Wirelessly Powered Secured Backscatter Communication for Wireless Sensor Network

By
VINITA DAIYA
ENGG02201204019

Indira Gandhi Centre for Atomic Research, Kalpakkam

A thesis submitted to the

Board of Studies in Engineering Sciences

In partial fulfillment of requirements

for the Degree of

DOCTOR OF PHILOSOPHY

of

HOMI BHABHA NATIONAL INSTITUTE

August, 2019

Homi Bhabha National Institute[1]

Recommendations of the Viva Voce Committee

As members of the Viva Voce Committee, we certify that we have read the dissertation prepared by **Vinita Daiya** entitled **"Wirelessly Powered Secured Backscatter Communication for Wireless Sensor Network"** and recommend that it may be accepted as fulfilling the thesis requirement for the award of Degree of Doctor of Philosophy.

Chairman - **Dr. B. K. Panigrahi** **Date:** 04/06/2020

Guide / Convener - **Dr. B.P.C.Rao** **Date:** 4/6/2020

Examiner – **Prof. Swades De** **Date:** 29/5/2020

Member 1- **Dr. K. Velusamy** **Date:** 04/6/2020

Member 2- **Dr. Anish Kumar** **Date:** 03/06/2020

Technology Advisor- **Ms. Jemimah Ebenezer** **Date:** 03/06/2020

Final approval and acceptance of this thesis is contingent upon the candidate's submission of the final copies of the thesis to HBNI.

I/We hereby certify that I/we have read this thesis prepared under my/our direction and recommend that it may be accepted as fulfilling the thesis requirement.

Date: 4/6/2020
Place: Kalpakkam

Guide

[1] This page is to be included only for final submission after successful completion of viva voce.

STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at Homi Bhabha National Institute (HBNI) and is deposited in the Library to be made available to borrowers under rules of the HBNI.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgement of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the Competent Authority of HBNI when in his or her judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

Vinita Daiya

Vinita Daiya

DECLARATION

I, hereby declare that the investigation presented in the thesis has been carried out by me. The work is original and has not been submitted earlier as a whole or in part for a degree / diploma at this or any other Institution / University.

Vinita Daiya

Vinita Daiya

LIST OF PUBLICATIONS ARISING FROM THE THESIS

Journal

a) Published:

1) **Vinita Daiya**, Jemimah Ebenezer, R. Jehadeesan, "Security Implementation in Wireless sensor Network by RF Signal Obfuscation", Wireless Personal Communication, Springer, 2019, Vol. 106, No.2, pp.805-827, https://doi.org/10.1007/s11277-019-06191-7 .
2) **Vinita Daiya**, Jemimah Ebenezer, R. Jehadeesan, "Rectenna panel design optimization for maximum RF power utilization". International Journal of Microwave and Wireless Technologies, Cambridge University Press, 2019, Vol. 11, No.10, pp.1024-1034, doi:10.1017/S1759078719000813.
3) **Vinita Daiya**, Jemimah Ebenezer, R. Jehadeesan, "Mapping Obfuscation based PHY Security Scheme for Resource-Constrained Wireless Sensor Network" in IETE Technical Review, Taylor & Francis, 2020, pp. 1-10, doi: 10.1080/02564602.2019.1709573 (Online on Jan 2020).

b) Communicated

1) **Vinita Daiya**, Jemimah Ebenezer, R. Jehadeesan, "Eliminating the need of RF Power Splitting, Floating Load based QPSK Backscatter Modulator" (Communicated in IEEE Letters)

Conferences

1) **Vinita Daiya**, T. S. Krishnan, G. S. Rani, J. Ebenezer, S. SatyaMurty and BPC. Rao, "Theoretical analysis on designing Full Functional Device of WSN using Wireless

Power Transfer," Annual IEEE India Conference (INDICON), New Delhi, 2015, pp. 1-5. doi: 10.1109/INDICON.2015.7443587 (Peer reviewed and published in IEEE Xplore)

2) **Vinita Daiya**, T. S. S. Krishnan, J. Ebenezer, K. Madhusoodanan, S. A. V. SatyaMurty and BPC. Rao, "Dynamic architecture for Wireless Sensor Network-implementation & analysis," International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2016, pp. 1206-1211.doi: 10.1109/WiSPNET.2016.7566328. (Peer reviewed and published in IEEE Xplore)

Vinita Daiya

Vinita Daiya

Dedicated to My Family

ACKNOWLEDGEMENTS

Undertaking this PhD work has been a truly life-changing experience for me and it would not have been possible to do without the support and guidance that I received from many people.

First and foremost, I would like to extend my sincere gratitude to my technology adviser, Ms. Jemimah Ebenezer, for her continuous support, guidance, cooperation, encouragement and for facilitating all the requirements, going out of her way. She has taught me another aspect of life, that, "goodness can never be defied and good human beings can never be denied". I owe a lot of gratitude to her for always being there for me and I feel privileged to be associated with a person like her during my life.

My special words of thanks should also go to my guide Dr. B. P. C. Rao for his valuable and constructive suggestions. His guidance, patience, motivation, and support have always kept me going ahead in tough times.

I sincerely thank my doctoral committee chairman Dr. B.K. Panigrahi and committee members Dr. K. Velusamy and Dr. Anish Kumar for their support, insightful comments and hard questions. My heartfelt thanks also goes to my former technical adviser, Dr. S.A.V Satya Murty, for offering me the opportunity to pursue this PhD.

My sincere gratitude to, Dr. A.K. Bhaduri, Director, IGCAR and Dr. S.A.V. Satya Murty, Dr. P.R. Vasudeva Rao and Shri S.C. Chetal, former Directors, IGCAR for providing excellent environment to carry out research work.

My special thanks to Shri. Jehadeesan, Head, Computer Division for providing his support for various experiments and developments. In addition, I would like to express my gratitude to Dr. M.L Jaylal, Head, Computer Systems Section and his team with Shri. DNVR Subrahmanyam, Ms. Molly, Ms. Deepika, Ms. Suja Ramchandra and

Ms. Sundari, for providing their support to utilize their section computing and virtual desktop facilities.

My heartfelt thanks to Shri. T.S. Shri Krishnan and other colleagues Shri. Sukant Kothari, Ms. D. Baghyalakshmi, Ms. Sandhya Rani, Shri. Sanam Khan, Shri M. Harish and Shri Sandeep for their technical guidance and moral support. They were always standing by my side and sharing a great relationship as compassionate friends.

My special thanks to Dr. Prema who was research associate in my WSN lab, and Dr. Madhushmita from material science group, they have helped me to improve over my research work presentation style. Including them, I will always cherish the warmth shown by my friends Dr. Soumee, Dr. Gurpreet, Ms. Bakkiam, Dr. Deepak, Mr. Atul, Mr. Suranjan, Ms. Molly, and Ms. Deepika. Both technical and non-technical discussion with them has helped me to overcome the research stress.

My special regards to my teachers and especially Dr. R.T. Paturkar of DRDO, my engineering internship mentor, because of knowledge and research motivation gained by them it is possible for me to see this day.

I must thank my lab technical assistants, Shri. Dinesh and Shri. Kannan, for their kind support in hardware error debugging, soldering, and experimental setup establishment.

I owe my deepest gratitude towards my better half, Dr Harish for his eternal support and understanding of my goals and aspirations. His infallible love and support has always been my strength. I am thankful to my son Hardik for being such a good little baby for past three years, and making it possible for me to complete what I started.

My heart felt regard goes to my father in law and mother in law, for their love and moral support. I especially appreciate my mother in law efforts; her support has been unconditional in these last three years.

I feel a deep sense of gratitude to my mother, father, brother, and three sisters for always believing in me and encouraging me to follow my dreams. I also extend my gratitude to my two brothers in laws; they all have always motivated me to complete a healthy doctorate degree.

Thank you everyone.

Vinita Daiya.

Vinita Daiya

CONTENTS

ABSTRACT

A Wireless Sensor Network (WSN) performs critical functions in many applications such as military surveillance, nuclear monitoring, health care monitoring, rescue operations, and detection of fires. These applications involve wireless transmission of critical and sensitive information. Thus, any wireless technology, including WSN is prone to various kinds of attacks that target different layers of the network. Also, remote deployment of a WSN node demands maintenance-free nodes. Thus, considering the requirements of critical monitoring applications with limited or no access, development and deployment of a secured WSN node capable to operate with wireless power solution is of great interest.

Secured data transmission is a power-hungry phenomenon, as both security implementation and wireless transmission demand voracious power. Even though energy-harvesting technology equips the device to harvest power, its non-deterministic and environment-dependent nature makes them unsuitable for critical monitoring applications. Thus, with current research scenario, sustainable secured wireless monitoring system concept for inaccessible area monitoring is very limited. This work focuses on realizing it, by secure backscatter communication technology. This technology can simultaneously mitigate the power and security issues of WSN. The research gap identified in the domain of secure backscatter communication has been addressed in this thesis.

This thesis proposes a novel physical layer security scheme suitable for ad hoc type wireless networks, unaware about the presence of eavesdropper. The existing security schemes available for the secure backscatter communication are suitable for the scenario when eavesdropper/ attacker presence is known and identified. WSN is an ad hoc type resource-constrained network, it is infeasible to identify and locate the

eavesdropper. Thus, to address this spread spectrum based physical layer security scheme has been explored for WSN. Through the rigorous analytical approach, the significance of M-ary spread spectrum obfuscation for WSN has been demonstrated. Further, to implement the same for the physical layer of the WSN, using software-defined radio a novel physical layer block has been developed. Based on the experimental analysis, a novel mapping obfuscation technique for M-ay spread spectrum has been proposed. The proposed technique inhibits real-time eavesdropping irrespective of eavesdropper location with zero security overhead. Moreover, considering the power friendly attribute and its capability to inhibit eavesdropping, the proposed technique is a promising physical layer security technique for secure backscatter communication.

In the thesis, a quad phase modulated backscatter tag has been designed and developed with the unique approach of floating load based backscattering over dual port straight-line microstrip track. Even though, the backscatter signaling has evolved and gained acceptance in RFID domain, the backscatter technology energy and data rate tradeoff is an unresolved issue. The novelty of the developed backscatter tag is twofold; i) it resolves energy-data rate tradeoff issue by using a floating ground backscattering with frequency shifting, and ii) dual port microstrip track allows it to generate and store DC power from RF source during active and sleep modes.

This thesis has also focused towards design of sustainable far-field wireless power solution for secure long–lived WSN based inaccessible area monitoring. RF power during prorogation disperses in space, thus, far-field wireless power generation has been conceptualized in literature by the usage of high power microwave transmission. This high power microwave have adverse biological impacts, thus, to avoid non-ionizing radiation emission limit violation, maximum RF power sampling in

spatial domain has been investigated through efficient rectenna panel design. To design an efficient rectenna panel, a mathematical model has been formulated to optimize its parameters such as rectenna spacing, count, and arrangement pattern. The novelty of the developed rectenna panel design model is that it can be used to design a rectenna panel for any wireless power application. The developed panel model has been validated through experimental analysis and it is verified that the hexagonal shape panel with total number of 10 rectenna can generate steady wireless power for secure backscatter based WSN node placed at the far-field distance of 70m indoor.

The physical layer security scheme, phase modulated backscatter tag and wireless power generation scheme developed in this work are the main contributions in the domain of wireless technology. Overall, the developed wirelessly powered secured backscatter based WSN node is expected to provide continuous secure wireless access to locations with limited or no access application areas including nuclear sector, healthcare sector, military, and disaster management.

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ADC	Analog to Digital Converter
AES	Advanced Encryption Scheme
AN	Artificial-Noise
BF	Beam-Forming
BT	Backscatter Technology
CCT	Capacitor Charging Time
CD	Coordinator
CDMA	Code Division Multiple Access
CET	Chip Error Threshold
CR	Cooperative Relay
CRC	Cyclic Redundancy Check
CWM	Conventional Wireless Monitoring
DSSS	Direct Sequence Spread Spectrum
EC	Error-Correction Coding
ED	End Device
EMPS	Exa Mapping operations Per Second
EPDR	Eavesdropper Packet Delivery Ratio
$EPDR_A$	*actual* Eavesdropper Packet Delivery Ratio
$EPDR_P$	*practical* Eavesdropper Packet Delivery Ratio .
ET	Eavesdropping Test
FCS	Frame Check Sequence
FFD	Full Functional Devices
GPIO	General Purpose Lines Input Output
GRC	GNU Radio Companion
HBT	Hybrid Backscatter Technology
HFSS	High Frequency Structure Simulator
I Signal	In-Phase Signal
IA	Index Alteration
IoT	Internet Of Things
LNA	Low Noise Amplifier

MAC	Medium Access Layer
MaSS	M-Ary Spread Spectrum
MD	Multi-antenna Diversity
MIMO	Multiple Input and Multiple Output
MO	Mapping Obfuscation
MO(IA)	IA based MO
MO(R)	Random MO
MPS	Mapping operations Per Second
OOK	ON-OFF Keying
oQPSK	offset Quadrature Phase Shift Keying
PA	Power Amplifier
PDR	Packet Delivery Ratio
PHR	PHY Header
PHY	Physical Layer
PLS	Physical Layer Security
PN	Pseudo-Noise
PO	Preamble Obfuscation
Q Signal	Quadrature-Phase Signal
RA	Relay Assisted
RF	Radio Frequency
RFD	Reduced Functional Devices
RFID	Radio Frequency Identification
RPUF	Rectenna Panel Utilization Factor
RWM	RF Power Based Wireless Monitoring
SA	Signal Analyzer
SBC	Secure Backscatter Communication
SBWSN	Secured Backscatter based WSN
SDR	Software Defined Radio
SFD	Start of Frame Delimiter
SHR	Synchronization Header
SINR	Signal to Interference & Noise Ratio
SNR	Signal to Noise Ratio

SS	Spread Spectrum
SSeO	Spreading Sequence Obfuscation
SSO	Spread Spectrum Obfuscation
SWIPT	Simultaneous Wireless Information and Power Transfer
TMS	Total Mapping time in Seconds
TNR	Total Number of Rectenna
VM	Voltage Multipliers
WDSSS	Watermark Direct Sequence Spread Spectrum
WSN	Wireless Sensor Network
YMPS	Yotta Mapping Operations Per Second
ZMPS	Zetta Mapping Operations Per Second
µC	Microcontroller

CHAPTER 1

Introduction

This Chapter introduces Wireless Sensor Network and challenges associated with wireless based inaccessible zone monitoring. With detailed survey, it highlights the significance of secure backscatter communication for resource–constrained wireless monitoring. Based on the research gap identified, and motivation obtained, optimization of secure backscatter communication for inaccessible zone monitoring is discussed. The Chapter enumerates the research objectives, and thesis structure.

1.1 WIRELESS SENSOR NETWORK

Wireless Sensor Network (WSN) technology [1] is permeating in our day-to-day monitoring, controlling and communication activities. In WSN, the sensors are connected wirelessly to each other and they forward their data with the aid of wireless routers or clusters either to a central network controller, the basestation or to the gateways of wireless and wired network. The advantages associated with WSN such as mobility, scalability and infrastructure-less deployment have led to their adoption for multiple applications. Considering the significance of WSN in various applications [2], the WSN technological importance tree shown in Figure 1-1 has been drawn. As shown in Figure 1-1, WSN is used either for process automation, to increase system reliability and for enhanced living, or to facilitate, integral monitoring and control activities for biologically high impact, inaccessible areas.

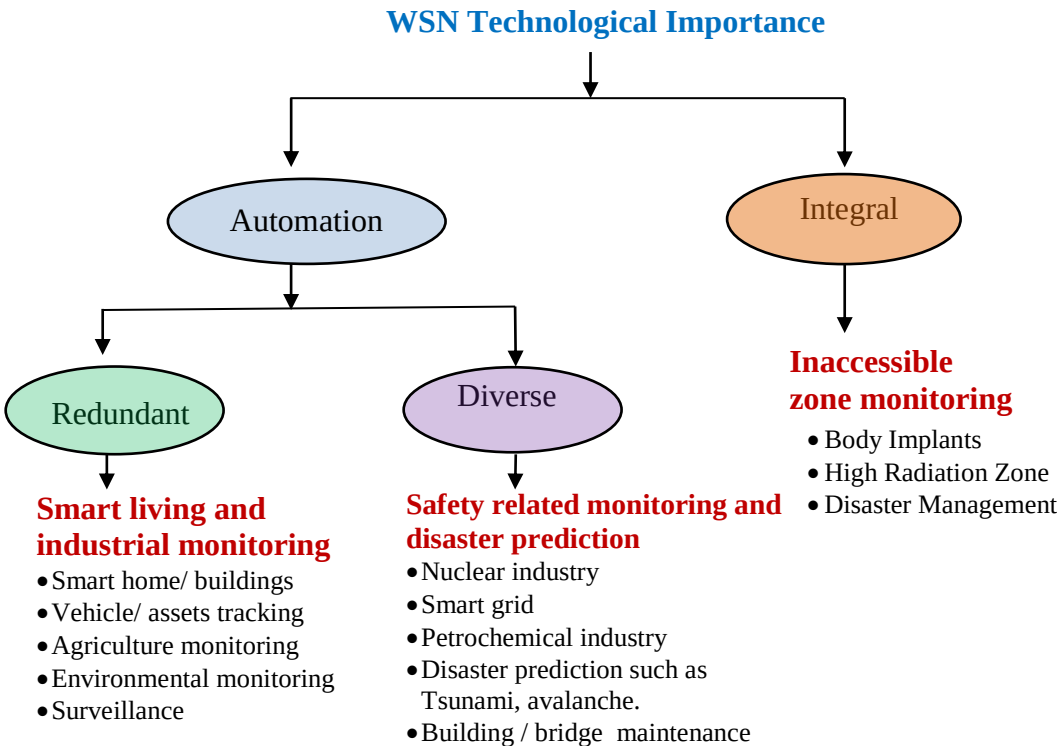

Figure 1-1: Technological importance of WSN in various applications

1.1.1 WSN as Automation Technology

The recent advancement in the concept of smart homes, buildings [3], and offices would have been realized with the aid of WSN [1]. Similarly, for vehicle tracking [4], industrial manufacturing process monitoring with controlling action, asset tracking, soil /pest monitoring in agriculture field [5], [6] and in various surveillance monitoring [7], [8], WSN is used as a redundant technology for remote automation. However, in the nuclear [9], [10], petrochemical industries and various other industries dealing with safety related processes, the WSN is used as diverse technology to increase system reliability [2]. In addition, with conventional wired or manual monitoring, WSN is also used for disaster prediction [11]–[13] and building maintenance [14].

Overall, the WSN based automation in the above-discussed applications has improved system performance in context of remote access, increased reliability, availability, and faster event prediction.

1.1.2 WSN as Integral Technology

Unlike to autonomous application scenario, for the inaccessible zone monitoring, the WSN is the solitary solution. It facilitates monitoring and provides the remote accessibility to the processes, which inhibits wired monitoring or manual entry due to either structural issue [15] or hidden hazardous targets/elements [16] or adverse biological impact [17]–[19]. Even though, the inaccessibility can be in terms of difficult terrain or dense installations of mechanical structures such as piping and equipment in any industry, for illustration the discussion has been focused towards inaccessibility scenarios related to healthcare sector and nuclear sector.

1.1.2.1 Scenarios of inaccessibility in healthcare sector

In the domain of healthcare sector, many implantable medical devices are used for life saving or transformation [20], [21]. Among these devices, the lifesaving medical devices that regulate the cardiac activity are implantable cardioverter defibrillator (ICD), pacemakers, and left ventricular assist device (LVAD) [22]. ICD and pacemakers are required for heart rhythm control while LVAD is required to maintain the blood pumping ability of the heart. These vital battery operated electronic devices are implanted in human body through surgery; the communication with implanted devices through wired technology and associated complications has been reported in literature [23], [24]. Thus, the wireless connectivity is the only safe option available to monitor their healthiness and to ensure steady functionality throughout the person’s life. Similarly, all bionic implants are inaccessible without wireless technology.

Other than implantable device, electronic based medical devices are also used to take internal organ imaging, like endoscopy. In endoscopy procedure, the patient needs to swallow the sensor cable; usage of wireless camera eliminates the patients discomfort and anxiety arising due to test procedure [25].

1.1.2.2 Scenarios of inaccessibility in nuclear sector

The vision of nuclear sector is to generate clean electricity from nuclear energy. As shown in Figure 1-2, the nuclear cycle for electricity generation involves processing of radioactive material for fuel assembly fabrication, a nuclear reactor to harness energy from radioactive fuel and spent radioactive fuel reprocessing [26]. In this scenario, all the processing associated with nuclear fuel handling limits the human intervention due to hazardous effect associated with ionizing radiations emitted by the fuel, especially spent fuel. Hotcells with shielding walls made of oil-encapsulated lead glass is used for fuel processing and post irradiation examination [27]–[29]. To limit the exposure to ionizing radiations, cable penetrations in hotcell structure is discouraged. In addition, the radioactive waste generated from spent fuel assembly reprocessing is either intrinsically radioactive, or has been contaminated by radioactivity; thus, radioactive waste need to be stored and managed for years (>10) without compromising human life safety[17]. Hence, safe monitoring of radioactive material processing is feasible only through wireless technology.

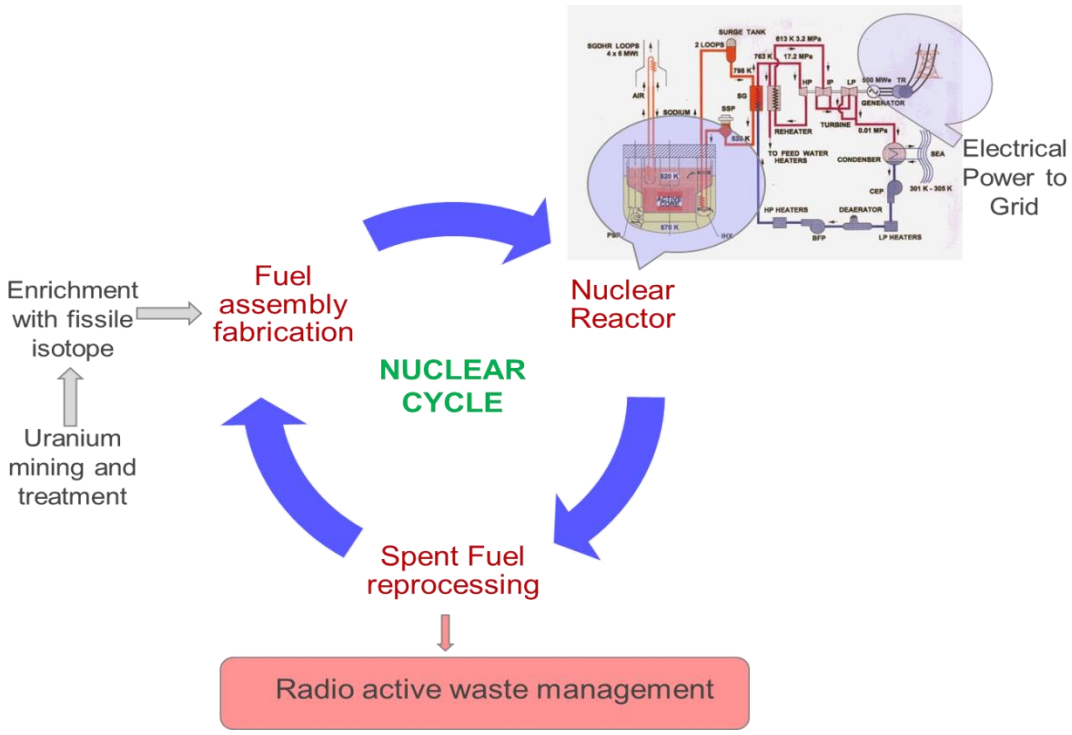

Figure 1-2: Nuclear cycle for electricity generation [26]

Owing to the impact on society, WSN is a necessary integral technology for the inaccessible scenarios of healthcare sector, nuclear sector, and other hazardous elements related industrial plants. In addition to these applications, WSN becomes primary technology for disaster management [12], [13], [19], [30] in the scenario of avalanche, flood, fire or industrial/ nuclear accident.

Henceforth, the vision of the thesis will be focused towards WSN for inaccessible zone/ scenario monitoring.

1.2 Challenges for WSN based Inaccessible Zone Monitoring

The foremost challenge associated with any wireless technology is security. Unlike wired communication, wireless works in broadcast mode; radio frequency (RF) signal used for establishing communication, can be accessed by anyone without disturbing signal level for source and destination. Therefore, this common problem

associated with wireless communication is also associated with any type of WSN monitoring.

Further, focusing towards inaccessible zone monitoring, it is inevitable that power available for WSN node need to be treasured without compromising monitoring task. Depending on the network lifetime required for application monitoring, the WSN node power consumption becomes the biggest network constraint.

The power options available for WSN node deployed for inaccessible zone monitoring are the battery, energy harvesting source, wireless power, or their combination. Even though the battery is the source of stable power supply for WSN node, it has limited storage capacity. The battery size is dependent on its storage capacity, thus, its size is the major constraint for the applications which demands miniaturized monitoring devices (for e.g. health care sector). In addition, the conventional batteries such as lithium-ion and lead-acid are not suitable to operate above 70°C without any thermal ventilation [31], [32]. In the nuclear fuel processing applications and radioactive waste management, it is difficult to provide thermal ventilation for the batteries. However, for disaster management, which is a temporary short duration application, conventional battery-powered WSN node may serve the purpose.

Looking forward to the energy harvesting and wireless power regimes to power the WSN node, the former is non-deterministic and environmental dependent [33], [34]while the latter need to be explored for far field wireless power generation in the domain of inaccessible area monitoring.

Hence, for WSN based inaccessible zone monitoring, data communication security, node power consumption and its power source are three major challenges. In addition, the WSN nodes used specifically for life saving healthcare devices or

radioactive waste management can be declared as resource-constrained as these applications demands long-lived monitoring. Thus, considering all the wireless requirements for long-lived inaccessible zone monitoring, the vision of this thesis is to design a sustainable secure wireless monitoring system for it.

1.3 LITERATURE SURVEY

WSN based long-lived inaccessible zone/ scenario monitoring, demands resource-constrained WSN node to transmit secure data periodically for years. This section presents the overview on existing work available in the above-mentioned domain. Further, it proceeds with basic power minimization techniques for WSN node, security techniques available for resource-constrained WSN nodes and RF based wireless power solutions are discussed.

1.3.1 Wireless Monitoring for Inaccessible Zone Applications

In this section, the existing work on wireless based inaccessible zone monitoring has been discussed. Event though, for some research work wireless technology used is not WSN, it has been discussed to emphasize the need of WSN for inaccessible zone monitoring. The literature articles with their work description and inferences obtained are discussed below. For lucidity, the literature has been segregated based on application nature.

1.3.1.1 Wireless in healthcare sector

Ferguson et al.[88], investigated on implant-to-surface communication technology in their work. They have used galvanic coupling to send signals from an implanted device to electrodes on the skin. In the technology used by them the conductive properties of body is used to establish the communication. It results in high

attenuation when the signal meets the skin because skin is highly resistive to alternating current. In addition, the technique is completely ineffective when the receiver is detached from the human body.

Park H. and Ghovanloo M. [89] explored three frequencies in industrial, scientific, and medical bands (27 MHz, 433.9 MHz, and 2.48 GHz) in terms of their data link performance based on path loss and radiation patterns over horizontal and vertical planes for wireless communication establishment with intraoral tongue drive system. Their experimental result shows that 27 MHz has the smallest path loss in the near field while 433.9 MHz and 2.48 GHZ are suitable for far field. With transmit power of 0dBm; they were able to establish communication up to the distance of 123cm and 39cm respectively for 433.9MHz and 2.48GHz. Thus, human body attenuation increases with increase of communication frequency.

Liu. et al. [90] designed a offset quadrature phase-shift keying (O-QPSK) transmitter operating at 400-MHz with 0.18µm CMOS technology for implantable neural recording application. Their developed transmitter consumes power of 3.48mW. Even though, the communication standard has been not specified in their work, the modulation scheme implemented by them is same as used for WSN.

Zhang et al. [91] introduced the concept of BT with on-body sensor monitoring. They have implemented frequency shifted- BT using on-off keying (OOK) modulator with ring oscillator to shift the backscatter signal frequency. They have demonstrated the communication range of 4.5m.

Vasisht et al. [92], designed a ReMix system to demonstrate in-body deep-tissue backscatter communication and localization. They have first time demonstrated the usage of BT for in-body medical imaging and localization study. They have used BT to reduce the power consumption for wireless medical device. In their work, they have

implemented BT using OOK and to eliminate in-band interference they have used body characteristics to shift he frequency of backscattered signal.

Agarwal et al. [93], presented a review on various wireless power transfer strategies suitable for implantable bioelectronics. They have compared inductively coupled, capacitively coupled, ultrasonic, mid-field, and far-field based wireless power transfer technologies based on their power budgets and wireless power transfer range. In their work they mentioned that compared to all wireless power transfer techniques, far-field method can support a long range (few tens of mm); they can power the deep-seated implants using antennas much smaller than those used in the near-field implants. However, they have emphasized that for GHz frequency far-field power transfer, power rectification losses are high. The concluded that advancement in rectenna design can improve the power transfer efficiency in the far-field domain. In addition, they mentioned that wireless implants consuming ultra-low power could be benefited by using far-field signal for power and wireless communication. This combined usage of far-field is referred as simultaneous wireless information and power transfer technology (SWIPT) [94].

Camara et al [95] performed the survey on main security goals for the next generation of implanted medical devices and analytical study on the most relevant protection mechanisms proposed so far. They specified that inherent security- scheme design constraints for these implanted devices are energy, storage, and computing power. They have concluded that existing security solutions are effective from theoretical point of view, but an adequate balance between the safety of the patient and the security level offered, with the battery lifetime are critical parameters need to be addressed simultaneously.

1.3.1.2 Wireless in nuclear sector

Gomez et al. [18], designed a self-sustainable wireless sensor node for the monitoring radiation in contaminated and poorly accessible areas. The node is designed to work in collaboration with an unmanned aerial vehicle. The developed node uses an ultra-low power controller, supports short-range radio communication, solar energy harvesting, adaptive power management and duty cycling, and a nano-watt wake-up radio. They have minimized the power consumption of the node by incorporating the techniques1-3 from Table 1-1. In addition, they have used solar based harvesting for network sustenance.

Wu et al. [96] paper presents a nuclear radiation detection and monitoring system based on WSN, ZigBee protocol. To save the node power they have adopted sleep mechanism. Further, to enhance the monitoring system reliability they have designed uninterrupted power supply to mitigate the power fluctuation issue for direct mains powered WSN node.

Shikaze et al.[97] have performed field test around Fukushima Daiichi nuclear power plant site using improved Ce:Gd3$(Al,Ga)_5O_{12}$ scintillator Compton camera mounted on an unmanned helicopter. The helicopter's flight path and speed were pre-programmed to lines interspaced by 5 and 10 m intervals and 1 m/s, respectively, facilitating measurements over areas of 65×60 m^2 and 65×180 m^2 at a height of 10 m for approximately 20 and 30 min, respectively. For this field test, Compton camera system consisting of a detector and data logger equipped with a GPS and a wireless modem was used.

Tonglin Zhang [16] proposed WSN for radioactive target detection, which is important with respect to public safety and national security. He has used the physical law for nuclear radiation isotopes and proposed a statistical method for

WSN data to detect and locate a hidden nuclear target in a large study area. Even though he has not discussed about network lifetime and strategies used for node power reduction, his research work have wide applications in the nuclear safety and security problems.

Jha et al. [98] proposed the use of WSN for measuring radioactive contamination in the water. They have selected WSN for large scale monitoring as this technology has attributes of self-maintaining and scalability.

Shimura et al. [99] developed the system of wireless communicating area monitor with surveillance camera for radioactive dose detection and work efficiency improvement for nuclear power plant zones that have high dose.

Constantinou et al. [100] proposed a WSN system for monitoring nuclear waste stored in sealed underground repositories. Considering the harsh conditions of radioactive waste repositories, they have selected a magnetic spring to store energy and power on WSN system when desired they have mentioned that radioactive waste monitoring does not require continuous monitoring, thus, to activate the WSN system they have implemented two techniques. In the first technique, the stimulus is supplied through RFID communication to energy supply unit. Second technique is sensor event triggered; a change in environmental conditions of waste state activates the WSN system.

