that one eavesdrops just to get the private information of a patient or there may be a case where there is competition between manufacturers to obtain information on IMD equipment. An eavesdropper may have higher capabilities than that of legitimate nodes such as higher computational power, higher antenna gains, etc. In this work, we consider a single passive eavesdropper with the same capabilities as the legitimate node trying to eavesdrop the communication. We also consider a case where the eavesdropper has higher antenna gain.

5.1. Eavesdropper Model

In this section, the probability of successful eavesdropping (\mathcal{P}_{se}) is provided by considering the path-loss models depicted during our measurement campaign, both for UWB and the ISM frequency band. To find \mathcal{P}_{se} , we use an approach of channel capacity as a measure. Using channel capacity as a basis, for a given information rate (R), there exists a minimum received power to successfully decode the transmission based on a certain threshold SNR. Using this concept, the channel's capacity is expressed by Shannon capacity formula as

$$C = B \times \log_2(1 + \gamma_{th}) \quad (3)$$

where B is channel bandwidth, C is capacity and γ_{th} is the threshold SNR. To determine the threshold SNR required to support the information rate (R), (3) can be expressed as

$$\gamma_{th}(R) > 2^{\frac{R}{B}} - 1 \quad (4)$$

Thus, when SNR at the input of a receiver chain falls below certain threshold level [35], the communication can be termed as in outage and can be expressed as

$$\mathcal{P}_{out}(\gamma_{th}) = \mathcal{P}[\gamma < \gamma_{th}] \quad (5)$$

where γ is received SNR. Thus, we can say that when the link is an outage then the eavesdropper will not be able to eavesdrop the communication. Thus, an outage probability can be complemented in terms of probability of successful eavesdropping.

5.2. Probability of Successful Eavesdropping (\mathcal{P}_{se})

To find the probability of successful eavesdropping, received SNR is required, which can be achieved at a particular distance using the IB2OFF channel model, both for UWB and ISM frequency band Sections 4.1.1.2 and 4.1.2.2. The received SNR can be expressed as,

$$\gamma_{dB} = P_{t_{dBm}} - PL(d)_{dB} - N_o B_{dBm} \quad (6)$$

where, $N_o B$ is the noise power, P_t is transmit power and $PL(d)$ is the IB2OFF path loss at distance (d) (Eve distance). For a communication between legitimate nodes, the value of SNR (γ) should be greater than threshold, otherwise the communication link will be in outage. However, we want an eavesdropper link to be in outage. Using the concept of outage probability (5), we must take certain

cutoff thresholds represented by γ_{th} . The eavesdropper can eavesdrop communication with certain probability, when the SNR (γ) between the leadless capsule and eavesdropper is greater than the set cutoff threshold γ_{th} . i.e., $\gamma > \gamma_{th}$. The probability of successful eavesdropping can be expressed as,

$$\mathcal{P}_{se} = 1 - p_{out}(\gamma_{th}) \quad (7)$$

As SNR (γ) is log normally distributed (Table 2) with mean μ_γ and standard deviation σ_γ , we can express (7) by Q-function as

$$\mathcal{P}_{se} = 1 - \left(1 - Q \left(\frac{\gamma_{th_{dB}} - \mu_{\gamma_{dB}}}{\sigma_{\gamma_{dB}}} \right) \right) \quad (8)$$

$$\begin{aligned} \mathcal{P}_{se} &= Q \left(\frac{\gamma_{th} - \mu_\gamma}{\sigma_\gamma} \right), \\ \mathcal{P}_{se} &= 1 - \varphi \left(\frac{\gamma_{th} - \mu_\gamma}{\sigma_\gamma} \right), \\ \mathcal{P}_{se} &= 1 - \frac{1}{2} \left(1 + \operatorname{erf} \left(\frac{\gamma_{th} - \mu_\gamma}{\sigma_\gamma \sqrt{2}} \right) \right) \end{aligned} \quad (9)$$

The eavesdropper can increase the probability of successful eavesdropping by using high-gain antennas. An antenna with high gain has a reception from greater distances and has higher SNR. However, nothing comes without cost, and higher gain results from larger dimensions of antennas. Different antennas have different antenna gain and aperture relation but in general it can be expressed as

$$A_e = \frac{\lambda^2 G_e}{4\pi} \quad (10)$$

From the eavesdropper perspective, Eve wants to eavesdrop without noticing. However, with large aperture antennas it cannot happen easily. Therefore, the gain of an antenna cannot be increased above certain limits e.g., if we want to have an antenna gain of 20 dBi then the effective aperture of an antenna will be around 18 cm² (for frequency of 2 GHz) which cannot go unnoticed within the short distance of a patient.

5.2.1. \mathcal{P}_{se} for ISM and UWB Frequency Band

To find the eavesdropping risk, path loss at different eavesdropper distances is determined using (1) and the model parameters provided in Table 2 for an eavesdropper link. This helps determining the received SNR for fixed transmitted power. In addition, we also measured the receiver sensitivity for a bandwidth of 1 MHz, which is found to be -90 dBm. Furthermore, different information rates (R) are considered for communication between legitimate nodes, and determine corresponding cutoff thresholds by using (4). We assume the information rates that reflect the real-life application rates such as EMG, ECG, and pulse rate, that are listed in Table 3 [36]. Finally, using (9), we determine the probability of successful eavesdropping risk for a cardiac leadless pacemaker communicating to a subcutaneous implant. Figure 15 shows the probability of successful eavesdropping with varying eavesdropper distance for the ISM frequency band. We consider a channel bandwidth of 1 MHz. The probability of a successful eavesdropping for an information rate of 600 kbps (EMG) is about 97.68% at an eavesdropper distance of 1.3 m and approaches approx 28.13% at an eavesdropper distance of 4.2 m. Similarly, the eavesdropping risk for heart pulse is about 100% at 1.3 m and 4.2 m, whereas for ECG signal the risk is 99.68% at 1.3 m and 65.93% at 4.2 m. When the information rate goes up, the requirement for threshold SNR increases, resulting in lower eavesdropping probability. Similarly, the effect of an eavesdropper antenna is also considered which

shows that increase in eavesdropping risk occurs when the eavesdropper uses a high-gain antenna as shown in Figure 15, one without antenna gain and one with antenna gain of 4 dBi for information rate of medical image and electromyogram (EMG).

Table 3. IMD data traffic.

Sensing Parameter	Required Data Rate
Heart rate	1 sample/s or 600 bps
Medical image	1 Mbps
Blood pressure	1.2 kbps
EMG	600 kbps
EEG	4.2–32 kbps
ECG	250 kbps

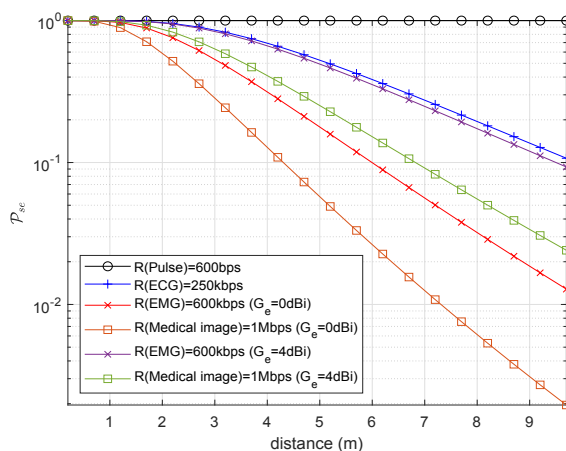


Figure 15. Probability of Successful eavesdropping w.r.t Eve Distance (ISM Band).

Furthermore, for the UWB frequency band, Figure 16 shows the probability of successful eavesdropping. Here it would be good to notify that we consider the path-loss model without blood because it would be the best-case scenario for an eavesdropper. Due to high losses in UWB, the eavesdropping risk is considerably less than the ISM band which is one of the advantages of using UWB for in-body networks along with high data rate capabilities. Figure 16 shows the \mathcal{P}_{se} on a per-MHz basis similar to ISM frequency band. Similarly, for an information rate of an EMG, the eavesdropping risk drops to 0.2847% at an eavesdropping distance of 0.22 m in the case of the UWB frequency band.

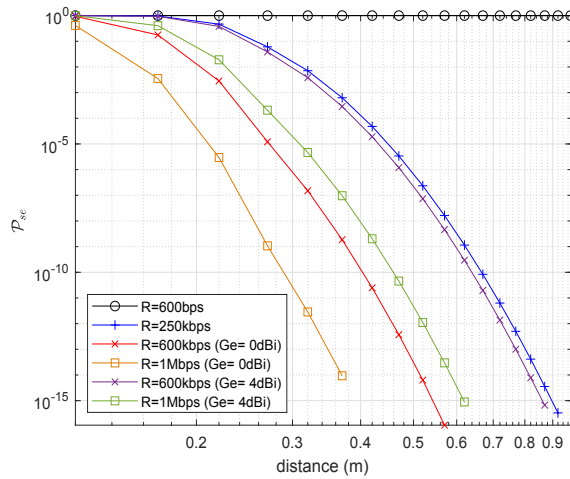


Figure 16. Probability of successful eavesdropping w.r.t Eve distance (UWB).

6. Secrecy Capacity Analysis

From risk analysis, it is evident to have some secure mechanisms to keep the pacemaker safe from an eavesdropper. As mentioned earlier, this section focuses on the potential of securing pacemakers using a physical-layer security method. Our intention is to use the keyless security method by using the concept of secrecy capacity and secure channel. We deal with exploring the availability of secrecy capacity by using the channel models obtained in Section 4.

Secrecy capacity is the maximum attainable communication rate between legitimate nodes without any leakage of information to the eavesdropper. Consider the wireless system depicted in Figure 1, where a leadless pacemaker communicates with a subcutaneous implant and the eavesdropper attempts to eavesdrop the communication, by recalling [37] for an additive Gaussian wiretap channel, where both channels are corrupted by Gaussian noise in a way that the eavesdropper channel is noisier than legitimate channel i.e., $W_e > W_r$. Then, the instantaneous secrecy capacity is given as,

$$C_s = C_r - C_e \quad (11)$$

where,

$$C_r = \frac{1}{2} \log_2(1 + \gamma_r) \quad (12)$$

is the instantaneous channel capacity of legitimate link and

$$C_e = \frac{1}{2} \log_2(1 + \gamma_e) \quad (13)$$

is the instantaneous channel capacity of eavesdropper link, which follows instantaneous secrecy capacity as,

$$C_s = \begin{cases} \left[\frac{1}{2} \log_2(1 + \gamma_r) - \frac{1}{2} \log_2(1 + \gamma_e) \right]^+, & \text{if } \gamma_r > \gamma_e. \\ 0, & \text{otherwise.} \end{cases} \quad (14)$$

γ_r is legitimate channel (IB2IB) SNR and γ_e is eavesdropper channel (IB2OFF) SNR. C_s is positive when $\gamma_r > \gamma_e$, which means that the legitimate nodes can communicate securely at that positive secrecy rate. Furthermore, SNR of each link can be expressed as

$$\gamma_i = \frac{P_t \times |h_i|^2}{W_i}, \quad i \in (r, e) \quad (15)$$

where, P_t is transmitted power, $|h_r|^2$, $|h_e|^2$ are channel gains of respective links and W is noise power. As we observed, the channel gains follow log-normal distribution. Thus, γ_r and γ_e will also follow the log-normal distribution at any measuring point with mean and standard deviation (μ_r, σ_r) and (μ_e, σ_e) , respectively. The fundamental parameters in the context of secrecy capacity are probability of positive secrecy capacity (\mathcal{P}_{pc_s}) and outage probability of secrecy capacity (OP_{c_s}). When the legitimate link SNR is better than the eavesdropper link, the secrecy capacity is positive and can be referred to as positive secrecy capacity. The outage probability of secrecy capacity is the probability of outage for certain fixed secrecy rate (R_s) with respect to eavesdropper distance. As γ_r and γ_e are mutually independent and log normally distributed, then for single realization of a legitimate channel and eavesdropper channel, the probability of positive secrecy capacity can be expressed as,

$$\mathcal{P}(C_s > 0) = \mathcal{P}(\gamma_r > \gamma_e) \quad (16)$$

To find OP_{c_s} and \mathcal{P}_{pc_s} together, if we consider a certain fixed secrecy rate (R_s) then the outage probability can be expressed as

$$\mathcal{P}(C_s < R_s) = 1 - \mathcal{P}(C_s > R_s) \quad (17)$$

Thus, by using definitions of probability,

$$\begin{aligned} \mathcal{P}(C_s > R_s) &= \mathcal{P}\left(\log_2\left(\frac{1 + \gamma_r}{1 + \gamma_e}\right) > R_s\right) \\ &= \mathcal{P}(\gamma_r > e^{R_s \ln 2}(1 + \gamma_e) - 1) \\ &= \int_0^\infty f_{\gamma_e}(\gamma_e) \left(\int_{e^{R_s \ln 2}(1 + \gamma_e) - 1}^\infty f_{\gamma_r}(\gamma_r) d\gamma_r \right) d\gamma_e \\ &= \int_0^\infty f_{\gamma_e}(\gamma_e) \left(1 - F_{\gamma_r}(e^{R_s \ln 2}(1 + \gamma_e) - 1) \right) d\gamma_e \\ &= 1 - \int_0^\infty f_{\gamma_e}(\gamma_e) F_{\gamma_r}(e^{R_s \ln 2}(1 + \gamma_e) - 1) d\gamma_e \\ &= e^{R_s \ln 2} \int_0^\infty F_{\gamma_e}(\gamma_e) f_{\gamma_r}(e^{R_s \ln 2}(1 + \gamma_e) - 1) d\gamma_e \end{aligned} \quad (18)$$

where,

$$F_{\gamma_r}(\gamma_r) = 1 - Q\left(\frac{\ln \gamma_r - \ln \mu_{\gamma_r}}{4a}\right) \quad (19)$$

$$F_{\gamma_e}(\gamma_e) = 1 - Q\left(\frac{\ln \gamma_e - \ln \mu_{\gamma_e}}{4b}\right) \quad (20)$$

$F_{\gamma_r}(\gamma_r)$ and $F_{\gamma_e}(\gamma_e)$ are cumulative distribution functions of γ_r and γ_e . In addition, where, $\ln E(\gamma_e)$ is the mean SNR of eavesdropper link and $\ln E(\gamma_r)$ is mean SNR for legitimate link (see Equation(15))

and $a = \frac{\sigma_r \ln 10}{40}$ and $b = \frac{\sigma_e \ln 10}{40}$, where σ_e is the channel deviation of eavesdropper link and σ_r is of legitimate link provided in Table 2. Substituting in (18)

$$\mathcal{P}(C_s > R_s) = \frac{e^{R_s \ln 2}}{4a\sqrt{2\pi}} \int_0^\infty \frac{1}{e^{R_s \ln 2}(1 + \gamma_e) - 1} \times \left(1 - Q\left(\frac{1}{4b} \ln \frac{\gamma_e}{\mu_{\gamma_e}}\right)\right) \times \exp\left(\frac{1}{2} \left(\frac{1}{4a} \ln\left(\frac{e^{R_s \ln 2}(1 + \gamma_e) - 1}{\mu_{\gamma_r}}\right)\right)^2\right) d\gamma_e \quad (21)$$

Equation (21) can be evaluated by numerical methods. The preposition obtained is

$$\mathcal{P}(C_s < R_s) = Q\left(\frac{\ln \frac{\mu_{\gamma_r}}{\mu_{\gamma_e}} + 8(b^2 - a^2) - R_s \ln 2}{4\sqrt{a^2 + b^2}}\right) \quad (22)$$

The proof of (22) is provided in [38] and for convenience also in Appendix A. For strictly positive secrecy capacity R_s is set to 0, Thus, (22) can be expressed as [38]

$$\mathcal{P}(C_s > 0) = 1 - Q\left(\frac{\ln \mu_{\gamma_e} - \ln \mu_{\gamma_r} + 8(b^2 - a^2)}{4\sqrt{a^2 + b^2}}\right) \quad (23)$$

Based on legitimate node and eavesdropper location, $\gamma_r \propto \frac{1}{d_r^\alpha}$ and $\gamma_e \propto \frac{1}{d_e^\alpha}$. Thus, if $d_e \gg d_r$ and $\gamma_r \gg \gamma_e$, then $\mathcal{P}(C_s > 0) \approx 1$. In our case scenario, the legitimate nodes are inside the body, whereas an eavesdropper is outside the body, due to which probability of secrecy capacity is depicted in near proximity of implanted devices.

6.1. Probability of Positive Secrecy Capacity (\mathcal{P}_{pc_s})

The probability of positive secrecy capacity for ISM and UWB frequency band is depicted in this section. By using (23), the probability of positive secrecy capacity for different legitimate distance against eavesdropper distance is plotted in Figure 17 for ISM and UWB frequency band. Two fixed distances for legitimate links are considered and for each distance, the probability of positive secrecy capacity is plotted against varying eavesdropping distance. Figure 17, shows that as the eavesdropping distance increases, probability of positive secrecy capacity approaches to one $\mathcal{P}(C_s > 0) \approx 1$. It also shows that if the eavesdropper is exactly at the same distance to that of the legitimate node i.e., 120 mm, there is still about 44.88% probability of positive secrecy capacity and it approaches approximately 97% at eavesdropping distance of 400 mm for an ISM frequency band whereas for UWB frequency band at the same legitimate distance i.e., 120 mm, \mathcal{P}_{pc_s} is about 96.84% and similarly approaches to 100% at eavesdropping distance of 400 mm. Thus, UWB frequency band has a higher probability of positive secrecy capacity at the same distance in comparison to the ISM frequency band. This is because of higher attenuation values in the UWB frequency band, which turns out to be a friend and not a foe, for secrecy purposes.

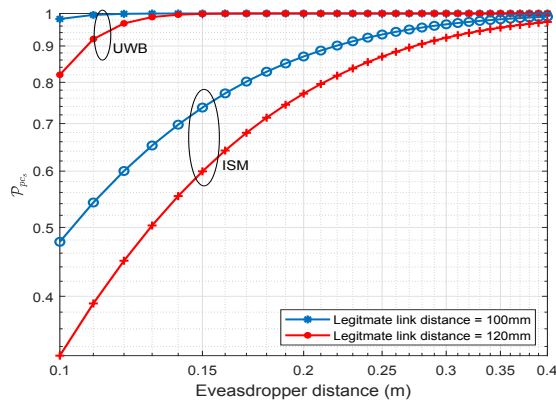


Figure 17. P_{pes} regarding legitimate link SNR.

6.2. Outage Probability of Secrecy Capacity (OP_{cs})

Similarly, if we consider certain fixed secrecy rate for our application, then we can determine the outage probability for the given secrecy rate. It is observed that by setting a secrecy rate (R_s) = 2 bps/Hz and legitimate distance of 120 mm, outage probability is about 80.81% at an eavesdropping distance of 120 mm, whereas at eavesdropping distance of 400 mm it falls to 11.12% for ISM frequency band as shown in Figure 18. For UWB frequency band, considering the same statistics, outage probability at an eavesdropping distance of 120 mm is about 78%, whereas for eavesdropping distance of 400 mm it falls to about $0.5 \times 10^{-6}\%$, which shows the rapid decay in outage probability of secrecy rate.