Irrespective of healthcare sector or nuclear sector application, long-lived WSN monitoring is required for permanent deployment. For WSN node power reduction, ultra-low power consuming chip design, sleep cycle, and BT is explored.

In the domain of healthcare sector, battery energy density and size tradeoff is an issue [63]. while in nuclear, harsh conditions due to high ionizing radiations and high

temperature is an issue for conventional battery technology [71] Even though, application specific energy harvesting or power generation techniques exist, concerning the health safety aspect and to have uninterrupted maintenance free monitoring a wireless power solution becomes a necessity.

Backscatter communication is being explored in the healthcare sector as it can serve two purposes, wireless power transmission, and wireless communication establishment[92]. Even though, backscatter has not been explored in nuclear application, it can be envisaged from the work of Constantinou et al. [100], that it can revolutionize the monitoring in that domain if instead of RFID and conventional WSN transceiver, backscatter tag is used. They have used RFID for sending stimulus to activate WSN system, which further sense and transmit the data. BT based WSN system can eliminate the need of energy unit and will transmit information through the stimulus signal.

Nevertheless, the wireless communication security is highly important in both the sectors, it is underdeveloped due to the resource constraints. Considering the BT as promising technology for inaccessible area monitoring, the existing work in BT and the security scenario in the domain of backscatter communication will be discussed in following sections.

1.3.2 WSN Node Architecture with Basic Power Consumption Minimization Techniques

A WSN node consists of sensing, processing, communication, and power subsystem as shown in Figure 1-3. The processing subsystem consists of a microcontroller (µC), it stores and executes the communication protocols as well as data processing algorithms. Sensing subsystem is governed by analog to digital converter (ADC) chip and sensor associated signal-conditioning circuit. ADC can be a

µC peripheral of or an external chip, depending on the application requirements. The digitized sensor values provided by sensing subsystem are processed by µC and forwarded to the communication subsystem as a data packet. Communication subsystem performs digital and analog processing based on the physical layer attributes defined by WSN communication standard IEEE 802.15.4 [35]. IEEE 802.15.4 standard defines medium access layer (MAC) and physical layer (PHY) for WSN communication protocol. Based on standard defined attributes, WSN node controller and radio chip have operation trade-off between flexibility and efficiency – both in terms of energy and performance. Thus, considering this trade-off, the power-consumption minimization techniques available from controller and radio chip attributes are discussed in this sub section.

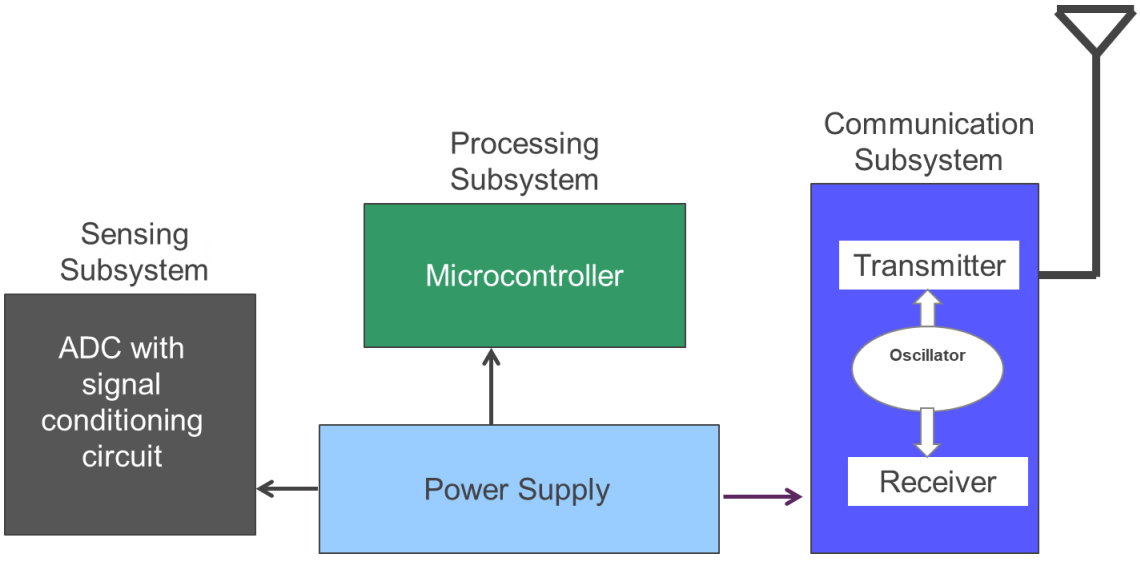

Figure 1-3: WSN node architecture

1.3.2.1 Power minimization using WSN node controller attributes

WSN node is microcontroller based embedded dvice. The current embedded controllers are built over complementary metal-oxide semiconductor technology; thus, as mentioned by Venkatachalam et al. [36], the embedded chip power consumption $\boldsymbol{P_{ed}}$

is the aggregate of dynamic power consumption $\boldsymbol{P_{dynamic}}$ and static power consumption $\boldsymbol{P_{static}}$ as indicated by equation (1-1). The static power consumption is the dominant source of power consumption, it is leakage power, [13], persisting whether the device is active or idle. The power consumption due to device activity is referred as dynamic power. It can be approximately determined by equation (1-2).

$$P_{ed} = P_{static} + P_{dynamic} \tag{1-1}$$

$$P_{dynamic} = sCV^2f \tag{1-2}$$

where,

s : *the switching activity factor that relates to how many transitions occur between digital states (i.e., 0 to 1 or vice versa) in the processor*

C : *the total load capacitance*

V : *supply voltage*

f : *clock frequency of the processor*

According to equation (1-2), there are four ways to reduce the dynamic power consumption. However, the switching activity s, the total capacitance load C and the supply voltage V range are related to chip design parameters, such as clock gating, transistor size and connection lengths; the low power consuming chips are designed by controlling these factors. On the other hand, the low power microcntroller permits the user to optimize/ minimize the controller operating frequency to minimize power consumption. Supply voltage scaling can also aid in power reduction, but controllers menat for resource contraint developments, does not allow this scaling. However, the chip designers permit to cut-off the supply and clock for various pheipherals of the controller, also they support different power saving modes.

Thus, WSN node power consumption using controller attributes is mainly minimized in various WSN applications by adopting any one or combination of the below mentioned operations:

1) Selection of low power consuming controllers.

2) Reducing operating frequency of the controller.

3) Cutting-off the power and clock for unused peripherals

4) Enabling the sleep mode during the idle period.

For example, Raghunathan et al. [37] presented the vision of autonomous long-lived network in their work. They have incorporated all the above-discussed techniques to minimize the WSN node controller power consumption. In addition, they have focused on the design of energy-efficient routing algorithm. However, energy-efficient software/ algorithm also optimally utilize the CPU cycles and reduce the device active time.

Hence, the approach presented by Venkatachalam et al. [36], is in general used in all WSN based applications to minimize the controller power consumption.

1.3.2.2 Power minimization using WSN node radio chip attributes

RF chip processes GHz analog signal and consumes more energy than the digital processing [38]. As shown in block diagram of a radio chip (Figure 1-4), the red highlighted blocks, namely, frequency synthesizer (local oscillator generating GHz signal), power amplifier (PA) and low noise amplifier (LNA) are most power hungry components. Radio chip energy model presented by Li et al. [39], demonstrates that analog domain of RF chip consumes 80% power of radio chip. Power consumption due to PA and LNA is instantaneous, i.e. depends on radio chip operating mode but, frequency synthesizer block consumes 60% power and is operating continuously (except when radio is in deep sleep state).

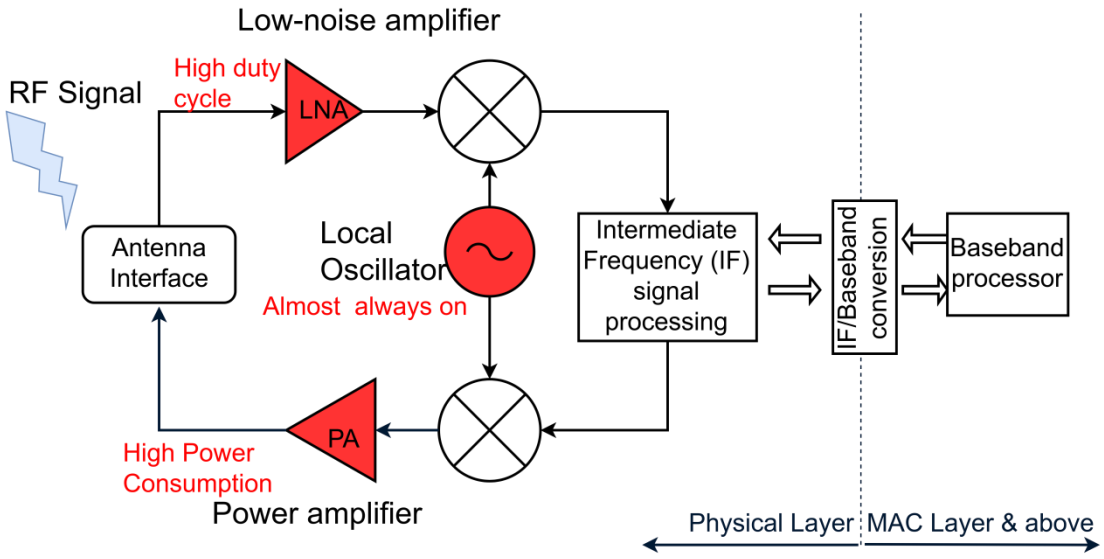

Figure 1-4: Block diagram of radio chip [38]

Thus, in WSN applications power consumption due to radio chip is reduced by following arrangements:

1) Sleep state enable during idle mode [18], [37], [40].

2) Reducing the RF packet transmission power, it minimizes the power consumption due to PA[18], [35], [41].

3) Off-loading the RF chip GHz oscillator, elimination of RF chip analog processing block. This attribute is attained by the usage of backscatter technology (BT) for RF packet transmission.

Backscatter technology uses incoming/ ambient RF signal to transmit the data; thus, they leverage the need of RF signal generation for wireless communication establishment [42]–[47]. This signaling approach shifts the device maximum energy costs to the off node RF signal generator, which is generally part of the infrastructure The concept of BT was proposed by Stockman in 1948 [48]. In his work, he has established a point-to-point communication by replacing the transmitter by modulating reflector.

Depending on data bits to be transmitted, BT reflects the electromagnetic waves by modulating the reflection coefficient of the transmission line. By varying the antenna load impedance as shown in equation (1-3), reflection coefficient can be varied.

$$\Gamma_i = \frac{Z_i - Z_a^*}{Z_i + Z_a} \tag{1-3}$$

where,

Z_a : *The antenna impedance and* * *is the complex conjugate operator*

Z_i : *Antenna load impedance corresponding to switch state and* i *=1,2,4,8…. represents the switch state*

Γ_i : *Reflection coefficient for switch state, i*

In BT, typically two state modulations $i = 2$ is used because of its simplicity. The most prominent application of two-state BT is RFID. ON-OFF keying (OOK) enables BT to switch between load impedance, Z_1 and Z_2 which results in reflection and absorption of RF signal respectively. Even though, it is easy to implement amplitude modulation using BT, other modulation schemes can be implemented by combination of 2-state RF switches [49], [50].

1.3.2.3 Power reduction for various power minimization techniques

The reduction in the node power consumption for various power minimization techniques available in literature for µC and radio are summarized in Table 1-1.

Among all the power minimization techniques compared in the Table 1-1, the maximum power saving is achieved by the usage of backscatter radio. However, BT can replace only the conventional radio of WSN node. Thus, power minimization techniques specific to µC will provide extra power saving for the WSN node.

Table 1-1: Power reduction percentage for various WSN node power minimization techniques [18], [38]–[40], [51]

Technique No	Technique	Reference for calculating power reduction	Power reduction %
1.	µC sleep + reduction in CPU cycle + power cut off for unused peripherals	µC active	10
2.	Reduction in RF packet transmission power	Radio active	5-7
3.	Radio sleep	Radio active	70
4.	Backscatter radio	Radio active	80-90

1.3.3 Security Techniques for Resource Constrained Wireless Network

In the domain of wireless communication systems, security techniques are classified, as cryptographic technique or physical layer security (PLS) technique.

Cryptographic techniques involve compute-intensive operations, among cryptographic techniques viz. symmetric, asymmetric and hybrid, the symmetric (private) key technique is mostly used for resource-constrained wireless applications as mentioned by Zhang et al in their work [52]. However, for widespread symmetric security scheme, advanced encryption scheme (AES) [53], Hung and Hsu [54] specified that AES block demands 50-70% more power. Further, as per the investigations performed by Chaudhry et al. [55] for Bluetooth security, the AES block consumes energy of 1.21µJ/byte for encryption process. Hence, based on wireless network data rate and payload size, power demand for packet encryption varies. Overall it is challenging to implement cryptography based security for BT based WSN node.

PLS based security [56], is a different paradigm from cryptography, it explores physical channel randomness to implement security. They are considered suitable for resource constrained wireless network, as they do not involve any computation complexity for their implementation. The commonly used PLS techniques are namely,

artificial-noise (AN) addition (intentional jamming) [57], [58], beam-forming (BF) techniques [59], [60], multi-antenna diversity (MD) technique[61], cooperative relay assisted (CRA) technique [62] , and coding based[63] techniques. In comparison to cryptography, PLS techniques inhibit eavesdropping. Important findings in the domain of PLS are discussed below.

Yener and Ulukus [64] have mentioned in their work that the PLS techniques, AN, BF, MD and CR requires knowledge about eavesdropper presence and have hardware overhead; hence, they have concluded that wireless security due to mentioned PLS techniques cannot be achieved without the aid of external devices with unlimited power.

Chopra et al. [65] have specified in their work, that PLS techniques increases the overhead for the legitimate sender and receiver devices.

Liu et al [66], have proposed friendly jammer based AN technique in the scenario when presence of eavesdropper is unknown. The proposed technique demands extra power for generating jamming signal.

Zurita et al. [67], have proposed the technique to maintain the legitimate receiver's signal to interference & noise ratio (SINR) by the usage of beam-forming for intended receiver and broadcasting of artificial noise for unknown passive eavesdropper. The drawback of their technique is that it demands for extra power and optimum-power allocation strategy for beam forming and noise generation.

Shiu et al. [56] have highlighted in their PLS tutorial, that coding based PLS techniques are of two types, error correcting code based and spread spectrum (SS) based. He has emphasized that both these techniques does not require the knowledge of eavesdropper presence for their implementation and have no hardware overhead.

Abbasi et al. [68] have used turbo codes with AES to enhance the security strength of satellite channel. The turbo codes are part of coding based PLS. However, coding based PLS does not need information regarding the presence of eavesdropper. Hence, when used with cryptographic technique they limit eavesdropping and provide two level of security.

Sedaghatnejad and Farhang [69] have declared in their work that SS based PLS, part of coding based PLS technique, demands for chaotic sequence. They have demonstrated that chaotic SS based PLS have high detection probability; hence, they are unsuitable for security implementation.

Li et al. [70] proposed the AES based Code Division Multiple Access (CDMA) CDMA to provide two level of security; as the CDMA is an example of SS based PLS.

Muntwyler et al. [71] implemented security by obfuscating the spreading sequences for M-ary SS (MaSS) used in IEEE 802.15.4 standard of WSN. For MaSS, the number of spreading sequences used is M in number, while for 1-ary SS, single spreading sequence is used. CDMA is an example of 1-ary SS. They have eliminated the problem of faster detection probability associated with chaotic 1-ary SS[69]. However the drawback associated with their technique is that it demands M secret sequences per node.

Liu et al. [72] proposed watermark direct sequence spread spectrum (WDSSS) technique for implementing security using MaSS. In WDSS, selected chip bit of chipping (spreading) sequence are flipped to transmit secure data. The drawback associated with their technique is that it limits the secret data transmission capacity; as their exist a tradeoff between signal SNR and secret data rate tradeoff.

Nain and Rajalakshmi,[73] proposed steganography, it demands for an extended pseudo-noise sequence set. Thus, their technique increases overhead for generation and management of extended pseudo-noise sequence set.

Overall, the SS based PLS is different from other PLS techniques, as it inherently does not require any information regarding the presence of eavesdropper. However, for other PLS techniques, network cooperation based strategies are available to implement them with power and hardware overhead when the presence of eavesdropper is unknown.

1.3.4 RF based Wireless Power Generation Strategies

In the domain of wireless power generation or harvesting through RF wave, in the work [74], [75] and [76] to enhance rectenna efficiency, authors have explored the options for rectifier design such as series & shunt diode based rectifiers, bridge rectifier and voltage-doubler rectifier. In the studies [77] , [78], authors have explored photonic band gap structure to enhance antenna performance. Sinha et al [79] demonstrated in their work that antenna gain and bandwidth improves with the usage of superstrate layer. Such efficient antenna designs when integrated with rectifiers will result in efficient rectenna design.

Further, to meet the growing power demands of wireless devices, rectenna panel concept is being explored in various applications. Former researcher Shinohara et al [80], have designed a rectenna array and focused their study on identifying the rectenna connection configuration that results in highest output power. For their experimental analysis, the authors have arranged the rectenna in square grid. However, work does not discuss about the rectenna panel design parameters such as panel size, rectenna spacing, etc. A similar study was presented by Olgun et al. [81], they have done analysis on the

effect of rectenna connection configurations (series, parallel and cascade) on the panel generated power. Massa et al. [82] presented the efficiency comparison for the two approaches used for designing the RF energy harvesting array namely, (i) rectenna array based design and (ii) antenna array with a single rectifier based design in their work. Marshall et al. of work [83] have quantified the peak available power for N^2 rectenna array. In their work, N is the number of rectenna in one row/ column of the designed rectenna array; although, the criteria for its selection is not specified. Gretskih et al. [84] implemented mathematical model to represent vast rectenna array as the single equivalent element of the rectenna in their work. The developed model by them is useful for RF harvesting system performance characterization, although work does not discuss about rectenna panel design parameters. Rectenna panel design and development consist of rectenna design, rectenna connection configuration, and panel design parameters. All the aforementioned works does not discuss about panel design parameters.

With the extensive literature survey, three main research papers [85], [86], [87] have been identified which discusses about panel design parameters. In the work [85], Otsuka et al. focused on rectenna spacing optimization to enhance rectenna panel efficiency. Based on experimental study, the work concluded that rectenna panel efficiency degrades with increase of rectenna spacing beyond 0.7λ (λ is governed by operating frequency of rectenna). The study was performed for square grid rectenna pattern only. However, the result appears to be specific to the particular antenna chosen for rectenna, i.e. panel design. Strassner and Chang [86], designed honeycomb pattern rectenna panel with aperture overlap using circularly polarized rectenna. Their work suggests that "little" aperture overlap eliminates the power voids, but they have not quantified the percentage of overlap required. Liu et al. [87], designed a fixed size

rectenna array with fixed rectenna spacing. For short distance harvesting, equilateral triangle approach for rectenna placement with aperture, overlap was proposed in their work; but, criteria for rectenna spacing selection has not been mentioned by the them.

1.3.5 Implementation Strategies used for Backscatter Technology

Based on the literature survey conducted in the domain of inaccessible area monitoring, BT is the best technology for battery-constrained WSN nodes. Memon et al. [45], presented in their BT survey paper details on backscatter communication tag architecture, communication modes, modulation schemes, channel coding, interference mitigation techniques, decoding and signal detection schemes. In addition, they have highlighted BT applications and challenges associated with reliability and security of the BT based network. However, focusing towards the WSN based inaccessible area monitoring; the important findings in the domain of BT are presented in Table 1-2.

Table 1-2: Summary of important findings in the research domain of BT

References	Attributes desired for WSN and related work summary
	➢ **Modulation technique:** WSN uses QPSK modulation, it is advanced form of M-PSK, M being 4 and all the phase angle are orthogonal to each other.
[49]	• M-PSK is implemented using phase delay tree as shown in Figure 1-5, impedance matching complexity at each tree node junction. Also, demands for software techniques for in-band interference mitigation.
[50]	• M-PSK is implemented using multiplier based switching as shown in Figure 1-6, RF multiplexer operating at GHz frequency consumes more power than RF switches operating at GHz frequency
[46], [51]	• M-PSK implemented by performing phase modulation of control signal used for controlling the RF switch of OOK based backscatter communication. It eliminates the in-band interference issue. However, the control signal frequency limits the wireless communication data rate [101]
	➢ **Compatibility with conventional wireless communication and support for data rate:** Conventional WSN node should be able to receive packets transmitted by BT based WSN. In addition, compromise on data rate is also not desired.
[49]	• Data rate achieved is 5Mbps for Wi-Fi communication. Demands specific communication protocol for reading data from Wi-Fi based BT also Wi-Fi access points need a separate decoder for extracting information from backscattered signal. Not compatible with conventional Wi-Fi access points without any hardware overhead.
[47]	• Compatible with existing Wi-Fi communication, but data from BT based Wi-Fi tag is communicated by absorbing and reflecting the existing Wi-Fi packets. It needs the aid of Wi-Fi helper, data rate achievable is 2kbps.
[51]	• Fully compatible with conventional Wi-Fi communication, as the tag is equipped with RF stack to generate complete Wi-Fi frame. As the modulation is implemented by phase modulating the RF switch control signal, the maximum achievable data rate is bottleneck.
[46]	• Fully compatible with conventional Wi-Fi communication, but he tag does not generate Wi-Fi frame on its own. It uses existing Wi-Fi signal to relay its information. It perform codeword translation for the incoming Wi-Fi packet, the presented technique is specific to Wi-Fi technology cannot used for other wireless communication.
	➢ **Undesired BT tradeoff between communication rate and harvested energy:** BT tags need to harvest energy and transmit the data. This can become a bottleneck for critical monitoring applications
[102]	• The time required for harvesting depends on the distance of BT from the RF source. The duty cycle for RF harvest and backscatter need to be adjusted accordingly. Data rate drops with increasing distance, as harvesting time increases.
[103]	• Time splitting and power splitting strategies has been discussed. Time splitting add the penalty of degrading communication transmission rate. Power splitting eliminates the data rate degradation issue by using two separate RF sources for harvesting and backscattering. Power splitting increase the infrastructure based complexity.

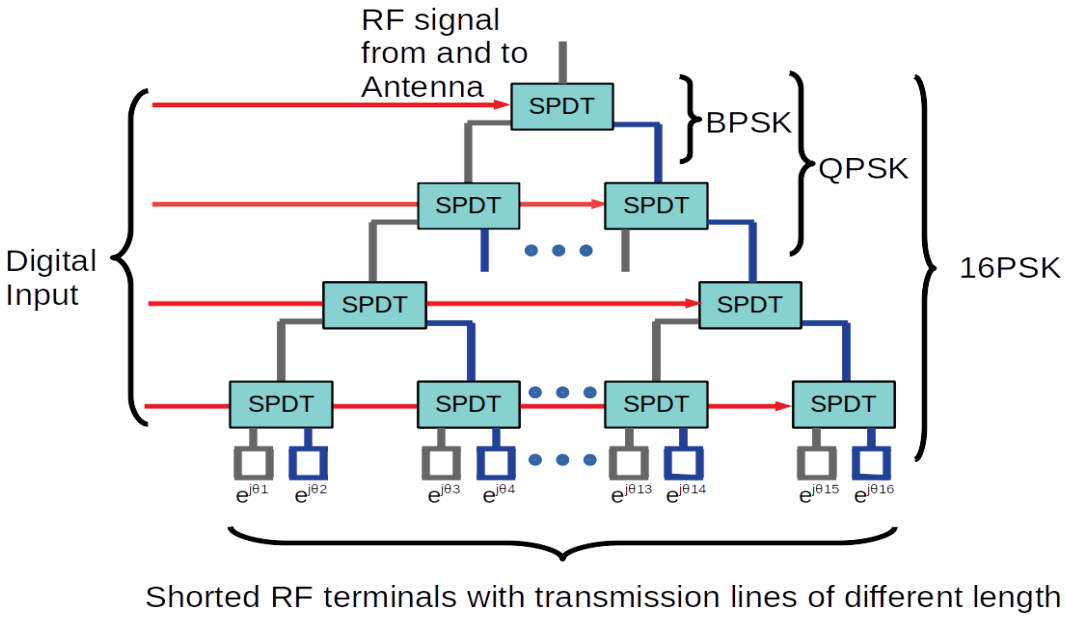

Figure 1-5: Phase delay tree for implementing M-PSK modulation scheme for backscatter communication [49]

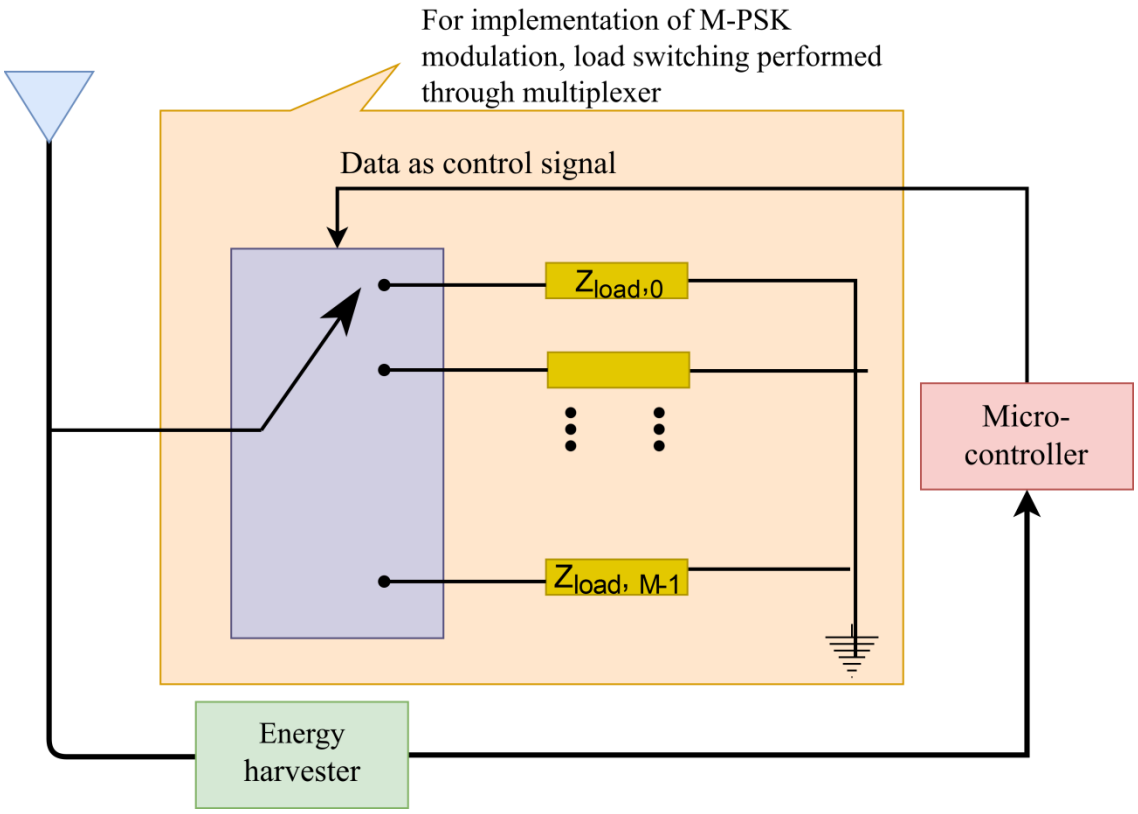

Figure 1-6: Multiplexer based switching for implementing M-PSK modulation scheme for backscatter communication [50]

1.3.6 Secure Backscatter Communication

Secure Backscatter Communication (SBC), is backscatter signaling combined with PLS technique. SBC is underexplored research area, for SBC only two types PLS techniques namely, AN and CRA have been explored in the literature. The first usage of these PLS techniques in the domain of BT is enumerated below.

1) Saad et al. [104], have made the initial attempt on using AN based PLS for SBC. This technique was used in their work for a basic single-reader, single-tag model. The AN-SBC is reader dependent and useful only when eavesdropper location is known [104], [105].

2) Wang et al. [106] have proposed the CRA technique for SBC. In their work, they have assumed that eavesdropper is not in the range of the tag, hence, their proposed solution is suboptimal for this thesis vision.

The major drawback associated with AN and CRA based SBC is that they require knowledge about eavesdropper presence. In addition, with CRA technique security can be achieved only if eavesdropper is detected and its identity is known. Considering the scenario of inaccessible monitoring, it is not feasible to detect or locate the eavesdropper.

1.4 MOTIVATION

The critical monitoring applications demand secure reliable data transmission and the add-on constraint of inaccessibility, demands sustainable wireless network. Considering the resource constraint attribute of inaccessible area wireless monitoring, hypothetically SBC is a promising technology. However, following research gaps in SBC domain are bottleneck for implementing it for WSN. Thesis motivation associated with each research gap is also discussed.

The PLS techniques available for SBC demands the prior knowledge or intelligence for eavesdroppers presence identification and detection. For resource-constraint, SBC based WSN it is impossible to perform this task. On other hand, for the application scenario of inaccessible monitoring it is difficult to deploy conventional WSN node to perform the task for eavesdropper detection. Further, the unawareness of eavesdroppers' presence or misdetection of legitimate node as eavesdropper may hamper security or reliability respectively for the network. Overall, eavesdropping is the biggest threat for SBC based WSN as specified by Mudasar et al. [45].

Shiu et al. [56] have mentioned that SS based PLS inherently does not require the awareness of eavesdropper and its implementation is not dependent upon the channel state information. However, WSN physical layer uses MaSS and considering the underrated research scenario in the domain of MaSS, it motivates to extensively explore the MaSS, design a power-friendly security scheme for SBC and eliminate the eavesdropping threat associated with SBC.

In the domain of backscatter communication, there are three major challenges associated with in-band interference mitigation, compatibility with conventional wireless communication and data rate -energy tradeoff. Based on Table 1-2, elimination of in-band inference through frequency shifting technique becomes bottleneck for data rate while usage of extra hardware at receiver site for interference mitigation violates the compatibility. In addition, the energy demand for SBC will be greater than unsecured backscatter communication; thus, the data energy tradeoff may result in undesired reduction in secure communication data rate. Therefore, energy harvesting and data rate is the inherent constraint linked with BT or SBC, based on the strategy used for other challenges either one will be affected as specified by Ma et al. [103].

Even though the research domain of BT appears to be saturated, the above-mentioned tradeoff is a pressing issue. A hybrid backscatter modulation technique need to be investigated which incorporates the high data rate advantages of phase delay tree [49] based backscatter modulation and also eliminates the in-band interference by using frequency shift technique [51]. In addition, the developed design should exhibit compatibility with conventional WSN without subsequent power overhead.

SBC tag is inherently wireless powered device. However, considering the battery limitations in the domain of healthcare and nuclear sector and poor RF to DC conversion efficiency [107], the far-field network sustenance cannot be guaranteed.

The basic element for RF based wireless power generation scheme is rectenna; in the work of solar power satellite system [82], [108], [109], rectenna panel is used to generate electricity from high power microwave transmitted from space. This high power microwave signal has adverse biological effects [110]. However, discarding the aspect of high power microwave transfer, the rectenna panel concept need to be explored for designing an efficient rectenna panel for maximum utilization of non-ionizing radiations emitted within standard defined limits. Considering the research scenario in the domain of rectenna panel design [85], [86], [87], the work is specific to antenna selected for their application. Also, the authors of artifacts [86], [87] have not performed comparative performance analysis for their developed rectenna panel with different rectenna arrangement patterns. Thus, for real world applications associated with inaccessible zones of nuclear sector, a concrete investigation is required to design an optimized rectenna panel. The motivation is to develop a unified/ standard approach for designing a rectenna panel

1.5 OBJECTIVES

The aim of this work is to conceptualize the vision of sustainable secure wireless monitoring system by advancing the current state of SBC to the point that they can go beyond conventional wireless monitoring and provide long-lived uninterrupted continuous monitoring. Looking forward, RF-powered backscatter devices have the potential to reach any corner of application area and they provide flexibility to network manager to control their data transmission rate. This dissertation targets indoor environments where powered RF infrastructure is feasible, and aims to achieve following three objectives:

1) To explore the attributes of M-ary SS (MaSS) for PLS implementation, to design, develop obfuscated M-ary SS for WSN using software defined radio and carry out eavesdropping analysis to quantify its security strength .
2) To design and develop WSN transceiver using BT with hybrid approach, such that it leverages the data energy tradeoff, mitigates the in-band interference, and maintains the compatibility with conventional WSN nodes.
3) To investigate and optimize rectenna panel design parameters, to design a panel that have maximum panel utilization factor with least number of rectennas. Based on the knowledge gained, to develop and test a rectenna panel with SBC tag.

1.6 THESIS STRUCTURE

This thesis is structured into five chapters; contents of each Chapter are summarized below.

The **Chapter 2** discusses the significance of spread spectrum obfuscation for wireless sensor network through mathematical analysis and simulation based analysis.

Further, to implement the same for physical layer of wireless sensor network, it discusses about software defined radio based physical layer block development. It also provides the details on various security schemes. Based on the experimental analysis, in this Chapter a novel mapping obfuscation technique involving zero security overhead will be proposed and tested.

The **Chapter 3** aims to design an ultra-low power transmitter for wireless sensor node. For minimizing the node power demands, it explores backscatter technology and complexity involved in implementing the same for WSN. With detailed discussion on backscatter tag design and experiments, the chapter ends by highlighting attributes of the developed tag.

The **Chapter 4** explores RF power generation and presents a detailed methodology for rectenna panel design. It gives a detailed account of theoretical base developed for maximum utilization of incoming RF power by designing a rectenna panel with minimum number of rectennas arranged in an optimum pattern. Further, the proposed rectenna panel design will be fabricated and validated by performing integrated testing with the developed secured backscatter based WSN node.

The **Chapter 5** summarizes the research work carried out for sustainable secure wireless monitoring system design. The conclusions derived from this study are briefly outlined in this Chapter. Further, the scope for future works in this field is also highlighted.

CHAPTER 2

Design of Novel Physical Layer Security for Wireless Sensor Network

This chapter discusses the significance of spread spectrum obfuscation for Wireless Sensor Network through mathematical analysis and simulation-based analysis. It emphasizes that for ad-hoc and resource-constrained networks, it is difficult to detect/ localize eavesdropper. To combat this issue, it proposes a novel spread spectrum obfuscation technique involving zero overhead for security implementation. To implement the proposed security scheme, it discusses software defined radio based physical layer block development and provides the details on various security schemes. Further, the implemented security scheme has been experimentally evaluated.

2.1 Framework for Spread Spectrum based Physical Layer Security

WSN node PHY follows the IEEE 802.15.4 standard[35]. The main blocks of the PHY RF signal generation chain are spreading, pulse shaping, and modulation, as shown in Figure 2-1.

As shown in Figure 2-1, to the PHY payload (PSDU), the PHY header (PHR) and the synchronization header (SHR) are concatenated. The PHY payload is received from the medium access layer (MAC) and the payload length is part of PHR. Synchronization header (SHR) consisting of preamble and start of frame delimiter (SFD), they are required for receiver to establish frame synchronization and to identify the beginning of the frame respectively. Followed by this, M-ary Spread Spectrum

(MaSS) block spreads the bit stream by the gain of eight using pseudo-noise (PN) signal. The binary output of spreading block is fed to the modulator block after subjecting it to the pulse-shaping filter. The filter modifies the shape of binary pulses, which is required to limit the bandwidth of modulated signal.

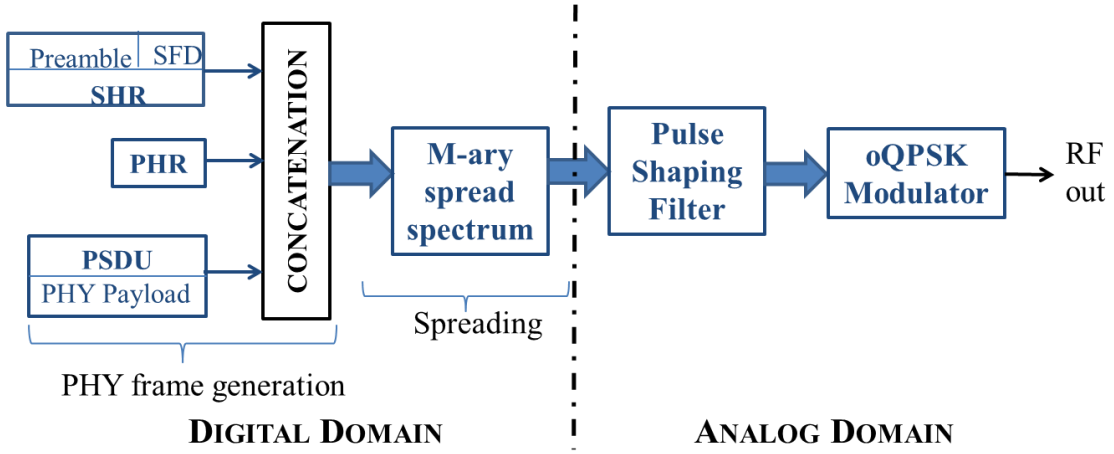

Figure 2-1: Block diagram of the WSN PHY transmitter chain

To implement SS based PLS, the obfuscation is performed before feeding the signal to the analog domain; hence, the binary signal of the PHY is obfuscated in the digital domain of PHY.

2.1.1 M-ary Spread Spectrum (MaSS)

The 2.4GHz band of IEEE 802.15.4 standard [35] uses MaSS with offset quadrature phase shift keying(oQPSK) modulation. The SS technology used for MaSS is direct sequence spread spectrum (DSSS). MaSS for 2.4GHz band provides spreading gain of eight by mapping a low-rate (250 kb/s) symbol of 4-bit size with a higher-rate (2 Mchip/s) chip-sequence of 32 chips (bits). Thus, 16-ary (M is 16) quasi-orthogonal sequences are required for DSSS implementation.

As shown in Table 2-1, all the WSN nodes implement DSSS by the usage of common chipping sequences with fixed symbol mapping. By using this publically

available spreading sequence set, an adversary can de-spread data by referring to the mapping table. The implementation technique of MaSS indicates that it has the potential to provide security at the digital domain of the physical layer by obfuscating its chipping (spreading) sequence or obfuscating the symbol to chipping sequence mapping.

Table 2-1: Symbol to chip mapping for 16-ary DSSS of IEEE 802.15.4 standard

Data symbol (decimal)	Data symbol (binary) ($b_0b_1b_2b_3$)	Chip values (c0 c1 ….. c30 c31)
0	0000	11011001110000110101001000101110
1	1000	11101101100111000011010100100010
2	0100	00101110110110011100001101010010
3	1100	00100010111011011001110000110101
4	0010	01010010000101110110110011100011
5	1010	00110101001000101110110110011100
6	0110	11000011010100100010111011011001
7	1110	10011100001101010010001011101101
8	0001	10001100100101100000011101111011
9	1001	10111000110010010110000001110111
10	0101	01111011100011001001011000000111
11	1101	01110111101110001100100101100000
12	0011	00000111011110111000110010010110
13	1011	01100000011101111011100011001001
14	0111	10010110000001110111101110001100
15	1111	11001001011000000111011110111000

2.1.2 The Mathematical Formulation for M-ary Spread Spectrum

Based on the IEEE 802.15.4 standard[35] PHY layer definition, the mathematical formulation for MaSS is as follows:

Let say *D* is concatenated signal fed to M-ary DSSS block of Figure 2-1 is represented by equation (2-1).

$$D = \{b_1, b_2, b_3, \dots\dots\dots\ b_{n-3}, b_{n-2}, b_{n-1}, b_n\} \quad (2\text{-}1)$$

where,

n : *Number of data bits*

b_i : *The data bit, it is 0/1 as per signal,* $0 \leq i \leq n$

For M-ary DSSS, before spreading a bit to symbol conversion is required. M is 16 for WSN, so, 16 different values of symbols can exist. Hence, each symbol size is 4 bit. Equation (2 2) represents the symbol sequence *S*. Mapping of symbol elements of S to its corresponding 32-bit chipping sequence in Table 2-1 generates the M-ary DSSS signal, *DS* shown in equation (2 3).

$$S = \{s_1, s_2, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, s_r\} \quad (2\text{-}2)$$

$$DS = \{c_1, c_2, c_{32}, , \ldots\ldots\ldots\ldots\ldots\ \ldots\ldots\ldots\ldots, c_x\} \quad (2\text{-}3)$$

where,

r : $n/4$ *(n need to be multiple of 4, if not- then zeros are concatenated in D)*

s_j : *The equivalent decimal representation of 4 consecutive data bits,* $0 \leq j \leq r$ *has 16 possible values, and for each value, an associated 32-bit PN spreading/chipping sequence exists.*

c_k : *chip bit 1/ 0*

$c_1 - c_{32}$: *The 32-bit sequence corresponding to the symbol* s_1*. There are 16 different 32-bit PN sequences. 64-byte storage is needed for spreading sequence block.*

x : $8 \times n$

If spreading signal *DS* is generated by using a secret spreading sequence set or secret mapping or combination of both, and then, the *DS* can be referred to as obfuscated spread spectrum signal. This scenario of generating obfuscated M-ary DSSS signal would be referred to as ***Case-1*** in this thesis.

16-ary MaSS provides a spreading gain of eight to the 4-bit size symbol of IEEE 802.15.4. 1-ary DSSS (M is 1) or simple DSSS with the single 8-bit spreading sequence can also provide a spreading gain of eight if symbol size is 1-bit. This

scenario of 1-ary DSSS would be referred to as ***Case-2*** hereafter throughout this thesis. Currently, the 2.4GHz band of IEEE 802.15.4 standard does not support ***Case-2***. This scenario will be analysed in obfuscation study to quantify the strength and weaknesses of MaSS based obfuscation. Analogous to ***Case-1***, the mathematical redefinitions for ***Case-2*** are shown by following equations.

$$Since, \quad b_i = s_j \ \& \ r = n$$

$$\therefore D = S = \{s_1, s_2, \dots\dots\dots\dots\dots\dots\dots\dots, s_r\} \tag{2-4}$$

$$DS = \{c_1, c_2, c_{32}, , \dots\dots\dots\dots\dots \ \dots\dots\dots, c_x\} \tag{2-5}$$

Where,

$c_1 - c_8$: *8-bit chipping sequence symbol with a bit value of '1'. If symbol value is '0' then, the complement of* $c_1 - c_8$ *is used.*

x : $8 \times n$

2.2 PRELIMINARY ANALYSIS FOR MASS OBFUSCATION

The general principle, followed by the receiver or eavesdropper is to demodulate the RF signal, de-spread it by correlation method and search for preamble. For successful synchronization, an attacker should possess or retrieve the spreading and preamble sequence used by the transmitter. As shown in Figure 2-1, preamble and SFD are part of SHR, embedded at the start of RF frame to ease the legitimate receiver's synchronization process. If one amongst the two; spreading/ preamble sequence is unknown, it will create an extensive delay in synchronization. When both are unknown, synchronization will become much more difficult for the eavesdropper. Thus, the parameters available for implementation of spread spectrum obfuscation (SSO) for MaSS are spreading sequence obfuscation (SSeO), sequence to symbol mapping obfuscation (MO), and preamble obfuscation (PO). MO is valid only for M-ary SS, i.e for ***Case-1***.

For SSeO and PO, the maximum obfuscation key size is limited to 32 bit, while for MO it is hybrid key. The MO key is referred as hybrid because it is not a single bit stream key; it requires a sequence/ data structure, with 16 elements. Each element is of 4bits size. In comparison to AES-128 bit cryptography it is trivial that security available with theses obfuscation key length is not significant.

Even though the number of brute force operations would be less for obfuscated MaSS, the time available for online eavesdropping is limited by the wireless signal data/ symbol rate. Here, online eavesdropping is referred to real-time eavesdropping. Unlike, higher layer cryptography offline key extraction is a cumbersome task for PLS. For the former case, as physical layer headers are unencrypted it is easy for an attacker to identify the beginning and end of packet. Therefore, attacker can estimate the amount of storage required, capture the packets and can perform offline analysis. In PLS, an attacker needs to sample the analog RF signal and store the floating-point data obtained by analog to digital conversion.

In this section, preliminary theoretical analysis has been done to estimate the minimum processing speed required for an attacker to sniff the packets on the fly. The data rate and chipping rate for 2.4GHz band of IEEE 802.15.4 standard are 250kbps and 4Mchips/sec respectively. Considering this data and chipping rate, eavesdropping analysis has been performed for SSeO, MO and PO. The obfuscation analysis has been compared for both ***Case-1*** and ***Case-2*** in Table 2-2.

Table 2-2: Preliminary eavesdropping analysis for various MaSS obfuscation scenarios

Obfuscation Scenario	Case	Number of Correlation required[*1]	The time needed per correlation	Feasibility for online eavesdropping
SSeO	1	$\frac{16^{2L}\,(2^{32})!}{16!\,(2^{32}-16)!}$	<<*fs*	NO
	2	2^{8}	~ *ns*	YES
MO	1	16^{2L}	<*fs*	NO
	2	1	*NR*[*2]	YES
PO	1&2	2^{32}	<*as*	YES
MO +PO	1	$16^{2L}2^{32}$	<*fs*	NO
SSeO+PO	1	$\frac{16^{2\times L}\,2^{32}(2^{32})!}{16!\,(2^{32}-16)!}$	<<*fs*	NO
	2	2^{40}	<*fs*	NO

[*1] *L in this column refers to packet length;* [*2]*NR is not required*

For SSeO obfuscation, ***Case-1***, chipping sequence length is 32-bit and the number of such sequences needs to be identified are 16. The number of combinations an eavesdropper needs to exploit for identifying the 16-ary sequence set used by the sender will be ${}_aC_b$ (here $a = 2^{32}$ and $b = 16$), as mapping is also unknown. Further, the packet length *L* scales the total number of operations by factor of 16^{2L}. For other obfuscation schemes, the total number of operations is implicit based on the obfuscated parameter size. The minimum time required for processing each operation has been approximated based on new bit /symbol arrival rate, which is at every 1µs/ 16µs respectively.

PHY level analysis/ processing demands for software-defined radio (SDR) architecture. Various SDR based IEEE 802.1.5.4 and OFDM implementations discusses that delay in PHY synchronization results in packet loss [111]–[114]. In addition, SDR are field programmable gate array based device, based on the clock speed available, it

is not feasible to perform a correlation operation in the femtosecond scale. [115] Therefore, the remark on feasibility for online sniffing of obfuscated MaSS signal has been made based on minimum correlation time anticipated and processing speed feasible with SDR.

The inferences drawn from Table 2-2 are listed below:

1. Compared to ***Case-1, Case-2*** 1-ary DSSS or normal DSSS is not a suitable technology for the implementation of SSO. Hence, SSO can be incorporated with any wireless technology supporting M-ary DSSS.
2. PO coupled with MO and SSeO reduces the online sniffing probability of an attacker and among all obfuscation approaches, SSeO prohibits packet sniffing.
3. The time required for mapping identification, Total Mapping time in Seconds (TMS) scales-up with increase in packet length and mapping operations. For ***Case-1***, TMS plot for MO, MO+PO and SSeO schemes is shown in Figure 2-2, Figure 2-3, and Figure 2-4 respectively. Comparison has been done with assumption that an attacker is able to perform mapping operations per second (MPS) at the speed of EMPS (Exa, 10^{18}MPS), ZMPS (Zetta, 10^{21} MPS) and YMPS (Yotta, 10^{24} MPS). This evaluation reveals that for MO (Figure 2-2), short length packets (<10byte) are vulnerable to eavesdropping. While, for MO+ PO (Figure 2-3), packets of size, less than 6Bytes can be sniffed in seconds. Thus, link-layer acknowledgment packets can be captured easily. In the case of SSeO (Figure 2-4), sniffing of acknowledgment packets with YMPS speed take 10^{128} s.
4. Based on the Figure 2-2,Figure 2-3,Figure 2-4 the time estimated for eavesdropper to fetch different length packets has been tabulated in . Also, based on the number of keys required for legitimate node, the remark on key complexity has been made.

Table 2-3: Time estimation for eavesdropping with remark on key complexity for different SSO techniques

SSO Type	TNMT for eavesdropper	Eavesdropping time estimation, TMS for different packet size for YMPS speed (s)			No of security keys for legitimate node	Remark on key complexity
		128B	10B	5B		
MO	$16^{2\times L}$	$>10^{300}$	10^{0}	10^{-12}	1	Low
MO +PO	$2^{32} \times 16^{2\times L}$	$>10^{300}$	10^{10}	10^{-3}	1+1	Low+
MO + SSeO	$\frac{(2^{32})! \times 16^{2\times L}}{16! \times (2^{32}-16)!}$	$>>10^{300}$	10^{140}	10^{128}	1+16	Very High

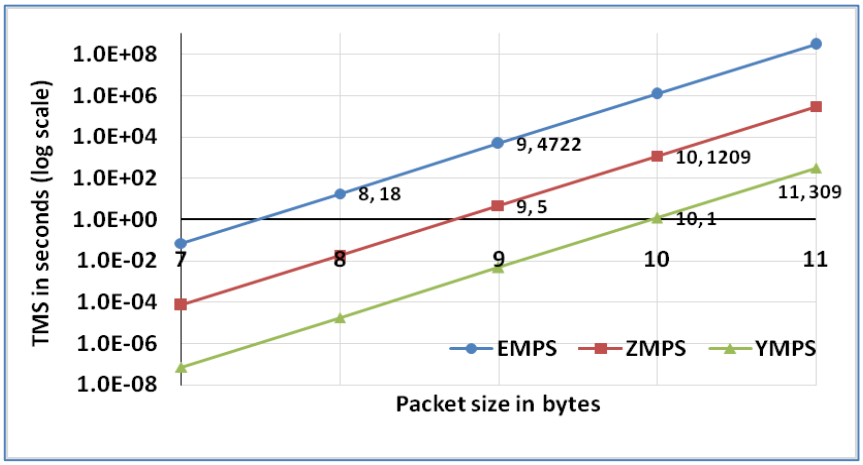

Figure 2-2: Time required for mapping identification for standalone MO, TMS for different packet length. It is feasible to decode mapping for 8 byte, 9 byte and 10 byte packet length for EMPS, ZMPS and YMPS respectively in18s, 5s and 1s.

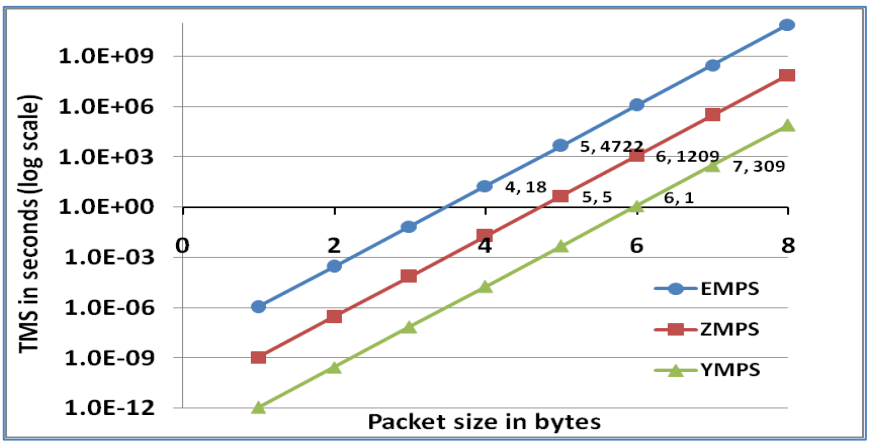

Figure 2-3: Time required for mapping identification for MO+PO, TMS for different packet length. It is feasible to decode mapping for 4 byte, 5 byte and 6 byte packet length for EMPS, ZMPS and YMPS respectively in18s, 5s and 1s.

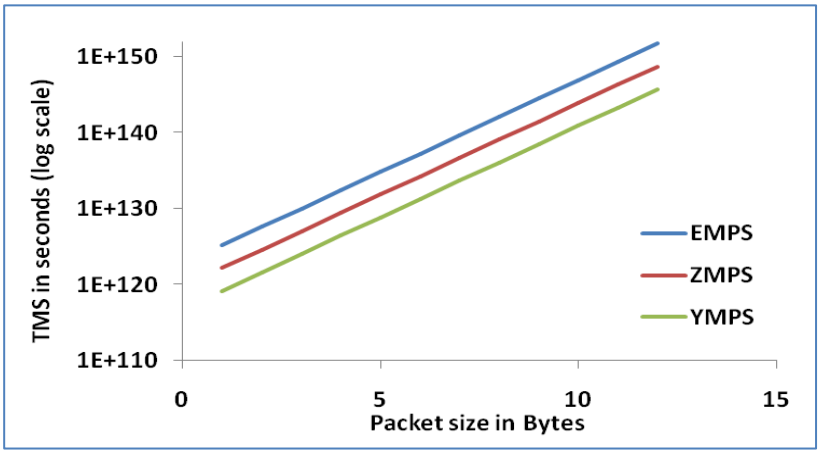

Figure 2-4: Time required for mapping identification for MO+SSeO, TMS for different packet length. It is not feasible to decode mapping for any length packet in few second; the decoding time for a 5 byte packet with EMPS, ZMPS and YMPS processing speed is in the order $>10^{125}$ *s.*

2.3 SIMULATION FOR MASS OBFUSCATION

Simulation based analysis was performed for MaSS obfuscation, to validate the preliminary analysis, and to calculate the time required for correct mapping sequence identification by exhaustive search. The analysis begins with implementation of MO based MaSS scheme and decoding of it by an attacker model.

For simulation, 10-byte random PHY payload was generated. As defined in IEEE 802.15.4 standard, 2.4GHz band of WSN uses CRC-16 polynomial; hence, to the generated random data, frame check sequence (FCS) generated through the cyclic redundancy check (CRC) algorithm was appended. For the generated PHY payload, PHY symbols were generated after adding SHR. Further, 16-ary DSSS was performed using the IEEE 802.15.4 spreading sequences. The symbol to sequence mapping combination was secret, i.e. different from the existing standard defined mapping. The generated spreading bits were oQPSK modulated and forwarded to the attacker model after noise addition.

During the simulation, the SNR of the RF signal fed to the attacker was also a variable parameter. The role of attacker is to demodulate and decode the symbol

mapping by an exhaustive search. For analysis purpose, the secret mapping sequence used for data spreading was also an argument to the attacker model. For every iteration of mapping sequence, the attacker has to perform de-spreading and has to regenerate FCS using CRC algorithm after identifying preamble with SFD. If the incoming packet FCS matches with the FCS generated by attacker's CRC generator block than FCS detection flag is set. Along with FCS check, the attacker has to check for the similarity of its de-spreading mapping sequence and the actual mapping sequence.

2.3.1 Attacker Model

The attacker model was developed to perform exhaustive search for correct packet detection from the obfuscated binary stream. The success probability of the attack for varying signal to noise ratio (SNR) was measured based on FCS detection. The eavesdropping algorithm for attacker model is shown in **Algorithm 2-1**.

Algorithm 2-1: Eavesdropping Algorithm

```
Demodulate the received signal
WHILE preamble not detected
   Sweep across binary stream for preamble search with spreading
   sequence search
   IF preamble found THEN check for SFD
       IF SFD found THEN
          SFD detected flag set
          BREAK WHILE  loop
        ELSE continue the preamble search
       END IF
   ELSE
        continue the preamble search
   END IF
END WHILE
WHILE  FCS not detected
   Partition the signal into chip sequence length
   Select a 16-ary chipping sequence set for de-spreading
   De-spreading of binary stream
   CRC generation and FCS check
   IF FCS detected THEN
       Calculate chip and bit error
   ELSE
```

```
21:      Continue frame decoding with different mapping /16-ary
         set.(based on obfuscation scenario)
22:      END IF
23:   END WHILE
24:   END of Algorithm 2-1
```

2.3.2 Observations and Inferences drawn

Observations and modifications made in the attacker model with inferences obtained during eavesdropping algorithm simulation are as follows:

1. Even though the mapping sequence match was not detected, the iterative loop terminated due to FCS detection. Thus, the detected FCS was false detection. Hence, to quantify the number of false detection in the iterative search, the attacker model was modified to count the number of false detections.
2. For 10-byte data payload, Figure 2-5 displays the number of false FCS count observed for varying SNR.

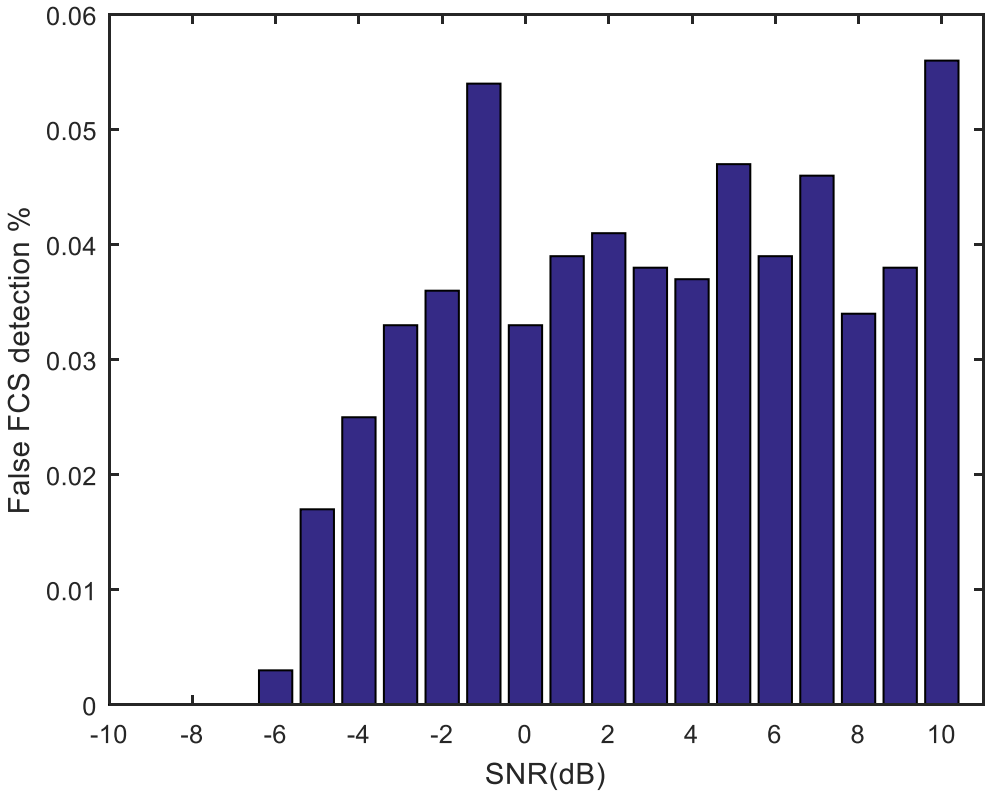

Figure 2-5: Attacker's false FCS detection percentage for 10-byte data payload

3. The inference drawn Figure 2-5 is that the wrong mapping combination for de-spreading of data has generated the FCS detection flag. The FCS for IEEE 802.15.4 frames is generated using 16-bit cyclic redundancy check (CRC) algorithm, this CRC algorithm is meant for bit error detection and not for symbol error detection. Thus, shuffled symbols are likely to result in the same FCS. The fluctuations in the wrong FCS count for varying SNR convey that it is a random phenomenon delinked with SNR. The corrupted packets due to low SNR can also pass the attacker's local FCS check.
4. To test the security strength, attacker model was upgraded to perform simultaneous mapping search for two random RF packets. The aim was to reduce the false FCS count for the attacker.
5. With dual packet analysis, attacker's false FCS detection percentage drops down drastically by order of 100, as shown in Figure 2-6.

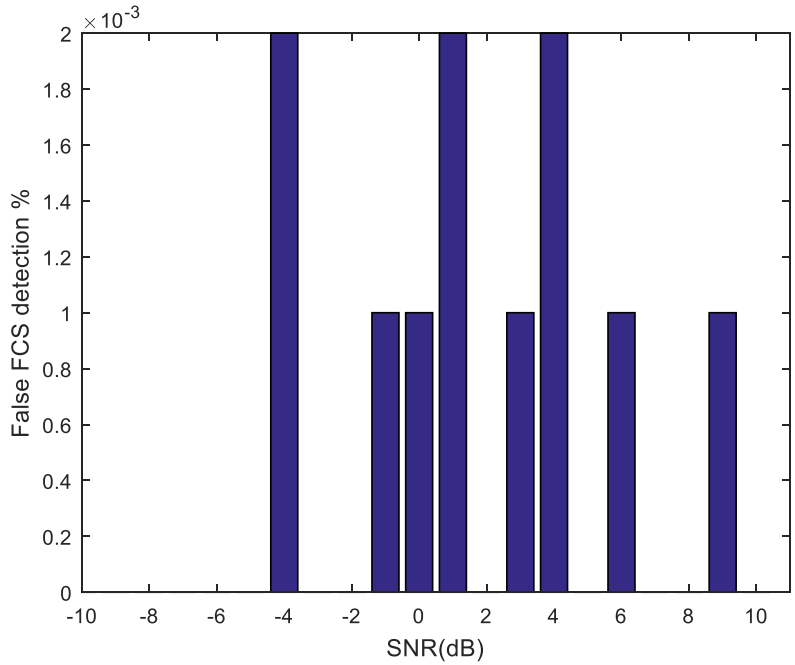

Figure 2-6: Attacker's false FCS detection percentage for two packets of 10-byte data payload

6. From Figure 2-6, it can be inferred that for an incorrect mapping sequence, symbol shuffling in two random packets reduces the probability of false FCS detection. If the attacker performs analysis for multiple packets then the probability of false FCS detection will lead to zero. Therefore, multiple packet analysis at eavesdropper site may pose security threat for mapping obfuscation scheme. However, false FCS count has reduced but attacker was not able to detect the valid FCS, i.e. iterative search is not complete, as valid mapping was not detected. In addition, valid packet detection is high dependent on signal SNR.
7. To identify attacker's SNR requirement for valid packet detection, attacker model was subjected to perform a limited mapping sequence search with ten mapping sequences. Among these ten, one mapping combination was corresponding to source mapping combination. Attacker model was configured to set the correct FCS flag for case when it detects FCS match with mapping key match.
8. The observations were made after executing attacker model 1000 times for each SNR value. As per Figure 2-7, the attacker’s valid packet detection for 60-byte payload starts from SNR of -1dB with a detection percentage of 1.4% only.
9. Observations for correct FCS detection percentage for varying length data payload is shown in Figure 2-8.

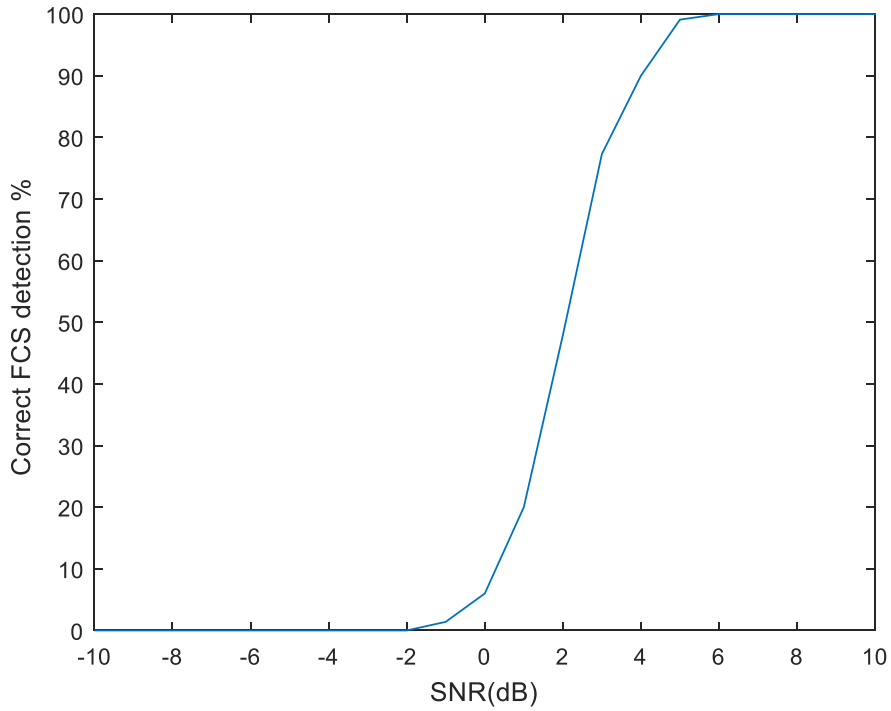

Figure 2-7: Correct FCS detection percentage for varying SNR for 60-byte packet payload.