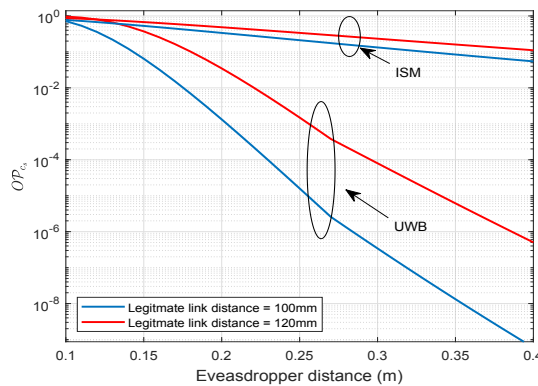


Figure 18. Outage probability of secrecy rate.

7. Discussions

In this section, we discuss the results and compare them for ISM and UWB frequency bands provided as contributions in Section 1. Our findings show that both IB2IB link and IB2OFF link in either case (ISM and UWB) follow the log-normal distribution, which can perfectly represent the real scenario of propagation through different body tissues, e.g., heart muscle, blood, and fat. It is evident that path loss in case of UWB frequency band is higher compared to the ISM band due to which the outage probability of link is also high, resulting in lower cases for eavesdropping. The probability of successful eavesdropping for an information rate of 600 kbps (EMG) is about 97% at an eavesdropping distance of 1.2 m and approaches to approximately 28% at an eavesdropping distance of 4.2 m. For similar

rate, the eavesdropping risk drops to 0.2847% at an eavesdropping distance of 0.22 m in case of UWB frequency band.

Similarly, for secrecy capacity analysis where both the links (IB2IB and IB2OFF) play roles, then in the case of UWB the probability of positive secrecy capacity is about 100% at an eavesdropping distance of 200 mm, considering the distance between legitimate nodes to be 120 mm, whereas for a similar scenario, considering ISM band the probability of positive secrecy capacity is about 76%. In addition, if we consider a certain fix secrecy rate $R_s = 2$ bps/Hz, then for UWB band the outage probability is about 3.4%, whereas for ISM band is about 48.53%, considering the distance between legitimate nodes to be 120 mm.

In fact, UWB has many advantages, including high bandwidth, high data rate, and continuous hopping to make it resilient to interference. In addition, UWB is also considered to be more secure. To eavesdrop in case of UWB is like tracking a person who changes clothes continuously while running at very high speeds. Considering our application of a cardiac leadless pacemaker, very little bandwidth and data rate is required, due to which transmission in an ISM band is more feasible. Furthermore, it is analyzed that the positive secrecy capacity still can be achieved, even when the eavesdropper is as close as 12 to 15 cm from an implanted node. It is been found that even if the eavesdropper is exactly the same distance as an implanted node to which the leadless capsule is transmitting, the probability of positive secrecy capacity is still about 45% and approaches approximately 97% at eavesdropping distance of 40 cm for the ISM band, whereas for UWB the stats are 96% and 100% at 40 cm. With the advent of positive secrecy capacity, Gaussian wiretap codes or LDPC codes can be used to achieve this secrecy rate.

The channel is considered to be secure if the transmissions are done on a secrecy rate. This physical-layer security (PLS) method can also be used along with conventional encryption algorithms on higher layers. If the secure channel rate is low, only encryption keys from higher layers can be shared over available low-rate secure channels, whereas encrypted data communications follows afterwards.

8. Conclusions

This work analyzes the eavesdropping risk and the potential of securing next-generation LCPs communicating between implanted nodes via PLS methods. The objective is achieved by adopting the methodology of phantom experiments. In conventional pacemakers, the electrodes in the right atrium and right ventricle are connected via wires to the subcutaneous implant, whereas in the case of a leadless pacemaker the electrodes will transmit wirelessly to the subcutaneous implant, due to which the security is of great concern from an eavesdropper perspective. A three-node model is considered where two nodes are implanted inside the body and an external node located outside the body acts as an eavesdropper.

Human heart-, fat-, and blood-like homogeneous and heterogeneous liquid phantoms are developed to mimic the behavior of electromagnetic wave propagation through the heart. Phantoms developed closely reflect the dielectric properties of heart, fat, and blood in the respective bands. Using these phantoms along with an automated channel measurement mechanism, the channel transfer functions are obtained for a legitimate link and link between implanted node and that of an eavesdropper. Channel measurements are performed for ISM and UWB frequency bands. Furthermore, these channel transfer functions are used to develop path-loss models for both IB2IB link (legitimate link) and IB2OFF link (eavesdropper link) in both bands. Once the path-loss models are depicted, the probability of successful eavesdropping is determined by using the concept of outage probability for different cardiac usable information rates. Afterwards, secrecy capacity analysis is applied to highlight the potential of PLS security methods for wireless cardiac implants.

Author Contributions: Conceptualization, M.F.A. and K.K.; Methodology, M.F.A.; Validation, K.K. and C.P.G.; Formal Analysis, M.F.A.; Software, M.F.A.; Investigation, M.F.A. and S.P.S.; Resources, M.F.A. and S.P.S.; Data Curation, M.F.A. and S.P.S.; Writing—Original Draft Preparation, M.F.A.; Writing—Review & Editing, S.P.S., C.P.G. and K.K.; Visualization, M.F.A.; Supervision, K.K. and C.P.G.; Project Administration, K.K., C.P.G. and N.C.; Funding Acquisition, K.K.

Funding: This work was supported by the Marie Curie Research Grants Scheme, with project grant no 675353, EU Horizon 2020-WIBEC ITN^{II} (Wireless In-Body Environment). Details can be found at a source https://cordis.europa.eu/project/rcn/198286_en.html.

Acknowledgments: We would like to thank Pritam Bose, Oslo University Hospital, and Ali Khaleghi, NTNU for their valuable discussions on antennas. We would also like to thank Sergio Castello-Palacios's for his insights on phantom preparations.

Conflicts of Interest: The authors declare no interest of conflict.

Abbreviations

The following abbreviations are used in this manuscript:

LCP	Leadless Cardiac Pacemaker
IB2IB	In-Body to In-Body
IB2OFF	In-Body to Off-Body
ISM	Industrial Scientific and Medical Frequency Band
UWB	Ultrawide Band
WBAN	Wireless Body Area Network
PLS	Physical-Layer Security
RF	Radio Frequency

Appendix A

$$\mathcal{P}(C_s > 0) = \frac{1}{4a\sqrt{2\pi}} \int_0^\infty \frac{1}{\gamma_e} \times \left(1 - Q\left(\frac{1}{4b} \ln \frac{\gamma_e}{n}\right) \right) \times \exp\left(\frac{1}{2} \left(\frac{1}{4a} \ln\left(\frac{\gamma_e}{m}\right)\right)^2\right) d\gamma_e \quad (\text{A1})$$

Consider,

$$x = \frac{1}{4b\sqrt{2}} \ln\left(\frac{\gamma_e}{n}\right) \quad (\text{A2})$$

Then (A1) becomes

$$\mathcal{P}(C_s > 0) = \frac{b}{a\sqrt{\pi}} (\alpha - \beta) \quad (\text{A3})$$

where,

$$\alpha = \int_{-\infty}^{\infty} \exp\left(-\left(\frac{b}{a}\right)^2 \left(x + \frac{1}{4b\sqrt{2}} \ln\left(\frac{n}{m}\right)\right)^2\right) dx \quad (\text{A4})$$

$$= \frac{a\sqrt{\pi}}{b}$$

$$\beta = \int_{-\infty}^{\infty} Q(x\sqrt{2}) \exp\left(-\left(\frac{b}{a}\right)^2 \left(x + \frac{1}{4b\sqrt{2}} \ln\left(\frac{n}{m}\right)\right)^2\right) dx \quad (\text{A5})$$

Using Middleton's work ([39], p. 1072), β can be expressed as

$$\beta = \frac{a\sqrt{\pi}}{b} Q\left(\frac{\ln(n/m)}{4\sqrt{a^2 + b^2}}\right) \quad (\text{A6})$$

which follows,

$$\mathcal{P}(C_s < R_s) = Q\left(\frac{\ln \frac{\mu_{\gamma_r}}{\mu_{\gamma_e}} + 8(b^2 - a^2) - R_s \ln 2}{4\sqrt{a^2 + b^2}}\right) \quad (\text{A7})$$

and

$$\mathcal{P}(C_s > 0) = Q\left(\frac{\ln \mu_{\gamma_e} - \ln \mu_{\gamma_r} + 8(b^2 - a^2)}{4\sqrt{a^2 + b^2}}\right) \quad (\text{A8})$$

References

- Mond, H.G.; Proclemer, A. The 11th world survey of cardiac pacing and implantable cardioverter-defibrillators: Calendar year 2009—A world society of Arrhythmia's project. *Pacing Clin. Electrophysiol.* **2011**, *34*, 1013–1027. [[CrossRef](#)] [[PubMed](#)]
- EU Horizon 2020 Project WiBEC. Available online: <https://www.ntnu.edu/wibec> (accessed on 20 November 2018).
- Medtronic Micra Leadless Pacemaker. Available online: <https://www.medtronic.com/us-en/patients/treatments-therapies/pacemakers/our/micra.html> (accessed on 20 November 2018).
- Halperin, D.; Heydt-Benjamin, T.S.; Ransford, B.; Clark, S.S.; Defend, B.; Morgan, W.; Fu, K.; Kohno, T.; Maisel, W.H. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 18–22 May 2008; pp. 129–142.
- Camara, C.; Peris-Lopez, P.; Tapiador, J.E. Security and privacy issues in implantable medical devices: A comprehensive survey. *J. Biomed. Inform.* **2015**, *55*, 272–289. [[CrossRef](#)] [[PubMed](#)]
- Zhang, M.; Raghunathan, A.; Jha, N.K. MedMon: Securing medical devices through wireless monitoring and anomaly detection. *IEEE Trans. Biomed. Circuits Syst.* **2013**, *7*, 871–881. [[CrossRef](#)] [[PubMed](#)]
- Son, S.; Lee, K.; Won, D.; Kim, S. U-healthcare system protecting privacy based on cloaker. In Proceedings of the 2010 IEEE International Conference on Bioinformatics and Biomedicine Workshops (BIBMW), Hong Kong, China, 18 December 2010; pp. 417–423.
- Gollakota, S.; Hassanieh, H.; Ransford, B.; Katabi, D.; Fu, K. They can hear your heartbeats: Non-invasive security for implantable medical devices. *Comput. Commun. Rev.* **2011**, *41*, 2–13. [[CrossRef](#)]
- Sastry, N.; Wagner, D. Security considerations for IEEE 802.15. 4 networks. In Proceedings of the 3rd ACM Workshop on Wireless Security, Philadelphia, PA, USA, 1 October 2004; pp. 32–42.
- Group, I.W. IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs). Available online: <https://ieeexplore.ieee.org/document/6185525> (accessed on 20 August 2018).
- Shannon, C.E. Communication theory of secrecy systems. *Bell Labs Tech. J.* **1949**, *28*, 656–715. [[CrossRef](#)]
- Wyner, A.D. The wire-tap channel. *Bell Labs Tech. J.* **1975**, *54*, 1355–1387. [[CrossRef](#)]
- Klinc, D.; Ha, J.; McLaughlin, S.W.; Barros, J.; Kwak, B.J. LDPC codes for the Gaussian wiretap channel. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 532–540. [[CrossRef](#)]
- Oggier, F.; Solé, P.; Belfiore, J.C. Lattice codes for the wiretap Gaussian channel: Construction and analysis. *IEEE Trans. Inf. Theory* **2016**, *62*, 5690–5708. [[CrossRef](#)]
- Liu, R.; Trappe, W. *Securing Wireless Communications at the Physical Layer*; Springer: Berlin, Germany, 2010; Volume 7.
- Xiao, S.; Gong, W.; Towsley, D. Secure wireless communication with dynamic secrets. In Proceedings of the INFOCOM, San Diego, CA, USA, 14–19 March 2010; pp. 1–9.
- Chae, S.H.; Choi, W.; Lee, J.H.; Quek, T.Q. Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 1617–1628. [[CrossRef](#)]

18. Maurer, U.M. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory* **1993**, *39*, 733–742. [[CrossRef](#)]
19. Jana, S.; Premnath, S.N.; Clark, M.; Kasera, S.K.; Patwari, N.; Krishnamurthy, S.V. On the effectiveness of secret key extraction from wireless signal strength in real environments. In Proceedings of the 15th Annual International Conference on Mobile Computing and Networking, Beijing, China, 20–25 September 2009; pp. 321–332.
20. Garcia-Pardo, C.; Andreu, C.; Fornes-Leal, A.; Castelló-Palacios, S.; Perez-Simbor, S.; Barbi, M.; Vallés-Lluch, A.; Cardona, N. Ultrawideband Technology for Medical In-Body Sensor Networks: An Overview of the Human Body as a Propagation Medium, Phantoms, and Approaches for Propagation Analysis. *IEEE Antennas Propag. Mag.* **2018**, *60*, 19–33. [[CrossRef](#)]
21. Gabriel, C. *Compilation of the Dielectric Properties of Body Tissues at RF and Microwave Frequencies*; Technical Report; King's Coll London Department of Physics: London, UK, 1996.
22. Garcia-Pardo, C.; Fornes-Leal, A.; Cardona, N.; Chávez-Santiago, R.; Bergsland, J.; Balasingham, I.; Brovoll, S.; Aardal, Ø.; Hamran, S.E.; Palomar, R. Experimental ultra wideband path loss models for implant communications. In Proceedings of the 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Valencia, Spain, 4–8 September 2016; pp. 1–6.
23. Sayrafian-Pour, K.; Yang, W.B.; Hagedorn, J.; Terrill, J.; Yazdandoost, K.Y. A statistical path loss model for medical implant communication channels. In Proceedings of the 2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications, Tokyo, Japan, 13–16 September 2009; pp. 2995–2999.
24. Garcia-Pardo, C.; Chávez-Santiago, R.; Cardona, N.; Balasingham, I. Experimental UWB frequency analysis for implant communications. In Proceedings of the 2015 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), Milan, Italy, 25–29 August 2015; pp. 5457–5460.
25. Chávez-Santiago, R.; Garcia-Pardo, C.; Fornes-Leal, A.; Vallés-Lluch, A.; Vermeeren, G.; Joseph, W.; Balasingham, I.; Cardona, N. Experimental Path Loss Models for In-Body Communications Within 2.36–2.5 GHz. *IEEE J. Biomed. Health Inform.* **2015**, *19*, 930–937. [[PubMed](#)]
26. Simbor, S.P.; Barbi, M.; Pardo, C.; Palacios, S.C.; Cardona, N. Initial UWB In-Body Channel Characterization Using a Novel Multilayer Phantom Measurement Setup. In Proceedings of the IEEE Wireless Communications and Networking Conference, Barcelona, Spain, 15–18 April 2018.
27. Kurup, D.; Vermeeren, G.; Tanghe, E.; Joseph, W.; Martens, L. In-to-out body antenna-independent path loss model for multilayered tissues and heterogeneous medium. *Sensors* **2015**, *15*, 408–421. [[CrossRef](#)] [[PubMed](#)]
28. Castelló-Palacios, S.; Vallés-Lluch, A.; Garcia-Pardo, C.; Fornes-Leal, A.; Cardona, N. Formulas for easy-to-prepare tailored phantoms at 2.4 GHz ISM band. In Proceedings of the 2017 11th International Symposium on Medical Information and Communication Technology (ISMICT), Lisbon, Portugal, 6–8 February 2017; pp. 27–31.
29. Lazebnik, M.; Madsen, E.L.; Frank, G.R.; Hagness, S.C. Tissue-mimicking phantom materials for narrowband and ultrawideband microwave applications. *Phys. Med. Biol.* **2005**, *50*, 4245–4258. [[CrossRef](#)] [[PubMed](#)]
30. Castelló-Palacios, S.; Garcia-Pardo, C.; Fornes-Leal, A.; Cardona, N.; Vallés-Lluch, A. Wideband phantoms of different body tissues for heterogeneous models in body area networks. In Proceedings of the 2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), Seogwipo, Korea, 11–15 July 2017; pp. 3032–3035.
31. Bose, P.; Khaleghi, A.; Albatat, M.; Bergsland, J.; Balasingham, I. RF Channel Modeling for Implant to Implant Communication and Implant to Sub-Cutaneous Implant Communication for Future Leadless Cardiac Pacemakers. *IEEE Trans. Biomed. Eng.* **2018**, *65*, 2798–2807. [[PubMed](#)]
32. Castelló-Palacios, S.; Garcia-Pardo, C.; Fornes-Leal, A.; Cardona, N.; Vallés-Lluch, A. Tailor-made tissue phantoms based on acetonitrile solutions for microwave applications up to 18 GHz. *IEEE Trans. Microw. Theory Tech.* **2016**, *64*, 3987–3994. [[CrossRef](#)]
33. Andreu, C.; Garcia-Pardo, C.; Fornes-Leal, A.; Cabedo-Fabrés, M.; Cardona, N. UWB in-body channel performance by using a direct antenna designing procedure. In Proceedings of the 2017 11th European Conference on IEEE Antennas and Propagation (EUCAP), Paris, France, 19–24 March 2017; pp. 278–282.
34. Tarin, C.; Marti, P.; Traver, L.; Cardona, N.; Diaz, J.A.; Antonino, E. UWB Channel Measurements for hand-portable devices: A comparative study. In Proceedings of the IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, Athens, Greece, 3–7 September 2007; pp. 1–5.

35. Tse, D.; Viswanath, P. *Fundamentals of Wireless Communications*; Cambridge University Press: Cambridge, UK, 2005.
36. Islam, M.N.; Yuce, M.R. Review of medical implant communication system (MICS) band and network. *ICT Express* **2016**, *2*, 188–194. [[CrossRef](#)]
37. Leung-Yan-Cheong, S.; Hellman, M. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory* **1978**, *24*, 451–456. [[CrossRef](#)]
38. Liu, X. Secrecy capacity of wireless links subject to log-normal fading. In Proceedings of the 2012 7th International ICST Conference on Communications and Networking in China (CHINACOM), Kunming, China, 8–10 August 2012; pp. 167–172.
39. Middleton, D. *An Introduction to Statistical Communication Theory*; IEEE Press: Piscataway, NJ, USA, 1996.



© 2018 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

Appendix D

Simulation Based Secrecy Capacity for MICS, WMTS and ISM 868 MHz

Paper D: Evaluating Secrecy Capacity for in-body Wireless
Channels

Muhammad Faheem Awan, Xiao Fang, Mehrab Ramzan, Kimmo Kansanen,
Niels Neumann, Qiong Wang, and Dirk Plettemeier

Entropy 2019

Article

Evaluating Secrecy Capacity for In-Body Wireless Channels

Muhammad Faheem Awan ^{1,*}, Xiao Fang ², Mehrab Ramzan ², Niels Neumann ²,
Qiong Wang ², Dirk Plettmeier ² and Kimmo Kansanen ¹

¹ Department of Electronic Systems, Norwegian University of Science and Technology, NTNU, NO-7491 Trondheim, Norway

² Chair of RF and Photonics Engineering, Technische Universität Dresden, 01067 Dresden, Germany

* Correspondence: faheem.awan@ntnu.no; Tel.: +47-9224-0132

Received: 12 August 2019; Accepted: 2 September 2019; Published: 3 September 2019

Abstract: The next generation of implanted medical devices is expected to be wireless, bringing along new security threats. Thus, it is critical to secure the communication between legitimate nodes inside the body from a possible eavesdropper. This work assesses the feasibility of securing next generation multi-nodal leadless cardiac pacemakers using physical layer security methods. The secure communication rate without leakage of information to an eavesdropper, referred to as secrecy capacity, depends on the signal-to-noise ratios (SNRs) of the eavesdropper and legitimate channels and will be used as a performance metric. Numerical electromagnetic simulations are utilized to compute the wireless channel models for the respective links. These channel models can be approximated with a log-normal distribution which can be used to evaluate the probability of positive secrecy capacity and the outage probability of this secrecy capacity. The channels are modeled for three different frequency bands and a comparison between their secrecy capacities is provided with respect to the eavesdropper distance. It has been found that the positive secrecy capacity is achievable within the personal space of the human body for all the frequency bands, with the medical implant communication systems (MICS) band outperforming others.