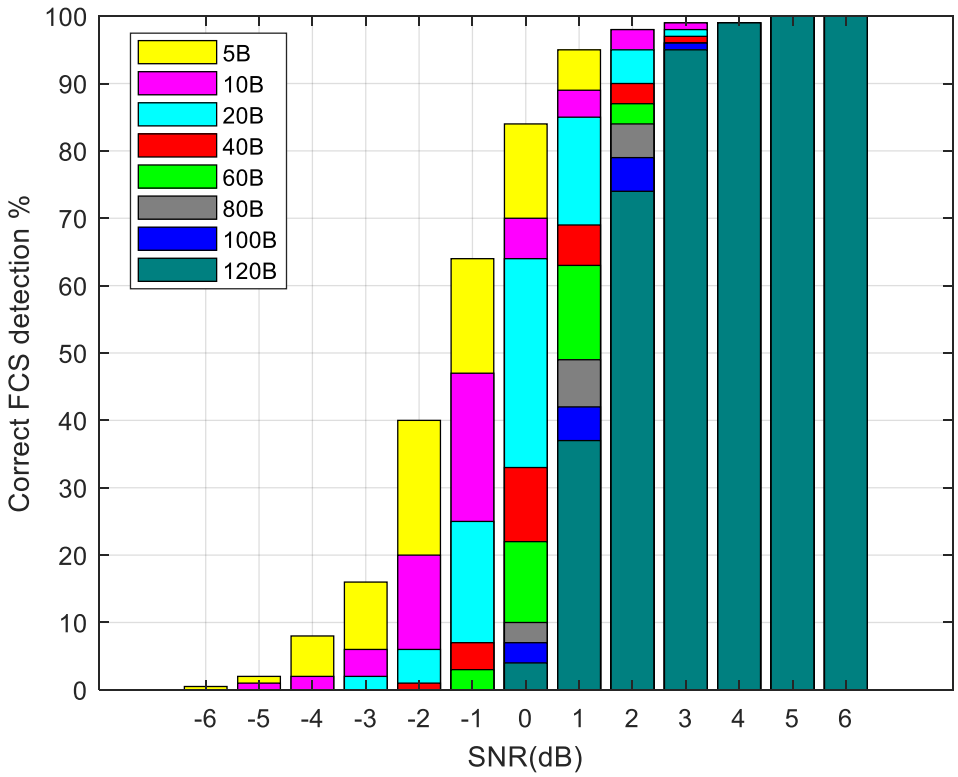

Figure 2-8: Correct FCS detection percentage for varying SNR for different size of the packet payload.

10. From Figure 2-8, it can be inferred that the SNR requirement for eavesdropper increases with increase of packet payload length. Detection of short length packets of size 5-byte, 10-byte and 20-byte begins at SNR of -5dB, -3dB and -2dB respectively. However, the detection probability is lower than 10%. Except for 5-byte payload packet, success rate for other packets is less than 50% upto -1dB SNR.
11. All the simulations have been carried on 24-core workstation by parallel processing. The computation time for the number of iteration performed has been tabulated in Table 2-4. Overall, exhaustive search for mapping detection and correct FCS detection demands for clusters. Also, computation time scales with packet payload size. Even though, multiple packet analysis at attacker site, reduces its false FCS count but increases computational complexity as shown in Table 2-4.

Table 2-4: Simulation time for various MO scenarios

Simulation Scenario	**Packet payload size (Bytes)**	**No of iterations per SNR**	**Computation time per SNR**	**Time required for exhaustive search**
Mapping search with 1 RF packet	10	1 crore	0.5 hr	13days
	60	1 lakh	0.5hr	>3y, Not Performed
Mapping search with 2 RF packets	10	1 crore	1hr	1 month
	60	1 lakh	1hr	>>3yr, Not Performed
Correct FCS detection with 10 mapping combination	Varying payload length	1000 per payload length	2.06sec	Not performed with exhaustive search

Based on the preliminary analysis shown in Figure 2-2, it was observed that MO is vulnerable to short length packets. However, based on simulation analysis, it can be envisaged that the ambiguity created by MO (Figure 2-5) increases computational time

complexity (Table 2-4) of the attacker for short length packets also. Proceeding towards the validation of preliminary analysis with simulation results, it can be observed from Table 2-5, computation time for preliminary and limited search simulation is comparable. As FCS check is not accounted in preliminary analysis, results are not matching with exhaustive MO sequence search detection. Nevertheless, the obscurity attribute inherited by MO based MaSS, makes it a computationally friendly PHY security solution for resource-constrained wireless devices. Thus, MO based novel PHY security scheme proposed by the MaSS simulation will be experimentally evaluated by hardware implementation in the following section.

Table 2-5: Computation time comparison for preliminary and simulation results for MO based MaSS

Analysis approach	**Computation time for MO based MaSS (secs)**
Preliminary (formula based)	1
Simulation (limited search)	2.06
Simulation(exhaustive)	1800

2.4 SECURITY IMPLEMENTATION AT PHY

WSN standard IEEE 802.15.4 inherently does not support any security at its PHY layer. Thus to embed security at its PHY, the secure IEEE 802.15.4 need to be designed and developed. The various SSO technique explored in the previous section are the obfuscated version of conventional MaSS used in IEEE 802.15.4 PHY. Thus, this section begins with the new features of secure PHY and further provides details on various obfuscation schemes integrated with conventional PHY.

2.4.1 New features of Secured IEEE 802.15.4 PHY

Following features need to be incorporated in IEEE 802.15.4 PHY to implement SSO based security:

1. Configurable spreading sequence size (in bits) and spreading sequences without violating standard pre-defined spreading factor.
2. Configurable symbol based on spreading factor and spreading sequence size.
3. Dynamic spreading sequence to symbol mapping, currently in PHY fixed mapping is being used.
4. Configurable preamble sequence with feature to dynamically modify it based on network scenarios.
5. PHY security enable/ disable.
6. SSeO, PO and MO enable/ disable.
7. Options to implement various obfuscation schemes at PHY, i.e. application specific security scheme implementation
8. Display of parameters required for PHY testing such as chip error threshold measurement, RSSI, and number of times valid preamble & SFD detected.
9. Transmission of RF frames with variable power.

2.4.2 Novel Block Design for WSN Physical Layer

Simulation based eavesdropping analysis carried out in the previous section, demands a dynamic re-configurable M-ary DSSS block for WSN PHY. For conventional WSN PHY except channel no and power other parameters are fixed, not accessible to user. However, to integrate MaSS obfuscation with PHY, this work for the first time in literature proposes and develops a dynamically reconfigurable spread spectrum block for IEEE802.15.4 PHY. This block should have above mentioned

unique features to provide the security attributes to standard PHY, as per the application demands.

PHY novel block has been designed using GNU radio [116] to test it using software defined radio (SDR) kit. GNU radio interface is open source software development kit for SDR. It is user friendly and has a block type interface which give better understanding of the system. Each block code is written in C++. Developed blocks are connected to each other using python script. GNU Radio also has a graphical tool, GNU Radio Companion (GRC). GRC has been used to design flow diagram for a WSN transceiver.

Transceiver flow diagram with the secured PHY block is shown in Figure 2-9; this block functioning is based on **Algorithm 2-2**. Using this any of the following schemes can be implemented for software defined WSN.

Scheme 1. Different chipping sequence per node (SSeO)

Scheme 2. Different preamble per node (PO)

Scheme 3. Different mapping logic per node (MO)

Scheme 4. Different chipping sequence and preamble sequence per node (SSeO+PO)

Scheme 5. Different preamble sequence and mapping logic per node(MO+PO)

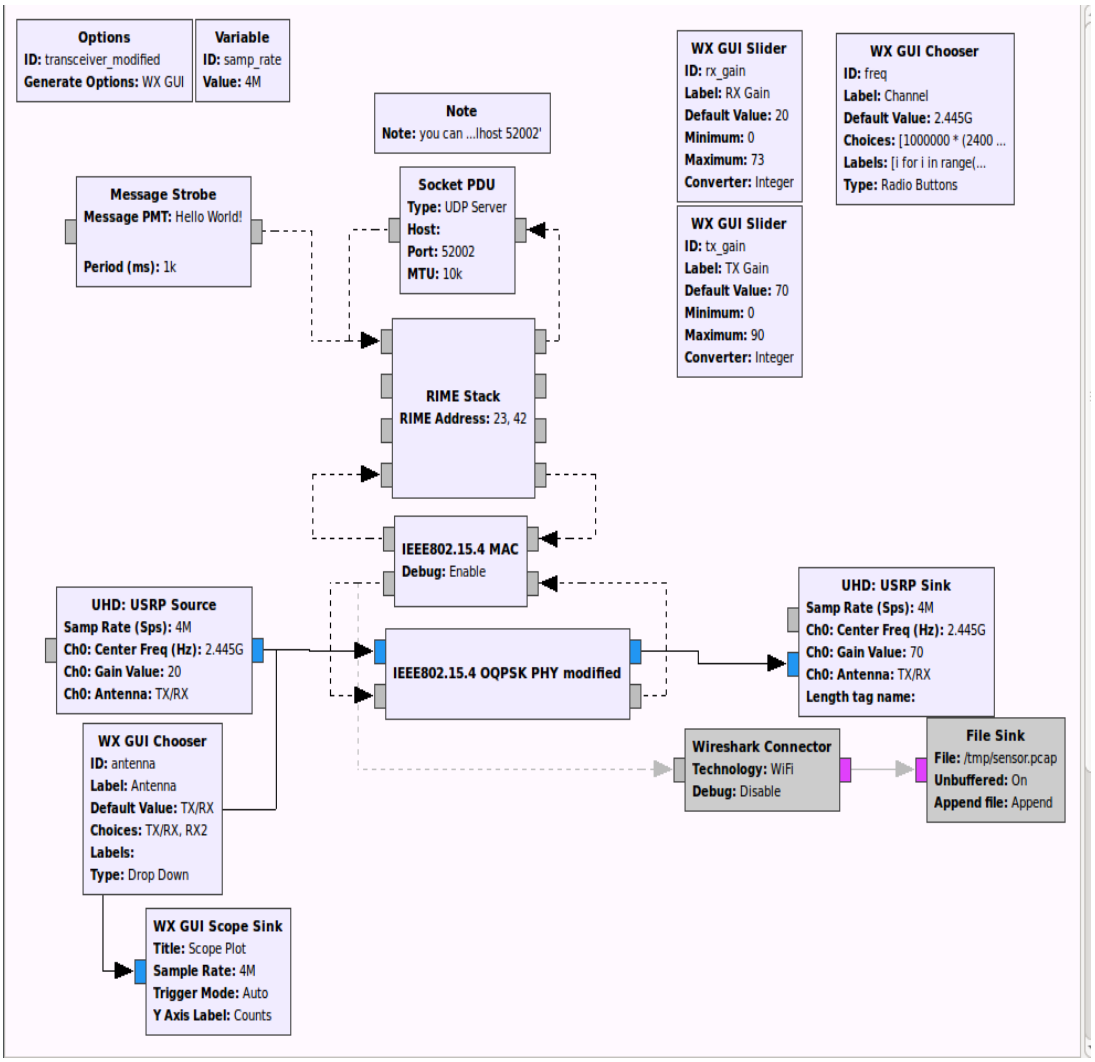

Figure 2-9: Transceiver Flow Diagram developed using GRC

Algorithm 2-2: Spread Spectrum Obfuscation

INPUT:

Spread spectrum Obfuscation enable & disable, SSO_E

Define scheme type, Schemetype; %Type of SSO based security scheme

Chipping Sequence bit length, CS_{Nbits}; %Spreading sequence length

Chipping Sequence; %Includes spreading sequences set: CS_{N32B}(existing chipping sequence set) , CS_{SSeO8_i}, CS_{SSeO32_i}, CS_{MO_i}, CS_{SSeMO_i}

Preamble sequence; %Includes Preamble sequences: PS_N (existing preamble), PS_{PO_i} Here, i =0 is for common key & i>0 represent node id

MPDU; %MAC layer Protocol Data Unit. It is payload for PHY

Data frame flag, D_f; % For DATA frame, destination specific key is used for frame transmission

Configured Transmit power level, P_t;

Received signal power level, P_r;

Minimum receiver detectable power, P_{rc};

Receiver power threshold for data frame, P_{rd};

Chit error threshold, CET;
Self-Node ID, $Node_{SELF}$;
Destination ID, $Node_{DEST}$;

OUTPUT:

Frame Transmission to Modulator block;

Packet Delivery Ratio, PDR;

Start of Frame delimiter detection time, SFDtime;

Preamble detection/ synchronization time, Psynctime;

Captured frame log;

```
1:  PROCEDURE TRANSMIT(MPDU,SSO_E,Schemetype,Df) %MAC frame bits are
    PHY payload & Df is flag for Data frame
2:  CALL[CS,PS]=OBFUSCATION_SEQUENCE(SSOE,Schemetype,Df,CSNbits,NodeDEST);
    %Based on security scheme, returns destination node obfuscation
    sequence
3:  Create PPDU (PHY protocol data unit by adding SFD and PS),
    D (equation (2-1) )
4:  Bit to symbol conversion, S (equation (2-2))
5:  Perform DSSS and generate signal DS  (equation (2-3))
6:  Perform Modulation
7:  IF (Df == TRUE) THEN
8:     Pt ← Pt −2dBm
9:  END IF
10: Transmit frame at power, Pt
11: END PROCEDURE
```

```
1:  PROCEDURE RECEIVE(Prd,Prc, SSOE,Schemetype, RFbits)
2:  Measure incoming signal power, Pr
3:  IF Prd > Pr > Prc THEN
4:       Df = TRUE; %Data Frame
5:  ELSE
6:       Df = FALSE; %Broadcast Frame
7:  END IF
8:  CALL[CS,PS]= OBFUSCATION_SEQUENCE(SSOE,Schemetype,Df,CSNbits,NODESELF);
9:  Perform preamble sync and despreading with PS and CS
    LOG Psynctime if preamble detected
    LOG SFDtime if SFD detected
    LOG FRAME
    MONITOR PDR
10: END PROCEDURE
```

```
1:  PROCEDURE[CS,PS]=OBFUSCATION_SEQUENCE(SSOE,Schemetype,Df,CSNbits,NODE_ID)
```

```
    %Returns the Chipping sequence, CS; Preamble Sequence, PS
2:      IF (SSO_E == TRUE) THEN %Check if SSO is enabled
3:          IF (Df == TRUE) THEN
4:              SWITCH(Schemetype, CSNbits, NODE_ID )
5:                  %Based on the case, destination or self (NODE_ID)
    chipping sequence and preamble sequence loaded in CS and PS
6:              END SWITCH
7:          ELSE %Common key used for network management packets
8:              SWITCH(Schemetype, CSNbits,0)
9:  %Based on the case, broadcast chipping sequence and preamble
    sequence loaded in CS and PS
10:             END SWITCH
11:         END IF
12:     ELSE %Existing WSN scenario
13:             CS← CSN32B
14:             PS← PSN
15:     END IF
16: END procedure
17: End of Algorithm  2-2
```

Feature to transmit the frames with variable power is also added to PHY [117], [118]. This variable power technique is used to distinguish between broadcast and unicast frames.

2.4.3 Experiment Methodology

For detailed testing and analysis, the following parameters from the modified PHY layer are variables, available for user configuration:

1. Chipping/ spreading sequence bit size
2. Spreading sequence for node
3. Spreading sequence for broadcast & unicast mode
4. Preamble sequence
5. PHY security enable disable
6. Chip Error Threshold (CET)

7. Type of scheme being implemented

CET is the parameter required during de-spreading. If the bit wise cross-correlation of the incoming bits to spreading sequence is less than or equal to CET, then de-spreading would be performed with the selected sequence.

2.4.3.1 Experimental setup

For testing the developed PLS, USRP, B210 kit [117], [118] was used. It is USB based wide band operating SDR. The kit was programmed using GNU radio. For the experimentation, two preprogrammed SDR kit were connected separately to two different systems placed at 2m distance from each other, Figure 2-10. All experiments were conducted in lab environment, without any other known wireless communication in the test channel.

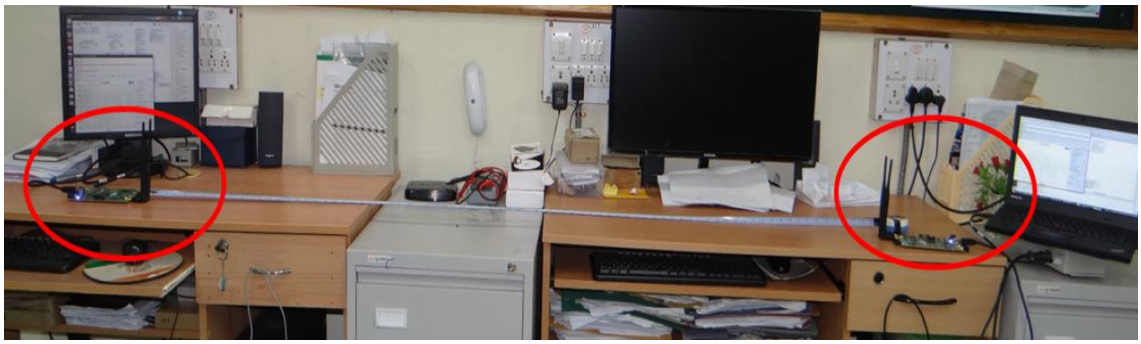

Figure 2-10 : Experiment setup, used for testing the developed PLS

2.4.3.2 Experiment procedure

For obfuscation scheme testing, receiver is always kept ON in sync search mode. During this mode, receiver will continuously hunt for the defined preamble by using the defined spreading sequence. If both are undefined or unknown as may be the case for eavesdropper, it has to perform brute force search. Suitable notifications for sync search, chip errors, and packet delivery were logged in a text file.

For MO, initially the obfuscation was explored by Index Alteration (IA) of symbol to chipping sequence mapping for existing IEEE 802.15.4 PHY. In the IA technique, only the starting index of symbol to chipping sequence mapping arrangement is secret for different nodes but the sequence order is same. For example, IEEE 802.15.4 uses 16 numbers of 32-bit chipping sequences, as shown in Table 2-1 symbol '0x0' is mapped to chipping sequence "0xD9C3522E" and so on symbol "0x7" corresponds to " 0x9C3522ED". Now as per IA technique, if one more node shares the same chipping sequence set then for it, symbol "0x0" can be mapped to sequence "0x9C3522ED". Further, if moving in cyclic order as sequences are maintained, then for this node symbol "0x7" will correspond to "0x96077B8C" which actually corresponds to sequence 14 in the standard mapping list. Hence, IA based MO, MO(IA) have 15 obfuscation possibilities, keeping one setting reserved for broadcast communication.

Unlike other SSO techniques, another approach explored for MO implementation is using random mapping configuration per node. In this Thesis, this MO technique is referred as MO(R). Eavesdropping analysis has been performed for both types of MO techniques.

For experimentation random number generator has been used for generating obfuscation sequences for SSeO, PO, and MO(R). Based on obfuscation technique, appropriate conditioning has been applied for key length and type of key generation. Key management and key sharing has not been covered in this work.

2.4.3.3 Types of experiments

1. **CET Test**: The most important significance of spreading is that it allows extracting the data bits even though some of chipping bits are corrupted. CET test determines the chip error threshold beyond which correct data bit extraction is difficult or

impossible. CET varies based on the spreading sequence set and its size. This test was performed to determine CET for Case-***1*** (16-ary DSSS) and ***Case-2*** (1-ary DSSS). During this test, both the SDRs' are legitimate nodes and they know each other spreading sequences. Transmitter SDR was configured to transmit frame at 1 sec rate for 10 min for one CET setting. Packet delivery ratio (PDR) for each CET was calculated from the logged data at the receiver. Test for one type of case was performed 10 times. Later, Eavesdropping Test (ET) was performed for the range of CET that gives more than 95% PDR.

2. **Eavesdropping Test (ET):** This test was conducted for the PHY security enabled scenarios. In this test, one SDR acts as eavesdropper while the other node sends data at 1 sec interval with one set of spreading and preamble sequence (depending on Scheme) until the configuration settings is altered by the user. During this test, eavesdropper records the time taken for preamble, SFD detection, and logs the received packets. Based on number of correct packets received by the eavesdropper, Eavesdropper Packet Delivery Ratio (EPDR) is calculated.
3. **Receiver Sensitivity Test**: This is performance evaluation test for 16-ary and 1-ary DSSS. Under this test it is evaluated how the DSSS scheme affects the receiver sensitivity. For this test, experimentation has been performed by transmitting fixed frames keeping constant distance between the transmitter and receiver. Received signal strength was made to intentionally drop by continuously reducing the transmit power of RF frame. By mapping the PDR of receiver to the received packet signal strength, comment on receiver sensitivity was drawn.

2.5 EXPERIMENTAL ANALYSIS OF OBFUSCATED MASS

Using the developed secured PHY, various tests were performed for obfuscation analysis of different security scenarios based on SSeO, MO and PO. To perform ET for various SSO scheme, a reference test with security disabled was performed to quantify CET for M-ary DSSS. Further, ET was performed for CET value which results in almost 95% PDR.

2.5.1 Chip Error Threshold Detection Experiment

CET is user configurable parameter and is referred as C_t in the designed secure PHY block; its value can range from minimum one to maximum spreading sequence length. A receiver enters into the *frame reception* mode, only when the correlation threshold, C_{ct} of incoming stream of chips is less than or equal to C_t. C_t was varied across its full range and for each CET setting, PDR was measured.

For ***Case-1*** under ***Scheme-1*** with PHY security disabled, the deigned security block represents existing standard PHY layer scenario. Existing PHY uses 16-ary DSSS; CET for this PHY has been configured to accept value in the range of 1-15. If CET value is set higher than 15, then the receiver is not able to distinguish between noise and the valid signal. PHY for ***Case-2*** under ***Scheme-1*** uses 1-ary DSSS, with one 8-bit spreading sequence. For spreading, data bit '1' is replaced by the spreading sequence and data bit '0' is spread by the 1's compliment of the assigned spreading sequence. The acceptable range for PHY CET value is 1-8.

As part of CET test, PDR observed for ***Case-1*** and ***Case-2*** is shown in Table 2-6. For this analysis, PDR was calculated by generating the FCS from received payload bytes and comparing with frame embedded FCS bytes.

The peculiar thing was observed for ***Case-2***, that even when 4 to 7 chips (spreading bits) are erroneous, PDR >2% was observed. By manual evaluation of the receiver's logged frames it was inferred that even though MAC layer gave FCS detected signal, the logged data bytes were different from the transmitted bytes. The checking was manual as same frame was being transmitted continuously. In comparison to ***Case-1***, the false FCS detection signals were high for ***Case-2***. Owing to resolve this issue, the receiver PDR count logic was modified to check the self-generated FCS with packet embedded FCS and FCS generated at the source. The effect of CET on actual PDR for ***Case-1*** and ***Case-2*** is also shown in Table 2-6 and Figure 2-11.

The grey region of the Table 2-6, highlights the optimum CET value. For ***Case-1*** and ***Case-2*** the value are 8 and 2 respectively. The outlined region of table demonstrates the PDR difference owing to the false FCS detection. Decrease in *actual* PDR% is observed for higher value of CET when RF signal with higher number of corrupted bits /noise is not filtered.

Table 2-6: Effect of CET on PDR of M-ary DSSS

	Case-1, 16-aary DSSS		Case-2, 1-ary DSSS	
CET, C_t (bits)	**PDR %**	***actual* PDR %**	**PDR %**	***actual* PDR %**
15-13	0-1	0	-	-
12	10	9	-	-
11	60	45	-	-
10	90	88	-	-
9	97	97	-	-
8	99	99	0	0
7	95	95	2	0
6	80	80	10	1
5	50	50	15	5
4	30	30	30	13
3	20	20	95	95
2	9	9	98	99
1	1	1	70	50

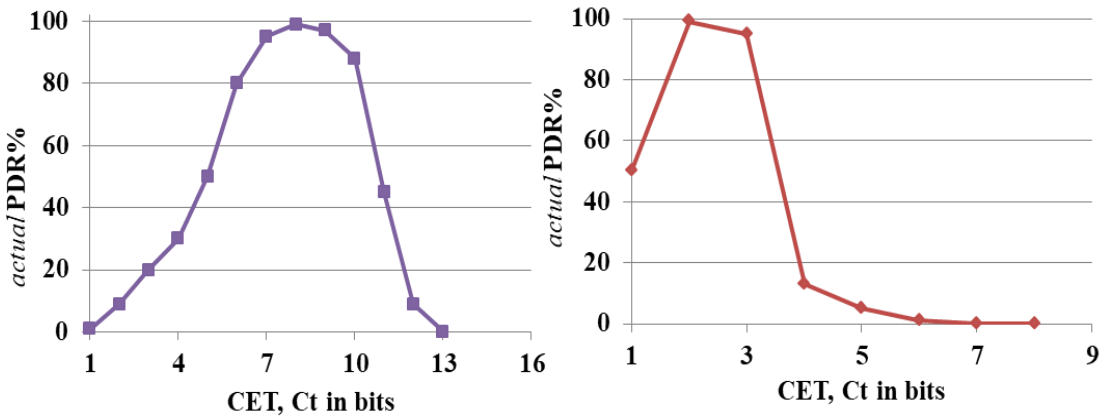

Figure 2-11: CET vs. actual PDR plot for 16-ary (Case-1) and 1-ary (Case-2) DSSS of physical layer

2.5.2 Eavesdropping Analysis

Under this analysis, ET was performed for various obfuscation schemes described in Section 2.5.2. ET experiment was repeated 30 times for one particular PHY security configuration setting. The SDR kit, USRP B210 cannot be used for complete brute force attack for ***Case -1***; thus, for ET a 1000 number of attack keys were generated with one key being the actual key. The eavesdropper packet delivery ratio was measured for every iteration of experiment. Whether false or valid preamble detection, its detection time was recorded for all the schemes. For Scheme-4, frequent false preamble detections were observed, as both spreading sequence and preamble were obfuscated. Owing to the mentioned issue, for Scheme-4 SFD detection time was also monitored. ET was performed to measure both practical PDR and actual PDR. In practical scenario, attacker will be unaware of source generated FCS, so, in such case attacker can measure its EPDR by generating FCS and comparing it with packet embedded FCS. EPDR obtained through this method has been tabulated in Table 2-7 and referred as *practical* EPDR ($EPDR_P$). For SSO security strength analysis, *actual* EPDR ($EPDR_A$) shown in Table 2-8 has also been measured. $EPDR_A$ gives the estimate about the attacker's passive attack success probability.

Based on Table 2-7 and Table 2-8, the inferences drawn for eavesdropping analysis are listed below:

1. Eavesdropping is not feasible for 16-ary based SSeO technique while for 1-ary SSeO it provides a very weak security.
2. Standalone PO technique is not suitable for implementing security at PHY. But, when clubbed with SSeO or MO technique they strengthens the eavesdropping inhibition. 1-ary DSSS can also provide competent PHY security if obfuscated using both SSeO and PO technique.

Table 2-7: Practical EPDR ($EPDR_P$) for various obfuscation scenarios

Obfuscation Scheme		Average preamble detection time (ms)	SFD detection time	$EPDR_P$ (%)				
				Case-1 CET value			Case-2 CET value	
No	Type			7	8	9	2	3
1.	SSeO	3	-	0	0	0	83	75
2.	PO	60	-	10	40	13	38	16
3.	MO (IA)	3	-	-	30	-	NA*	NA*
	MO (R)	3	-	-	5	-	NA*	NA*
4.	SSeO+PO	1	70min	0	0	0	1	0
5.	MO(IA)+PO	3	16min	-	2	-	NA*	NA*
	MO(R)+PO	3	16min	-	0.1	-	NA*	NA*

*NA is Not applicable

Table 2-8: Actual EPDR ($EPDR_A$) for various obfuscation scenarios

Obfuscation Scheme		$EPDR_A$ (%)					Remarks with reference to $EPDR_P$ (%)
		Case-1 CET value			Case-2 CET value		
No	Type	7	8	9	2	3	
1	SSeO	0	0	0	82	76	Not significant
2	PO	10	40	12	38	16	Not significant
3	MO (IA)	-	27	-	NA*	NA	Not significant
	MO (R)	-	0		NA	NA	Significant
4	SSeO+PO	0	0	0	1	0	Not significant
5	MO(IA)+PO	-	2	-	NA	NA	Not significant
	MO(R)+PO	-	0	-	NA	NA	Significant

3. Significant drop in $EPDR_A$ was observed for MO(R) instead of MO(IA). The probability of false FCS detection is more when random mapping is used. IA technique maintain the cyclic order of chipping sequence, thus it does not results in symbol shuffling.

2.5.3 Receiver Sensitivity Test

To practically study the performance of M-ary DSSS, the receiver sensitivity test was conducted by voluntary reducing transmit power for both the cases. As this is DSSS performance test, so PHY security was disabled. Receiver and transmitter were placed at 2m distance. To reduce the RF signal power arriving at receiver, a 30 dB attenuator between transmitter and antenna path was used. Also, transmit power was varied from -20dBm to -10dBm. For each setting, experiment was conducted for 30 minutes. Mean RSSI and PDR observed for each transmit power is displayed in Table 2-9.

Table 2-9: Receiver Sensitivity Measurement Test

Transmit Power (dBm)	**Case 1**		**Case 2**	
	RSSI (dBm)	**PDR %**	**RSSI (dBm)**	**PDR %**
-20	-99	3	-	-
-19	-95	15	-	-
-18	-94	20	-	-
-17	-96	55	-97	1
-16	-93	80	-95	5
-15	-93	95	-96	12
-14	-90	97	-94	20
-13	-91	98	-92	40
-12	-88	98	-89	77
-11	-85	99	-85	90
-10	-80	99	-83	98
-9	-81	99	-82	99
-8	-76	99	-80	99

In IEEE 802.15.4, receiver sensitivity is defined for 1%BER. Here, at coarse level we have considered PDR. From Table 2-9 highlighted region, for ***Case-1*** 99% PDR is observed for -85dBm while for ***Case-2*** it is around -82dBm. Thus, approximately receiver sensitivity for USRP based SDR kits for 16-ary DSSS and 1-ary DSSS is -85dBm and -82dBm respectively. The sensitivity varies based on the receiver noise figure, so for any other receivers these values may not match. Overall, it can be concluded that 16-ary DSSS has 3dB better reception range than 1-ary DSSS.

2.6 SUITABILITY OF DEVELOPED PHY SECURITY FOR LEGITIMATE NODES

2.6.1 Complexity Analysis

The resources required for an algorithm implementation and execution, verbalizes about its complexity. Memory, processing speed and power are the main bottleneck for resource-constrained devices.

The standard WSN node requires memory of 64bytes for spreading sequences, 16 bytes for mapping logic and 4 bytes for preamble sequence storage. The memory, requirement at PHY for all the obfuscation schemes has been compared with standard WSN node (PHY security not implemented) in Table 2-10. PHY secured WSN node requires extra memory for storage of obfuscation keys of its neighboring nodes. The increase in memory demand is in bytes and it scales with increase in number of network neighbors, N.

Table 2-10: Comparison of memory requirement for 16-ary obfuscation

Obfuscation Scheme	Memory required (Bytes)
No obfuscation, Standard WSN node	84
SSeO	$80 \times N + 4$
PO	$64 + 4 \times N$
MO	$64 + 16 \times N$
MO +PO	$64 + 20 \times N$
SSeO +PO	$84 \times N$

As the proposed obfuscation scheme does not involve any computation overhead for legitimate nodes, the power overhead for its implementation can be assumed zero. Based on the key generation technique used for obfuscation, power or processing overheads need to be investigated. It is inevitable that key generation and management complexity will be high for SSeO technique.

2.6.2 SNR and Secure Information Carrying Capacity Tradeoff Analysis

The proposed MO technique obfuscates the complete PHY frame, including its synchronization and preamble header. In comparison to conventional WSN frame, the only difference is that the symbol to chipping sequence mapping is shuffled. From the eavesdropping analysis shown in Figure 2-5 and Figure 2-6, it is inevitable that MO based misleading for eavesdropper is SNR independent. In addition, it conveys that chip error rate is not affected by MO. Thus, it is implicit that the MO technique will not result in extra chip error rate for a legitimate receiver. Hence, the legitimate nodes need not enhance the signal SNR to implement MO based PLS technique. Overall, the proposed PLS technique waives off the SNR and secure information carrying capacity tradeoff.

2.6.3 Security Analysis

As mentioned previously for PLS, the complexity involved in eavesdropping indirectly verbalizes about the level of security achieved. Based on simulation and experimental obfuscation analysis, it is impossible to retrieve valid frame in real time if SSeO based obfuscation is implemented.

Even though, as preliminary analysis MO appears to be vulnerable for short length packets, the FCS check reveals that the single RF packet analysis for obfuscation key detection may provide misleading results. For single packet analysis, false FCS detection probability is approximately 30 times more than the correct FCS detection probability. With the increase in the number of RF packets used for obfuscation analysis, though false FCS detection probability decreases, the computation time for eavesdropper scales up by order of the number of packets used for analysis. Correspondingly, with experimental testing it has been verified that for MO(R), *actual* EPDR for attacker is zero. Thus, usage of different mapping obfuscation keys for consecutive data packets at the cost of 16×K bytes of extra memory can mitigate the mapping key detection threat for MO technique.

Memory requirement can be reduced to half for MO technique, if compression of key elements is performed. Owing to WSN M-ary symbol size, each element of MO data structure key requires only 4-bits; thus, every byte can provide value for two elements. Considering this aspect, even though the key length required for MO scheme is not 128bit long, it has specific (mapping) characteristic to mislead the attacker by false packet detection.

Comparison of MO with existing SSO based PLS techniques are shown in Table 2-11. Complexity of the SSO techniques has been assessed in terms of coding and key complexity. Based on this comparative evaluation, the MO based PLS does not involve

any implementation complexity; it does not degrade the WSN throughput (successful number of bits transmitted per sec-bps) and allows confidential data transmission.

Table 2-11: Comparison of proposed PLS technique, MO with existing SSO based PLS techniques

Security Scheme	**Secure[*1] network throughput**	**Complexity**		**Achieved security requirement**
		Coding	**Key**	
Secret Spreading Sequence [71]	250kbps ideally	×	√	Confidentiality
WDSSS [72]	<1kbps	√	×	Authenticity
Steganography [73]	125kbps ideally	√	√	Confidentiality/ Authenticity
MO (proposed)	250kbps ideally	×	×	Confidentiality

[*1] It is the throughput for the secure data being transmitted.

As shown in Table 2-12, comparison of MO with higher layer security implementation in low power WSN devices has also been performed.

Table 2-12: Comparison of MO based SSO physical layer security with higher layer security implementation

	Legitimate WSN node		**Eavesdropper**	
	Extra power requirement	**Extra Memory and processing**	**Power Requirement**	**Memory and processing requirement**
Higher Layer (AES or non AES)	50-70%, Security implementation requires additional $3-5mA$ current [54].	YES	HIGH	**HIGH**. High memory & processing is needed to store packets and to perform cryptanalysis
MO based SSO (proposed)	0%, as it is part of existing DSSS technique	NO	VERY HIGH	**VERY HIGH,** Memory is required in order of GB's for offline processing, as without correct spreading sequence packet beginning cannot be identified. High processing speed is required to process more number of operations in milli-seconds.

It is comprehensible by Table 2-12 that the proposed MO based SSO implementation increases complexity for an attacker/ eavesdropper instead of an authorized WSN node. Hence, for resource-constrained WSN nodes, it is a potential security technique. MO based PLS scheme neither involves power overhead for its implementation nor it degrades the network throughput as observed for existing SS based PLS schemes.

2.7 SUMMARY

In this Chapter, physical layer security for WSN has been explored. Based on preliminary and simulation-based investigations spread spectrum obfuscation has been proposed. The proposed obfuscation scheme has been implemented at the physical layer of WSN. Eavesdropping analysis to access its suitability for resource constrained WSN has been performed. The important observations of this Chapter are enumerated below:

1) Obfuscation of MaSS to design a PLS technique can be done by obfuscating its spreading sequences or mapping logic and it does not involve power or hardware overhead as it is part of RF signal generation chain.

2) The analysis performed in this Chapter reveals that the easy detection scenario is not true for M-ary SS, based on Table 2-4 for MO based MaSS the valid packet detection takes 13 days' time. In literature, the SS based PLS has been overlooked due to the easy detection probability associated with 1-ary SS.

3) To integrate MaSS obfuscation with IEEE802.15.4 PHY, this work proposes the concept of dynamically reconfigurable DSSS block. Based on network requirements, this block allows to configure spread spectrum parameters for PHY security implementation.

4) The ambiguity created by MO based MaSS can be envisaged from both simulation and experimental evaluation. This ambiguity attribute is peculiarity for MO that makes it an outstanding PLS scheme. MO technique proposed in this work, not only increases the time complexity for eavesdropper but also misleads the eavesdropper to interpret the invalid frame as valid frame. Above all, WSN network integrated with MO based PLS will have same network throughput as achievable for unsecure WSN network and same time it is power budget friendly for resource-constrained WSN devices.

CHAPTER 3

Backscatter based Transmitter Design for Wireless Sensor Network

Backscatter signaling uses incoming RF signal to transmit the data; thus, they eliminates the need of RF signal generation for wireless communication establishment. To design a sustainable secure wireless monitoring system, for long-lived inaccessible zone monitoring, this Chapter targets at the technology growth limiting lacuna of backscatter technology, power- data rate tradeoff. With detailed discussion on backscatter tag design, development and experiments, the Chapter presents a novel quad phase shift keying based backscatter modulator. The compatibility of the developed backscatter modulator with conventional WSN devises has also been evaluated.

3.1 CHALLENGE ASSOCIATED WITH DESIGNING A BACKSCATTER BASED TRANSMITTER FOR WSN

The challenge associated with designing a backscatter technology (BT) based transmitter for WSN is linked with its modulation technique and BT tradeoff associated with data rate and harvested energy [102]. WSN, 2.4GHz band of IEEE 802.15.4 standard demands offset quadrature phase shift keying (oQPSK) modulation technique. The first challenge is associated with implementation of backscatter-based oQPSK; this requires 4-state phase switching as shown Figure 3-1, instead of 2-state amplitude switching followed for radio frequency identification (RFID) devices. Maximum throughput supported by IEEE 802.15.4 is 250kbps, but practically achievable is

<150kbps (for conventional WSN) [119]–[122]. Further, the power splitting shown in Figure 3-1, for energy harvesting and communication should not result in degradation of throughput. Hence, second challenge is associated with degradation of backscatter network throughput. Overall, complexity involved with the implementation of higher-order modulation schemes for BT and power-data rate trade-off has limited the integration of backscatter technology with existing wireless sensor technology.

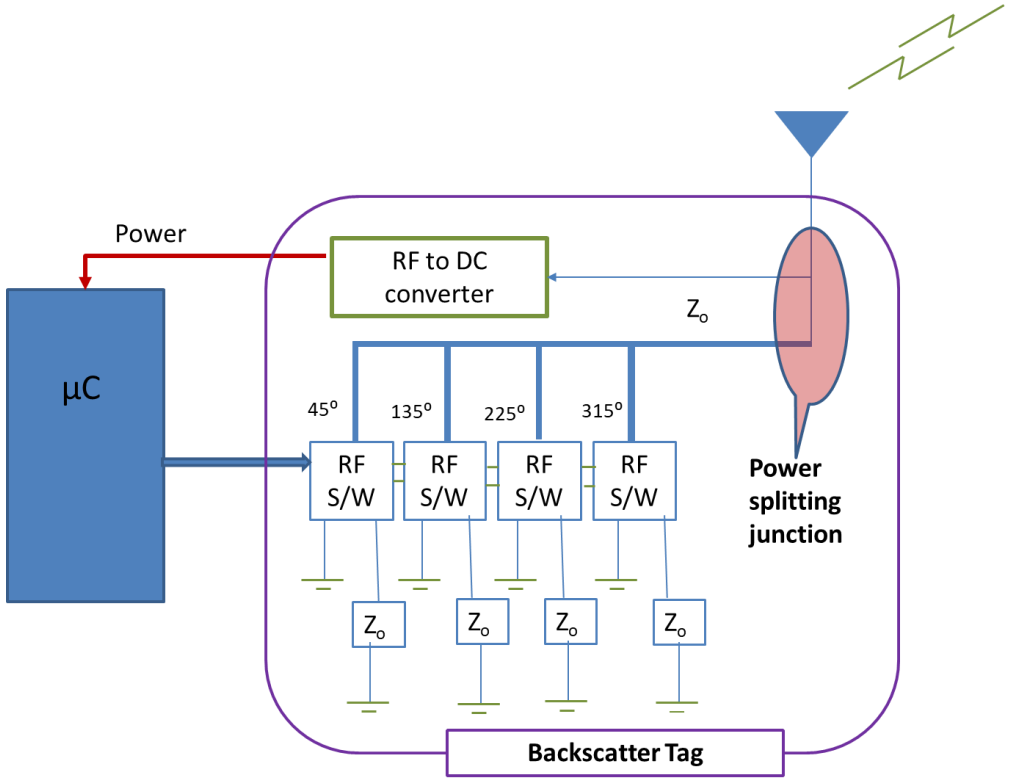

Figure 3-1: Block diagram of backscatter based WSN node

3.2 Backscatter Tag Design and Development for WSN

For QPSK based backscatter signalling, reflection coefficient's magnitude Γ_m should be same and only phase, Φ_i should be altered as shown in equation (3-1). It is required to reflect back the RF signal with different phase delay based on data bits.

$$\Gamma_i = |\Gamma_m| \angle \Phi_i \tag{3-1}$$

The technique explored for designing backscatter tag for WSN is the hybrid BT (HBT) technology, HBT is combination of phase-delay tree and time –varying switching based backscatter techniques.

Phase delay tree based backscatter: This technique uses phase delay tree Figure 1-5, for modulating the phase of incoming RF signal. For backscatter QPSK implementation three RF switch are required. These switches are controlled by digital Q (quadrature-phase) lines and I (in-phase). Based on I & Q bit combination, the respective RF switch reflects back the signal

Phase-varying switching: This technique eliminates the need of multiple-state (>2) switching BM. It implements QPSK with two-state BM by modulating the phase of control signal required for RF switch state change. Governing the QPSK scheme and based on baseband signal's symbol value, the phase delay is introduced in the control signal of BM switch. This phase modulation of RF switch control signal demands time varying signal. So, to implement this technique, square wave signal, is used to control the state of RF signal reflection switch. The equation (3-2)-(3-6), shows that the square wave switching signal modulates the incoming RF signal and generates backscattered RF signal which is reflected by RF switch.

$$F_s(t) = \frac{4}{\pi}\sum_{k=1}^{\infty}\frac{\sin(2\pi(2k-1)ft)}{2k-1} \tag{3-2}$$

$$C_s(t) = \frac{4}{\pi}\sum_{k=1}^{\infty}\frac{\sin\left(2\pi(2k-1)ft + (2s_q(t)+1)\,\pi/4\right)}{2k-1} \tag{3-3}$$

$$RF_{in}(t) = \sin\left(2\pi f_{rf}t\right) \tag{3-4}$$

$$RF_{BS}(t) = RF_{in}(t)C_s(t) \tag{3-5}$$

$$RF_{BS}(t) = \frac{4}{\pi}\sum_{k=1}^{\infty}\frac{\sin\left(2\pi\left(f_{rf} + (2k-1)f\right)t + (2s_q(t)+1)\,\pi/4\right)}{2k-1} \quad (3\text{-}6)$$

Where,

$\boldsymbol{F_s(t)}$: *The square wave signal with frequency* $\boldsymbol{f}$

$\boldsymbol{C_s(t)}$: *The phase modulated control signal*

$\boldsymbol{s_q(t)}$: *The QPSK symbol value = 0,1,2,3*

$\boldsymbol{RF_{in}(t)}$: *Incoming RF signal with frequency* $\boldsymbol{f_{rf}}$

$\boldsymbol{RF_{BS}(t)}$: *The backscattered RF signal*

As shown in equation (3-6) the backscattered signal is radiated in different frequency channel with respect to incoming RF signal. This frequency translation eliminates the self-interference issue of backscatter communication.

In HBT, phase delay tree has been used for precise phase modulation while square wave control signal is used for self-interference mitigation. Phase modulated square wave control signal has not been used to implement phase modulation, as control signal frequency will limit the communication data rate. Thus, HBT has advantages of both techniques, (i) it mitigates the self-interference (ii) does not limit the communication data rate due to modulation implementation strategy.

3.2.1 Tag Design and Development

For phase delay tree design, branch length need to be optimized depending on the required phase delay. The commercial electromagnetic software, ANSYS EM suites' high frequency structure simulator (HFSS) module has been used to optimize the branch length. Branch length has been calculated and optimized for all the four angles of QPSK modulation. Two variant of backscatter tag has been designed; one based on

the phase tree model discussed in literature [49] (Figure 1-5) and the other based on the design proposed in this work, single branch phase tree model.

Initially the phase delay tree shown in Figure 1-5 is explored for tag design. Considering antenna characteristic impedance of 50Ω , a two level phase delay tree has been designed. Based on WSN operating frequency, 2.45GHz (center frequency of 2.4GHz ISM band) tree branch length, L is calculated using the equation (3-7).

$$\Phi = \beta L \tag{3-7}$$

where,

Φ : *Round trip path delay introduced in reflected RF signal with respect to incoming RF signal*

L : *Path length in m*

β : $2\pi/\lambda_{rf} = 2\pi f_{rf}/c$ *phase constant,* f_{rf} *is RF signal frequency*

For desired phase angle, length of 50Ω microstrip track was calculated and modeled in HFSS (refer Figure 3-2). Simulation is performed for short-circuited microstrip track. In simulation, phase of S_{11} parameter was optimized by parameterization of track length and width. Optimization goal was to achieve the required phase difference in incoming and reflected signal. Calculated track lengths with simulated phase angle for implementing QPSK through BT, are tabulated in Table 3-1. Figure 3-3 displays the simulation results for phase angle 135°.

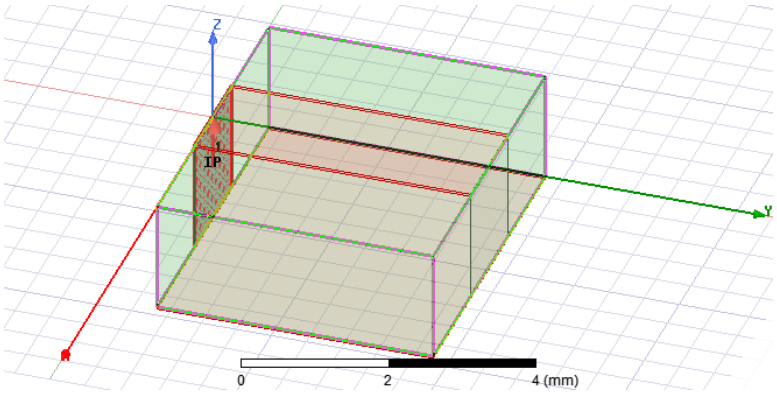

Figure 3-2: For phase delay tree branch length optimization, short circuit microstrip transmission line modeled in HFSS. One end of the track is an input port and other end is short-circuited to ground.

Table 3-1: Track length of short-circuited microstrip transmission line to implement QPSK through BT

Track length for 2.45GHz signal		**Required round trip phase difference (deg)**	**S_{11} phase angle (deg)**
Calculated	**Optimized (mm)**		
$\lambda/32$	3.9	135°	130°
$3\lambda/32$	11.6	45°	50°
$5\lambda/32$	19.5	-45°	-47°
$7\lambda/32$	27.2	-135°	-130°

Figure 3-3: S11 parameter for track length corresponding to phase angle 135 ° .

3.2.1.1 Design- 1: Standard phase tree model based design

This design is based on the phase delay tree diagram shown in Figure 1-5. The schematic of the tag design-1 is shown in Figure 3-4. The circuit consist of two main components namely, (i) a triple inverter gate IC, SN74LVC3G04DCUR for generating complement of I and Q signal, and (ii) three RF-switch IC, AS214-92.

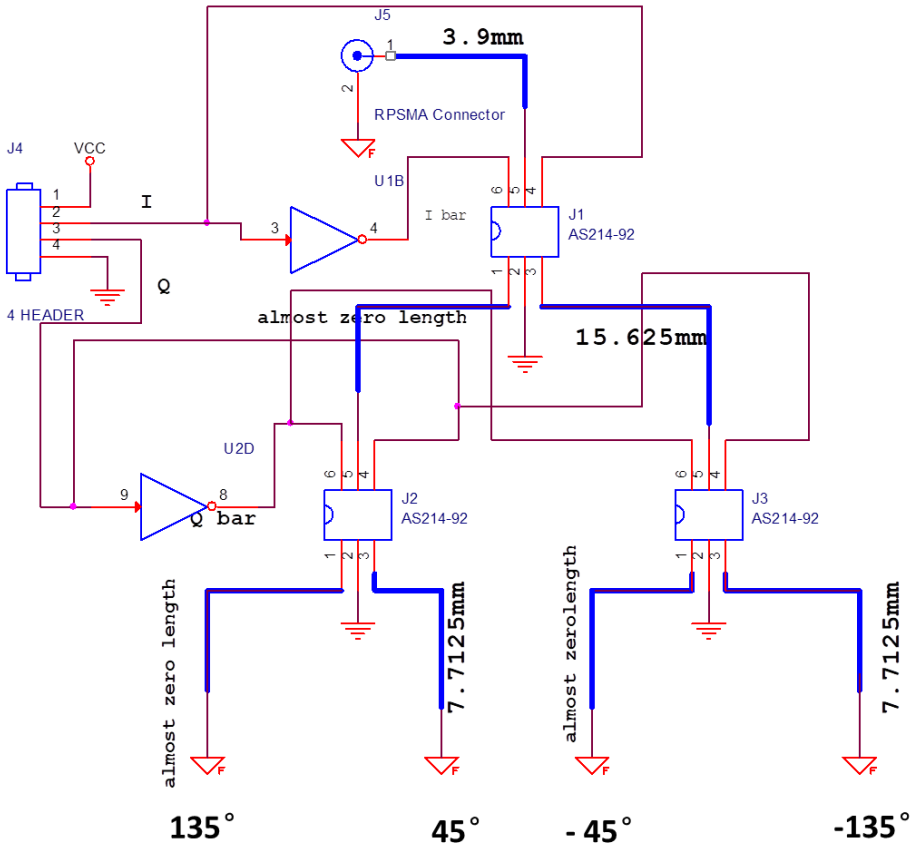

Figure 3-4: Design-1: Schematic with split branch phase delay tree

In schematic, Figure 3-4 the highlighted blue tracks are microstrip tracks, their length is obtained from Table 3-1, The incoming RF signal from antenna connector, J5 flows through the particular microstrip track based on the RF-switch activated by the I and Q lines originating from 4-pin header, J4. At the end of microstrip branch, ground port is connected and the signal reaching to this point gets reflected back on seeing a short circuit. Through embedded programming, control signal for I and Q lines is

generated based on PHY bits value. The tag developed based on Figure 3-4 design, is shown in Figure 3-5.

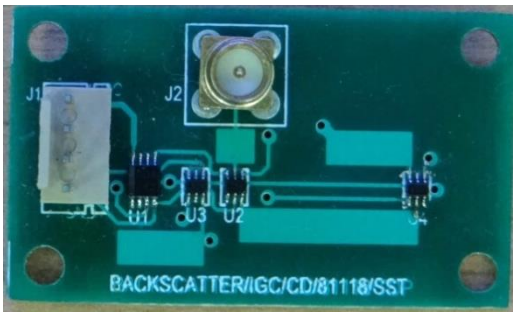

Figure 3-5: Developed WSN backscatter tag from Design-1

3.2.1.2 Design- 2: Single branch phase tree model based design

In this design, all the four branches of QPSK phase delay has been concatenated to form a single branch phase delay tree. Before venturing into fabrication, the single branch phase tree model was simulated in HFSS. The HFSS model of single microstrip QPSK phase delay tree is shown in Figure 3-6. The RF s/w port positions were identified by using a single short-circuited RF s/w on a $>\lambda$ length microstrip track. The S_{11} parameter' phase angle observed by varying the RF s/w position is shown in Figure 3-7.

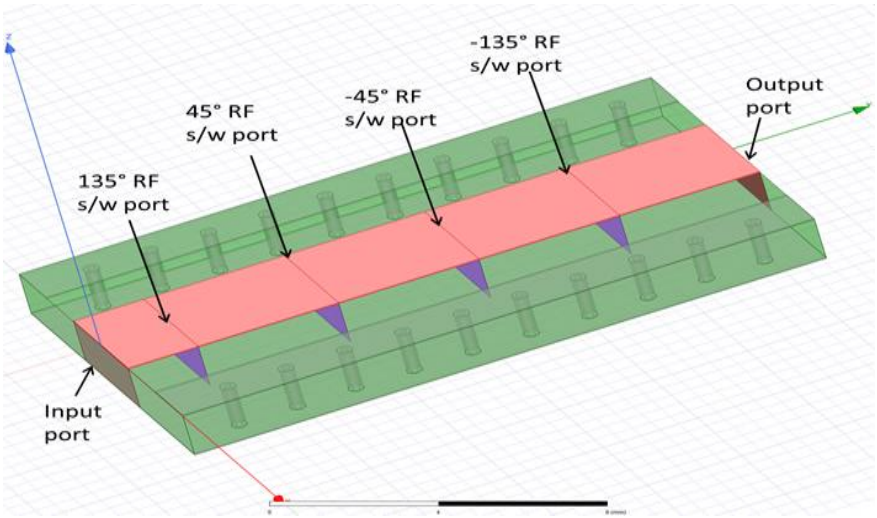

Figure 3-6: HFSS model of single microstrip ,QPSK phase delay tree

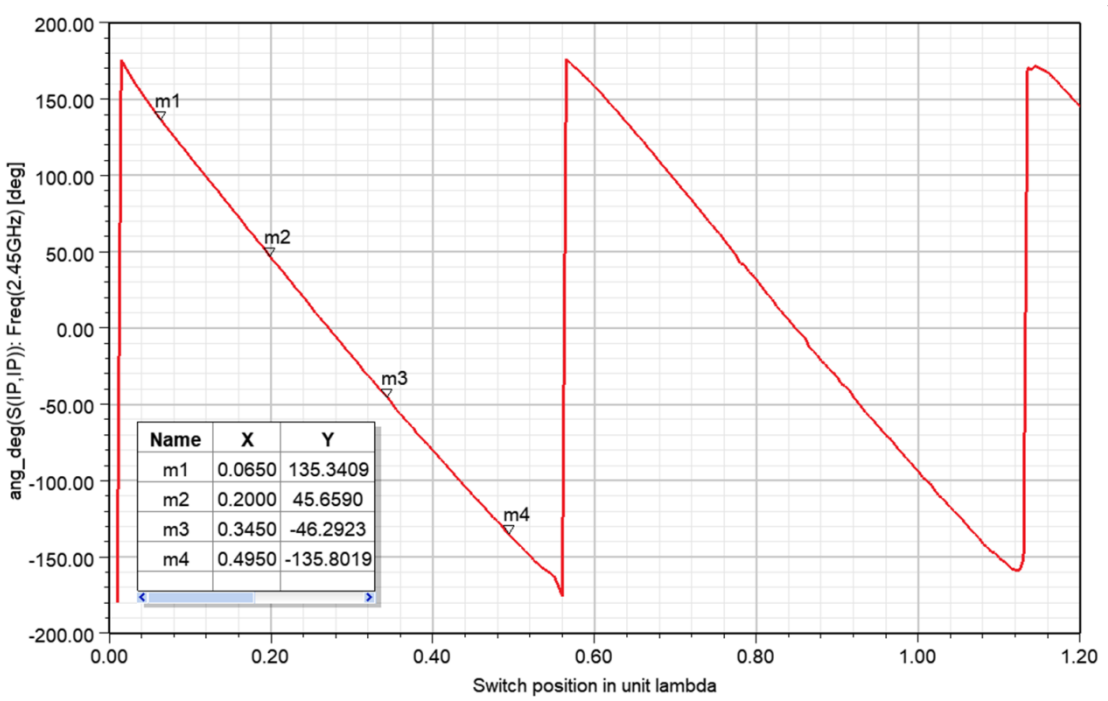

Figure 3-7: Phase angle for S_{11} for varying RF switch position

For phase-delay tree simulation, RF switch (s/w) ports in Figure 3-6, corresponding to different phase angles were switched to ground one at a time; hence, the short-circuit load floats across the transmission line. The phase observed for S_{11} parameter during simulation is tabulated in **Error! Not a valid bookmark self-reference.** and depicted in . In this model when RF s/w port is unused, it acts as OPEN and allows uninterrupted movement of RF signal through it.

Table 3-2: Phase observed for S_{11} of single microstrip QPSK phase delay tree

RF s/w Port Status				Required round trip phase difference (deg)	Observed S_{11} phase angle (deg)
135˚	45˚	-45˚	135˚		
SHORT	OPEN	OPEN	OPEN	135°	135.5°
OPEN	SHORT	OPEN	OPEN	45°	44°
OPEN	OPEN	SHORT	OPEN	-45°	-43°
OPEN	OPEN	OPEN	SHORT	-135°	-137°

The schematic of Design-1, shown in Figure 3-4 was modified to design tag with single microstrip track. The Design-2 schematic is shown in Figure 3-8. The dissimilarity observed with Design-2 schematic with respect to HFSS model, Figure 3-6 is that, based on the schematic control lines (I and Q) state, either of the RF-switch port will remain short-circuited to ground. Hence, it will not allow the incoming RF signal from antenna connector, J5 to pass uninterrupted/ without attenuation to antenna connector, J6 (other end of microstrip track).

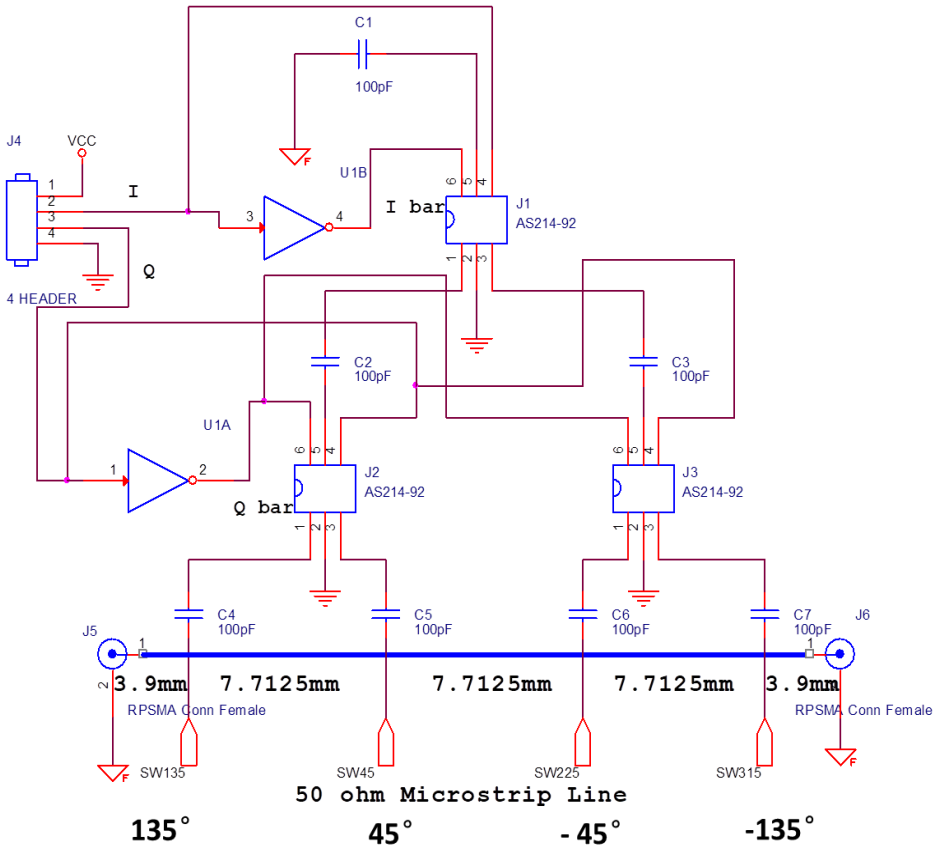

Figure 3-8: Design 2: Schematic with single microstrip QPSK phase delay tree

The Design-2 was modified with separate RF-switch and control signal for individual phase port. The control signals were mapped in embedded programming with QPSK symbols. The modified schematic of Design-2 and developed board is shown in Figure 3 8 and Figure 3 9 respectively.

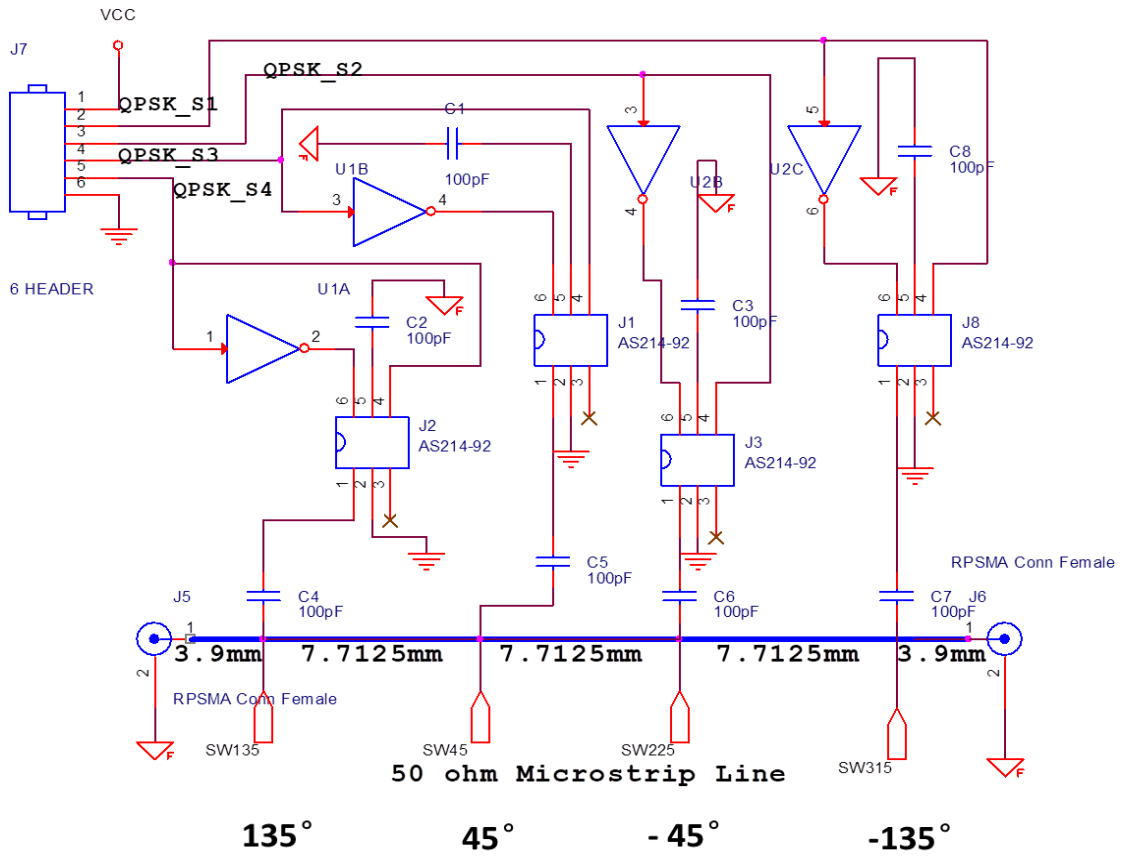

Figure 3-9: Design-2: Modified schematic with separate RF-switch for each angle of QPSK modulation

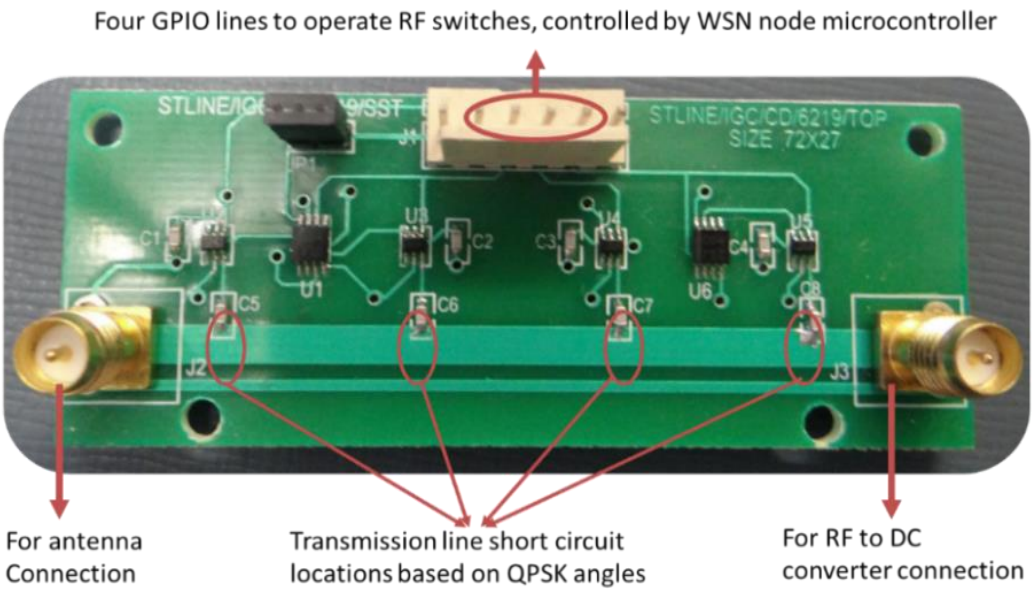

Figure 3-10: Developed WSN backscatter tag from Design-2

3.2.2 Embedded program development for backscatter tag

For WSN backscatter tag testing, the developed tag was interfaced with general purpose lines input output lines (GPIO) of the in-house developed industrial grade Cortex-M3 based LPC1768 [123] node shown in Figure 3-11. For this node, the embedded code for the physical layer of WSN was developed.