Keywords: implanted medical devices; wireless leadless cardiac pacemaker; in-body wireless channels; security and privacy; physical layer security; secrecy capacity

1. Introduction

The technological advancements in implanted medical devices have resulted in the rapid growth of personal health systems which include popular wireless medical devices like cardiac pacemakers, glucose monitors, and implantable cardioverter defibrillators (ICDs). These wireless medical devices are less invasive than traditional wired solutions and provide proper diagnosis and treatment.

One of the most important medical device is the cardiac pacemaker, which helps to maintain cardiac rhythms. There are almost one million pacemaker implantations worldwide annually [1]. The current generation of these pacemakers consists of a subcutaneous implant connected to electrodes in the right atrium and right ventricle by leads, whereas the next generation is expected to be wireless in all aspects including connectivity between the subcutaneous implant and electrodes. The electrodes of the so-called leadless cardiac pacemakers in the heart chambers will be wirelessly synchronized with each other and also with the subcutaneous implant which will be used to configure the leadless pacemakers and that acts as a relay for external devices.

Besides the unquestionable benefits of leadless pacemakers such as less invasive surgery, also some disadvantages arise. One of the key issues is to protect the life saving device from intruders and eavesdroppers. Successful eavesdropping results in fetching of patient's confidential information (medical/non-medical) or executing different types of attacks (e.g., forging and data manipulation).

Moreover, it may facilitate the modification of implant configuration without knowledge of the patient or physician [2]. Thus, the wireless nature of these devices could be a safety risk and must be secured from threats like eavesdropping, data tampering and device modification. This work does not cover all aspects related to the security of implanted medical devices and focuses only on secrecy capacity for in-body channels with the assumption of a passive eavesdropper outside the body. The passive eavesdropper only intercepts the communication without any active attacks. This can lead to future active attacks like data tampering, man-in-the-middle attack and un-authorized access. For example, in the case of SNR estimation spoofing, the active eavesdropper can adapt the strategy of reporting a worse SNR than the legitimate receiver, albeit having the better SNR, reflecting the secrecy capacity to be positive. Therefore, if the transmitter unit is not able to distinguish that forgery attempt, then eavesdropper will end up partially decoding the confidential information. On the other way around, the eavesdropper can report its SNR to be better than legitimate channel, which results in utilizing the resources from the transmitter unit [3]. Moreover, jamming also directly affects the secrecy metrics, because it changes the estimated and actual legitimate receiver SNR. A detailed investigation of active attacks is beyond the scope of this work.

Halperin et al.'s [4] work is believed to be the pioneer study in investigating the security risks of implanted medical devices and proofs with off the shelf antennas and external programmers (An external device used for data collection and configuration of a cardiac pacemaker) that the wireless nature of these devices can be exploited to control them. This work was followed by numerous studies providing the methodologies and techniques to secure wireless implanted medical devices [5–8]. Most of the work is focused on methods based on computational cryptography. Another alternative could be utilizing the physical layer to provide secure communication via information theoretic measures. In addition, risk management and evaluation are part of international standards for implanted medical devices [9,10]. Therefore, physical layer security (PLS) assessments together with traditional cryptographic measures should be part of these standards.

The theory of information theoretic security was initially suggested by Shannon [11] in 1949. Wyner [12] extended Shannon's work in 1975 and introduced the secrecy capacity of the Gaussian wiretap channel. Secrecy capacity is a communication rate with which the legitimate nodes can communicate securely in the presence of an eavesdropper. Secrecy capacity can be achieved if the legitimate channel signal-to-noise ratio (SNR) is better than the eavesdropper's (Eve's) channel. There have been considerable efforts to secure wireless networks [13] based on the PLS methods. Jameel et al. in [14] provided a comprehensive survey on cooperative relaying and jamming strategies for PLS methods whereas [15] proposed the multicasting cooperation strategy to enhance the security in large networks. Also, Neshenko et al. [16], provided an extensive survey on different types of vulnerabilities. However, these methods mainly focus on free space wireless networks and cannot be directly applied to in-body scenarios because of completely different media.

Information theoretic measures or security via PLS depend on wireless channel characteristics for securing the communication between legitimate nodes. These characteristics may involve received signal strength, angle of arrival, phase or the inherent noise in the wireless channels that degrades the signal-to-noise ratio [17–20]. Therefore, channel modeling is the key aspect to evaluating the possibilities of using the PLS methods for securing the information content between legitimate nodes.

Channel characterizations subject to the human body are commonly carried out in electromagnetic (EM) computational simulation tools like computer simulation technology (CST) [21] or High frequency structure simulator (HFSS) [22], phantom or in-vivo experiments. IEEE 802.15.6 is the specified standard for wireless body area network (WBAN) in which Medical Implant Communication (MICS) band is specified as the communication standard for the implant to implant communication. The MICS frequency band covers the frequency range of 402–405 MHz. Literature is also available on channel modeling in other frequency bands such as Wireless Medical Telemetry Service (WMTS, 608–614 MHz), ISM 868 MHz, Ultra Wide Band (3.1–5.1 GHz), and ISM 2.4 GHz [23–25]. Similarly, Kadel et al. [26], provide comparisons between different channel models proposed in the literature for on-body to

on-body scenarios in WBAN for 900 MHz and 3.1–10 GHz. Their simulation results are derived from a 2-D human model without considering the impacts of different human organs. Therefore, the results can be considered as less precise. Moreover, their channel models cannot be utilized for our application scenario, because the transmitter and receiver are considered on the body surface whereas in our case the transmitter is located inside the heart and the receiver is positioned in the subcutaneous space.

This work evaluates the secrecy capacity for in-body channels and explores the PLS methods for privacy and security of multi-nodal leadless cardiac pacemaker (LCP). The in-body to in-body legitimate channel and in-body to off-body eavesdropper channels are simulated in a computer simulation tool to derive the path loss models for channel attenuation. In comparison to channel models presented in [26], we evaluated the application-based channel model that involves propagation through organs in the cardiac scenario. In addition, the evaluation of channel models is based on a 3-D anatomical human model with an EM simulation method which is precise and considers all the electric properties of human organs and propagation characteristics of electromagnetic waves inside the human body. Based on the cardiac application scenarios, three different channel models, in-body to in-body, in-body to subcutaneous and in-body to off-body, are developed and lower frequency bands are mainly considered, i.e., MICS, WMTS and ISM. The channel attenuation is utilized to evaluate the respective link signal-to-noise ratio (SNR) for determining the probability of positive secrecy capacity along with the outage probability of the secrecy capacity. The secrecy capacity analysis is carried out in all the frequency bands under investigation. It has been observed that the MICS band outperforms other bands in terms of achieving secrecy capacity in near vicinity of the human body. However, if the practical considerations of antenna dimensions are to be considered, then the ISM 868 MHz is the viable choice.

The rest of the paper is organized as follows. Section 2 provides the system model and methodology and Section 3 contains the results. The discussions are provided in Section 4 and conclusions in Section 5.

2. System Model and Methodology

This section provides the system model for a multi-nodal leadless cardiac pacemaker which consists of a leadless pacemaker in the right ventricle and right atrium of the human heart, a subcutaneous implant in the pectoral pocket under the shoulder and an eavesdropper outside the body as shown in Figure 1. The leadless pacemakers, also referred to as capsules, communicate wirelessly with each other and with the subcutaneous implant. We define three links, two legitimate and one eavesdropper link—the link between $C1$ and $C2$ referred to as $L1$, the link between $C1$ and the subcutaneous implant ($L2$) and the link between $C1$ and the eavesdropper ($E1$).

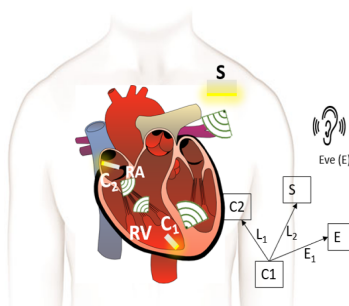


Figure 1. Multi-nodal leadless cardiac pacemaker scenario with leadless capsules $C1$ and $C2$, subcutaneous implant S and an eavesdropper E .

The legitimate nodes use MICS, WMTS, and ISM 868 MHz frequency bands in order to communicate with each other. To evaluate the secrecy capacity, the channels for all communication links between legitimate nodes and with the eavesdropper are modeled in CST. First, the methodology

to evaluate the secrecy capacity and its dependence on channel models is provided, followed by channel modeling using electromagnetic simulations.

2.1. Methodology

The wireless in-body network shown in Figure 1 depicts C1 communicating with C2 and S, whereas the eavesdropper (Eve) in the near vicinity of the body is attempting to spy on the communication. The legitimate nodes can communicate securely by using the secure transmission rate which is the maximum achievable confidential communication rate without the disclosure of information to Eve. All the noise sources are considered to be white and Gaussian e.g., thermal noise, shot noise of the Rx and Tx and we do not expect any nonlinearities from Rx, Tx and the communication medium. Therefore, by using [27] for an additive Gaussian wiretap channel, the instantaneous secrecy capacity is expressed as

$$C_s = C_r - C_e \quad (1)$$

where C_r and C_e are the channel capacities of legitimate and eavesdropper link respectively, which can be expressed as

$$C_r = \frac{1}{2} \log_2(1 + \gamma_r) \quad (2)$$

$$C_e = \frac{1}{2} \log_2(1 + \gamma_e) \quad (3)$$

Consequently, Equation (1) can be followed from Equation (2) and Equation (3) as

$$C_s = \begin{cases} \frac{1}{2} \log_2(1 + \gamma_r) - \frac{1}{2} \log_2(1 + \gamma_e), & \text{if } \gamma_r > \gamma_e. \\ 0, & \text{otherwise [27].} \end{cases} \quad (4)$$

γ_r represents the legitimate channel SNR and γ_e shows the SNR of Eve's channel. Equation (4) expresses that C_s is positive when the legitimate channel SNR is greater than Eve's channel i.e., ($\gamma_r > \gamma_e$). With positive C_s , the legitimate nodes can communicate securely. Furthermore, the SNR of a link can be computed as

$$\gamma_i = \frac{P * |h_i|^2}{W_i}, \quad i \in (r, e) \quad (5)$$

where $|h_e|^2$, $|h_r|^2$ represents the channel attenuations of the associated links, P is the transmitted power which is set to -16 dBm (power restrictions on implanted devices [28]) and W is the constant noise power. Therefore, channel attenuations are the only source of variations in channel capacities. Thus, in order to compute the secrecy capacity for in-body implanted legitimate nodes, the channel model for attenuation between the legitimate nodes and eavesdropper must be analyzed.

2.2. Channel Modeling

The simulation is performed in the anatomical human model provided by the CST family of voxel models. The transmitting antenna is an electrically small antenna which has a far-field radiation similar to a Hertzian dipole. Hence, for simplicity, it is represented by a Hertzian dipole source in the simulation. The ideal Hertzian dipole source does not take the mismatch and structural loss of the real antenna into consideration, however, in the practical case, these losses cannot be ignored, which will increase the path loss and deteriorate the channel SNR. Three polarizations of the Hertzian dipole have been investigated. In order to detect the electric and magnetic fields at different distances from the transmitting dipole, ideal electric and magnetic probes are utilized. Based on the LCP scenario,

the transmitting antenna is placed at the vertex of the right ventricle which is the actual pacemaker placement site.

The intra-cardiac simulation scenario or an intra-cardiac link ($L1$) is shown in Figure 2, where a pacemaker is placed in the right ventricle and different receiving probes in the right atrium. The intra-cardiac to the subcutaneous channel or link between $C1$ and S (i.e., $L2$) is illustrated in Figure 3. The probes are placed 2 cm below the skin surface under the left collar bone of the human body and is regarded as the actual placement site for the subcutaneous device. Figure 4 shows Eve's channel ($E1$) where the probes are positioned a few centimeters away from the body surface in front of the chest. The probes are located at a site with maximum received power. This is considered as the worst case scenario for the pacemaker (best case scenario for Eve) under practical conditions, i.e., limited antenna size for Eve. Figure 5 shows the spatial distribution of the strength of EM radiation outside the body, with maximum received power in front of the body showing the best case scenario for Eve. The power distribution at each position is evaluated using the Poynting vector which can be expressed as

$$S_{(x,y,z)}(t) = E_{(x,y,z)}(t) \times H_{(x,y,z)}(t) \quad (6)$$

where $E_{(x,y,z)}(t)$ and $H_{(x,y,z)}(t)$ are the time-domain electric and magnetic field vector. The average received power at a single position is determined from all three x,y,z polarized electric and magnetic probes. Finally, the path loss is calculated from the ratio of the averaged received power at the observation point to the average transmitted power. For computing simplicity of secrecy capacity and outage probability, a single path loss model is often desirable for both in-body and off-body links. Under the practical limitation of Eve using an antenna with limited size, this is an acceptable simplification. However, when exploring the absolute limits of the received power, the different nature of the loss inside and outside the body should be considered. The power lost inside the body is dissipated to heat (lossy medium) whereas the path loss outside the body is because of the spatial distribution of the electromagnetic wave. Using a theoretical antenna/receiver system that is able to receive all power radiated from the body, this path loss may be compensated completely. Due to the fact that this kind of system is extremely difficult to implement, especially without disclosure of Eve's intends, the practical case of limited antenna size and path loss outside the body will be used for the calculations. Therefore, the derivation of the path loss model is based on the following equation

$$PL_{dB} = PL_{0,dB} + 10n \log\left(\frac{d}{d_0}\right) + N(0, \sigma_{dB}) \quad (7)$$

where $PL_{0,dB}$ is the path loss at the reference distance d_0 and n is the path loss exponent. The cumulative distribution function (CDF) can be approximated by a log-normally distributed random variable $\mathcal{N}(0, \sigma)$ with zero mean and standard deviation σ .

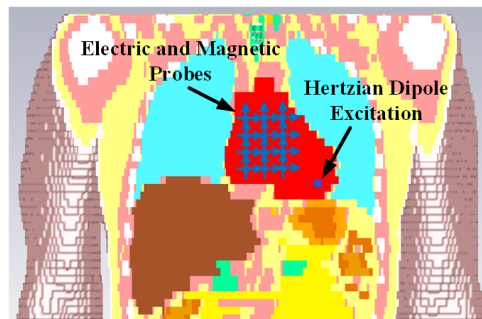


Figure 2. Cross section view of simulation scenario of Intra-cardiac to Intra-cardiac channel models.

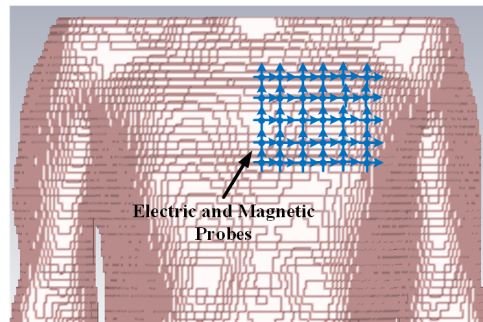


Figure 3. Cross section view of simulation scenario of Intra-cardiac to Subcutaneous channel models.

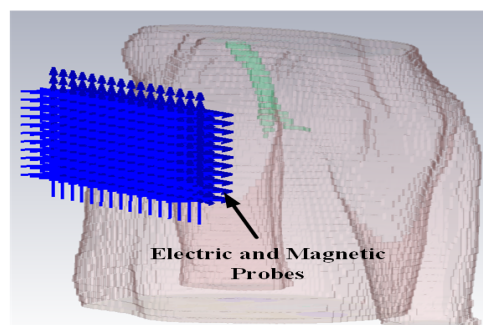


Figure 4. Side view of the simulation scenario of Intra-cardiac to Off-Body channel models.

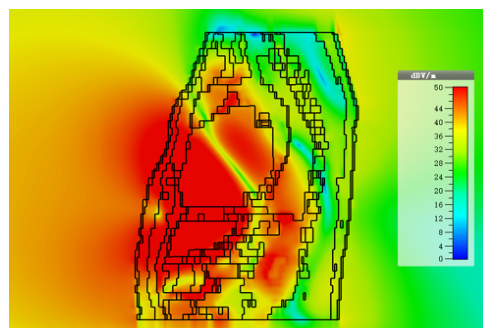


Figure 5. Radiation of EM waves outside the body.

The path loss values along with the fitted model for intra-cardiac simulation or *LI* link is shown in Figure 6. It shows that the path loss varies with respect to the frequency band used. The intra-cardiac to off-body channel models (*E1*) consist of free space and complex human body tissue medium. As mentioned before, for the computational simplicity of secrecy capacity and outage probability, a single path loss model is often desirable. Therefore, a single path loss model curve with average path loss exponent is extracted as shown in Figure 7. The slope of the fitted curves clearly indicates that when the receiver is in the near vicinity of the human body, the lossless medium influence can be neglected and as the receiver is being moved away there is slightly decreasing change in the slope indicating the influence of the presence of the free space medium. At distance larger than 150 mm, the path loss at ISM 868 MHz becomes less than that in the WMTS band. The complex nature of human organs causes reflection and scattering which may cause increased received power at certain

locations outside the human body due to constructive interference. This effect is more prominent at higher frequencies (i.e., smaller wavelengths). The intra-cardiac to subcutaneous channel model or *L2* link is shown in Figure 8. The increasing tendency of path loss is similar to that of intra-cardiac path loss. Table 1 shows the summary of all the nine models depicted using EM simulations for the corresponding legitimate and eavesdropper links in the frequency bands under investigation.

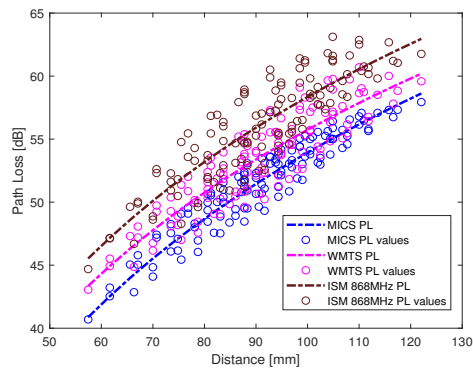


Figure 6. Intra-Cardiac link (*L1*) pathloss models.

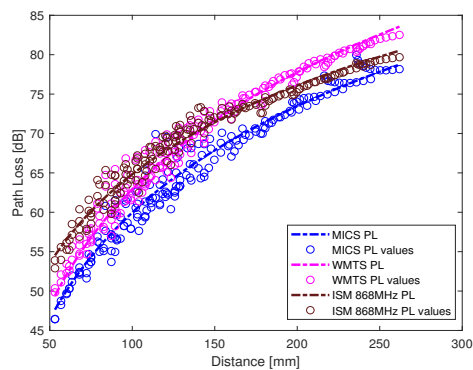


Figure 7. Off body link (*E1*) path loss models.

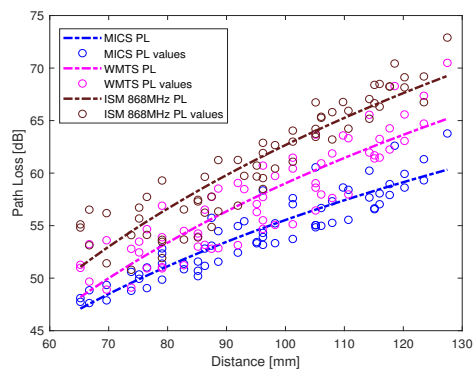


Figure 8. Subcutaneous link (*L2*) path loss models

Table 1. Summary of the path loss models for intra-cardiac (L1), subcutaneous (L2) and off-body eavesdropper (E1) link.

Parameter	MICS (402–405 MHz)			WMTS (608–614 MHz)			ISM 868 MHz (867–869 MHz)		
	L1	L2	E1	L1	L2	E1	L1	L2	E1
PL(d0) (dB)	42.5	48.5	50	44.9	50	52	47.2	53	56.5
d0 (cm)	6	7	6	6	7	6	6	7	6
n	5.12	4.54	4.465	4.86	5.83	4.970	4.99	6.24	3.773
μ	0	0	0	0	0	0	0	0	0
σ (dB)	1.26	1.64	1.379	1.83	2.64	1.275	2.14	2.24	1.143
d (cm)	5.7–12.2	6–13	5.6–24.4	5.7–12.2	6–13	5.6–24.4	5.7–12.2	6–13	5.6–24.4

3. Results

In this section, the secrecy capacity analysis of a multi-nodal leadless cardiac pacemaker is provided. As enlisted in Table 1, all the path loss models for channel attenuation are modeled with a log-normal distribution. Thus, the corresponding SNR values γ_r and γ_e will also follow the log-normal distribution at any measuring point with mean and standard deviation (μ_r, σ_r) and (μ_e, σ_e) , respectively. The fundamental parameters in the context of secrecy capacity are the probability of positive secrecy capacity (\mathcal{P}_{pc_s}) and the outage probability of secrecy capacity (OP_{c_s}). The secrecy capacity is positive when Eve’s link SNR is inferior to legitimate link’s SNR and is referred to as positive secrecy capacity. The outage probability of secrecy capacity can be defined by setting a fixed secrecy rate (R_s) and can be computed with respect to the eavesdropper distance. As γ_r and γ_e are mutually independent and log-normally distributed, then for a single realization of a legitimate channel and eavesdropper channel, the probability of positive secrecy capacity can be expressed as

$$\mathcal{P}(C_s > 0) = \mathcal{P}(\gamma_r > \gamma_e) \tag{8}$$

Similarly, by setting a fixed secrecy rate (R_s), the outage probability of secrecy capacity can be expressed as

$$\mathcal{P}(C_s < R_s) = 1 - \mathcal{P}(C_s > R_s) \tag{9}$$

After simplification (as provided in detail in Appendix A and adapted from [29]), \mathcal{P}_{pc_s} can be represented in the form of Q-function for log-normal channels [19,29] as

$$\mathcal{P}(C_s > 0) = 1 - Q\left(\frac{\ln \mu_{\gamma_e} - \ln \mu_{\gamma_r} + 8(b^2 - a^2)}{4\sqrt{a^2 + b^2}}\right) \tag{10}$$

whereas the outage probability (OP_{c_s}) can be expressed as

$$\mathcal{P}(C_s < R_s) = Q\left(\frac{\ln \frac{\mu_{\gamma_r}}{\mu_{\gamma_e}} + 8(b^2 - a^2) - R_s \ln 2}{4\sqrt{a^2 + b^2}}\right) \tag{11}$$

where μ_{γ_e} and μ_{γ_r} represents the mean SNR of respective links (legitimate and Eve Link, as expressed in Equation (5)). In addition, $a = \frac{\sigma_r \ln 10}{40}$ and $b = \frac{\sigma_e \ln 10}{40}$, where a and b is the standard deviation of the Gaussian distribution which corresponds to a log-normal distribution (if σ_e is the standard deviation of γ_e , then $a = \frac{\sigma_r \ln 10}{40}$). As shown in Figure 1 and numbers enlisted in Table 1, there are two legitimate links, one between node C1 and C2 i.e., L1 whereas other between C1 and S i.e., L2—and the eavesdropper link (E1). Thus, a separate analysis is provided for both the legitimate links considering the same link for Eve.

3.1. Probability of Positive Secrecy Capacity (\mathcal{P}_{pc_s})

First, the intra-cardiac link ($L1$) and the eavesdropper link ($E1$) are considered. Thus, by using Equation (10), the \mathcal{P}_{pc_s} for the intra-cardiac link is shown in Figure 9, whereas the \mathcal{P}_{pc_s} for the subcutaneous link ($C1$ and S or $L2$) is shown in Figure 10. In case of the intra-cardiac link, a fixed distance of 8 cm between node $C1$ and $C2$ is considered and the eavesdropper distance is varied. By considering Eve at a distance of 6 cm which ultimately means being attached directly to the body of a patient over the heart on the chest, \mathcal{P}_{pc_s} is approximately 68% for WMTS, around 75% for MICS and about 90% for ISM 868 MHz. When the eavesdropper is moved away just about 2 cm, the positive secrecy capacity approaches to approx. 100% for all the frequency bands. Normally, in case of lower frequencies with small in-body distance between nodes the probability of secrecy capacity is high. As shown in Figure 10, ISM 868 MHz has higher \mathcal{P}_{pc_s} than MICS and WMTS, but this is because of the small path loss exponent “ n ” and also the smaller standard deviation of path loss than MICS and WMTS. However, after 7.6 cm MICS and WMTS have higher secrecy capacity than ISM 868 MHz.

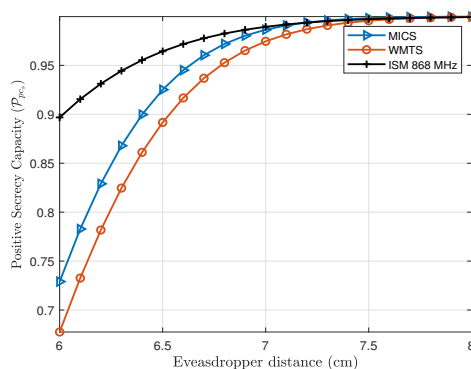


Figure 9. Probability of positive secrecy capacity of intra-cardiac ($C1$ and $C2$ or $L1$) link for the frequency bands under investigation.

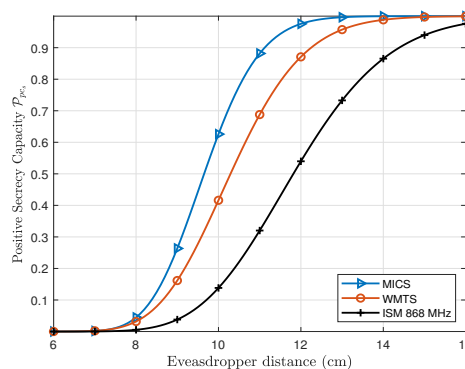


Figure 10. Probability of positive secrecy capacity of Subcutaneous link ($L2$) for frequency bands under investigation.

Similarly, in case of the subcutaneous link ($L2$), the distance between $C1$ and S is fixed to 12 cm which is the average distance between the capsule in the right ventricle and subcutaneous implant. If the eavesdropper is considered to be attached to the human body over the heart, the \mathcal{P}_{pc_s} is about 0%. However, if an eavesdropper moves away from the body \mathcal{P}_{pc_s} increases and approaches to approx. 100% at a distance of 15 cm in case of MICS and WMTS band, whereas about 99.97% at a

distance of 20 cm for ISM 868 MHz. In case of subcutaneous link ($L2$) as expected the MICS band has higher \mathcal{P}_{pc_s} at close premises to the body than WMTS and ISM 868 MHz.

3.2. Outage Probability of Secrecy Capacity (OP_{c_s})

In order to evaluate the outage probability of secrecy capacity, a secure communication rate between legitimate nodes is needed to be established. In case of pacemakers, the communication rate required to transmit different physiological parameters varies, e.g., the required communication rate for electrocardiography (ECG) is around 2.5–250 kbps, whereas electromyography (EMG) requires around 650 kbps [30]. If the secrecy rate is set to about 1 bps/Hz which for a bandwidth of 1 MHz is equivalent to 1 Mbps, the outage probability of secrecy capacity can be provided by using Equation (11). Figure 11 shows the outage probability of fixed secrecy rate for the legitimate link ($L1$). The distance of link $L1$ is fixed to 8 cm and the eavesdropper distance is varied. The OP_{c_s} of link $L1$ at an Eve distance of 6 cm is about 84% for MICS, 81% for WMTS and 50% for ISM 868 MHz and approaches nearly to 2% at Eve’s distance of about 8 cm. Similarly for subcutaneous link ($L2$), the OP_{c_s} is shown in Figure 12. In case of the subcutaneous link, the distance between $C1$ and S is about 12 cm. The OP_{c_s} at an Eve distance of 12 cm is about 28% for MICS, 48% for WMTS, and 86% for ISM 868 MHz whereas the OP_{c_s} approaches to approximately 0.076%, 3.1% and 21%, respectively, at a distance of Eve of 16 cm in case of MICS, 18 cm in case of WMTS and 22 cm in case of ISM 868 MHz. However, for a decent level of safety, lower outage probabilities are desirable.

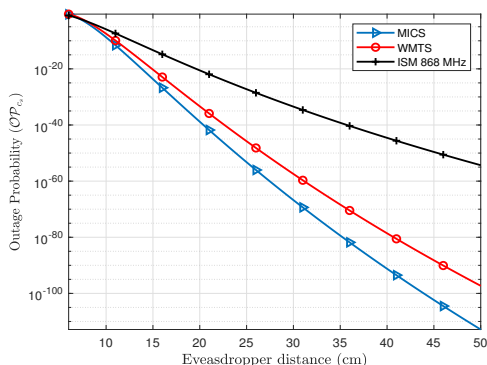


Figure 11. Comparison of outage probability of secrecy capacity for intra-Cardiac link for the investigated frequency bands.

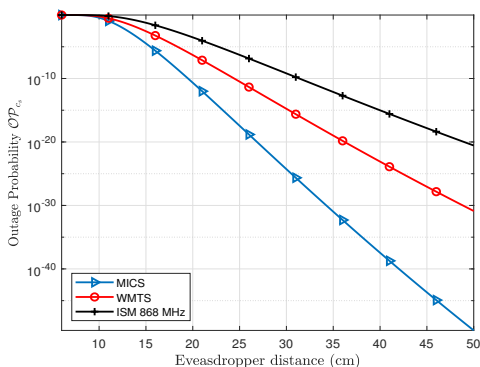


Figure 12. Comparison of Outage probability of secrecy capacity for subcutaneous link for the investigated frequency bands.

4. Discussion

So far, a scenario with an eavesdropper outside the body with a small antenna has been analyzed where multinodal leadless pacemakers are implanted in the right atrium and right ventricle of the human heart, along with a subcutaneous implant beneath the shoulder under the skin. Our findings show that the physical layer security methods with the use of the secrecy capacity is viable and can be an efficient alternative to secure the implanted medical devices on a physical layer. This is because the human body is a lossy medium for electromagnetic propagation, inherently providing high channel attenuation to off-body links e.g., the eavesdropper link *E1*. Eve being outside the body has an advantage of compensating the high path loss by use of different types of antennas and thus can improve the quality of a link with high gain antennas. Higher gain antennas can have a reception from a greater distance with high SNR, thus reducing the secrecy capacity rate. However, these kind of outperforming antennas are realized at a cost of larger dimensions of the antenna. The dimension of an antenna with provided gain can be estimated using

$$A_e = \frac{c^2 G}{4\pi f^2} \tag{12}$$

where A_e is the effective aperture, G is the antenna gain, and f is the frequency. Thus, in order to analyze the effect of antenna gain at the eavesdropper, the outage probability of secrecy capacity is evaluated by considering Eve having an ideal antenna with 10 dBi gain. As seen in Equation (12), the effective aperture (i.e., size) of antennas increases with its gain. As a result, 10 dBi was chosen to balance antenna dimensions and gain. Table 2 enlists the comparison of outage probabilities with and without antenna gain for both intra-cardiac (*L1*) and subcutaneous link (*L2*). The antenna aperture is given exemplary in quadratic dimensions for better imagination. In addition, a personal space of 50 cm is considered for an individual with a pacemaker. Eve will be noticed when operating within this space. It can be seen that for the intra-cardiac link, the outage probabilities are extremely low even with a high gain antenna on Eve’s side. This is because of the low path loss between intra-cardiac leadless pacemakers. For the subcutaneous link, the MICS band provides the best results with an outage probability of 10^{-6} at Eve’s distance of 25 cm and 10^{-26} at 50 cm. For an individual personal space of 50 cm, the worst results are for ISM 868 MHz with an antenna gain of 10 dBi at Eve’s side and have the outage probability of secrecy capacity to be 10^{-9} at 50 cm. But with required dimensions of e.g., $30 \times 30 \text{ cm}^2$, it will hardly be possible for an eavesdropper to remain unobserved.

Table 2. Comparison of outage probability (OP) of secrecy capacity for scenarios with and without antenna gain at the eavesdropper.

Frequency Band	Effective Aperture (cm ²)		Intra-Cardiac Link (L1)				Subcutaneous Link (L2)			
			OP at 0 dBi		OP at 10 dBi		OP at 0 dBi		OP at 10 dBi	
	For 0 dBi	For 10 dBi	25 cm	50 cm	25 cm	50 cm	25 cm	50 cm	25 cm	50 cm
MICS	21 × 21	66 × 66	10 ⁻⁵⁴	10 ⁻¹¹³	10 ⁻²⁴	10 ⁻⁶⁷	10 ⁻¹⁸	10 ⁻⁵¹	10 ⁻⁶	10 ⁻²⁶
WMTS	19 × 19	61 × 61	10 ⁻⁴⁶	10 ⁻⁹⁸	10 ⁻²³	10 ⁻⁶¹	10 ⁻¹¹	10 ⁻³²	10 ⁻⁴	10 ⁻¹⁸
ISM 868 MHz	10 × 10	30 × 30	10 ⁻²⁸	10 ⁻⁵⁶	10 ⁻¹²	10 ⁻³⁰	10 ⁻⁸	10 ⁻²²	1.8 × 10 ⁻¹	10 ⁻⁹

These results prove that there is a good probability to achieve positive secrecy capacity in near premises of the patient and also a secure communication rate can be achieved for the cardiac application, even if the eavesdropper is attached to the patient’s body. The cardiac application rates mainly correspond to heart rate, blood pressure (1.92 kbps), respiratory rate (1 kbps), pulse rate (2.4 kbps) and ECG with maximum required data rate of 2.5–250 kbps [30,31]. These data rates are well below the fixed secure communication rate for which Eve’s distances are specified.

In case of achieving positive secrecy capacity and low outage probability, MICS band could be

the best choice to be used for implanted medical devices. However, it is difficult to develop a small efficient antenna with good reflection coefficient taking into consideration its practical realization at lower frequencies. On the other hand, there is a good possibility to develop small efficient antennas at higher frequencies, but the losses definitely increase as well as the secrecy capacity is achieved at a greater distance than in the MICS band. Thus, from practical considerations, ISM 868 MHz will be a good choice for developing small antennas with good efficiency and acceptable outage probabilities of the secrecy capacity.

5. Conclusions

The secrecy capacity for wireless in-body channels has been evaluated in different frequency bands that include MICS, WMTS and ISM 868 MHz. With an application for multi-nodal leadless cardiac pacemakers, the probability of positive secrecy capacity and outage probability of fixed secure communication rate has been determined for legitimate links, i.e., intra-cardiac link (link *L1* between leadless pacemakers inside the heart) and subcutaneous link (link *L2* between leadless pacemaker inside the heart and subcutaneous implant). By considering an individual personal space of 50 cm, it has been found that the intra-cardiac link is not critical in terms of outage probability of secure communication rate of 1 bps/Hz, even with an antenna gain of 10 dBi for the eavesdropper. The maximum outage probability of the secrecy capacity for a subcutaneous link (*L2*) is 10^{-9} , for Eve at a distance of 50 cm having an antenna gain of 10 dBi. This corresponds to one patient in a billion which is a very good number considering the application sensitivity and the eavesdropping scenario.

In the future, the impact of active eavesdroppers will be considered on the secrecy metrics of the system. The channel models will also be developed further and refined using more simulations and experiments. The experiments could involve development of phantoms used for in-body experimentation, which is a chemical solution that replicates the dielectric properties of human organs.

Author Contributions: Conceptualization, M.F.A., M.R. and K.K.; Methodology, M.F.A.; Validation, N.N. and K.K.; Formal Analysis, M.F.A.; Software, M.F.A. and X.F.; Investigation, M.F.A., M.R. and X.F.; Resources, M.F.A. and X.F.; Data Curation, M.F.A., M.R. and X.F.; Writing—Original Draft Preparation, M.F.A.; Writing—Review & Editing, M.R., X.F., N.N. and K.K.; Visualization, M.F.A.; Supervision, K.K. and N.N.; Project Administration, K.K., N.N., Q.W. and D.P.; Funding Acquisition, K.K.