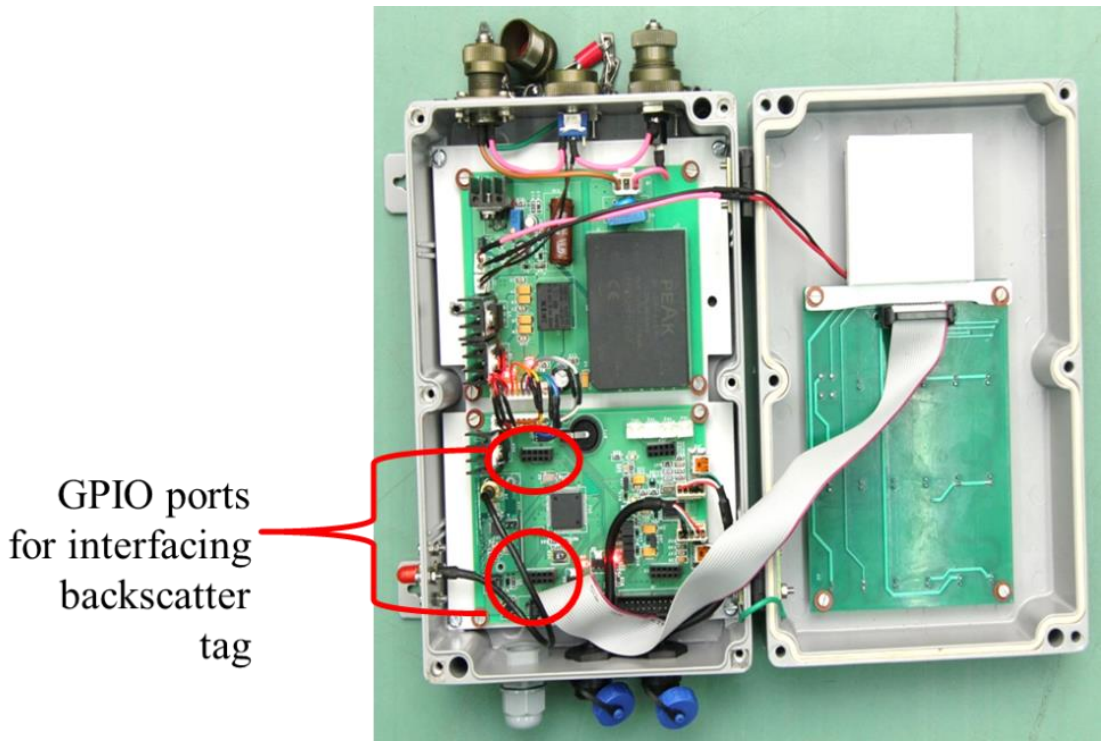

Figure 3-11: Industrial grade Coretex-M3 based LPC1768 node used for backscatter tag testing

The developed embedded code is written in C using Keil software [124]. The mentioned controller has been selected for functional testing of the developed tag. For development of ultra-low power backscatter based WSN node, an ultra –low power microcontroller needs to be selected. The developed embedded program is based on **`Algorithm 3-1`**.

Algorithm 3-1: WSN embedded PHY Algorithm

1: Receive the MPDU from MAC layer

2: **CALL**[CS,PS]=OBFUSCATION_SEQUENCE(SSO_E,Schemetype,D_f,CS_{Nbits},$Node_{DEST}$)of **Algorithm 2-2** %Based on security scheme, returns destination node obfuscation sequence

3: Create PPDU (PHY protocol data unit by adding SFD and PS to MPDU), D (equation (2-1))

4: Bit to symbol conversion, S (equation (2-2))

5: Perform DSSS and generate signal DS (equation (2-3))

6: Configure 4 -GPIO lines as output to control backscatter tag

7: Generate square wave signal, $F_s(t)$ (equation **(3-2)**)

8: DERIVE I & Q signal from DS

9: Provide time delay to Q signal for oQPSK % developed tag genrates QPSK modulation, for oQPSK , offset is added in software

10: **IF** DESIGN-1/2 **THEN**

11: Modulate I & Q signal with $F_s(t)$

12: MAP 2-GPIO lines with modulated I & Q signal

13: **ELSE IF** MODIFIED DESIGN-2 **THEN**

14: Generate QPSK symbol, Q_S from I & Q signal

15: **SWITCH**(Q_S)

16: **CASE 0x1**: GPIO-1 **high**, other 3 GPIOs **low**

17: **END CASE**

18: **CASE 0x2**: GPIO-2 **high**, other 3 GPIOs **low**

19: **END CASE**

20: **CASE 0x3**: GPIO-3 **high**, other 3 GPIOs **low**

21: **END CASE**

22: **CASE 0x4**: GPIO-4 **high**, other 3 GPIOs **low**

23: **END CASE**

24: **END SWITCH**

25: MODULATE 4 GPIO signal with $F_s(t)$

26: **END IF**

27: **END IF**

28: GPIO signal controls the tag RF switches to backscatter the incoming RF signal

29: **END** of **Algorithm 3-1**

For self-interference cancellation, the backscatter control signal generated though microcontroller GPIO lines has been modulated using a square wave signal. The square wave modulated DSSS signal generated by embedded code for modified Design-2 is shown in Figure 3-12. The novelty of the developed embedded code based PHY is that all the security features discussed in Chapter 2 can be implemented and integrated with the WSN Backscatter node.

Figure 3-12: DSSS Signal generated based on RF packet bits to control RF switches

3.3 BACKSCATTER TAG EXPERIMENTS

The experiments carried out with developed backscatter tag are described in the following subsections.

3.3.1 Functionality Testing

This test involves transmission of IEEE 802.15.4. frame through the developed backscatter tag and reception of same with commercially available IEEE 802.15.4 complaint device. This single experiment covers following test scenarios:

(i) Phase modulated signal transmission through backscatter technology.

(ii) Validation of obfuscated MaSS based embedded PHY.

(iii) Compatibility testing of developed backscatter based WSN node with existing commercial WSN devices.

(iv) Co- channel interference mitigation evaluation.

3.3.1.1 Experimental setup

For this testing, the IEEE 802.15.4 frame was generated by LPC1768 node and transmitted through backscatter tag. The embedded code modulated the tag control signal with the frequency of 15MHz. The device used for packet reception was a commercial WSN device, Texas instrument's packet sniffer dongle [125]. The continuous RF signal required for backscatter technology was generated through in-house developed Kinetis wireless microcontroller, MKW24xD512 [126] based transceiver. The Kinetis transceiver was programmed to transmit the un-modulated signal in 2.465 GHz band at 3dBm power. Agilent signal analyzer (SA), N9010A was used for capturing frequency spectrum and power delivered at other end of microstrip track of Design-2 (Figure 3-10) meant for connecting RF to DC converter.

The kinetis transceiver configured as RF signal generator was connected to port-1 of circulator and backscatter tag to port-2. The tag modifies the received RF signal and backscatter it to port-3 of circulator. Port-3 was connected to signal analyzer for spectrum capture and later it was connected to antenna to analyze the frame at sniffer. The above described experimental setup is shown in Figure 3-13.

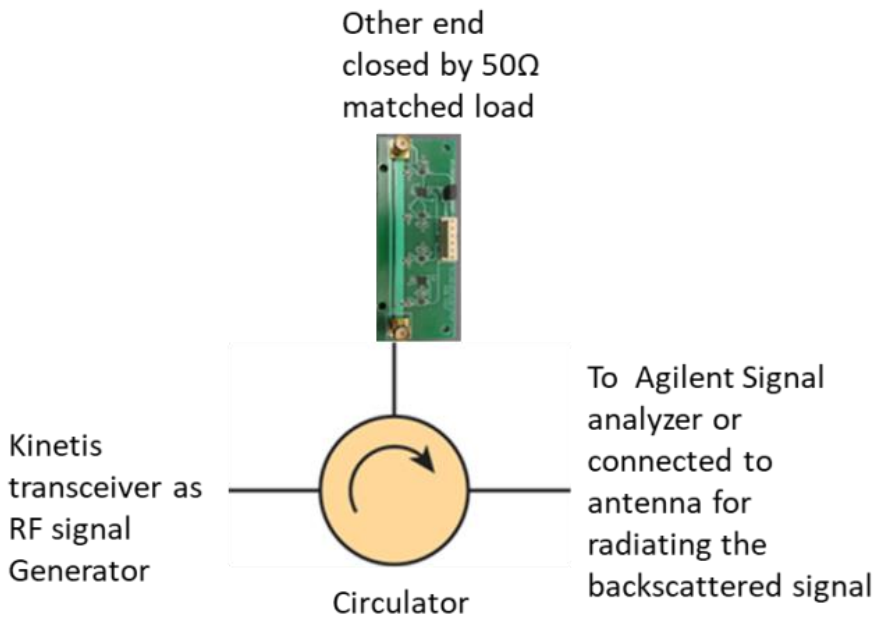

Figure 3-13: Experimental setup tag functional testing

3.3.1.2 Results

The results of experimental studies are enumerated below:

1. The frequency spectrum captured by Agilent SA connected to port-3 of circulator is shown in Figure 3-14. The power of the various frequency components (marker location of Figure 3-14) originating from tag with observed packet delivery ratio (PDR) is tabulated in Table 3-3. Packet detection (PD) % is also recoded in Table 3-3. PD is the ratio of total packets captured by sniffer (with correct and wrong FCS) and total packets transmitted by BT. PD% was measured by varying the sniffer module distance from the tag.

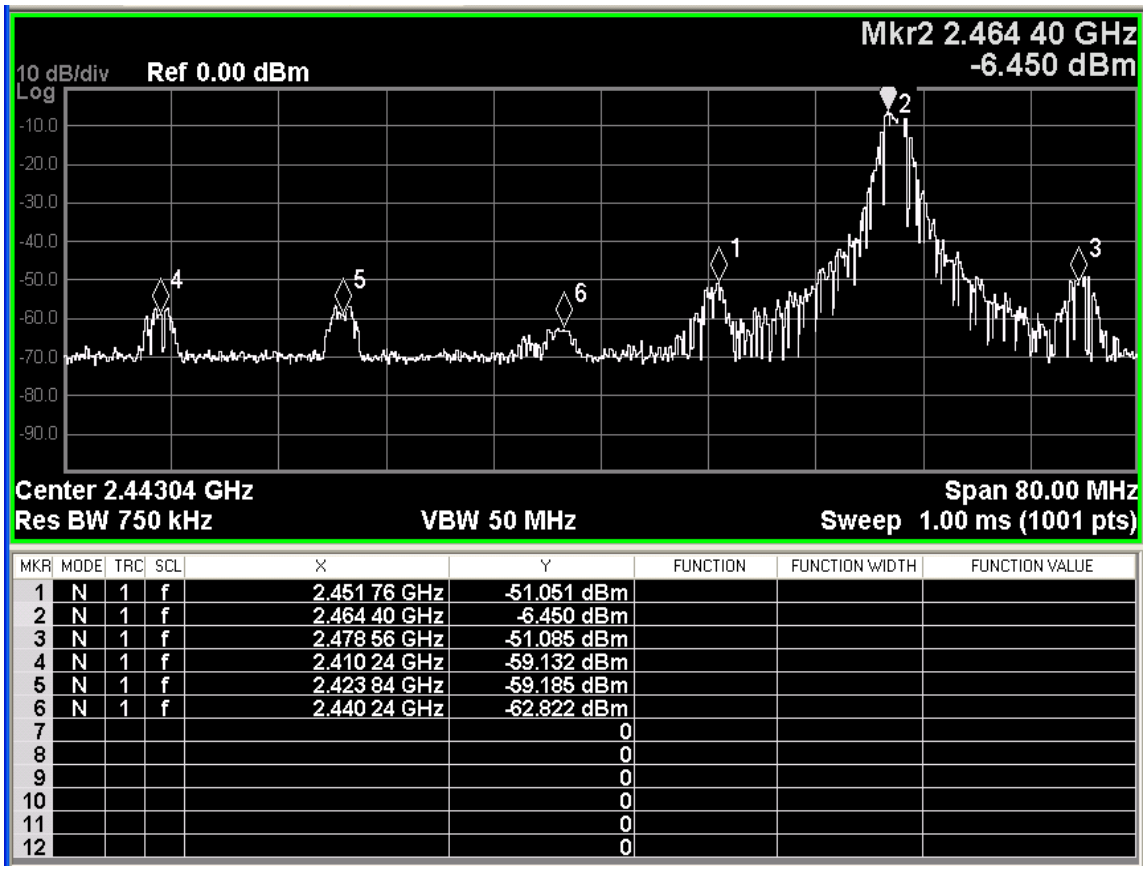

Figure 3-14: RF signal captured through SA for Design-2

Table 3-3: Frequency components originating from backscatter tag with respective packet delivery ratio (PDR)

		Tx signal	**Marker Number** from Figure 3-14					
			1	**2**	**3**	**4**	**5**	**6**
Frequency (Ghz)		2.465	2.45176	2.46440	2.47856	2.41024	2.42384	2.44024
Power (dBm)		3	-51.051	-6.45	-51.085	-59.132	-59.185	-62.822
PDR	**1m**		95	0.2	96	nil	70	nil
(%)	**2m**		93	0.2	93	nil	30	nil
with distance	**3m**		88	0.2	87	nil	5	nil
PD	**1m**		98	99.9	98	0	75	0
(%)	**2m**		96	99.7	96	0	40	0
with distance	**3m**		92	99.8	92	0	8	0
Remarks			1st harmonic	Main signal	1st harmonic	unknown	2nd harmonic	unknown

2. Throughput was also monitored at sniffer, by allowing backscatter node to transmit continuous packets. It was observed that embedded program was able to generate every new packet with the interval of 6-7ms. This packet interval time is based on the capture time displayed by the packet sniffer. PHY throughput of 230kbps and 149kbps of MAC throughput was observed.
3. The power measured by signal analyzer at the other end of straight-line microstrip track is -10dBm during idle mode and -30dBm during switching mode.
4. The power consumption for the developed tag was also measured. For the experimentation, the tag was powered ON with LPC1768 node's 3.3V DC power lines. **The current consumption at power line was observed to be 1.6mA when continuous switching operation is performed and 1.08µA when it is transmitting data at 1sec interval**.

3.3.1.3 Discussions

1. Even though, the PDR for co-channel is very poor, high PD in Table 3-3 conveys that sniffer is able to detect the frame with wrong FCS. Hence, it can be interpreted that tag is able to modify the RF signal phase as required by IEEE 802.15.4 standard. The drop in PDR is well justified with in-band interference due to the source signal.
2. The backscattered signal is translated to 1st and 2nd harmonics (on both side of main signal) generated due to baseband signal modulation by 15Mhz square wave signal. Due to low strength, the PDR is not 100% in translated frequency channels. For 2nd harmonic derived translated channel, PDR drops significantly with increase of distance between receiver and tag.
3. For the peaks associated with marker number 4 and 6, no detection was observed in sniffer. The exact reason for the captured peak by SA is unknown. It can be

anticipated that some extra frequency components are being generated as the modulation of baseband signal with square wave control signal is performed in the digital domain.

4. From throughput experiment, it is inevitable that for the developed tag throughput is not degraded due to simultaneous energy harvesting. The observed MAC throughput of 149kbps is comparable to 150kbps achieved for single link of conventional WSN nodes.
5. The power delivered at the other end microstrip track conveys that the developed tag can harvest energy both during its active and idle mode.

3.3.2 Experiment to Use Tag as Frequency Router

This experiment involves the testing of developed backscatter tag as frequency router/gateway between two WSN networks operating at different frequency channel.

3.3.2.1 Experimental setup

For this testing, two WSN networks (N1 & N2) were configured each with 2 nodes. The network was established in lab using XBee-pro (S2C) modules [122]. The network PAN ID (network identification parameter) was kept same for both network but their operating channel frequency was configured to 2.465GHz (0x17) and 2.475GHz (0x19). In each network, one XBee-pro device was configured as coordinator (CD) and other node as end device (ED). The end devices of both networks were made to transmit analog to digital converter(ADC) data periodically at the rate of 2sec and 3sec respectively. The developed backscatter tag (BT) was kept near the configured network EDs. Two Texas packet sniffers (S1 & S2) were also installed to capture the packets from both the networks operating in different frequency channels. The layout of experiment setup is shown in Figure 3-15.

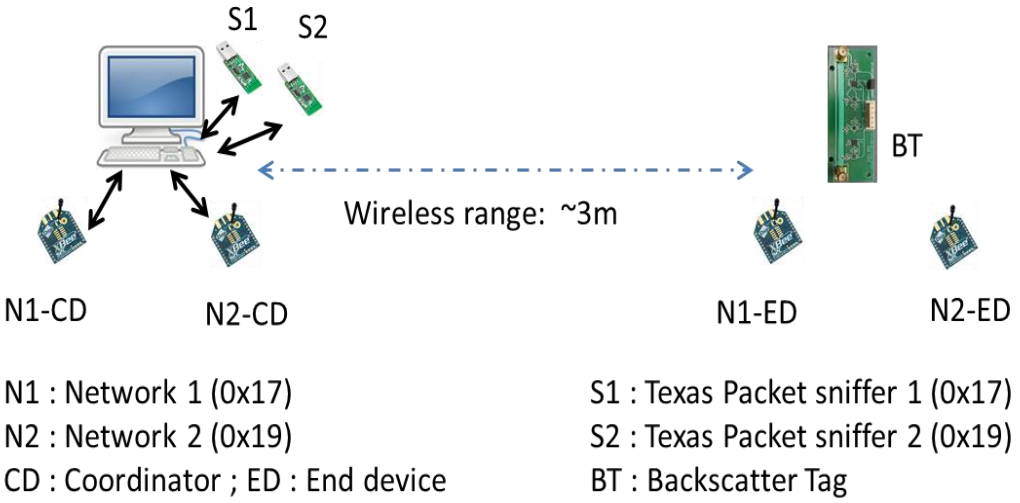

Figure 3-15: Experimental setup to test backscatter tag as frequency router

3.3.2.2 Results and discussions

The packet delivery ratio (PDR) observed across the networks is shown in Table 3-4 . The snippets of packets captured by both sniffers for N1 network data packet transmission cycle is shown in Figure 3-16. It is observed that the S2 is able to capture packets related to N1-ED. Following inferences can be drawn from the experiment:

1. The PDR across the network is above 99%. Hence, the developed tag can be used as a frequency router/ gateway across the networks.
2. Sniffer is able to capture all the packets of its network and frequency-routed packets from other network ED. The signal strength of the packets transmitted by the coordinator reduces until it reaches BT. Further, RF signal losses at BT, reduces the signal strength of the frequency-translated signal.

Table 3-4: Packet delivery ratio (PDR) for tag as frequency router between two WSNs

	Observed by N1-CD	Observed by N2-CD
PDR of N1	100	99.4
PDR of N2	99.1	99.8

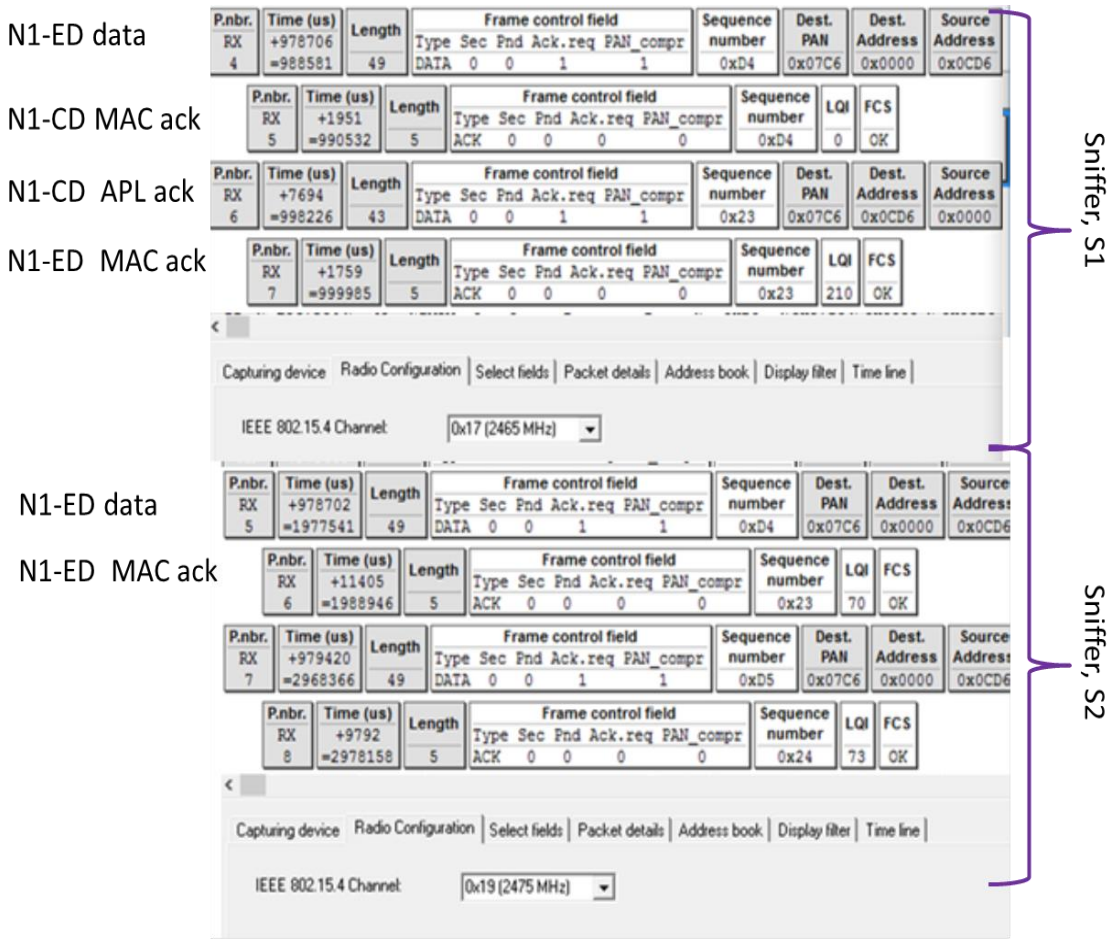

Figure 3-16: Snippets of packet captured by sniffer for frequency router testing

3.4 Comparison of the Developed Tag with Existing QPSK based Backscatter Designs

WSN uses oQPSK modulation at its PHY, while Wi-Fi technology uses QPSK modulation. However, for the developed WSN backscatter tag QPSK modulation is part of the tag hardware. Thus, comparison of the developed backscatter tag with existing backscatter design has been performed in Table 3-5. For this comparison, QPSK based wireless technology operating in 2.4GHz band (Table 1-2) for establishing backscatter communication has been considered. Owing to the modulation technique used for WSN, its competitor for backscatter communication is the Wi-Fi based backscatter devices. Conventional Wi-Fi is superior to WSN technology in the metric of data rate, and communication range; however, the backscatter mode of both the technology is

comparable as the mentioned metrics are dependent on incoming RF signal characteristics. Both WSN and Wi-Fi technology has different communication bandwidth, thus, standard defined theoretical data rate is different for them. Hence, for comparison relative data rate percentage has been used.

Table 3-5: Comparison of developed WSN backscatter tag with existing design

Reference	Technology	Relative data rate %	Power consumption (µW)	Compatibility
[46]	Wi- Fi	<1	33	YES
[47]	Wi-Fi	<<1	0.65	YES
[49]	Wi-Fi	9	0.1	NO
[51]	Wi-Fi	20	14.5	YES
This work	WSN	57	3.3	YES

From Table 3-5, it can be inferred that this work developed BT tag outstand in the parameter of achievable relative data rate. In addition, with advantage of compatibility with conventional WSN nodes, the power consumption is low.

3.5 SUMMARY

In this Chapter, an ultra-low power consuming backscatter tag for WSN is designed, developed, and tested. WSN uses oQPSK modulation; in this modulation scheme, QPSK is part of BT hardware while offset for oQPSK has been added through BT software. The floating ground based straight-line dual port microstrip has been used for designing backscatter based QPSK modulation. One port of microstrip is meant for receiving and backscattering the RF signal while the other port harvests the power from RF signal. For the developed BT, in band interference has been eliminated by

controlling the switching frequency of RF switches. The important findings of this Chapter are enumerated below:

1) The floating load based straight-line microstrip track eliminates the need for power splitting for RF harvesting and backscatter operation, as both are connected to two ends of microstrip track.

2) BT harvest power during idle mode; along with this, the frequency translation scheme over dual port transmission line allows the BT to harvest power during active mode of backscattering.

3) The developed WSN BT exhibits the compatibility with conventional WSN, and its implementation strategy does not compromise over the throughput. MAC throughput for link between BT and conventional WSN sniffer is 149kbps, which is almost equal to the 150kbps real time throughput obtained with conventional WSN link when auxiliary packets are eliminated.

4) The power consumption of the developed backscatter tag is 5000 times less than conventional WSN transmitter.

5) The developed tag can also be used as frequency router between the two networks operating at different channel frequency.

6) The developed WSN BT tag is able to mitigate in-band interference, maintain the compatibility and desired throughput without incurring power penalty. Hence, it waves off the energy –data rate tradeoff associated with conventional BT.

.

CHAPTER 4

Wireless Power Generation for Secured Backscatter based WSN Node

To resolve the power requirement issue associated with WSN based long-lived inaccessible zone monitoring, this Chapter explores the omnipresent and wireless communication, self-generated RF signal for generating power for WSN nodes. Initially, WSN devices power requirement has been theoretically quantified, and to meet that power demand a rectenna panel requirement has been envisaged. Power captured by rectenna panel is analogous to the discrete sampling in the spatial domain; thus, the rectenna panel size, rectenna spacing, number of rectenna and their arrangement pattern selection criterion is mathematically explored. Further, the proposed rectenna panel design has been experimentally validated by fabricating and integrating with developed secured backscatter based WSN node.

4.1 FEASIBILITY ANALYSIS TO POWER ON WSN DEVICES WIRELESSLY

4.1.1 WSN Device Power Requirement

As per IEEE 802.15.4 standard [35] WSN devices are classified as Full Functional Devices (FFD) and Reduced Functional Devices (RFD). FFD nodes are equipped with all the network functionalities, allowing them to act as network coordinator, aggregator, cluster head or as gateway nodes. RFD nodes are network end devices, equipped with sensor or actuators. Based on comparative study performed on popular low power consuming microcontrollers (µC) and transceivers, the Atmel

SAMD20[127] and AT86RF233[128] were selected for the design of FFD and RFD of WSN. The power estimate with battery requirement for the designed FFD and RFD is shown in Table 4-1 (row 1&2). FFD with sleep cycle ON has been addressed as RFD here. Cyclic sleep considered for RFD power estimate is to wake up after every 1sec for 10ms duration. The estimate has been made with information available in the datasheet of selected µC and radio chip. As shown in Table 4-1 (row 3&4), the power demand for FFD and RFD can be reduced further if instead of conventional radio chip the developed backscatter tag (BT) is used.

Table 4-1: Power Consumption Calculation for the designed FFD and RFD

S. No	Scenario	Power (mW)			2200mAh @3V Battery operation time
		µC	radio	device	
1.	**FFD active**	9.72	21.24	30.96	~ 8.8 days
2.	**RFD cyclic sleep**	0.131	0.227	0.358	~2.1yrs
3.	**FFD - BT active**	9.72	3.3	13.02	~ 21 days
4.	**RFD - BT in cyclic sleep**	0.131	0.0036	0.134	~5yrs

4.1.2 Suitability of RF Energy to Power WSN Devices

By default, a wireless technology radiates energy in the form of RF for establishing wireless communication. Hence, RF energy is omnipresent and it is feasible to transfer energy using RF waves even to inaccessible areas. Even though, the RF energy density decreases by inverse distance square law, their wave nature make them flexible to reach any corner of the world. This attribute of RF waves makes them the default option for wireless power applications.

Based on Friis law [129], Table 4-2 gives the value for RF power received, $\boldsymbol{P_{rf}}$ at the distance of 5m from radiating source of 4W for various RF frequencies. The value of 4W is selected based on radiation emission limits set by International

Commission on Non-Ionizing Radiation Protection (ICNIRP). For this calculation, receiver antenna gain is assumed as 6dBi. In view of the tradeoff between received power and rectenna size (depends on antenna and its operating wavelength), a rectenna capable to generate RF power from RF waves of frequency >900MHz is required. Considering the $\boldsymbol{P_{rf}}$ values obtained in Table 4-2, and based on existing work [74]–[76], an eight-stage voltage multiplier is selected for rectenna design. Theoretically, this rectenna will be able to generate ~1.1V@2mA with -10dBm of RF power[40]. Hence, to design a FFD with wireless power solution, a single rectenna is not sufficient.

Table 4-2: RF power received by WSN node for various RF frequencies at the distance of 5m from 4W RF source

RF wave frequency (MHz)	**430**	**860**	**915**	**2400**	**5800**
Power received, P_{rf} (dBm)	+2.91	-3.16	-3.65	-12.02	-19.68

As the radiated RF energy propagates, it disperses in space and its power density drops. Therefore, a single rectenna is able to intercept very little energy governed by its effective antenna aperture. For such scenario, if power-sampling area is increased, the intercepted power will increase. To achieve this, it is not feasible to use an antenna with a large aperture. The practical option is to aggregate the power intercepted by the multiple numbers of rectenna.

Based on all above illustrations, power generated by rectenna, Table 4-1 and Table 4-2, the FFD consuming maximum power, requires a 5×20 array rectenna panel shown in Figure 4-1. To capture the maximum transmitted RF power an efficient rectenna grid/ panel need to be designed. The first condition for rectenna panel design is to identify the maximum limit for the panel dimension, beyond which there is no further scope of efficiency improvement in a particular scenario. Further, rectenna spacing, their number and arrangement pattern need to be optimized.

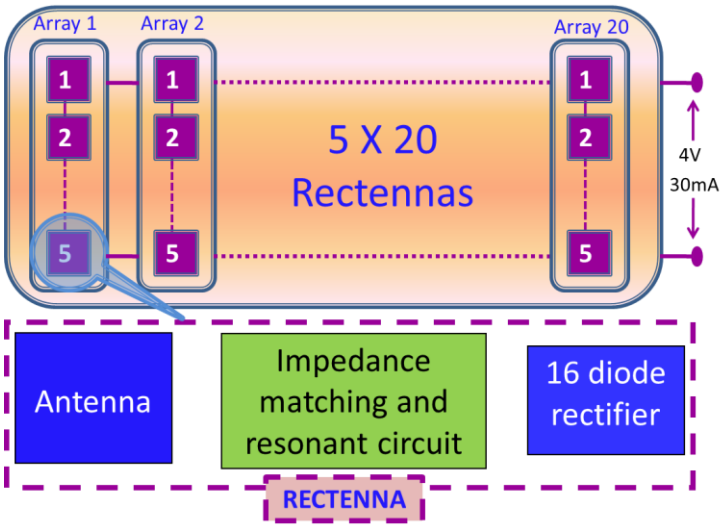

Figure 4-1: Proposed rectenna panel for WSN FFD

4.2 RECTENNA PANEL DESIGN & DEVELOPMENT

4.2.1 Rectenna Design and Development

The basic unit of rectenna panel is rectenna. Initially, for rectenna design schottky diode based voltage doubler rectifier was explored. The designed rectifier took more than 2 min to charge a 3F super-capacitor to a voltage 1.22V when placed at distance of 30cm from RF source of 4W. Hence, to experiment with multi-stage voltage multipliers (VM), a rectenna with configurable cascading option as shown in Figure 4-2 was designed and developed (Figure 4-3). The capacitor charging time for different VM stages is shown in Figure 4-4 . Increase of VM stages reduces capacitor-charging time but increases hardware complexity. Thus, considering this tradeoff and based on theoretical estimate (previous section), an eight-stage VM rectenna was selected for panel development.

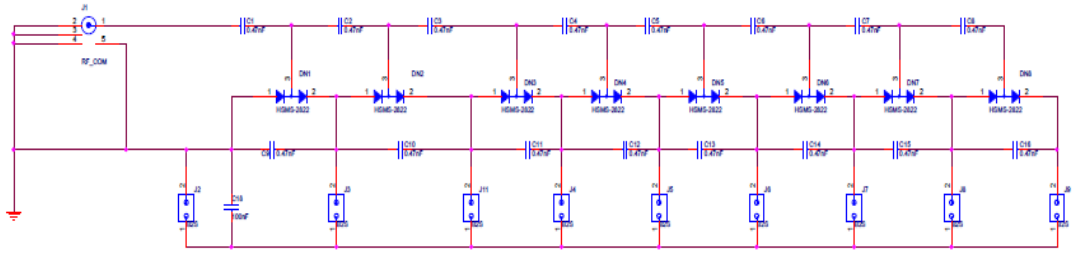

Figure 4-2: Configurable, multiple stage voltage multiplier rectenna schematic

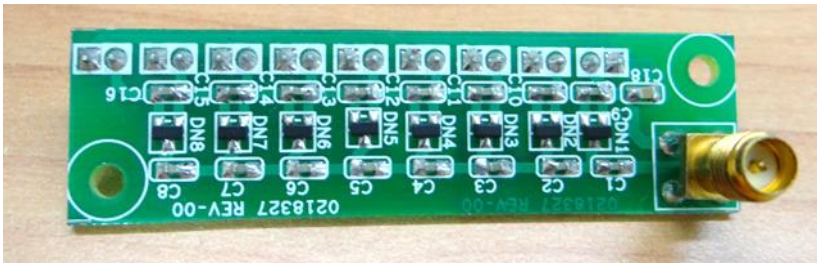

Figure 4-3: Configurable, multiple stage voltage multiplier rectenna

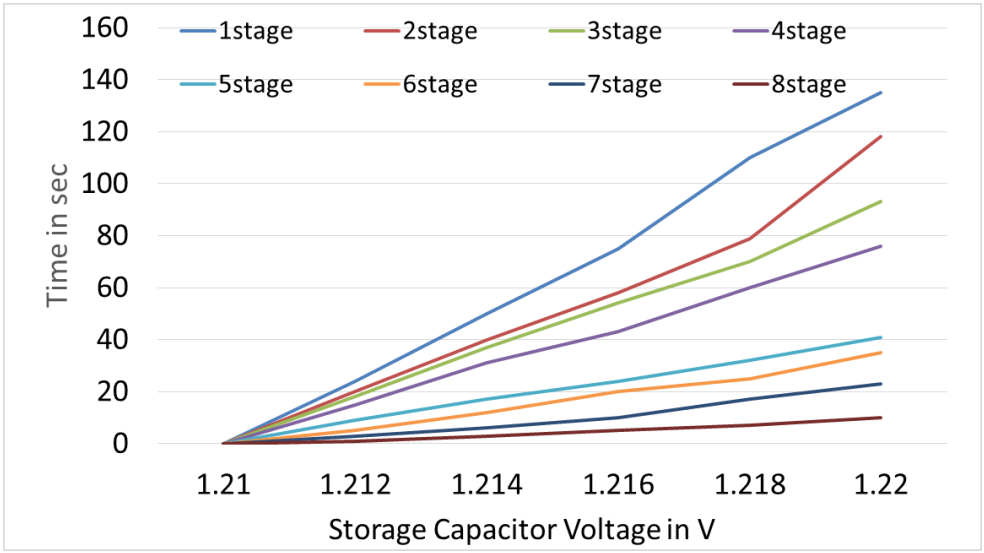

Figure 4-4:Super-Capacitor charging time for different stage voltage multiplier rectenna placed at distance of 30cm from 915MHz 3W RF source

4.2.2 Rectenna Panel Design

Rectenna panel is the series and parallel interconnection of multiple rectennas. Based on the power generated by the rectenna and the power requirement of the load, the minimum rectenna count and their interconnection circuit for panel design can be

decided. RF power disperses during propagation, hence, apart from rectenna interconnection, the rectenna spatial arrangement is expected to affect the panel aggregated power. Thus, detailed analysis on rectenna panel design parameters and their optimization is required for panel design.

4.2.2.1 Rectenna panel design parameters

Four main rectenna panel design parameters which influence the performance of overall RF power generation system are namely, (i) rectenna panel size (*RPS*), (ii) the number of rectenna, (iii) rectenna spacing and (iv) rectenna panel design pattern. All these parameters are interconnected. Based on rectenna spacing and the number of rectenna in a row/column, *RPS* can be calculated.

If the transmit antenna solid angle ($\Theta_H\Theta_V$) governs its directivity; then, the maximum power radiated by the source will be focused in it solid angle direction [130]. Here Θ_H & Θ_V are half power bandwidth of transmit antenna in horizontal and vertical plane respectively. If rectenna is located at the distance, R from RF source, then rectenna panel should be designed to cover the full transmit antenna wavefront patch $\Theta_H\Theta_V R^2$ (m^2). Hence, rectenna panel size *RPS,* can be derived from the following equation (4-1).

$$Area_{RP} = f(RPS) \geq \Theta_H\Theta_V R^2 \tag{4-1}$$

where,

Area_{RP} : *Area of rectenna panel in m^2. If rectenna panel is of square shape, RPS is L^2, where L rectenna panel side is in meters*

If n numbers of rectenna are placed with spacing d, then L can be calculated from equation (4-2).

$$L = (n-1)d \tag{4-2}$$

The value of rectenna spacing, d is coupled with its effective aperture, A_e. Considering equation (4-3) and assuming aperture as a circle (or if any other shapes) then its largest dimension d_a, can be approximated based on equation (4-4).

$$\mathrm{A_e} = \mathrm{e_a A_p} = \frac{\lambda^2}{4\pi}\mathrm{G} \tag{4-3}$$

$$\mathrm{d_a} \approx \frac{\lambda}{\pi}\sqrt{\frac{\mathrm{G}}{\mathrm{e_a}}} \tag{4-4}$$

where,

A_p : *Antenna physical aperture*

e_a : *Antenna aperture efficiency*

λ : *Wavelength in cm based on antenna operating frequency*

G : *Antenna gain*

Thus, to eliminate aperture overlap in rectenna panel design, minimum horizontal and vertical spacing d, between two rectenna should be equal to or greater than d_a. Equation (4-5) condition will eliminate the physical overlap of antennas and will minimize coupling & overlap of the virtual reception zone of two antennas.

$$\mathrm{d} \geq \mathrm{d_a} \tag{4-5}$$

Other than rectenna spacing parameter, the number of rectenna required for panel design is also affected by rectenna placement pattern.

As depicted in Figure 4-5, four grid patterns – Grid-1, Grid-2, Grid-3 and Grid-4 with varying degree of compactness with aperture overlap has been analyzed. In the figure, red dots symbolize antenna; orange dots represent active rectenna, intercepting

maximum radiations in the area governed by the yellow circle. The transmitter antenna wavefront governed by its radiation direction solid angle is signified by yellow circle. For maximum interception of the power, the panel normal should be along the RF wave propagation and antenna polarization should match with the transmit antenna polarization.

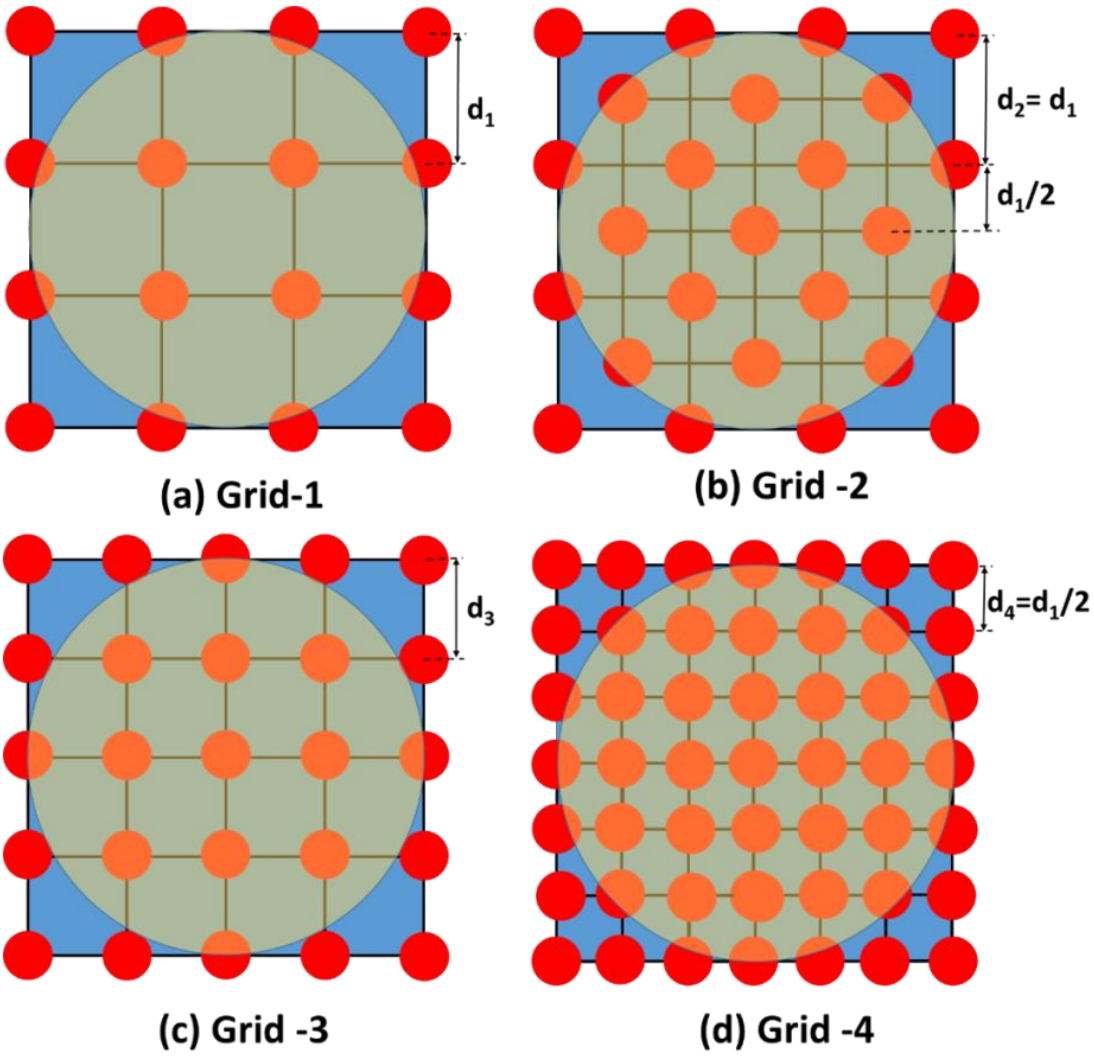

Figure 4-5: Rectenna Placement pattern for panel design, (a) Grid-1 with rectenna spacingd, (d_1 equal to $d = d_a$), (b) Grid-2 with main and sub grid rectenna spacing as d_1. Sub grid placed at offset of $d_1/2$ from main grid, (c) Grid -3 with rectenna spacing d_3, (d_3, less than d_a), (d) Grid -4 with rectenna spacing d_4, (d_4 equal to $d_1/2$). In all grid patterns Red and orange dots represent rectenna and yellow circle represent transmit antenna wavefront. Orange dots represent active rectenna, i.e. rectenna covered by the yellow circle, intercepts direct radiation from RF source.

As the pattern arrangement is different for all the Grids, the number of rectenna covering the transmit antenna wavefront is different. The rectenna covered by transmit antenna wavefront will actively contribute for RF harvesting while uncovered rectenna will harvest scattered or reflected RF power. Hence, Rectenna Panel Utilization Factor (*RPUF*) need to be calculated for each grid.

RPUF is the ratio of the number of active rectenna to the total number of rectenna (*TNR*) used for panel design. The rectenna covered by yellow circle area has been referred as active antennas. With diagrammatic view of grid designs, it can be interpreted that count of active rectenna is almost equal to *TNR* of the grid with one column less than existing grid.

For all grids, rectenna arrangement pattern would be discussed with reference to Grid-1. For illustration and derivation, Grid-1 has been designed using 4×4 rectenna panel, but calculation has been done for generic grid size $n \times n$ (for Grid-1). Horizontal and vertical rectenna spacing for the four grids with *TNR* and *RPUF* is summarized in Table 4-3.

Table 4-3: Comparison of rectenna panel parameter for various grid patterns

Grid type	Rectenna spacing	Number of rectenna in single row/columun	Total number of rectenna (TNR)	Rectenna Panel utilization Factor (RPUF)
Grid-1	$d_1 = d_a$	n	n^2	$\frac{(n-2)^2+4}{n^2}$
Grid-2	d_1 (main grid) $d_1/2$ (sub grid)	n (main grid) $n-1$ (sub grid)	$n^2 + (n-1)^2$	$\frac{(n-1)^2+(n-2)^2+4}{n^2 + (n-1)^2}$
Grid-3	$d_3 < d_1$	$\sqrt{(n^2+(n-1)^2)}$	$n^2 + (n-1)^2$	$\frac{(n-1)^2+4}{n^2 + (n-1)^2}$
Grid-4	$d_1/2$	$2n-1$	$(2n-1)^2$	$\frac{(2n-3)^2+4}{(2n-1)^2}$

Figure 4-6 reveals that the *TNR* for the same size panels varies with rectenna spacing and placement pattern. *RPUF* graph for all the four designed panels is shown in Figure 4-7. It is observed that the *RPUF* of Grid-2 and Grid-4 is similar, superior compared to Grid-1, and Grid-3 design. However, comparison with *TNR* metric (Figure 4-6) reveals that Grid-2 can achieve the same *RPUF* as for Grid-4 but with lesser number of total rectennas. Figure 4-7, elucidates that *RPUF* curve does not linearly increase with increase in number of rectenna. Compact rectenna arrangement pattern results in reduction of rectenna spacing. Effect of reduced rectenna spacing is increase in rectenna aperture overlap, number of rectenna and *RPUF* saturation. Hence, with optimum placement approach (type of grid), optimum value of rectenna spacing d should be selected.

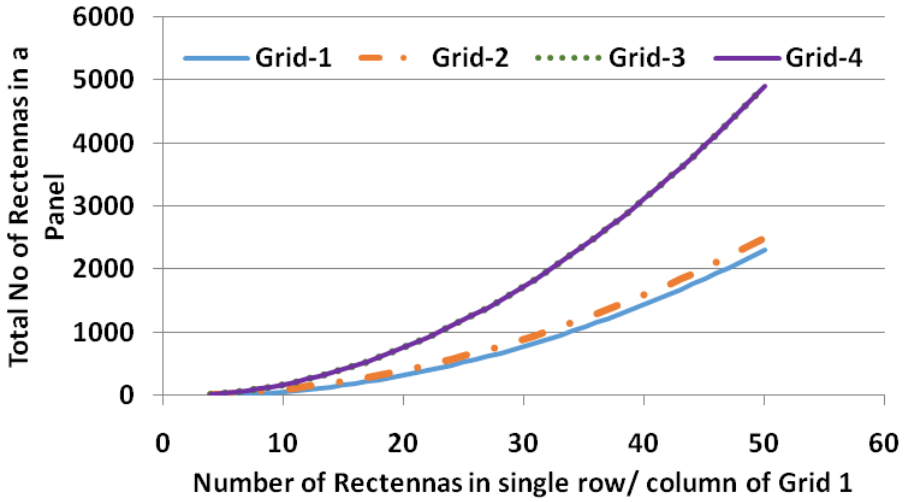

Figure 4-6: Total no of antennas required to design Panel of different grid structure with reference to Grid-1 design

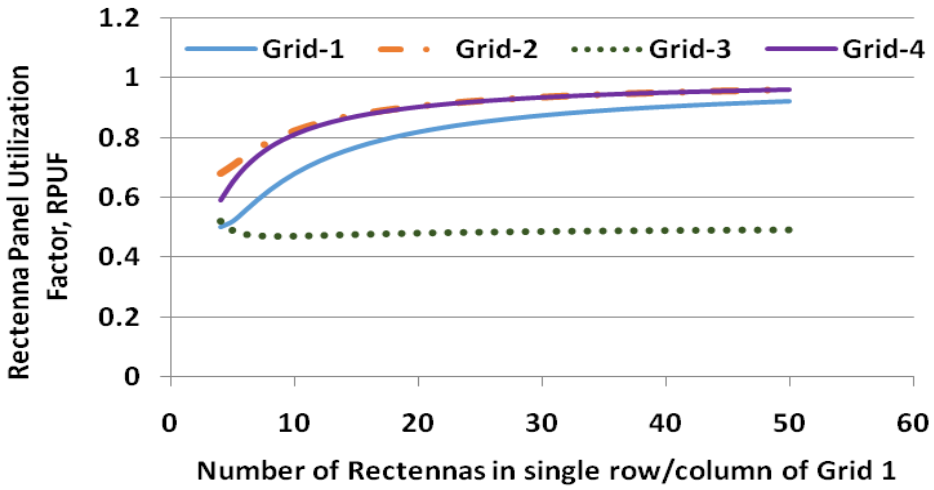

Figure 4-7 Rectenna Panel Usage Factor for different grid structures with respect to Grid-1 design

4.2.2.2 Optimization of rectenna spacing

For a panel of fixed size, increase of rectenna count in row/column will result in reduction of rectenna spacing. If equation (4-5) is violated, then chosen rectenna spacing will result in rectenna aperture overlap. This overlap will affect the individual rectenna RF reception capabilities. As per current grid pattern definitions, Grid-1 is designed with rectenna spacing d as d_a ; thus, it does not have rectenna aperture overlap. For Grid-3 and 4, certainly overlap exists, as their rectenna spacing is less than non-overlap rectenna spacing. In case of Grid-2, as sub grid is placed at distance less than rectenna spacing, overlap is expected.

Grid pattern definitions, Grid-3 and Grid-4 merge to Grid-1 if rectenna spacing is increased to eliminate the overlap region. Scenario for Grid-2 is different as sub grid is placed at offset of distance $d/2$ from the main grid location. For Grid-2 overlap region will become zero if rectenna spacing is more than $\sqrt{2}d_a$; although, with rectenna spacing of $\sqrt{2}d_a$ Grid-2 will result in the decrease of *RPUF* as the value of *n* will drop by $\approx \sqrt{2}$.

In the Grid-2 pattern, with different rectenna spacing for horizontal and vertical rectenna arrangement unused power can be reduced without rectenna aperture overlap. As shown in Figure 4-8, by equilateral triangulation approach rectenna arranged with spacing, d_a will not have any overlap and uncovered region will be low.

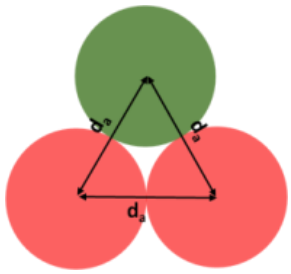

Figure 4-8: Equilateral triangulation approach for rectenna panel design

For designing a grid with triangulation placement, the spacing between columns and rows should be d_a and $\sqrt{3}d_a$ respectively for both main grid and sub grid. The resultant arrangement will be tightly compact structure with negligible power voids. Figure 4-9 shows the comparison of Grid-1 and Grid-2 pattern with three type of rectenna spacing namely, (d_a, d_a) *homo*, $(\sqrt{2}d_a, \sqrt{2}d_a)$ *homo* and $(d_a, \sqrt{3}d_a)$ *hetero*. The pattern formed with non-overlap spacing $(\sqrt{2}d_a, \sqrt{2}d_a)$ will be referred as Grid-2_NO and pattern with heterogeneous spacing$(d_a, \sqrt{3}d_a)$ as Grid-2hetero.

Figure 4-9, emphasize that as the rectenna spacing changes, the number of rectenna used for panel design also changes. The main visible advantage with Grid-2hetero is that scenario of no overlap with negligible transmit power wastage (non-intersecting region of transmit antenna wavefront with the rectenna aperture result in transmit power wastage) is feasible. The best comparative metric will be the evaluation of *RPUF* value for Grid-2_NO and Grid-2hetero.

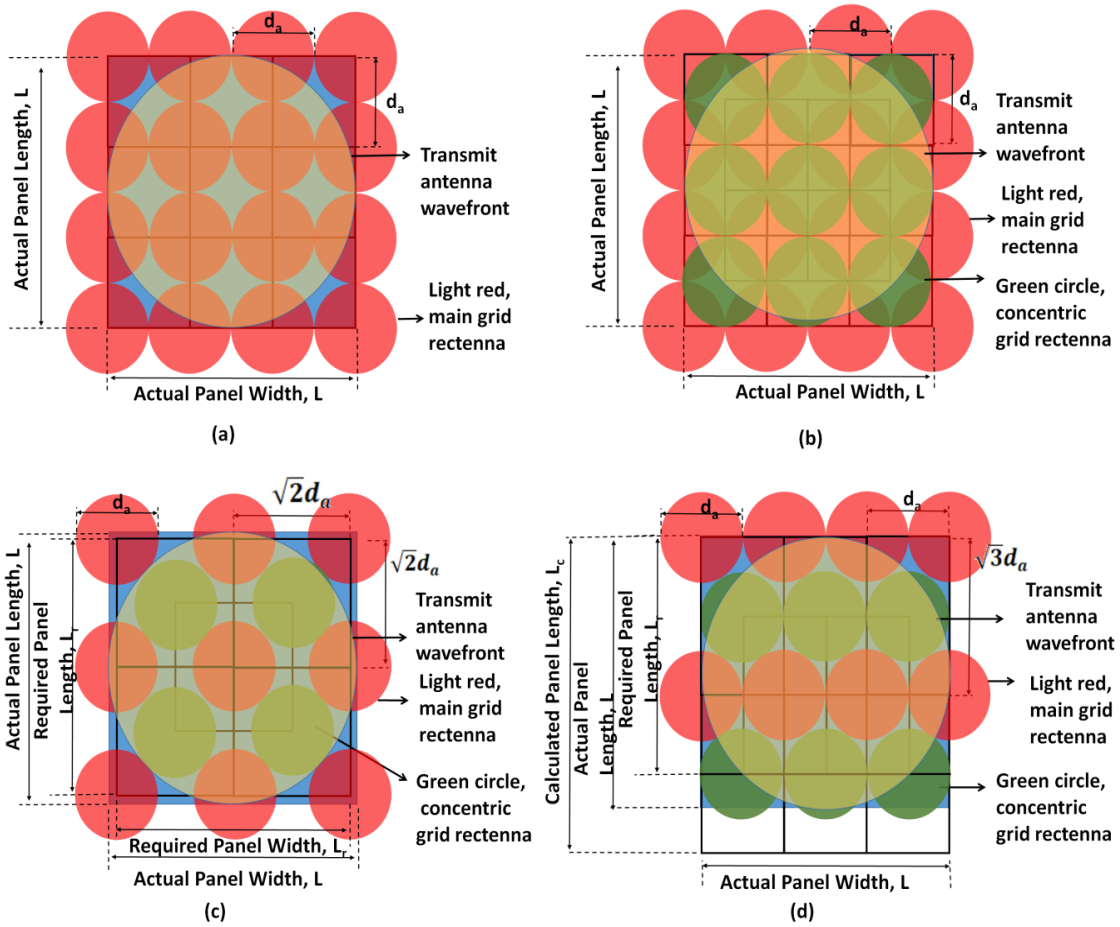

Figure 4-9: Grid pattern Comparison (a) Grid-1 with uniform rectenna spacing, d_a (b) Grid-2 with equal rectenna spacing, d_a (c) Grid-2_NO with equal non-overlap rectenna spacing, $\sqrt{2}\,d_a$ (d) Grid-2hetero with non-uniform spacing d_a and $\sqrt{3}\,d_a$

For Grid-2_NO (Figure 4-9(c)), *TNR* and *RPUF* can be calculated using equations (4-6) and (4-7).

$$\mathrm{TNR_{G\_2\_NO}} = \mathrm{n_1^2} + (\mathrm{n_1} - 1)^2 \tag{4-6}$$

$$\therefore \mathrm{RPUF_{G\_2\_NO}} = \frac{(\mathrm{n_1} - 1)^2 + (\mathrm{n_1} - 2)^2 + 4}{\mathrm{n_1^2} + (\mathrm{n_1} - 1)^2} \tag{4-7}$$

Where,

n_1 : *Number of rectennas in single row/column of main grid of Grid-2_NO. As for this grid, rectenna spacing is* $\sqrt{2}d_a$ *so based on equation* (4-2), $n_1 = \frac{(n-1)}{\sqrt{2}} + 1$

$$\therefore \quad \mathrm{RPUF}_{\mathrm{G\_2\_NO}} = \frac{(\mathrm{n}-1)^2 - \sqrt{2}(\mathrm{n}-1) + 5}{(\mathrm{n}-1)^2 + \sqrt{2}(\mathrm{n}-1)} \tag{4-8}$$

For Grid-2hetero (Figure 4-9(d)), number of columns in rectenna panel is same as Grid-2. *If* there exist $2n_2$ number of rows (including main and sub grid) in rectenna panel *then*, based on vertical rectenna spacing of $\sqrt{3}d_a$ and equation (4-2), n_2 can be calculated by equation (4-9). Hence, *TNR* and *RPUF* can be calculated from equations (4-10) and (4-11).

$$\mathrm{n}_2 = \frac{(\mathrm{n}-1)}{\sqrt{3}} + 1 \tag{4-9}$$

$$TNR_{G_{2_{hetero}}} = \mathrm{n}_2 n + n_2(n-1) \tag{4-10}$$

$$\therefore \quad \mathrm{RPUF}_{\mathrm{G_{2_{hetero}}}} = \frac{(\mathrm{n}_2-1)\mathrm{n} + \mathrm{n}_2(\mathrm{n}-1)}{\mathrm{n}_2(2\mathrm{n}-1)} = \frac{(\mathrm{n}-1)\left(2\mathrm{n}+1+\sqrt{3}\right)}{\left(\mathrm{n}-1+\sqrt{3}\right)(2\mathrm{n}-1)} \tag{4-11}$$

Figure 4-10 shows the comparison of *RPUF* of all the variants of Grid-2 design based on rectenna spacing and Figure 4-11 presents the comparison for the *TNR* required for Grid-2 design variants. From these figures, following inferences can be made: (i) The number of rectenna required for panel design is the least for non-overlap configuration, Grid-2_NO. But, reference to *TNR* plot, significant difference between *RPUF* of Grid-2 and Grid-2_NO is not there. Hence, with overlap configuration more rectenna are required to design the panel of same size. (ii) Grid-2hetero based on equilateral triangulation approach results in maximum utilization of rectenna (highest *RPUF*).

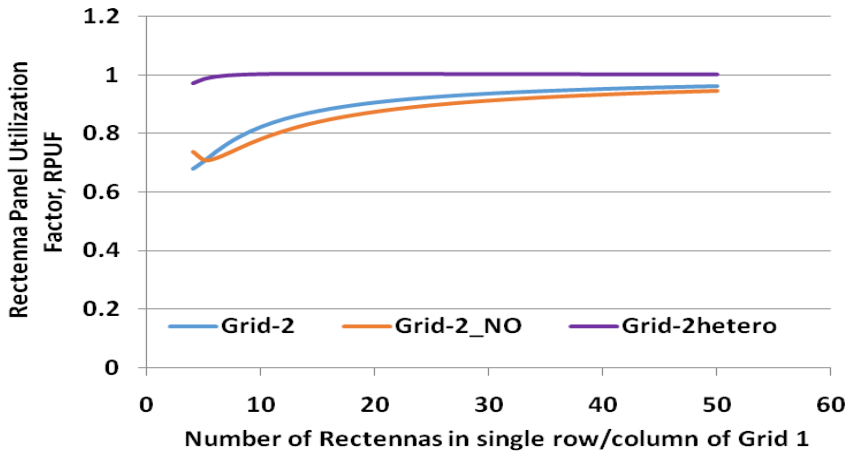

Figure 4-10: Rectenna panel Utilization Factor Comparison for Grid-2 (with rectenna spacing d_a), Grid-2_NO and Grid-2hetero

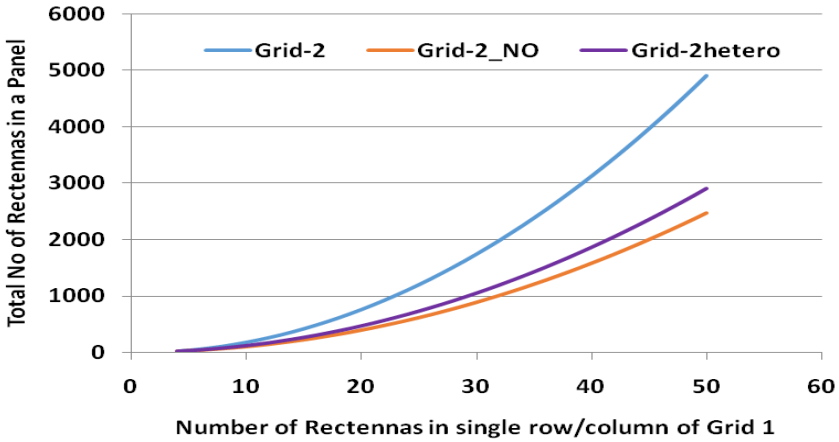

Figure 4-11: Comparison of the total number of rectenna required for Grid-2 (with rectenna spacing d_a,), Grid-2_NO and Grid-2hetero pattern to design panel of varying size

4.2.2.3 Optimization of number of rectenna for Grid-2hetero pattern

It can be observed from Figure 4-9 that corner rectenna does not intercept power; so, unutilized rectenna should be eliminated to reduce design cost. Other aspect is, for equilateral triangulation based rectenna panel design, unutilized rectenna count varies with rectenna size. Hence, some methodology is required to identify and quantify the unutilized rectenna. Equation (4-2) gives information regarding maximum number of columns required for main grid and sub gird are n and $n-1$ respectively. Based on the value of n and n_2 (required for Grid-2hetero), the number of rows in main grid, M_R and

rows in sub grid, S_R also need to be optimized to minimize the count of unutilized rectenna. Value of M_R and S_R can be calculated using **Algorithm 4-1 .**

Algorithm 4-1: Main grid and sub gird row calculation for Grid-2hetero

1: M_R = rounddown (n_2), value of n_2 calculated from equation (4-9)
%Here, rounddown () is a function which rounds the number down.

2: Calculate modified length of rectenna, $L_{M1} = \sqrt{3} \times n_2$ and $L_{M2} = \sqrt{3}(n_2 - 1)$

3: **IF** $(L - L_{M1}) > (L - L_{M2})$ **THEN** % Here, L is length of rectenna calculated from equation (4-2)

4: $S_R = n_2 - 1$

5: **ELSE** $S_R = n_2 + 1$

6: **END IF**

7: **END Algorithm 4-1**

Based on **Algorithm 4-1**, the number of rows in sub grid can be more than main grid. Accordingly, for Grid_2hetero *TNR* can be calculated using following equation (4-12).

$$TNR = nM_R + (n-1)S_R + K \tag{4-12}$$

In equation (4-12), K is a factor governed by the number of unutilized rectennas removed and additional rectenna added to improve the rectenna panel performance. Value of K depend on M_R and S_R , it's value for following four different cases can be calculated from equation (4-14)

1. Case1: M_R *is even and greater than* S_R
2. Case2: M_R *is even and lesser than* S_R
3. Case3: M_R *is odd and greater than* S_R
4. Case4: M_R *is odd and lesser than* S_R

$$K = \begin{cases} -M_R^2 + M_R(2n+3) - (n+1) \; for \; Case1: \\ -M_R^2 + M_R(2n+1) + (n+1) \; for \; Case \; 2 \\ -M_R^2 + M_R(2n+1) - n \quad for \; Case \; 3 \\ -M_R^2 + M_R(2n-1) + n \quad for \; Case \; 4 \end{cases} \tag{4-13}$$

Grid_2hetero design for four different value of n is shown in Figure 4-12. In the Figure 4-12, the circles with no fill (in main and sub grid) symbolizes the unutilized rectenna. The rectenna indicated with blue colour are additional rectenna required to utilize the dispersed RF signal from wavefront edge. It was observed that for the case when value of M_R is even, there is a need to add two extra rectenna for better diagonal coverage of wavefront. Rearrangement of rectenna and elimination of un-utilized rectenna converts the square type grid to a hexagonal grid.