Funding: This work was supported by the Marie Curie Research Grants Scheme, with project grant no 675353, EU Horizon 2020-WIBEC ITN (Wireless In-Body Environment). Details can be found at a source https://cordis.europa.eu/project/rcn/198286_en.html (accessed on 2 September 2019)

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

C1	Leadless pacemaker in Right Atrium
C2	Leadless pacemaker in Right Ventricle
C_s	Secrecy Capacity
CST	Computer Simulation Technology
CDF	Cumulative Distributive Function
E1	Link between C1 and Eve
ECG	Electrocardiography
EM	Electromagnetic
EMG	Electromyogram
IB2IB	In-Body to In-Body
IB2OFF	In-Body to Off-Body
ICD	Implanted Cardioverter Defibrillator
ISM	Industrial Scientific and Medical Frequency Band

L1	Link between C1 and C2
L2	Link between C1 and subcutaneous implant (S)
LCP	Leadless Cardiac Pacemaker
MICS	Medical Implant Communication Systems
OP_{cs}	Outage probability of secrecy capacity
\mathcal{P}_{psc}	Probability of Positive Secrecy Capacity
PL	Path Loss
PLS	Physical-Layer Security
RF	Radio Frequency
R_s	Fixed Secure Communication Rate
Rx	Receiver
SNR	Signal to Noise Ratio
Tx	Transmitter
UWB	Ultrawide Band
WMTS	Wireless Medical Telemetry Service
WBAN	Wireless Body Area Network
WiBEC	Wireless In-body Environment

Appendix A

$$\mathcal{P}(C_s > 0) = \frac{1}{4a\sqrt{2\pi}} \int_0^\infty \frac{1}{\gamma_e} \times \left(1 - Q\left(\frac{1}{4b} \ln \frac{\gamma_e}{n}\right)\right) \times \exp\left(\frac{1}{2} \left(\frac{1}{4a} \ln\left(\frac{\gamma_e}{m}\right)\right)^2\right) d\gamma_e \quad (A1)$$

Consider,

$$x = \frac{1}{4b\sqrt{2}} \ln\left(\frac{\gamma_e}{n}\right) \quad (A2)$$

Then (A1) becomes

$$\mathcal{P}(C_s > 0) = \frac{b}{a\sqrt{\pi}}(\alpha - \beta) \quad (A3)$$

where,

$$\alpha = \int_{-\infty}^\infty \exp\left(-\left(\frac{b}{a}\right)^2 \left(x + \frac{1}{4b\sqrt{2}} \ln\left(\frac{n}{m}\right)\right)^2\right) dx = \frac{a\sqrt{\pi}}{b} \quad (A4)$$

$$\beta = \int_{-\infty}^\infty Q(x\sqrt{2}) \exp\left(-\left(\frac{b}{a}\right)^2 \left(x + \frac{1}{4b\sqrt{2}} \ln\left(\frac{n}{m}\right)\right)^2\right) dx \quad (A5)$$

Using Middleton’s work ([32], p. 1072), β can be expressed as

$$\beta = \frac{a\sqrt{\pi}}{b} Q\left(\frac{\ln(n/m)}{4\sqrt{a^2 + b^2}}\right) \quad (A6)$$

which follows,

$$\mathcal{P}(C_s < R_s) = Q\left(\frac{\ln \frac{\mu_{\gamma_r}}{\mu_{\gamma_e}} + 8(b^2 - a^2) - R_s \ln 2}{4\sqrt{a^2 + b^2}}\right) \quad (A7)$$

and

$$\mathcal{P}(C_s > 0) = Q \left(\frac{\ln \mu_{\gamma_e} - \ln \mu_{\gamma_r} + 8(b^2 - a^2)}{4\sqrt{a^2 + b^2}} \right) \quad (\text{A8})$$

References

- Mond, H.G.; Proclemer, A. The 11th world survey of cardiac pacing and implantable cardioverter-defibrillators: Calendar year 2009—A world society of Arrhythmia's project. *Pacing Clin. Electrophysiol.* **2011**, *34*, 1013–1027. [[CrossRef](#)] [[PubMed](#)]
- Awan, M.F.; Kansanen, K. Estimating eavesdropping risk for next generation implants. In *Advances in Body Area Networks I*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 387–398.
- Chorti, A.; Perlaza, S.M.; Han, Z.; Poor, H.V. Physical layer security in wireless networks with passive and active eavesdroppers. In Proceedings of the 2012 IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, USA, 3–7 December 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 4868–4873.
- Halperin, D.; Heydt-Benjamin, T.S.; Ransford, B.; Clark, S.S.; Defend, B.; Morgan, W.; Fu, K.; Kohno, T.; Maisel, W.H. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In Proceedings of the 2008 IEEE Symposium on Security and Privacy (sp 2008), Oakland, CA, USA, 18–21 May 2008; IEEE: Piscataway, NJ, USA, 2008; pp. 129–142.
- Camara, C.; Peris-Lopez, P.; Tapiador, J.E. Security and privacy issues in implantable medical devices: A comprehensive survey. *J. Biomed. Inform.* **2015**, *55*, 272–289. [[CrossRef](#)] [[PubMed](#)]
- Zhang, M.; Raghunathan, A.; Jha, N.K. MedMon: Securing medical devices through wireless monitoring and anomaly detection. *IEEE Trans. Biomed. Circuits Syst.* **2013**, *7*, 871–881. [[CrossRef](#)] [[PubMed](#)]
- Son, S.; Lee, K.; Won, D.; Kim, S. U-healthcare system protecting privacy based on cloaker. In Proceedings of the 2010 IEEE International Conference on Bioinformatics and Biomedicine Workshops (BIBMW), Hong Kong, China, 18–21 December 2010; IEEE: Piscataway, NJ, USA, 2010; pp. 417–423.
- Gollakota, S.; Hassanieh, H.; Ransford, B.; Katabi, D.; Fu, K. They can hear your heartbeats: Non-invasive security for implantable medical devices. *ACM SIGCOMM Comp. Commun. Rev.* **2011**, *41*, 2–13. [[CrossRef](#)]
- PTC. *Meeting International Standards for Medical Device Reliability and Risk Management*; The Product Development Company (PTC): Needham, MA, USA, 2011. Available online: <https://3hti.com/wp-content/uploads/documents/Medical-Device-Reliability-White-Paper.pdf> (accessed on 2 September 2019).
- Fries, R.C. *Reliable Design of Medical Devices*; CRC Press: New York, NY, USA, 2016.
- Shannon, C.E. Communication theory of secrecy systems. *Bell Labs Tech. J.* **1949**, *28*, 656–715. [[CrossRef](#)]
- Wyner, A.D. The wire-tap channel. *Bell Labs Tech. J.* **1975**, *54*, 1355–1387. [[CrossRef](#)]
- Bloch, M.; Barros, J.; Rodrigues, M.R.; McLaughlin, S.W. Wireless information-theoretic security. *IEEE Trans. Inf. Theory* **2008**, *54*, 2515–2534. [[CrossRef](#)]
- Jameel, F.; Wyne, S.; Kaddoum, G.; Duong, T.Q. A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 2734–2771. [[CrossRef](#)]
- Atallah, M.; Kaddoum, G. Secrecy Analysis in Wireless Network with Passive Eavesdroppers by Using Partial Cooperation. *IEEE Trans. Veh. Technol.* **2019**, *68*, 7225–7230. [[CrossRef](#)]
- Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2702–2733. [[CrossRef](#)]
- Awan, M.F.; Kansanen, K.; Perez-Simbor, S.; Garcia-Pardo, C.; Castelló-Palacios, S.; Cardona, N. RSS-Based Secret Key Generation in Wireless In-body Networks. In Proceedings of the 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), Oslo, Norway, 8–10 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
- Liang, Y.; Poor, H.V.; Shamai, S. Information theoretic security. *Found. Trends Commun. Inf. Theory* **2009**, *5*, 355–580. [[CrossRef](#)]
- Awan, M.; Perez-Simbor, S.; Garcia-Pardo, C.; Kansanen, K.; Cardona, N. Experimental Phantom-Based Security Analysis for Next-Generation Leadless Cardiac Pacemakers. *Sensors* **2018**, *18*, 4327. [[CrossRef](#)] [[PubMed](#)]

20. Awan, M.F.; Perez-Simbor, S.; Garcia-Pardo, C.; Kansanen, K.; Bose, P.; Castelló-Palacios, S.; Cardona, N. Experimental phantom-based evaluation of Physical Layer Security for Future Leadless Cardiac Pacemaker. In Proceedings of the 2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Bologna, Italy, 9–12 September 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 333–339.
21. Studio, M. CST-Computer Simulation Technology. *Bad Nuheimer Str.* **2008**, *19*, 64289.
22. ANSYS-HFSS. Available online: <https://www.ansys.com/products/electronics/ansys-hfss> (accessed on 2 September 2019).
23. Garcia-Pardo, C.; Fornes-Leal, A.; Cardona, N.; Chávez-Santiago, R.; Bergsland, J.; Balasingham, I.; Brovoll, S.; Aardal, Ø.; Hamran, S.E.; Palomar, R. Experimental ultra wideband path loss models for implant communications. In Proceedings of the IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Valencia, Spain, 4–7 September 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–6.
24. Garcia-Pardo, C.; Chávez-Santiago, R.; Cardona, N.; Balasingham, I. Experimental UWB frequency analysis for implant communications. In Proceedings of the 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), Milano, Italy, 25–29 August 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 5457–5460.
25. Chávez-Santiago, R.; Garcia-Pardo, C.; Fornes-Leal, A.; Vallés-Lluch, A.; Vermeeren, G.; Joseph, W.; Balasingham, I.; Cardona, N. Experimental path loss models for in-body communications within 2.36–2.5 GHz. *IEEE J. Biomed. Health Inform.* **2015**, *19*, 930–937. [[CrossRef](#)] [[PubMed](#)]
26. Kadel, R.; Islam, N. Comparison of Channel Models for Wireless Body Area Networks (WBANs). In Proceedings of the 2018 IEEE Conference on Wireless Sensors (ICWiSe), Langkawi, Malaysia, 21–22 November 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 77–82.
27. Leung-Yan-Cheong, S.; Hellman, M. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory* **1978**, *24*, 451–456. [[CrossRef](#)]
28. Amar, A.B.; Kouki, A.B.; Cao, H. Power approaches for implantable medical devices. *Sensors* **2015**, *15*, 28889–28914. [[CrossRef](#)] [[PubMed](#)]
29. Liu, X. Secrecy capacity of wireless links subject to log-normal fading. In Proceedings of the 7th International Conference on Communications and Networking in China (CHINACOM), Kunming, China, 8–10 August 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 167–172.
30. Islam, M.N.; Yuce, M.R. Review of medical implant communication system (MICS) band and network. *Ict Express* **2016**, *2*, 188–194. [[CrossRef](#)]
31. Wang, J.; Wang, Q. *Body Area Communications: Channel Modeling, Communication Systems, and EMC*; John Wiley & Sons: Chichester, UK, 2012.
32. Middleton, D.; Institute of Electrical and Electronics Engineers. *An Introduction to Statistical Communication Theory*; IEEE: Piscataway, NJ, USA, 1996.



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

Appendix E

Information Theoretic Analysis for IMDs

Paper E: Information Theoretic Analysis for Securing Next
Generation Leadless Cardiac Pacemaker

Muhammad Faheem Awan, Kimmo Kansanen, and Deepak Palaksha
2018, 13th EAI International Conference on Body Area Networks

This article is not included due to copyright

Appendix F

Evaluation of Spatial Secrecy Capacity

Paper F: Evaluation of Secrecy Capacity for Next-Generation

Leadless Cardiac Pacemaker

Muhammad Faheem Awan, Pritam Bose, Ali Khaleghi, Kimmo Kansanen,
Ilanko Balasingham

IEEE Transactions on Biomedical Engineering, 2019



Evaluation of Secrecy Capacity for Next-Generation Leadless Cardiac Pacemakers

Muhammad Faheem Awan, Pritam Bose, Ali Khaleghi, *Senior Member, IEEE*, Kimmo Kansanen, *Senior Member, IEEE*, and Ilanko Balasingham, *Senior Member, IEEE*

Abstract—Secure communication can be considered as an integral part of the next generation implantable medical devices. With the advent of physical layer security (PLS) methods, confidential messages can be transmitted without the use of encryption keys. For analyzing the effectiveness of PLS for next-generation leadless cardiac pacemakers, we provide secrecy analysis using a performance metric of secrecy capacity. Secrecy capacity defines the secure transmission rate between legitimate nodes without leakage of information to an eavesdropper and depends on respective channel attenuations. The legitimate and eavesdropper channel attenuations are evaluated by 3D numerical electromagnetic simulations using a detailed human model. We do not assume eavesdropper to be located in specific directions or positions and considers it to be located anywhere around the body. We evaluate the secrecy capacity by defining a spherical grid for eavesdropper positions around the body with a radius of 1 m. The secrecy capacity of the entire space is evaluated by extrapolating the grid to different radial distances using free space path loss model. Moreover, by fixing application based secure communication rate, the entire space is divided into secure and in-secure volumes. The in-secure volume consists of all the eavesdropper positions from which the pacemaker can be eavesdropped. We also evaluated the angle from which the maximum leakage of information takes place and referred it as “Eve’s sweet spot angle”. Data for channel attenuations from phantom and in-vivo experiments is also utilized to validate and observe the differences between simulations and experiments. This work will help in design of the communication module of implanted leadless cardiac pacemakers with enhanced security on the physical layer.

Index Terms—Physical layer security; Secrecy capacity; Leadless cardiac pacemakers; Privacy and Security, Implantable medical devices

Manuscript received 31 May, 2019; Revised 25 Oct, 2019; Accepted 03 Dec, 2019. This work was supported by the EU’s H2020 MSCA-ITN grant for the Wireless In-Body Environment (WiBEC) project with grant no: 675353 and “Research council of Norway project — Wireless In-Body Sensor and Actuator Networks - WINNOR — with grant no. 270957/070. (Corresponding author: Muhammad Faheem Awan.)

Muhammad Faheem Awan and Kimmo Kansanen are with the Department of Electronic Systems, Norwegian University of Science and Technology, Trondheim, 7491 Norway e-mail: faheem.awan@ntnu.no and kimmo.kansanen@ntnu.no

Ali Khaleghi and Ilanko Balasingham are with the Intervention Center, Oslo University Hospital, NO-0027 Oslo and with the Department of Electronic Systems, Norwegian University of Science and Technology, 7491 Trondheim, Norway (e-mail: ali.khaleghi@rr-research.no and ilanko.balasingham@medisin.uio.no)

Pritam Bose is with Intervention Center, Oslo University Hospital, NO-0027 Oslo, Norway (e-mail: pritam.bose@studmed.uio.no)

I. INTRODUCTION

The technological advancements in personal health systems have led to the development of different wearable and implantable medical devices and systems. These developments also motivate transformation of decades old implantable medical devices (IMD’s) such as cardiac pacemakers and implantable cardioverter defibrillators (ICDs).

A. Cardiac Pacemakers

Pacemakers are medical devices that are implanted in patients with abnormal heart rhythms. About 1 million pacemakers are implanted annually worldwide [1]. Traditional pacemakers contain a subcutaneous implant (usually called “Can”) implanted in the pectoral pocket below the shoulder. The Can is connected to the transvenous wires or ‘leads’ that pierce into, and run down, the subclavian vein where they are fixed to the inner walls of the heart. These leads contain electrodes to the distal ends that sense irregularities and provides electric excitation to maintain proper heart rhythm. Depending on the specific cardio-pathology, the electrodes can lie in the right ventricle, right atrium or in the coronary sinus above the left ventricle [2]. The transvenous leads are considered to be the weak side of a traditional pacemaker system because they can fracture, they may lead to infection, and also their explantation carries significant risk of mortality [3], [4]. Consequently, the next generation of these pacemaker systems is becoming wireless by getting rid of transvenous leads. Fig. 1 shows the traditional cardiac re-synchronization therapy (CRT) management system and one of the variant of next generation pacemaker system, hosting battery driven, physically small leadless capsules that may be placed in multiple heart chambers and being able to communicate with a subcutaneous implant wirelessly which can relay data to an external monitor¹. These capsules need to be computationally less complex and consume less power than the traditional pacemakers. Besides unquestionable benefits, the wireless communication expose the leadless cardiac pacemaker (LCP) to the potential eavesdroppers compromising privacy, confidentiality and most importantly patient safety.

B. Motivation and Background

The comprehensive survey on privacy and security issues related to IMD’s is provided in [5]. Similarly, [6] discusses

¹EU Horizon 2020 Project WiBEC “Wireless In Body Environment.

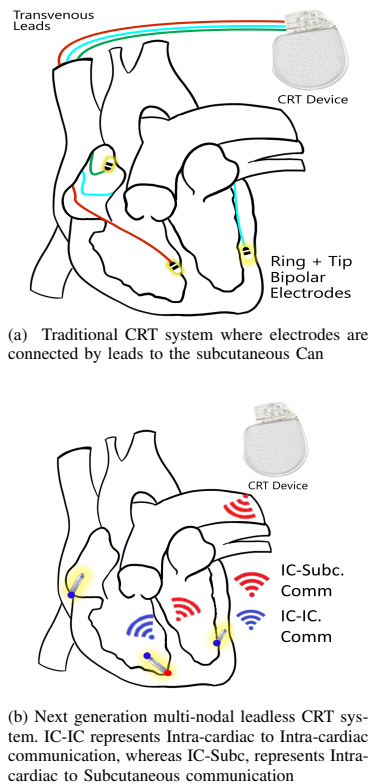


Fig. 1: Comparison between traditional (a) and a variant (b) of the next generation CRT systems.

the challenges, goals, and need of securing IMD's. In order to show the security concerns, Halperin et al. in [7] performed eavesdropping attacks on an insecure communication link of ICD device to obtain the patient's data, using an off the shelf programmer, directional antennas and software defined radio. This work was followed by a number of scientific publications [8]–[11] to address the security concerns of IMD's.

Traditionally, the wireless communication networks are secured by conventional cryptographic methods at the upper layers of communication paradigm. However numerous challenges arise in key establishment and distribution for newly evolved paradigms like wireless in-body networks. Lately, physical layer security (PLS) has been identified as a feasible alternative to secure wireless transmissions via exploiting different characteristics of wireless channels [12]–[14]. The concept of PLS was first presented by Shannon [15] in 1949 which was further extended by Wyner in [16] with introduction to wire-tap channel. Csiszar et al. [17] broaden the idea by presenting the transmission of confidential messages over broadcast channels. These works demonstrated the benefits of using different secure transmission techniques at physical layer.

The approaches to achieve physical layer security can exist

either as keyless or key based usually referred to as channel model and source model approaches respectively. Using the source model approach, the legitimate nodes utilize the correlated randomness of different wireless channel characteristics e.g. received signal strength (RSS), channel impulse response, phase, angle of arrival (AoA) or human biometrics in case of wireless body area network (WBAN) [18]–[22]. A comprehensive survey is provided in [23].

In contrast to the source model approach, the keyless approach or channel model approach, information theoretically secure the transmissions by utilizing the physical medium (channel fluctuations, attenuations, and noises), and make use of the channel difference between legitimate receiver and eavesdropper to benefit the legitimate party. Different methods are proposed in the literature to secure standard wireless network transmissions using channel model approach with focus to degrade the Eve channel by making it noisier than legitimate channel. It can be achieved by using cooperative jamming, with external helpers, relays, full duplex receiver with multiple antennas or adding the artificial noise. Biao et al. in [24] secure the single antenna systems by introducing artificial noise. Similarly, in [25], different theoretical limits for practical design of PLS jamming in standard wireless networks are presented with introduction to transmit and receive jamming whereas [26], [27] explores different secrecy rate optimization techniques for multicast networks. A comprehensive survey on PLS channel model approaches is provided in [28], [29].

The key performance metric in channel model approaches is secrecy capacity, playing a central role in PLS. It characterizes the fundamental limit on secure communications over noisy channels and is mainly associated to a channel model referred as wire-tap channel. Secrecy capacity captures the maximum transmission rate (R) that can be achieved ensuring the reliability, and by considering the extreme case of no information leakage to eavesdropper. In contrast to capacity of a link which is a communication rate for reliable communication, secrecy capacity reflects both reliability and confidentiality with a cost of reduction in communication rate. It is a system performance metric that characterizes the bound based on the channel characteristics. Once the design limits are known, one can choose among different wiretap codes² for transmission of confidential information without encryption³.

The wireless in-body network e.g. Leadless cardiac pacemaker, with an eavesdropper outside, motivates a similar scenario of a wiretap model. This is because the human body being a lossy medium for electromagnetic propagation can inherently provide high attenuations to off body links. Hence, utilizing channel model approach of PLS in context of in-body networks could have substantial benefits that includes from avoiding the key management and distribution challenges to existing along with traditional cryptographic methods to provide an extra layer of security at the physical layer for sensitive applications like pacemakers. Furthermore, to the best of authors knowledge, none of the work exist in context of detail

²e.g LDPC, Polar wiretap codes

³We do not delve in detail of encoding and decoding of wiretap coding, and kept the information theoretic part to as minimum as possible

evaluation of the secrecy capacity for in-body wireless sensors network where one can utilize the naturally available wiretap channel between in-body and off-body nodes (eavesdropper) to provide secrecy on the physical layer.

To reap the aforementioned benefits of channel model approach of PLS, the feasibility analysis of securing next generation leadless cardiac pacemaker has been explored. This is done by considering the wiretap scenario of Wyner's model, and modeling the legitimate and eavesdropper channel, using electromagnetic (EM) simulations, phantoms and in-vivo experiments. Considerable literature exists on channel modeling of WBAN. Sayrafian *et. al.* in [30] proposes a statistical path loss model for implant to implant communication, considering different in-body scenarios. Similarly, Antonietta *et. al* in [31] characterizes in-body to off-body link in medical implant communication systems (MICS) band for upper limb prostheses using electromagnetic simulations. Concepcion, *et al* in [32] discuss different approaches for propagation analysis in an ultrawide (UWB) frequency band. Similarly, earlier works [33], [34], based on EM simulations examines different antennas for implanted and on-body communication systems in industrial scientific and medical (ISM) and MICS frequency band. A comprehensive review on different propagation models, frequency bands, and communication scenarios is provided in [35] whereas [36] provides a review on human body communication as an alternative for communication between body area network nodes.

The channel modeling methods of this work introduces different forefronts over existing models. The EM simulations performed in this work considers the highly detail human model (Hugo model) and are specifically application based (Cardiac pacemakers). Furthermore, for experiments, a small battery powered antenna with transmitter is utilized instead of using conventional coaxial cables and vector network analyzer (VNA) for generation of sounding signal. This is because, in case of small dimensions of antenna, the adjoined coaxial cables also radiate which is being ignored by authors in the literature [37]. Another aspect of this work is that it evaluates the in-body to off-body link (Eve link) directly from deep implant (inside the right ventricle) and computes the channel attenuation of entire space around the body.

In this work, simulations and tests are performed in the ISM frequency band (2.4 GHz). The selection of ISM frequency band is done due to smaller antenna dimensions with good radiation efficacy and matching [38]. In addition, Federal Communications Commission (FCC) also includes ISM 2.36-2.40 GHz spectrum in medical device communication (MedRadio) for body area networks [39].

C. Contributions

To the best of authors knowledge, this work is the first to explore channel model approach of PLS methods for in-body wireless networks with an application of next generation leadless cardiac pacemaker. A popular three-node model is considered, where the legitimate node, Alice (Leadless pacemaker/capsule, *A*) in the right ventricle of a human heart is communicating with Bob (Subcutaneous implant, *B*). In

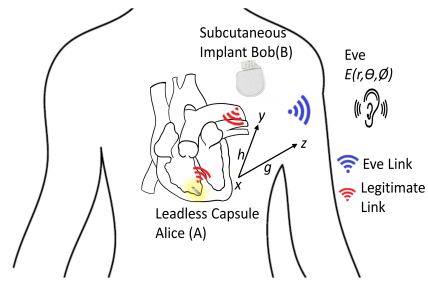


Fig. 2: Leadless capsule (Alice) communicating confidential message “X” through the in-body channel with a subcutaneous implant (Bob), and Eve, eavesdropping the communication through a channel which is a combination of in-body and free space

contrast to considering Eve at a certain specific position as usually done in literature for free space wireless networks, in this work Eve is considered to be located anywhere at any angle in three dimensional space around the body and her location can be presented using spherical coordinates (r, θ, ϕ) — r is the radius, θ is the elevation angle and ϕ is the azimuth angle. The key contributions in the paper are:

- Characterization of the Alice-Bob (AB) and Alice-Eve (AE) channels by numerical electromagnetic (EM) simulations using a detailed computational human model (HUGO Model), a phantom and in-vivo experiments.
- EM-Simulation based evaluation of secrecy capacity of the entire space around the body, first by defining a spherical grid for Eve at a radius of 1 m, then using the free space path loss model to extrapolate it over the entire space for different radial distances.
- EM-Simulation based evaluation of secure and in-secure volume around the body by considering the cardiac application based fixed secure transmission rate. The in-secure volume consists of all Eve's positions from which the leadless capsule can be eavesdropped.
- Worst-case analysis of secrecy capacity by considering eavesdropper at a sweet spot angle — the angle with maximum information leakage.
- For validation and comparison of EM-simulation results, the phantom and in-vivo experiments are also performed.

The paper is structured as follows. Section II provides System model and methodology whereas Section III, contains the results. Section IV discusses the results and finally Section V concludes the paper.

II. SYSTEM MODEL AND METHODOLOGY

In Fig. 2, a future LCP is depicted where Alice communicates with a subcutaneous implant Bob and Eve, outside the body, tries to eavesdrop the communication. Alice is located in the right ventricle (RV) of the heart whereas Bob is placed in the subcutaneous space under the shoulder. Eve is not assumed to be in any specific position and can be located anywhere, at any angle around the body in three-dimensional

space presented in the spherical coordinate system.

Alice transmits a confidential message X to Bob. Thus, for a single channel realization, the input-output relation between Alice-Bob (AB) and Alice-Eve (AE) can be expressed as

$$\begin{aligned} y &= hx + n_1 \\ z &= gx + n_2, \end{aligned} \quad (1)$$

where x is the transmitted signal, y is the channel output to the Bob and z is the channel output to the Eve. The channel coefficients between Alice and Bob and Alice and Eve are represented by h and g where n_1 and n_2 are the complex Gaussian noises with mean μ and variance σ^2 and can be represented as $\mathcal{CN}(0, \sigma^2)$. We assume that x , n_1 , and n_2 are stochastically independent. The signal to noise (SNR) ratio at Bob and Eve can be expressed as

$$\gamma_b = \frac{|h_{(x,y)}|^2 P}{\sigma^2}, \quad (2)$$

$$\gamma_e = \frac{|g_{(r,\theta,\phi)}|^2 P}{\sigma^2}, \quad (3)$$

where, $|h_{(x,y)}|^2$ and $|g_{(r,\theta,\phi)}|^2$ are the respective channel attenuations by considering Bob at position (x,y) and Eve at (r, θ, ϕ) respectively. Eve could have higher SNR outside the body at some respective angles than AB channel, even at larger distances. This is because the body provides more loss to EM radiations than free space. Thus, at some specific angles, the transmission path encounters more non-homogeneous medium (less in-body than free space) causing the power received outside the body to be higher. Therefore, our system model can be considered as a non-degraded version of Gaussian wiretap channel, in which the AE channel can have better SNR than the AB channel. In order to transmit securely between Alice and Bob, the secrecy capacity for non-degraded Gaussian wiretap channel [17], [40] can be expressed as

$$C_S = \begin{cases} [C_B - C_E]^+, & \text{if } \gamma_b > \gamma_e \\ 0, & \text{otherwise} \end{cases} \quad (4)$$

where C_B and C_E are the channel capacities of AB and AE link which can be expressed as

$$\begin{aligned} C_B &= \log_2(1 + \gamma_b) \\ C_E &= \log_2(1 + \gamma_e). \end{aligned} \quad (5)$$

The resultant secrecy capacity by considering eavesdropper at any direction around the body can be expressed as

$$C_S(r, \theta, \phi) = \begin{cases} \left[\log_2 \frac{\left(1 + \frac{|h_{(x,y)}|^2 P}{\sigma^2}\right)}{\left(1 + \frac{|g_{(r,\theta,\phi)}|^2 P}{\sigma^2}\right)} \right]^+, & |h_{x,y}|^2 < |g_{r,\theta,\phi}|^2 \\ 0, & \text{Otherwise} \end{cases} \quad (6)$$

After evaluating the secrecy capacity of all the AB-AE link channel attenuations in the entire space, we divide the space around the body into secure and in-secure volumes. For fixed AB attenuation and communication rate, we solve for all the AE attenuations that lie in the secure and in-secure volumes.

The in-secure volume defines all the Eve distances from which LCP can be eavesdropped, and can be expressed as

$$d_{E(r,\theta,\phi)} \leq r \times 10^{\left(\frac{P - \beta - 10 \log_{10}(2^{(C_B - C_S) - 1}) - \sigma^2}{10n} \right)}. \quad (7)$$

$\forall (r, \theta, \phi)$

The derivation of (7) is provided in Appendix I for simplicity.

For a given power, AB attenuation and secrecy rate, (7) holds for all (r, θ, ϕ) . Beyond the in-secure volume, communication is considered to be secure for a given secrecy rate. In (7), $d_{E(r,\theta,\phi)}$ is the eavesdropper distance at a specific angle from Alice, C_B is the capacity of the AB link, C_S is the fixed secrecy rate for communication, r is the reference eavesdropper distance and is equal to 1 m, σ^2 is the noise power and β is the Eve channel attenuation at the reference eavesdropper distance.

The secrecy capacity depends on AB and AE channel attenuations as shown in (6) and (7). Thus, we simulate the in-body environment to evaluate the respective channel attenuations. To validate the EM-simulation results, experimental tests are also performed. This helps in assessing the differences and similarities between results from simulations and experimentation⁴. In addition, the experiments can also help validate whether the EM simulations in CST can efficiently predict the channel losses or not. Thus for channel modeling, EM simulations are presented first, followed by phantom and in-vivo experiments.

A. Electromagnetic (EM) Simulations

For estimating channel attenuations, EM simulations are performed by using the 3D EM simulation tool CST⁵ [41]. This work utilizes the anatomical data set of the Visible Human Project [42], [43], from which the developed voxel model in CST is referred as HUGO model. The HUGO model is developed from a dissected male corpse that is segmented into multiple layers. These layers are then sampled and interpolated to provide a highly efficient computational model of the human body. The dielectric properties of each individual biological tissue have been considered in the model. The model offers different tissues and resolutions (1 mm to 8 mm) to select. Due to shorter wavelengths in 2.4 GHz, in this work, we opted for a resolution of $1 \times 1 \text{ mm}^2$. The communication element, the capsule (Alice), is modeled as an ideal dipole antenna with 100 % efficiency. The antenna is 5 mm in length and 2 mm in diameter. The antenna is encapsulated inside a vacuum tube of 1 mm in width to avoid the direct contact with body tissues.

1) *Legitimate/AB-link*: The AB link is simulated by placing a capsule (dipole antenna, Alice) in the right ventricle (RV) of the heart along with the placement of other dipole antennas (Bobs) in the subcutaneous space as shown in Fig. 3. The subcutaneous space is the space under the skin beneath the shoulder. In addition, to observe the effect of antenna polarization on channel attenuation ($|h_{(x,y)}|^2$), two set of experiments are conducted, one by placing the dipole antenna in the horizontal direction (transverse plane) and the other in

⁴We concentrate only on antennas, not the entire TX/RX communication chain

⁵<https://www.cst.com/>

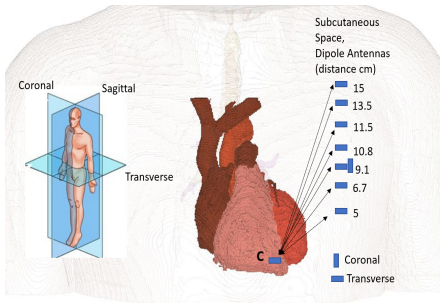


Fig. 3: Position of the leadless capsule (Alice) in the right ventricle, transmitting to the antenna (Bob) positioned at different distances in subcutaneous space. Reference representation of coronal, sagittal and transverse planes with respect to the human body

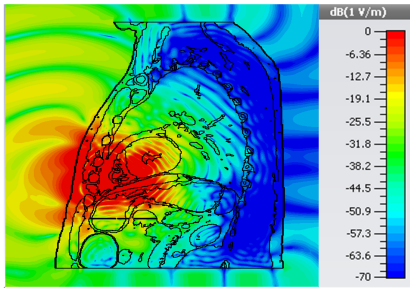


Fig. 4: Radiation of electric field strength, by placing the dipole antenna inside the right ventricle. The bar shows the field intensity (V/m), in and around the body. (Side view)

vertical direction (coronal plane). First, all the antennas are placed in the transverse plane to determine the attenuation between Alice and Bob. Then, the receiving antenna at one of the subcutaneous position is changed from transverse to coronal plane and the difference in the attenuation is observed. The results with EM simulations contain both the observations.

2) Eavesdropper/AE-link: The electromagnetic radiations from the Alice radiate in all directions outside the body as shown in Fig. 4. We place in a total of 100 electric probes in three-dimensional space around the body with a sphere of radius 1 m. The entire sphere is partitioned in five elevation angles (θ), each of which is further partitioned into twenty azimuth angles (ϕ) (Fig. 5), totaling a spherical grid of 100 Eve positions to observe the field strength. Couple of electric probes are also positioned at large radial distances in order to verify the applicability of the free space path loss model. This helps in extrapolating the spherical grid to different radial distances. The electric probes are used because by placing dipole antennas outside the body at the distance of 1 m, results in a very huge mesh size to resolve. Therefore, due to the extensive computational cost of using dipole antennas, electric probes are used to determine the electric field intensity which

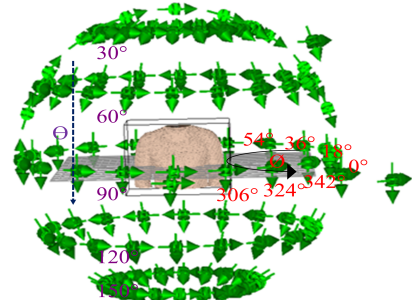


Fig. 5: Placement of electric probes around the body to receive electric field intensity. In total 100 electric probes are placed at a radius of 1 m, 20 probes along azimuth angle (ϕ), 18° apart and 5 elevation angles (θ) with 30° apart. The left arm is considered as 0° for azimuth angle and then rotated anti-clockwise. Couple of probes are outside the sphere at a radius of 2 m

is then transformed to the power density using

$$S(r, \theta, \phi) = \frac{1}{2} \frac{|E(r, \theta, \phi)|^2}{Z_o}, \quad (8)$$

where S is the received power density (W/m^2) at each probe, E is the received electric field and Z_o is the intrinsic impedance of free space. The total power received at each probe depends upon the effective aperture of an antenna and can be expressed as

$$P(r, \theta, \phi) = S(r, \theta, \phi) \times A_{eff}, \quad (9)$$

where $P(r, \theta, \phi)$ is the total power received, S is the power density and A_{eff} is the effective aperture of the antenna. From received power, the Eve channel attenuation ($|g_{(r,\theta,\phi)}|^2$) is evaluated. The AE-link attenuation can be expressed as

$$\beta = |g_{(r,\theta,\phi)}|^2_{dB} = P - P(r, \theta, \phi), \quad \forall (\theta, \phi) \quad (10)$$

where r is the reference distance of 1 m, θ and ϕ are reference angles in the spherical coordinates, and P is the transmit power which for simplicity is considered as 0 dBm. In order to extrapolate the path loss over the entire space for different radial distances, the free space path loss model is utilized which can be expressed as

$$PL_{r,\theta,\phi}(d_E) = \beta + 10 \times n \times \log_{10} \left(\frac{d_E}{r} \right), \quad (11)$$

where, n is the free space path loss exponent with a value of 2. d_E is the distance to extrapolate beyond 1 m with the reference β , evaluated using (10) from the EM simulations.

B. Phantom Experiment

The methodology used in the phantom experiments is adapted to corroborate the results obtained from simulations. It also helps to observe the differences by implementing the setup in practical scenarios using realistic antennas. To evaluate channel attenuations, the phantom with dielectric

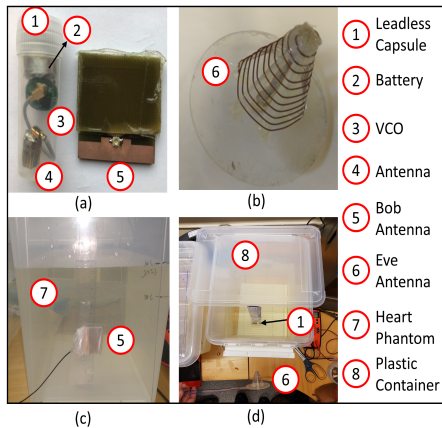


Fig. 6: Phantom experiment setup (a) Legitimate link antennas (Alice and Bob) (b) Eve antenna (c) legitimate link setup (d) Eve link setup

properties of the human heart was developed. The phantom was prepared using 39.2 % of sucrose in water, provided in [44]. The transmitter antenna (Alice) was a 1 mm in radius meander-shaped, connected to voltage control oscillator (VCO). VCO generates a sinusoidal signal at 2.4 GHz and operates on a button cell. The antenna, VCO and cell battery were encapsulated by a small plastic container to avoid direct contact with the phantom. Subcutaneous antenna (Bob) was a wideband patch antenna with dimensions of $3 \times 3 \text{ cm}^2$. These two antennas replicate the AB link. Similarly, an off-body circular polarized spiral antenna is utilized to replicate the Eve. Fig. 6 shows the container with liquid phantom, antennas placement and antennas itself. More details on antennas can be found in [38].

1) *Legitimate/AB-link*: Fig. 6a shows the AB link antennas and Fig. 6c shows the setup for AB link where the leadless capsule was implanted inside the phantom filled container with the help of a ruler and the subcutaneous antenna was mounted on a wall of the container.

2) *Eavesdropper/AE-link*: Fig. 6b shows the eavesdropper antenna whereas Fig. 6d shows the AE link. The leadless cardiac pacemaker (LCP/capsule) was fixed inside the phantom with a ruler at a depth of 10 cm, and the Eve antenna attached with another ruler was moved to different positions outside the container.

C. In-vivo Experiment

The animal experiment was carried out in an operating room at the Intervention Center, Oslo University Hospital, Oslo, Norway, which is qualified to perform such procedures. All the experiments were performed according to ethical standards and regulations provided by the responsible agencies. The experiment was performed on a female pig weighing about 61 Kg. Fig. 7a shows the operating room along with the pig, which had been given general anesthesia for the experiment.

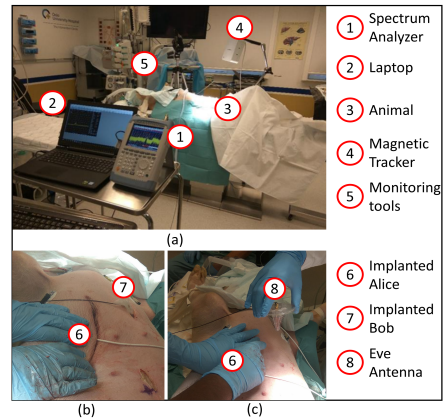


Fig. 7: In-vivo experiment setup (a) Operating room (b) Legitimate link (c) Eve link

We did not take into account the posture change of the animal during the experiments that might effect the antenna coupling. However, we believe that to some extent the coupling effects have been compensated by changing the antenna positions. Similar set of antennas were used in in-vivo experiments, as described in section II-B.

1) *Legitimate/AB-Link*: An antenna (Alice) within a plastic container was placed behind the right ventricle of a pig heart whereas subcutaneous antenna (Bob) was positioned under the skin below shoulder as shown in Fig. 7b. An electromagnetic distance measurement system, *Medical Aurora* by NDI Medical, Canada, was used to evaluate the distance between transmitting and receiving antenna. We moved the in-body antenna at different positions (in mm) within the subcutaneous space and took multiple measurements around the same distance which was averaged to minimize the measurement errors.

2) *Eavesdropper/AE-Link*: For AE link, the Alice was placed at the same position as in case of AB link, and the Eve antenna was held outside the pig body as shown in Fig. 7c. The Eve antenna coupling was evaluated across different angles over the chest of the animal, and later considered the best-case scenario for an Eve (worst case for a pacemaker).

III. RESULTS

This section focuses on results based on the system methodology. First, we present the channel measurements using EM simulations in CST. We evaluate the legitimate link channel attenuation and the attenuation of each eavesdropper position on the spherical grid from the leadless capsule in the RV. Afterwards, the distance of the legitimate link is fixed and the secrecy capacity of the defined spherical grid at a radial distance of 1 m is evaluated. In order to cover the entire space around the body, path loss model for free space is utilized to extrapolate the secrecy capacity. Moreover, the results for the in-secure volume are presented by fixing the cardiac application based secrecy rate. The results are concluded by presenting the phantom and in-vivo results.

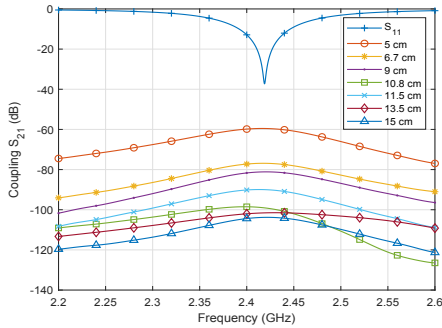


Fig. 8: Antennas coupling. Alice is in RV whereas Bob is placed at different positions in the subcutaneous space. The S_{11} around 2.4 GHz, shows the efficient matching between antennas.

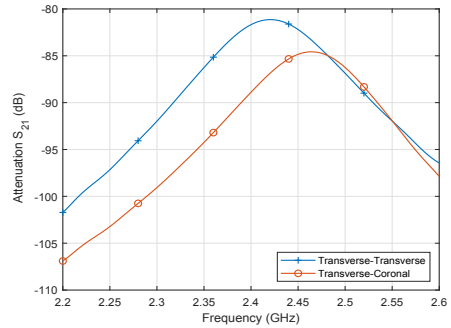


Fig. 10: The difference in the coupling between antennas by changing the direction of the antenna from Transverse to Coronal plane

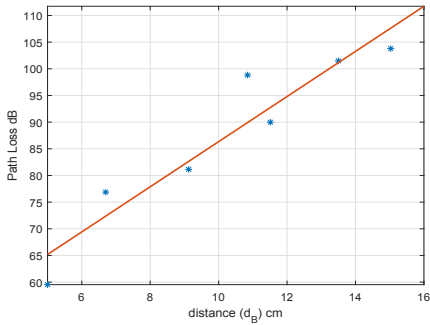


Fig. 9: AB link path loss model w.r.t subcutaneous distance (Bob distance)

A. EM simulation results

1) *Legitimate/AB-link:* Fig. 8 shows the channel attenuation between an antenna in the right ventricle and the antennas in the subcutaneous space. The antennas (transmitter and receiver antennas) are matched at 2.42 GHz represented as S_{11} and is shown in Fig. 8. Fig. 9 shows the extracted path loss model where dots represent the attenuation at a respective distance from Alice and the straight line shows the linear fitted model which can be expressed as

$$PL(d_B) = P_1 \times d_B + P_2, \quad (12)$$

where $P_2 = -44.03$ dB, $P_1 = -4.231$ dB/cm and d_B is the distance in cm between Alice and Bob. This path loss is valid for the distance between $5 \text{ cm} \leq d_B \leq 16 \text{ cm}$. As mentioned earlier, $|h_{(x,y)}|^2$ is the AB link attenuation in linear scale, thus in dB scale, it can be expressed as

$$\alpha = |h_{(x,y)}|_{dB}^2 = PL(d_B). \quad (13)$$

The extracted path loss model for the AB link is obtained by placing the antennas (in the right ventricle and the subcutaneous space) in the transverse plane. Aforementioned, to

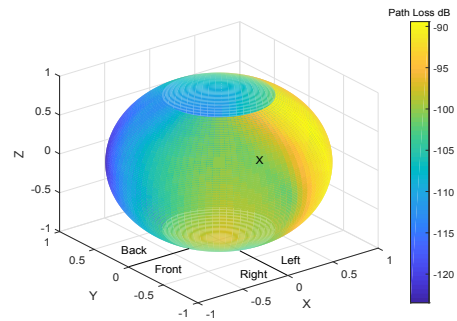


Fig. 11: Channel attenuation between Alice and Eve in 3d Sphere with a radius of 1 m. The axis is converted from spherical coordinates into Cartesian coordinates. Front represents the frontal side of the human body. The cross (X) represents the approximate heart position inside the sphere

observe the effects of the antenna polarization, simulation is also performed by placing the antenna in the coronal plane. Fig. 10 shows the difference observed in the attenuation by changing the direction of the antenna at the distance of 9.1 cm from the transverse plane to the coronal plane. It has been observed that the attenuation is increased by 3 dB due to polarization mismatch. Thus, placing the antennas in the transverse plane is efficient and results in less attenuation between antennas as compared to the coronal plane. The channel attenuations are comparable to the results presented in [45], [46] with slightly higher values of attenuation due to the use of a highly accurate Hugo model for transmission through heterogeneous medium.

2) *Eavesdropper/AE-link:* The attenuation determined at each electric probe after conversion from E-field using (9) is expressed in three-dimensional space around the body in Fig. 11. It has been observed that at $\theta = 60^\circ, \phi = 306^\circ$, the eavesdropper has the minimum attenuation with the leadless capsule and is considered as the Eve sweet spot angle. To

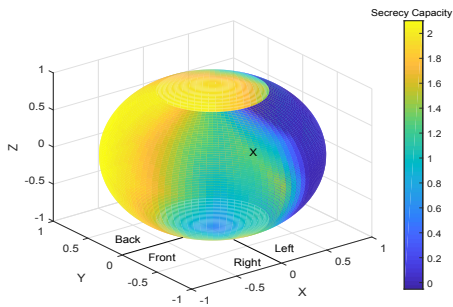


Fig. 12: Secrecy capacity across all the spatial positions surrounding the body at a distance of 1 m. The axis is converted from spherical coordinates into Cartesian coordinates. Front represents the frontal side of the human body. The cross (X) represents the approximate heart position inside the sphere

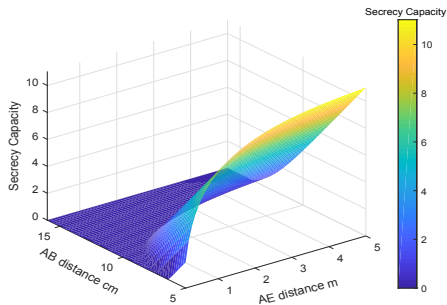


Fig. 13: Secrecy capacity with variation in both AB and AE distance, for eavesdropper at sweet spot angle ($\theta = 60^\circ, \phi = 306^\circ$)

observe the difference in the AE link attenuation by changing the orientation of the antenna from transverse to the coronal plane, we change the orientation of the leadless capsule inside the right ventricle. As the transmitting antenna is very small in size, thus changing the orientation doesn't effect the attenuation values at larger distances (1 m).

3) Secrecy Capacity: For evaluation of the secrecy capacity, AB link distance of 12 cm is fixed. Using (6), Fig. 12 shows the secrecy capacity of a spherical grid at the radial distance of 1 m around the body. It has been observed that most of the sphere has positive secrecy capacity except the low attenuation eavesdropping angles (17 out of 100). Thus, to find the distance where the secrecy capacity is positive across all Eve angles, the secrecy capacity of the spherical grid is computed with the radial distance of 2 m by using (11). It has been found that at the distance of 2 m, the positive secrecy capacity is observed over the entire spherical grid.

The variation in secrecy capacity is also viewed by changing both the AB and AE link distance. For the AE link, Eve is considered at the "sweet spot angle". Fig. 13 shows the resultant secrecy capacity, where x-axis is AE distance and

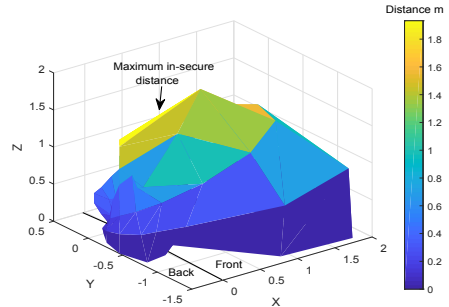


Fig. 14: Boundary of in-secure volume around the body for fixed secrecy rate of 0.5 bps/Hz

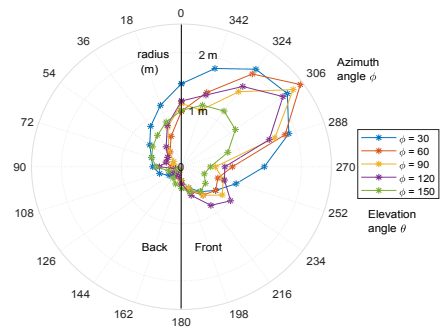


Fig. 15: 2-D representation of in-secure volume around body for fixed secrecy rate of 0.5 bps/Hz

varies from 0.12 – 5 m, y-axis is the AB distance and varies from 5 – 16 cm and z-axis is the resultant secrecy capacity. The movement of Eve, away from the legitimate nodes results in higher secrecy capacity.

4) In-Secure Volume: The in-secure volume is the volume that contains all the Eve positions from which the leadless pacemaker can be eavesdropped and is expressed in (7). Equation (7) provides the minimum Eve distance required across different angles in order to achieve the fixed communication secrecy rate. The pacemaker usually requires the transmission rate of approximately 100 kbps in order to transmit the cardiac parameters (ECG, pulse rate, respiratory rate, blood pressure, etc.) [47]. Thus, we fix the secrecy rate to 0.5 bps/Hz (bits per complex symbol), which for the bandwidth of 1 MHz is around 250 kbps. Similarly, the AB distance is fixed to 12 cm and the minimum Eve distance required to support the secure communication rate is evaluated across all the angles. Fig. 14 shows the in-secure volume around the body. The volume is uneven because the attenuation values across different angles through the body provides different secrecy capacity. For more visual clarity the same information is provided in 2-dimensional space in Fig. 15. Thus, to transmit 0.5 bps/Hz securely with transmit power of 0 dBm, the Eve at the "sweet spot angle" (worst case scenario for the pacemaker)

with receiver⁶ sensitivity of -100 dBm should be at a distance of 2.5 m or beyond. The boundary of the in-secure volume is considerably less for other angles e.g at $\theta = 150^\circ, \phi = 306^\circ$, the insecure volume stretches till 1.1 m. Regarding the back side of the human body, the boundary of the in-secure volume stretches till 1 m for the worst case representing the distance from RV of the human heart. The worst case angle to the back side is $\theta = 30^\circ, \phi = 18^\circ$. It is worth mentioning that the implanted nodes generally transmit with power ranging between -16 – -27 dBm due to which the in-secure volume at Eve sweet spot angle will be reduced. e.g for the transmit power of -16 dBm, the in-secure distance at Eve sweet spot angle reduces from 2.5 m to 2.1 m.

5) *Worst-Case Analysis*: In order to observe variation in the Eve distance with respect to the secrecy rate, we evaluate a bound on the minimum and the maximum Eve distance for a certain fixed AB distance. The analysis is done by considering Eve at the “sweet spot angle” or the worst case scenario for the pacemaker. When the secrecy rate approaches to zero, the Eve distance can be expressed as

$$\lim_{C_S \rightarrow 0} d_E(C_S) = r \times 10^{\frac{P_1 \times d_B + P_2 - \beta}{10 \times n}}, \quad (14)$$

where P_1 and P_2 are constants (see (12)), r is the reference Eve distance (1 m), d_B is the AB distance and β is the eavesdropper reference attenuation at the “sweet spot angle”. As C_S approaches to zero, this means AB and AE link have the same capacity, which apparently represents the same distance⁷. This could be true for free space wireless channels with homogeneous loss. But for the in-body networks where the eavesdropper is outside the body and legitimate receiver (Bob) is inside the body, we could have less attenuation at some angles around the body at Eve than that of the Bob. This is because of higher in-body loss than free space. Thus, the transmission path to the eavesdropper may encounter less in-body portion and larger free space portion resulting in a non-homogeneous loss. The Eve at the “sweet spot angle”, should be at a distance of 1.872 m for the secrecy capacity to be positive.

Similarly, when the secrecy rate approaches to the AB link capacity C_B , then the Eve distance approaches to infinity and can be expressed as

$$\lim_{C_S \rightarrow C_B} d_E(C_S) \rightarrow \infty. \quad (15)$$

Fig. 16 shows the minimum and maximum Eve distance with variation in secrecy capacity as a fraction of the legitimate (AB) link capacity.

B. Phantom Experiment Results

This section focuses on providing the secrecy capacity using path loss models developed from the phantom experiments in order to evaluate the AB and AE channel attenuations. The pathloss models has also been reported in earlier work [48]. We use directional antennas as mentioned in section II-B.

⁶0 dBi antenna gain

⁷If only the attenuation with distance is considered as a variation parameter for homogeneous loss

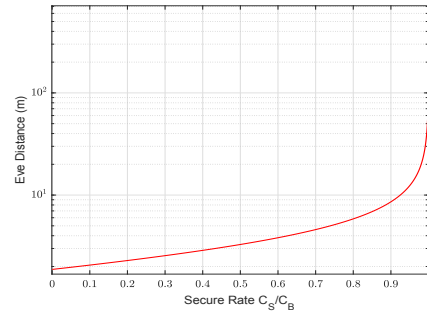


Fig. 16: Minimum and maximum eavesdropper distance at Eve sweet spot angle for pacemaker worst-case analysis

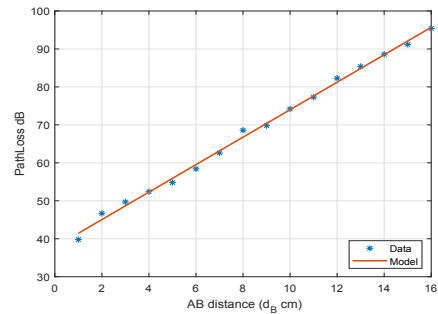


Fig. 17: Phantom Experiment: AB link attenuation and path loss model

For phantom experiments, we didn’t consider different spatial positions for the eavesdropper. Albeit, we evaluate the secrecy capacity by considering Eve at the sweet spot angle (worst case scenario for a pacemaker).

1) *legitimate/AB-link*: In case of AB link, the implanted antenna (capsule) was moved in the distance range of 1 cm to 16 cm from subcutaneous antenna and the corresponding received power was measured via spectrum analyzer connected to the subcutaneous antenna. Fig. 17 shows the measured values along with the fitted model. The AB link path loss follows a linear model and can be expressed as

$$PL(d_B) = P_1 \times d_B + P_2, \quad (16)$$

where $P_1 = -3.618$ dB/cm, $P_2 = -37.82$ dB and d_B is the AB distance. The path loss model is valid for $1 \text{ cm} \leq d_B \leq 16 \text{ cm}$.

2) *Eavesdropper/AE-link*: The AE link path loss model is shown in Fig. 18, where dots represent the measured values and line shows the fitted model which can be expressed as

$$PL(d_E) = PL(d_o) + 10 \times n \times \log_{10} \left(\frac{d_E}{d_o} \right), \quad (17)$$

where $PL(d_o) = 68.4$ dB is the path loss at a reference distance of 11 cm (10 cm implant depth + 1 cm from the

TABLE I: Summary of Simulation and experimental measurements for eavesdropper distance

Parameters	$C_S = 0$ bpcs/Hz				$C_S = 0.5$ bpcs/Hz		
	AB Distance	AE Distance			AE Distance		
		In-Body	From Body Surface	Total	In-Body	From Body Surface	Total
EM Simulations (Worst Case, Ideal Antenna)	12 cm			1.8 m			2.5 m
EM Simulations (Worst Case, Realized Antenna)	12 cm			13 cm			15 cm
Phantom Exp (Extrapolated)	12 cm	12 cm	2.5 cm	14.5 cm	12 cm	3.5 cm	15.5 cm
In-vivo Exp	12 cm	8 cm	4 cm	12 cm	8 cm	5 cm	13 cm

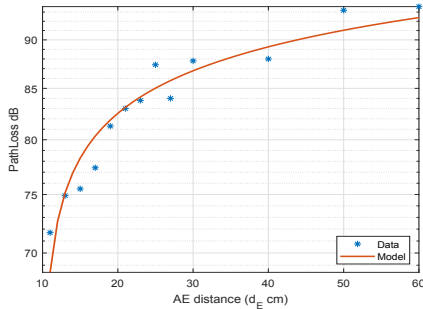


Fig. 18: Phantom Experiment: Eve link attenuation and path loss model

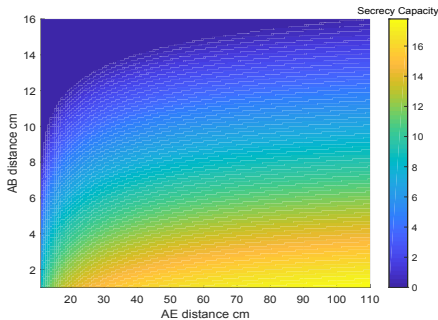


Fig. 19: Achievable secrecy rate from a phantom experiment

container surface), d_E is the Eve distance from the implant and n is the path loss exponent with a value of 1.411. The path loss model is validated only for a distance between 11 - 60 cm. After 60 cm free space path loss can be considered with $n = 2$.

3) Secrecy Capacity: The secrecy capacity for the phantom experiment is shown in Fig. 19. Considering the AB distance of 10 cm, and Eve at a distance of 16 cm from Alice, the secrecy rate is about 1.4 bpcs/Hz.

C. In-vivo Experiment Results

For AB link, the average attenuation found between an antenna (Alice) behind the RV and the subcutaneous antenna (Bob) at 12 cm was about -82.37 dB. Similarly, by holding the Eve antenna, 6 cm above the body surface (see Fig. 7c) with

the in-body antenna depth of 8 cm, the attenuation measured was -86.20 dB. The secrecy capacity that can be achieved is 1.2 bpcs/Hz at the total Eve distance of 14 cm from Alice. Similarly, path loss model for free space is utilized to extrapolate the secrecy capacity for different Eve distances.

IV. DISCUSSIONS

So far, the secrecy capacity is evaluated separately by adopting simulations and experiments, here the inter-correlation between results from different methodologies is discussed. Table I lists the summary of the results with corresponding Eve distance to achieve the secure communication rate by use of different evaluation methodologies. For EM simulations, if we consider worst case scenario for the pacemaker or the angle ($\theta = 60^\circ$, $\phi = 306^\circ$) where the leakage of information is maximum, the fixed secrecy rate of 0.5 bpcs/Hz is achievable at a distance of 2.5 m. In case of phantom and in-vivo experiments the same rate is achieved at 15.5- and 13 cm respectively. The experimental measurements have high correlation but differ from simulations. This is due to the use of different types of antennas for simulations and experiments. Simulations assume theoretical ideal antenna of small size with 100 % efficiency whereas in the practical scenario we can not realize such an ideal small antenna of size 5 mm (i.e. $\frac{\lambda}{25}$ (λ is the wavelength at 2.4 GHz)) due to the theoretical limitation of small antennas efficiency. Therefore lower antenna efficiency reduces the radiated power density in practical implementations compared to ideal simulations. The typical efficiency for such an antenna is about -10 - -15 dB. Thus the calculated secrecy capacity should be scaled to include the implant antenna effects. For conducting experiments, we have designed a meander antenna for the implant in which a capacitive coupling mechanism is applied [49] to provide high efficiency and impedance matching at 2.4 GHz. However, the efficiency (about -12 dB) results in the reception of low power outside the body compared to the ideal antenna in the simulation. If the ideal antenna is scaled with respect to a realized antenna, then the Eve distance to achieve the secrecy capacity of 0.5 bpcs/Hz is reduced from 2.5 m (250 cm) to about 15 cm ($10^{-1.2} \times 250$), approximately same as computed in the experiments. Thus, the simulations and the experimentation results show similar Eve distance in order to achieve the same secrecy capacity if the efficiency drop in case of realized antennas is taken care off. Thus, by considering a patient personal space of 50 cm with a maximum leakage angle to the front, it will be difficult for an Eve to enter into the space without going un-noticed.

The evaluated secrecy communication rate reflects both confidentiality and reliability. To draw a theoretical comparison of reliability with the reference provided in IEEE 802.15 standard, the required SNR should be approx. 2 dB [50] for the BER of 10^{-3} in case of DBPSK⁸ modulation scheme (commonly used for resource constrained devices [7]). The mentioned threshold SNR is achievable for legitimate link which for R of 250 kbps and bandwidth of 1 MHz is approx. 5 dB⁹. For AE link, after considering the realized antenna effects, the best case scenario of Eve at sweet spot angle has SNR of approx. 0 dB, which corresponds to BER of 10^{-1} and will be further degraded by use of channel coding, based on evaluated secrecy capacity.

The results of this work are promising and motivates to secure the next generation of leadless cardiac pacemaker via PLS methods. The results can also be utilized for other in-body sensor network applications. Nevertheless, PLS methods can be stacked with traditional cryptographic methods to provide extra layer of security at the physical layer to secure the sensitive application of a pacemaker.

V. CONCLUSION

In this work, we analyze the effectiveness of securing next generation leadless cardiac pacemaker using the channel model approach of PLS. This is done by evaluating the performance metric of secrecy capacity for a pacemaker implant inside the heart. The adopted methodology utilizes numerical electromagnetic simulations and the results are validated through measurements in phantom model and in-vivo experiments. From EM simulations, the angle where Eve has the minimum channel attenuation is found to the left from front, just above the heart and is termed as the "Eve sweet spot angle". Eve sweet spot angle has the least secrecy capacity among all the eavesdropper spatial positions with human heart as the reference position. In addition, by fixing cardiac application based secrecy rate of 250 kbps, the in-secure volume is provided across different angles around the body. By considering an ideal antenna for EM simulations, the in-secure volume has a maximum distance of 2.5 m at Eve sweet spot angle for a transmit power of 0 dBm and receiver sensitivity of -100 dBm. However, by considering a realistic scenario with implant antenna effects, the secrecy distance reduces to 15 cm which is in correlation with the experimental measurements (Phantom and in-vivo).

⁸Differential binary phase shift keying

⁹ $\text{SNR} = \frac{E_b}{N_o} \times \frac{R}{BW} \times \left(\frac{E_b}{N_o}\right)$ is the energy per bit, R is rate, and BW is bandwidth)

APPENDIX I

DERIVATION FOR AN IN-SECURE VOLUME

$$\begin{aligned}
 C_S &= C_B - C_E \\
 \log_2\left(1 + \frac{PL_{r,\theta,\phi}(d_E)P_t}{\sigma^2}\right) &= C_B - C_S \\
 \frac{PL_{r,\theta,\phi}(d_E)P_t}{\sigma^2} &= 2^{(C_B - C_S)} - 1 \\
 P_t - PL_{r,\theta,\phi}(d_E) - \sigma^2 &= 10 \times \log_{10}(2^{(C_B - C_S)} - 1) \\
 P_t - \left(\beta + 10n \log_{10}\left(\frac{d_E}{r}\right)\right) - \sigma^2 &= \\
 &= 10 \times \log_{10}(2^{(C_B - C_S)} - 1) \\
 d_{E(r,\theta,\phi)} &\leq r \times 10^{\left(\frac{P_t - \beta - 10 \log_{10}(2^{(C_B - C_S)} - 1) - \sigma^2}{10n}\right)}
 \end{aligned}$$

REFERENCES

- [1] H. G. Mond and A. Proclemer, "The 11th world survey of cardiac pacing and implantable cardioverter-defibrillators: calendar year 2009—a world society of arrhythmia's project," *Pacing and clinical electrophysiology*, vol. 34, no. 8, pp. 1013–1027, Aug. 2011.
- [2] M. Albatat, J. Bergsland, H. Arevalo, H. Odland, P. Bose, P. Halvorsen, and I. Balasingham, "Technological and clinical challenges in lead placement for cardiac rhythm management devices," *Annals of Biomedical Engineering*, pp. 1–21, Sept. 2019.
- [3] R. E. Kirkfeldt, J. B. Johansen, E. A. Nohr, O. D. Jørgensen, and J. C. Nielsen, "Complications after cardiac implantable electronic device implantations: an analysis of a complete, nationwide cohort in denmark," *European heart journal*, vol. 35, no. 18, pp. 1186–1194, Dec. 2013.
- [4] R. G. Hauser, W. T. Katsiyannis, C. C. Gornick, A. K. Almqvist, and L. M. Kallinen, "Deaths and cardiovascular injuries due to device-assisted implantable cardioverter-defibrillator and pacemaker lead extraction," *Europace*, vol. 12, no. 3, pp. 395–401, Nov. 2009.
- [5] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *Journal of biomedical informatics*, vol. 55, pp. 272–289, Jun. 2015.
- [6] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and privacy for implantable medical devices," *IEEE pervasive computing*, vol. 7, no. 1, pp. 30–39, Jan. 2008.
- [7] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *2008 IEEE Symposium on Security and Privacy (sp 2008)*. IEEE, May, 2008, pp. 129–142.
- [8] C.-S. Park, "Security mechanism based on hospital authentication server for secure application of implantable medical devices," *BioMed research international*, vol. 2014, Jun. 2014.
- [9] J. Astorga, J. C. Astorga, E. Jacob, N. Toledo, and M. Higuero, "Securing access to next generation ip-enabled pacemakers and icds using ladon," *Journal of ambient intelligence and smart environments*, vol. 6, no. 2, pp. 157–177, Jan. 2014.
- [10] M. Zhang, A. Raghunathan, and N. K. Jha, "Medmon: Securing medical devices through wireless monitoring and anomaly detection," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 7, no. 6, pp. 871–881, Apr. 2013.
- [11] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: non-invasive security for implantable medical devices," in *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4. ACM, Aug. 2011, pp. 2–13.
- [12] X. Zhou, L. Song, and Y. Zhang, *Physical layer security in wireless communications*. Crc Press, Apr. 2016.
- [13] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE wireless Communications*, vol. 18, no. 2, pp. 66–74, Apr. 2011.
- [14] Y. Liang, H. V. Poor, S. Shamai *et al.*, "Information theoretic security," *Foundations and Trends® in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, Jun. 2009.
- [15] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

- [16] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, Oct, 1975.
- [17] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE transactions on information theory*, vol. 24, no. 3, pp. 339–348, May, 1978.
- [18] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE transactions on information theory*, vol. 39, no. 3, pp. 733–742, May, 1993.
- [19] M. F. Awan, K. Kansanen, S. Perez-Simbor, C. Garcia-Pardo, S. Castelló-Palacios, and N. Cardona, "Rss-based secret key generation in wireless in-body networks," in *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*. IEEE, May, 2019, pp. 1–6.
- [20] N. Karimian, Z. Guo, M. Tehranipoor, and D. Forte, "Highly reliable key generation from electrocardiogram (ecg)," *IEEE Transactions on Biomedical Engineering*, vol. 64, no. 6, pp. 1400–1411, Sep, 2016.
- [21] S. Pirbhulal, H. Zhang, W. Wu, S. C. Mukhopadhyay, and Y.-T. Zhang, "Heartbeats based biometric random binary sequences generation to secure wireless body sensor networks," *IEEE Transactions on Biomedical Engineering*, vol. 65, no. 12, pp. 2751–2759, Mar, 2018.
- [22] P. Xu, K. Cumanan, Z. Ding, X. Dai, and K. K. Leung, "Group secret key generation in wireless networks: algorithms and rate optimization," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1831–1846, Apr, 2016.
- [23] Y. E. H. Shehadeh and D. Hogrefe, "A survey on secret key generation mechanisms on the physical layer in wireless networks," *Security and Communication Networks*, vol. 8, no. 2, pp. 332–341, Jan, 2015.
- [24] B. He, Y. She, and V. K. Lau, "Artificial noise injection for securing single-antenna systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9577–9581, May, 2017.
- [25] K. Cumanan, H. Xing, P. Xu, G. Zheng, X. Dai, A. Nallanathan, Z. Ding, and G. K. Karagiannis, "Physical layer security jamming: Theoretical limits and practical designs in wireless networks," *IEEE Access*, vol. 5, pp. 3603–3611, Dec, 2016.
- [26] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, "Secrecy rate optimizations for a mimo secrecy channel with a multiple-antenna eavesdropper," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 4, pp. 1678–1690, Oct, 2013.
- [27] K. Cumanan, Z. Ding, M. Xu, and H. V. Poor, "Secrecy rate optimization for secure multicast communications," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1417–1432, Aug, 2016.
- [28] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, Feb, 2014.
- [29] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, May, 2008.
- [30] K. Sayrafian-Pour, W.-B. Yang, J. Hagedorn, J. Terrill, and K. Y. Yazdandoost, "A statistical path loss model for medical implant communication channels," in *2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*. IEEE, Sep, 2009, pp. 2995–2999.
- [31] A. Stango, K. Y. Yazdandoost, F. Negro, and D. Farina, "Characterization of in-body to on-body wireless radio frequency link for upper limb prostheses," *PLoS one*, vol. 11, no. 10, p. e0164987, Oct, 2016.
- [32] C. Garcia-Pardo, C. Andreu, A. Fornes-Leal, S. Castelló-Palacios, S. Perez-Simbor, M. Barbi, A. Vallés-Lluch, and N. Cardona, "Ultrawideband technology for medical in-body sensor networks: An overview of the human body as a propagation medium, phantoms, and approaches for propagation analysis," *IEEE Antennas and Propagation Magazine*, vol. 60, no. 3, pp. 19–33, Apr, 2018.
- [33] J. Kim and Y. Rahmat-Samii, "Implanted antennas inside a human body: Simulations, designs, and characterizations," *IEEE Transactions on microwave theory and techniques*, vol. 52, no. 8, pp. 1934–1943, Aug, 2004.
- [34] P. S. Hall, Y. Hao, Y. I. Nechayev, A. Alomainy, C. C. Constantinou, C. Parini, M. R. Kamarudin, T. Z. Salim, D. T. Hee, R. Dubrovka *et al.*, "Antennas and propagation for on-body communication systems," *IEEE Antennas and Propagation Magazine*, vol. 49, no. 3, pp. 41–58, Aug, 2007.
- [35] D. B. Smith, D. Miniutti, T. A. Lamaheewa, and L. W. Hanlen, "Propagation models for body-area networks: A survey and new outlook," *IEEE Antennas and Propagation Magazine*, vol. 55, no. 5, pp. 97–117, Oct, 2013.
- [36] J. F. Zhao, X. M. Chen, B. D. Liang, and Q. X. Chen, "A review on human body communication: signal propagation model, communication performance, and experimental issues," *Wireless Communications and Mobile Computing*, vol. 2017, Sep, 2017.
- [37] M. Awan, S. Perez-Simbor, C. Garcia-Pardo, K. Kansanen, and N. Cardona, "Experimental phantom-based security analysis for next-generation leadless cardiac pacemakers," *Sensors*, vol. 18, no. 12, p. 4327, Dec, 2018.
- [38] P. Bose, A. Khaleghi, M. Albatat, J. Bergsland, and I. Balasingham, "Rf channel modeling for implant to implant communication and implant to sub-cutaneous implant communication for future leadless cardiac pacemakers," *IEEE Transactions on Biomedical Engineering*, Mar, 2018.
- [39] Federal Communications Commission, "Medical Body Area Network (MedRadio)," <https://www.fcc.gov/document/medical-body-area-networks>, May, 2015, online; accessed 3/02/2018.
- [40] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE transactions on information theory*, vol. 24, no. 4, pp. 451–456, Jul, 1978.
- [41] M. Studio, "Cst-computer simulation technology," *Bad Nuheimer Str*, vol. 19, p. 64289, 2008.
- [42] M. J. Ackerman, "The visible human project," *Proceedings of the IEEE*, vol. 86, no. 3, pp. 504–511, Mar, 1998.
- [43] V. Spitzer, M. J. Ackerman, A. L. Scherzinger, and D. Whitlock, "The visible human male: a technical report," *Journal of the American Medical Informatics Association*, vol. 3, no. 2, pp. 118–130, Mar, 1996.
- [44] S. Castelló-Palacios, A. Vallés-Lluch, C. Garcia-Pardo, A. Fornes-Leal, and N. Cardona, "Formulas for easy-to-prepare tailored phantoms at 2.4 ghz ism band," in *Medical Information and Communication Technology (ISMICT), 2017 11th International Symposium on*. IEEE, Feb, 2017, pp. 27–31.
- [45] R. Chávez-Santiago, C. Garcia-Pardo, A. Fornes-Leal, A. Vallés-Lluch, G. Vermeeren, W. Joseph, I. Balasingham, and N. Cardona, "Experimental path loss models for in-body communications within 2.36–2.5 ghz," *IEEE journal of biomedical and health informatics*, vol. 19, no. 3, pp. 930–937, Apr, 2015.
- [46] D. Kurup, W. Joseph, G. Vermeeren, and L. Martens, "Path loss model for in-body communication in homogeneous human muscle tissue," *Electronics letters*, vol. 45, no. 9, pp. 453–454, Apr, 2009.
- [47] J. Wang and Q. Wang, "Body area communications: Channel modeling, communication systems, and emc," Nov, 2012.
- [48] P. Bose, A. Khaleghi, and I. Balasingham, "In-body and off-body channel modeling for future leadless cardiac pacemakers based on phantom and animal experiments," *IEEE Antennas and Wireless Propagation Letters*, vol. 17, no. 12, pp. 2484–2488, 2018.
- [49] A. Khaleghi and I. Balasingham, "Wireless communication link for capsule endoscope at 600 mhz," in *Engineering in Medicine and Biology Society (EMBC), 2015 37th Annual International Conference of the IEEE*. IEEE, Aug, 2015, pp. 4081–4084.
- [50] A. Ba, M. Vidjokovic, K. Kanda, N. F. Kiyani, M. Lont, X. Huang, X. Wang, C. Zhou, Y.-H. Liu, M. Ding *et al.*, "A 0.33 nj/bit ieee802.15.6/proprietary mics/ism wireless transceiver with scalable data rate for medical implantable applications," *IEEE journal of biomedical and health informatics*, vol. 19, no. 3, pp. 920–929, Mar, 2015.

Appendix G

RSS-Based Secret Key Generation

Paper G: RSS-Based Secret Key Generation in Wireless
In-body Networks

Muhammad Faheem Awan, Kimmo Kansanen, Sofia Perez-Simbor, Concepcion
Garcia-Pardo, Sergio Castelló-Palacios and Narcis Cardona

*2019 13th International Symposium on Medical Information and Communication
Technology (ISMICT)*

This article is not included due to copyright

Appendix H

Physiological Signals Based Secret Key Generation

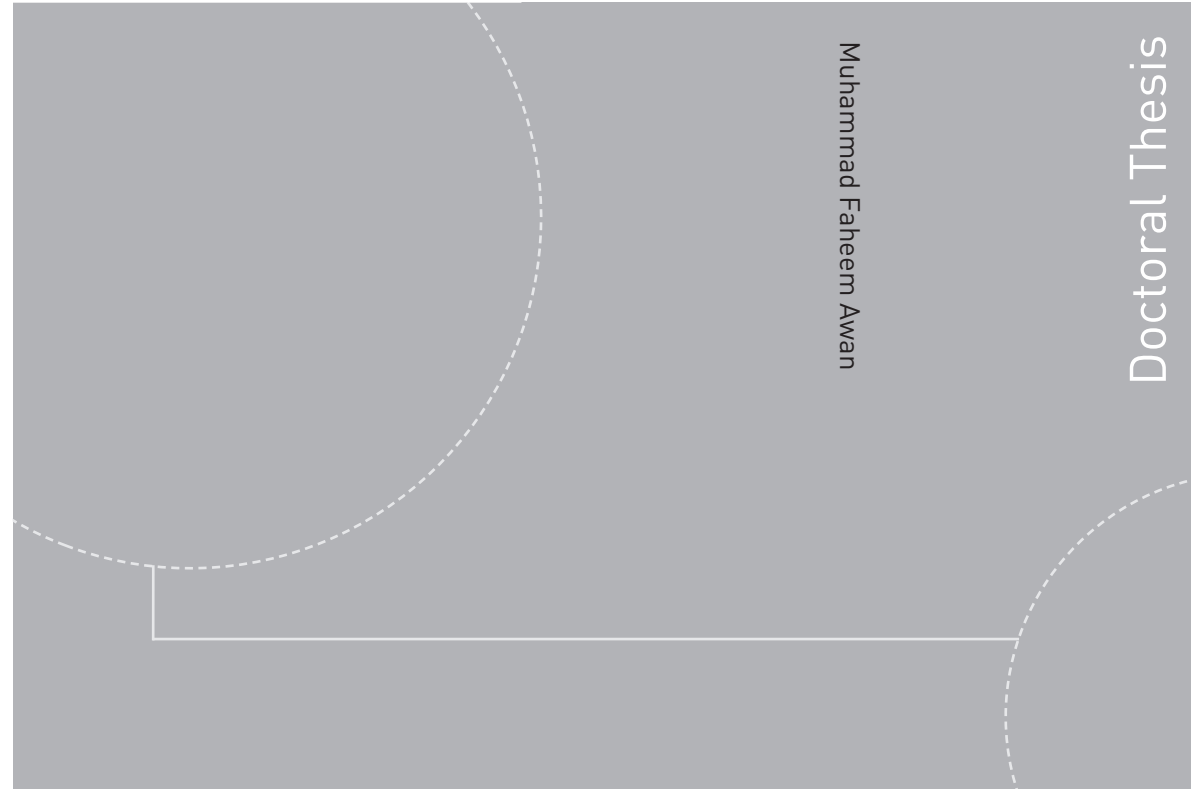
Paper H: Securing Next Generation Multinodal Leadless
Cardiac Pacemaker System: A Proof of Concept in a Single
Animal

Muhammad Faheem Awan, Rafael Cordero Alvarez, Kimmo Kansanen and
Delphine Feuerstein

Submitted in Annals of Biomedical Engineering

This article is awaiting publication and is not included in NTNU Open

ISBN 978-82-326-4620-3 (printed version)
ISBN 978-82-326-4621-0 (electronic version)
ISSN 1503-8181



Doctoral theses at NTNU, 2020:136

Muhammad Faheem Awan

Physical Layer Security for In-Body Wireless Cardiac Sensor Network

Doctoral theses at NTNU, 2020:136

NTNU
Norwegian University of
Science and Technology
Faculty of Information Technology
and Electrical Engineering
Department of Electronic Systems

 **NTNU**
Norwegian University of
Science and Technology

 **NTNU**

 **NTNU**
Norwegian University of
Science and Technology