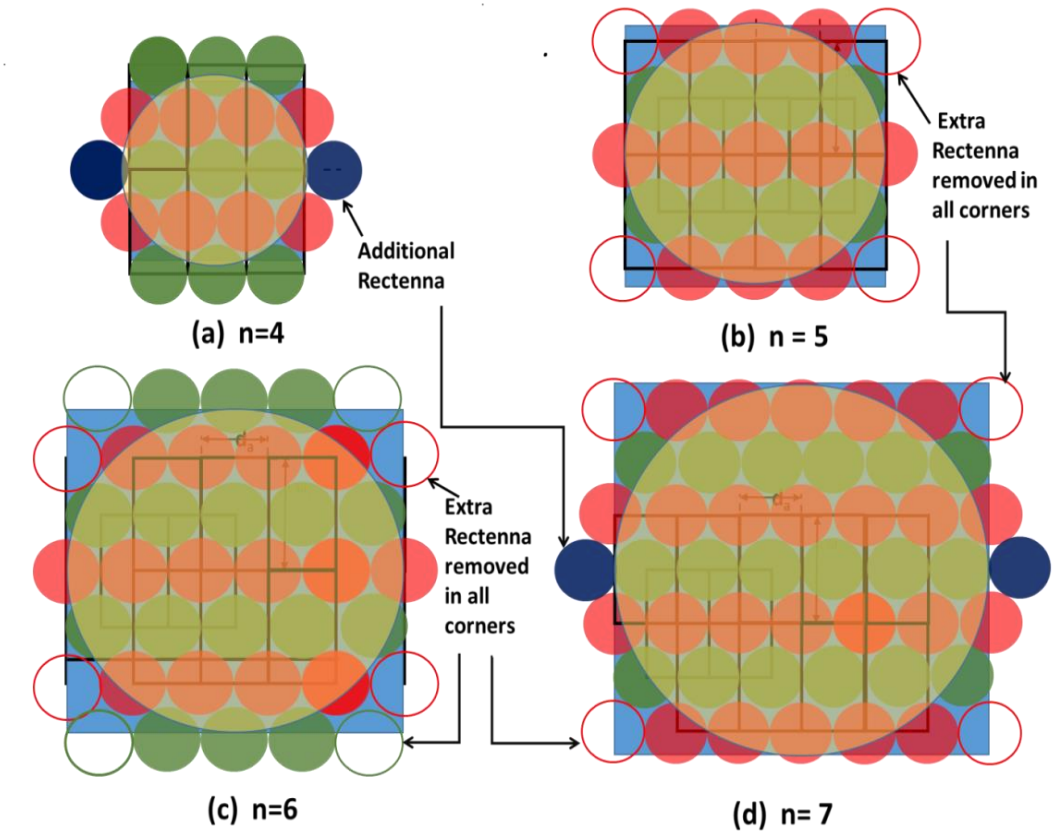

Figure 4-12: Rectenna arrangement in Grid-2hetero pattern for 4 different values of n, (a) n is 4, M_R is even and lesser than S_R, (Case 2), (b) n is 5, M_R is odd and greater than S_R, (Case 3), (c) n is 6, M_R is odd and lesser than S_R (Case 4) and (d) n is 7, M_R is even and greater than S_R, (Case 1)

. Number of active rectenna for Grid-2hetero will be different for each case based on value of M_R, S_R and K. As *RPUF* is directly proportional to active rectenna count, its value for the mentioned cases can be calculated using following equations.

Case 1

$$\mathrm{RPUF} = \frac{\mathrm{n} + 1 + (\mathrm{M_R} - 2)(2\mathrm{n} - 1) + \mathrm{K}}{\mathrm{TNR}} \tag{4-14}$$

Case 2:

$$RPUF = \frac{3n - 1 + (M_R - 2)(2n - 1) + K}{TNR} \tag{4-15}$$

Case 3:

$$RPUF = \frac{n + (M_R - 1)(2n - 1) + K}{TNR} \tag{4-16}$$

Case 4:

$$RPUF = \frac{3n - 2 + (M_R - 1)(2n - 1) + K}{TNR} \tag{4-17}$$

The *RPUF* graph for optimized Grid_2hetero is shown in Figure 4-13. It is observed that for odd number of rows in main Grid_2hetero it attains maximum value of *RPUF*, 1, i.e. value of unused power will be almost zero.

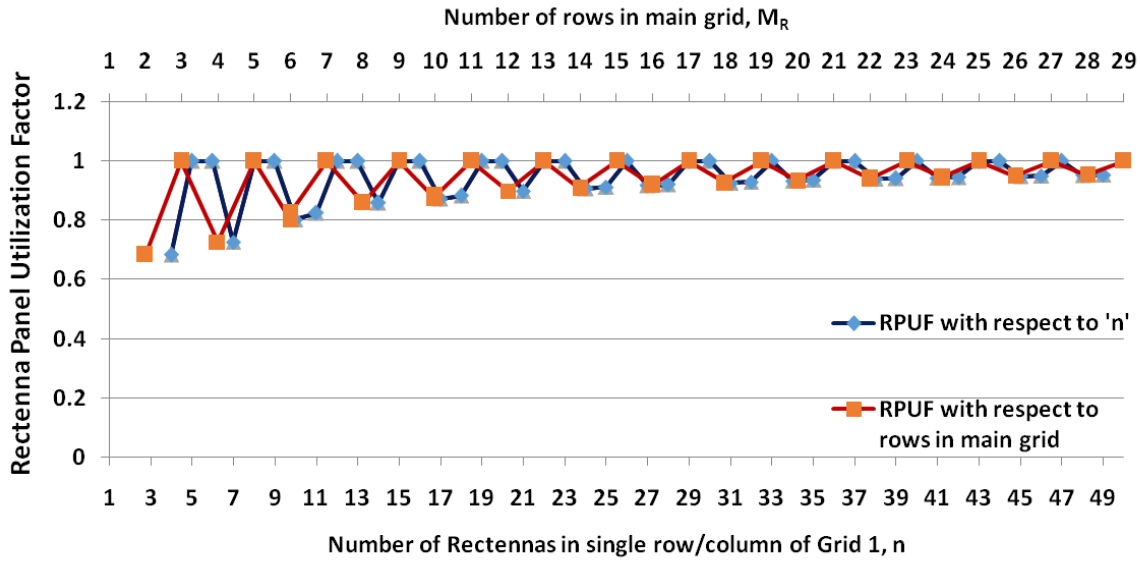

Figure 4-13: RPUF for Optimized Grid_2hetero design

4.2.2.4 Optimum rectenna arrangement pattern for panel design

TNR and *RPUF* plots for various grid configurations discussed in this section are displayed in Figure 4-14 and Figure 4-15 respectively. Comparison of Grid-3 and Grid-4 has been omitted as they are the compact version of Grid-1. It can be observed that optimized Grid_2hetero with hexagonal shape is able to attain highest RPUF value with the least number of rectenna.

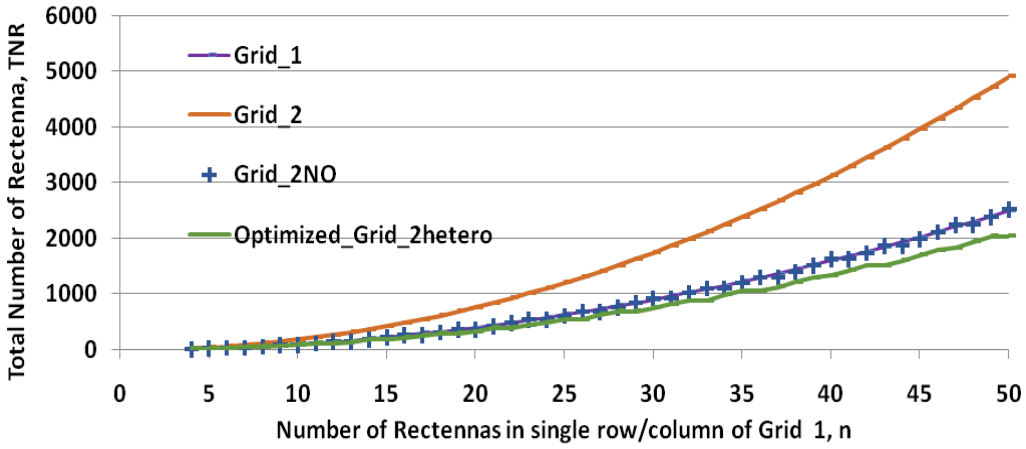

Figure 4-14: TNR value comparison for various Grid Configurations

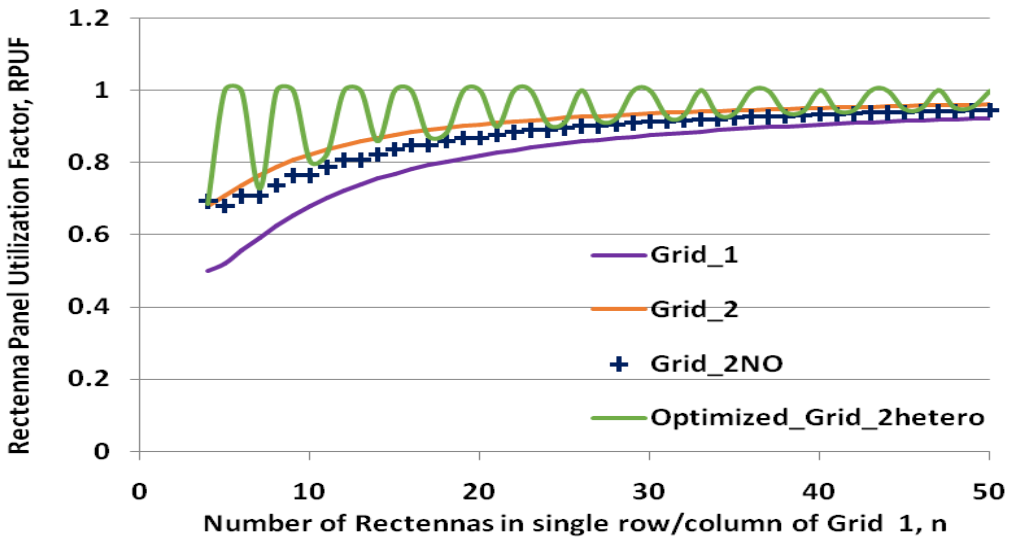

Figure 4-15: RPUF Comparison for various Grid Configurations

4.2.3 Developed Rectenna Panel

Based on theoretical investigation performed for optimum rectenna panel design in previous section, Grid-2hetro attains the highest *RPUF* with minimum number of *TNR*. However, to qualify the proposed Grid-2hetro pattern in terms of physical parameters a rectenna panel consisting of 5×10 rectennas was developed. The developed panel can generate power from 915 MHz RF signal. Different grid pattern has been analyzed and compared by the metric of the amount of electricity generated using this rectenna panel.

4.2.3.1 Panel features

The developed panel has two grids; they are referred as main grid and sub grid. The sub grid is placed at an offset from main grid. The main grid consists of three rows while sub grid has two rows. The number of column in both grid are same, they have 10 columns. Table 4-4, displays the developed panel dimension and rectenna spacing details. For the developed panel as shown in Figure 4-16, the M_R designates the main row and S_R designates the sub grid rows. The labels shown in the Figure 4-16 will be used for experimental observation recording. For the developed rectenna panel, jumper setting has been provided to manually connect rectenna in series and parallel as required. The fabricated panel with antenna is shown in Figure 4-17.

Table 4-4: Developed rectenna panel features

Parameter	Value
Panel size	36.2×32.8 cm^2
Column spacing for main and sub grid	2.8cm
Row spacing for main and sub grid	6.28cm
Offset for main and sub grid	1.4cm

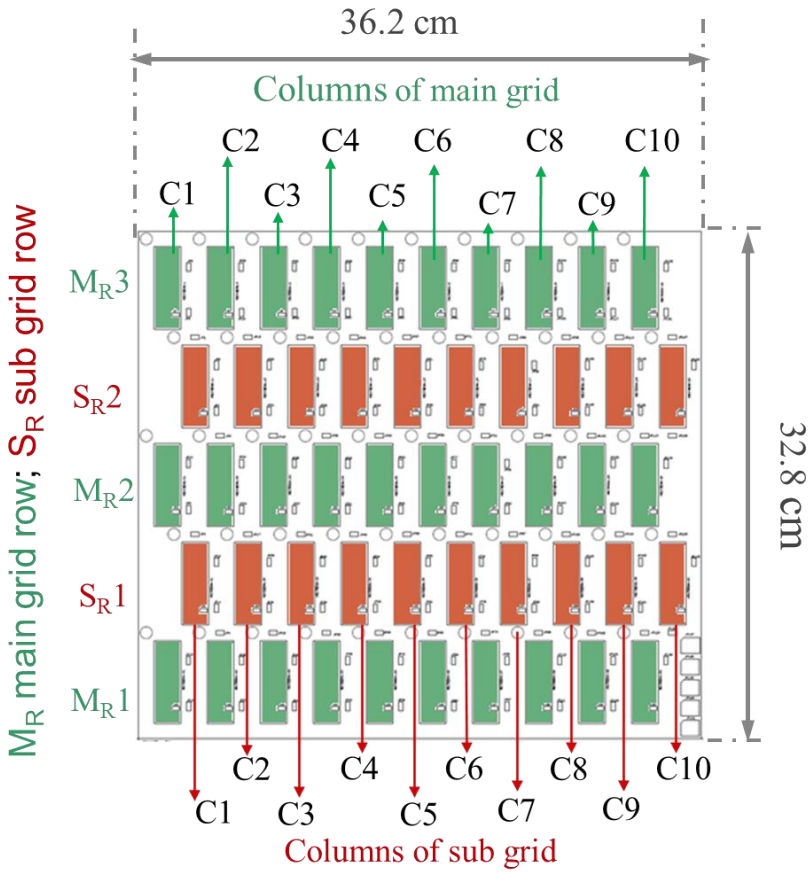

Figure 4-16: Row and column labeling for rectenna panel

Figure 4-17: Fabricated 5×10 *array rectenna panel with antenna*

4.3 EXPERIMENTS WITH DEVELOPED RECTENNA PANEL

Using a 915MHz, 4W RF source and developed rectenna panel two types of experiments were performed. The first experiment was to identify the best rectenna panel configuration, which generates maximum power with least number of rectenna. Second experiment was regarding performance evaluation of rectenna panel for varying distance from RF source. For both the experiments, the antenna used for rectenna was 2dBi dipole antenna and load was 3F super-capacitor. The mentioned capacitor when charged up-to 2V is sufficient to power the FFD consuming 30mW for 10secs. The capacitor charging time was recoded for both the experiments.

4.3.1 Identification of Best Rectenna Panel Configuration

Observations made for different rectenna connection configurations are presented in the following subsections. Evaluated patterns has been itemized by P.No (pattern number). The cells marked with √ are the rectenna connected in the panel and cell marked with × are unconnected rectenna. For better understanding and to mimic the actual arrangement of main grid and sub grid rows, in the observation table columns of main grid and sub grid are left justified and right justified respectively. The capacitor charging time (CCT) is recorded for each panel configuration. For this experiment, the connected rectennas of single row were connected in series while rows were connected in parallel. The panel was placed at the fixed distance of 1m from the RF source.

4.3.1.1 Observation 1

Observation made for all the column rectenna connected for different row combinations of main and sub grid is shown in Table 4-5.

Table 4-5: Observation 1: Rectenna panel load capacitor charging time (CCT) for different rectenna arrangements

P.No	Row No	Column No										CCT (s)
		C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	
P1	M_R3	×	×	×	×	×	×	×	×	×	×	130
	S_R2	×	×	×	×	×	×	×	×	×	×	
	M_R2	×	×	×	×	×	×	×	×	×	×	
	S_R1	×	×	×	×	×	×	×	×	×	×	
	M_R1	√	√	√	√	√	√	√	√	√	√	
P2	M_R3	×	×	×	×	×	×	×	×	×	×	120
	S_R2	×	×	×	×	×	×	×	×	×	×	
	M_R2	√	√	√	√	√	√	√	√	√	√	
	S_R1	×	×	×	×	×	×	×	×	×	×	
	M_R1	√	√	√	√	√	√	√	√	√	√	
P3	M_R3	√	√	√	√	√	√	√	√	√	√	110
	S_R2	×	×	×	×	×	×	×	×	×	×	
	M_R2	√	√	√	√	√	√	√	√	√	√	
	S_R1	×	×	×	×	×	×	×	×	×	×	
	M_R1	√	√	√	√	√	√	√	√	√	√	
P4	M_R3	×	×	×	×	×	×	×	×	×	×	145
	S_R2	×	×	×	×	×	×	×	×	×	×	
	M_R2	×	×	×	×	×	×	×	×	×	×	
	S_R1	√	√	√	√	√	√	√	√	√	√	
	M_R1	√	√	√	√	√	√	√	√	√	√	
P5	M_R3	×	×	×	×	×	×	×	×	×	×	140
	S_R2	×	×	×	×	×	×	×	×	×	×	
	M_R2	√	√	√	√	√	√	√	√	√	√	
	S_R1	√	√	√	√	√	√	√	√	√	√	
	M_R1	√	√	√	√	√	√	√	√	√	√	
P6	M_R3	×	×	×	×	×	×	×	×	×	×	142
	S_R2	√	√	√	√	√	√	√	√	√	√	
	M_R2	√	√	√	√	√	√	√	√	√	√	
	S_R1	√	√	√	√	√	√	√	√	√	√	
	M_R1	√	√	√	√	√	√	√	√	√	√	
P7	M_R3	√	√	√	√	√	√	√	√	√	√	150
	S_R2	√	√	√	√	√	√	√	√	√	√	
	M_R2	√	√	√	√	√	√	√	√	√	√	
	S_R1	√	√	√	√	√	√	√	√	√	√	
	M_R1	√	√	√	√	√	√	√	√	√	√	

4.3.1.2 Observation 2

Observation made for alternate column rectenna connected for different row combinations of main and sub grid is shown in Table 4-6.

Table 4-6: Observation 2: Rectenna panel load capacitor charging time (CCT) for different rectenna arrangements

P.No	Row No	Column No										CCT (s)
		C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	
P1	M_R3	×	×	×	×	×	×	×	×	×	×	125
	S_R2	×	×	×	×	×	×	×	×	×	×	
	M_R2	×	×	×	×	×	×	×	×	×	×	
	S_R1	×	×	×	×	×	×	×	×	×	×	
	M_R1	√	×	√	×	√	×	√	×	√	×	
P2	M_R3	×	×	×	×	×	×	×	×	×	×	116
	S_R2	×	×	×	×	×	×	×	×	×	×	
	M_R2	√	×	√	×	√	×	√	×	√	×	
	S_R1	×	×	×	×	×	×	×	×	×	×	
	M_R1	√	×	√	×	√	×	√	×	√	×	
P3	M_R3	√	×	√	×	√	×	√	×	√	×	100
	S_R2	×	×	×	×	×	×	×	×	×	×	
	M_R2	√	×	√	×	√	×	√	×	√	×	
	S_R1	×	×	×	×	×	×	×	×	×	×	
	M_R1	√	×	√	×	√	×	√	×	√	×	
P4	M_R3	×	×	×	×	×	×	×	×	×	×	130
	S_R2	×	×	×	×	×	×	×	×	×	×	
	M_R2	×	×	×	×	×	×	×	×	×	×	
	S_R1	√	×	√	×	√	×	√	×	√	×	
	M_R1	√	×	√	×	√	×	√	×	√	×	
P5	M_R3	×	×	×	×	×	×	×	×	×	×	133
	S_R2	×	×	×	×	×	×	×	×	×	×	
	M_R2	√	×	√	×	√	×	√	×	√	×	
	S_R1	√	×	√	×	√	×	√	×	√	×	
	M_R1	√	×	√	×	√	×	√	×	√	×	
P6	M_R3	×	×	×	×	×	×	×	×	×	×	133
	S_R2	√	×	√	×	√	×	√	×	√	×	
	M_R2	√	×	√	×	√	×	√	×	√	×	
	S_R1	√	×	√	×	√	×	√	×	√	×	
	M_R1	√	×	√	×	√	×	√	×	√	×	
P7	M_R3	√	×	√	×	√	×	√	×	√	×	138
	S_R2	√	×	√	×	√	×	√	×	√	×	
	M_R2	√	×	√	×	√	×	√	×	√	×	
	S_R1	√	×	√	×	√	×	√	×	√	×	
	M_R1	√	×	√	×	√	×	√	×	√	×	

4.3.1.3 Observation 3

Observation shown in Table 4-7 is made by connecting every third column rectenna and increasing the offset for main and sub grid by one rectenna.

Table 4-7: Observation 3: Rectenna panel load capacitor charging time (CCT) for different rectenna arrangements

P.No	Row No	Column No										CCT (s)
		C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	
P1	M_R3	×	×	×	×	×	×	×	×	×	×	140
	S_R2	×	×	×	×	×	×	×	×	×	×	
	M_R2	×	×	×	×	×	×	×	×	×	×	
	S_R1	×	×	×	×	×	×	×	×	×	×	
	M_R1	√	×	×	√	×	×	√	×	×	√	
P2	M_R3	×	×	×	×	×	×	×	×	×	×	120
	S_R2	×	×	×	×	×	×	×	×	×	×	
	M_R2	√	×	×	√	×	×	√	×	×	√	
	S_R1	×	×	×	×	×	×	×	×	×	×	
	M_R1	√	×	×	√	×	×	√	×	×	√	
P3	M_R3	√	×	×	√	×	×	√	×	×	√	80
	S_R2	×	×	×	×	×	×	×	×	×	×	
	M_R2	√	×	×	√	×	×	√	×	×	√	
	S_R1	×	×	×	×	×	×	×	×	×	×	
	M_R1	√	×	×	√	×	×	√	×	×	√	
P4	M_R3	×	×	×	×	×	×	×	×	×	×	125
	S_R2	×	×	×	×	×	×	×	×	×	×	
	M_R2	×	×	×	×	×	×	×	×	×	×	
	S_R1	×	√	×	×	√	×	×	√	×	×	
	M_R1	√	×	×	√	×	×	√	×	×	√	
P5	M_R3	×	×	×	×	×	×	×	×	×	×	100
	S_R2	×	×	×	×	×	×	×	×	×	×	
	M_R2	√	×	×	√	×	×	√	×	×	√	
	S_R1	×	√	×	×	√	×	×	√	×	×	
	M_R1	√	×	×	√	×	×	√	×	×	√	
P6	M_R3	×	×	×	×	×	×	×	×	×	×	79
	S_R2	×	√	×	×	√	×	×	√	×	×	
	M_R2	√	×	×	√	×	×	√	×	×	√	
	S_R1	×	√	×	×	√	×	×	√	×	×	
	M_R1	√	×	×	√	×	×	√	×	×	√	
P7	M_R3	√	×	×	√	×	×	√	×	×	√	70
	S_R2	×	√	×	×	√	×	×	√	×	×	
	M_R2	√	×	×	√	×	×	√	×	×	√	
	S_R1	×	√	×	×	√	×	×	√	×	×	
	M_R1	√	×	×	√	×	×	√	×	×	√	

4.3.1.4 Observation 4

CCT value for Grid2_NO, Grid_2hetero and optimized Grid_2hetero (hexagonal shape panel) is shown in Table 4-8.

Table 4-8: Observation 4: Rectenna panel load capacitor charging time (CCT) for Grid2_NO, Grid_2hetero and optimized Grid_2hetero configurations

Grid	Row No	Column No										CCT (s)
		C11	C12	C13	C14	C15	C16	C17	C18	C19	C20	
Grid-2_NO	M_R3	√	×	×	×	√	×	×	×	√	×	135
	S_R2	×	×	×	×	×	×	×	×	×	×	
	M_R2	×	×	√	×	×	×	√	×	×	×	
	S_R1	×	×	×	×	×	×	×	×	×	×	
	M_R1	√	×	×	×	√	×	×	×	√	×	
Grid_2hetero	M_R3	√	×	×	√	×	×	√	×	×	√	70
	S_R2	×	√	×	×	√	×	×	√	×	×	
	M_R2	√	×	×	√	×	×	√	×	×	√	
	S_R1	×	√	×	×	√	×	×	√	×	×	
	M_R1	√	×	×	√	×	×	√	×	×	√	
Optimized Grid_2hetero variant 1	M_R3	×	×	×	√	×	×	√	×	×	×	70
	S_R2	×	√	×	×	√	×	×	√	×	×	
	M_R2	√	×	×	√	×	×	√	×	×	√	
	S_R1	×	√	×	×	√	×	×	√	×	×	
	M_R1	×	×	×	√	×	×	√	×	×	×	
Optimized Grid_2hetero variant 2	M_R3	×	×	√	×	√	×	√	×	√	×	55
	S_R2	×	×	×	×	×	×	×	×	×	×	
	M_R2	×	√	×	√	×	√	×	√	×	√	
	S_R1	×	×	×	×	×	×	×	×	×	×	
	M_R1	×	×	√	×	√	×	√	×	√	×	

4.3.1.5 Discussions

From the observations shown in Table 4-5 to Table 4-8, panel specification table, Table 4-4 and considering the physical length of antenna used for experimentation following inferences can be drawn:

1) Even though, the rectenna count is more for Observation-1, due to increased aperture overlap along row and column rectenna, degradation in panel performance is observed. With respect to single row connected pane (P1)l, for fully connected rectenna panel(P7) 15% degradation in capacitor charging rate is observed.

2) The elimination of alternate rectenna in Observation-2 resulted in improvement in charging time. However, aperture overlap of sub grid and main grid rectenna did not permit charging time to improve more than 8% with respect to fully connected rectenna configuration (P7 row of observation 1 and 2)

3) Panel configuration used for Observation-3 has mitigated the aperture overlap issue by providing the enough separation between adjacent, vertical and sub-grid rectenna. With respect to P7 pattern of Observation-1, 73% improvement in charging time is observed for P7 pattern of Observation-3. Hence, aperture overlap plays a significant role in degrading rectenna performance.

4) From Observation-4, performance for Grid2_NO is poor due to less rectenna count. In comparison to pattern P3 of Observation-3, it does not have any aperture overlap; to increase its performance rectenna panel size need to be scaled up.

5) Grid_2hetero configuration of Observation-4 corresponds to P7 pattern of Observation-3. It can be observed that optimized Grid_2hetero variant-1(highlighted pattern) has same CCT value as of Grid_2hetero. Hence, corner rectenna are not significant and can be eliminated.

6) Optimized Grid_2hetero variant-2 (highlighted pattern) has less number of rectenna count compared to variant-1, but it charges the load capacitor in least time. This improvement may be due to reduced coupling between the rectenna.

The CCT performance graph for different rectenna arrangement pattern has been depicted in Figure 4-18. From this graph, it can be envisaged that optimum rectenna count results in least CCT value and it is highly dependent on arrangement pattern. Thus, the cost of rectenna panel, which is directly proportional to rectenna count, is governed by the tradeoff between CCT and arrangement pattern.

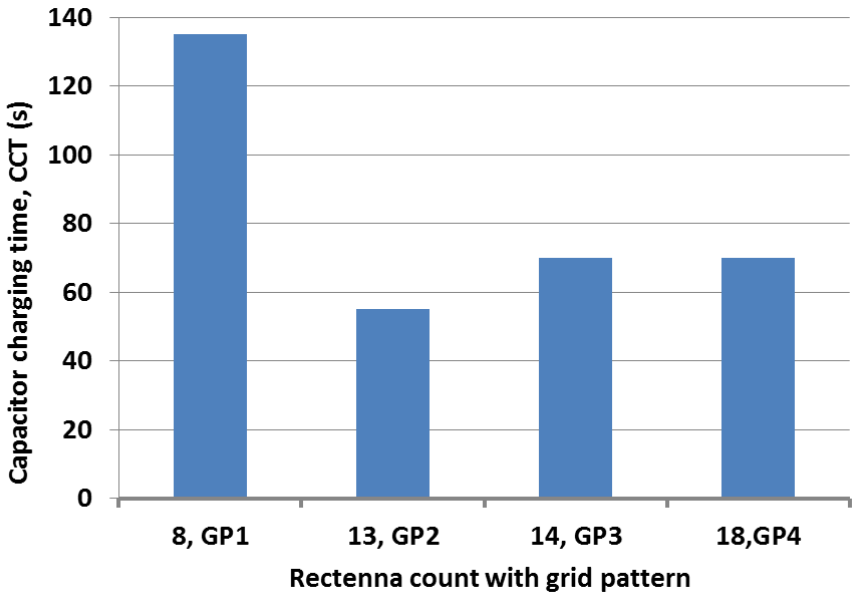

Figure 4-18: CCT performance curve for different rectenna arrangement pattern evaluated in Table 4-8. Here GP1 is Grid2_NO, GP2 is Grid_2hetero, GP3 is Optimized Grid_2hetero variant1 and GP4 is Optimized Grid_2hetero variant2

4.3.2 Performance Evaluation of Rectenna Panel for Varying Distance

The aim of this experiment was to observe how the performance of rectenna panel changes with increasing distance from RF source. This test was performed for Grid-2hetero variant-2 pattern. The first set of observation, shown in Table 4-9, was made by measuring the CCT for varying distance without connecting WSN device load. In this experiment for every distance, initially load capacitor was made completely discharged, and then the time required for capacitor to charge up to its full capacity was recorded.

Table 4-9: Performance evaluation of optimized rectenna panel with varying distance

Rectenna panel distance from RF source (m)	Load capacitor charging time
1	< 1min
5	8min
10	20min

20	45min
40	1.75hr
80	4hr
120	10hr

In the second part of the experiment, the XBee- pro (S2C) based device configured in FFD mode was connected as load to the panel. As per XBee-pro datasheet, it can operate with supply of 1.8V with 35mA. For this WSN device, a capacitor charged with 2.0 V allows it to operate continuously for 10sec until the capacitor voltage drops to 1.7V. Thus, for this experiment, the capacitor was not allowed to discharge below 1.7V and the WSN device was electrically connected to the panel only when capacitor voltage reaches to 2.0V. Hence, effectively the capacitor has to charge for 300mV only for varying distance. The time required to boost the capacitor voltage by 300mV for varying distance is shown in Table 4-10.

Table 4-10: Rectenna panel as voltage booster for varying distance

Rectenna panel distance from RF source (m)	**Time required to boost capacitor voltage by 300mV**
1	1s
5	40s
10	3min
20	5min
40	12min
80	25min
120	~1hr

The inferences drawn from the rectenna panel performance evaluation experiment are enumerated below:

1) The optimized Grid_2hetero panel takes long time for charging a completely discharged capacitor to its full capacity but takes minimal time to deliver the required power to the node if storage capacitor is not allowed to drain completely.

2) Rectenna panel can be used to maintain the network but may result in high dead time when used to startup a completely drained network.

4.4 VALIDATION OF RECTENNA PANEL DESIGN APPROACH

Validation of the developed rectenna panel design model, has been performed with existing rectenna panel designs used in literature and with experimental analysis performed in this Chapter.

In the work [85], the author has done analysis on optimizing rectenna spacing. Researchers of artifact [86], have designed panel by arranging rectenna in a honeycomb pattern with aperture overlap. Similarly, authors of [87], have designed rectenna panel with aperture overlap and fixed rectenna spacing of $\lambda/2$. For design validation, as shown in Table 4-11, a detailed comparison of various grid patterns discussed in this Chapter with experimental study and abovementioned works has been performed. . *TNR* for panel developed in [86] and [87] was not mentioned implicitly in their research work. Based on their design approach, *TNR* value for both the references has been deduced.

Table 4-11: Comparison with existing rectenna panel design work available in literature

Reference	Rectenna Spacing	Rectenna Arrangement pattern	Total Number of Rectenna (TNR)	Analogy with our analysis
[85]	≤ 0.7 λ	Square Grid pattern	n^2	**Grid -1**, It matches with our design analysis, as in our case rectenna spacing for rectenna with gain 1 and 100% efficiency will be 0.3 λ
[86]	Derived from antenna **physical aperture**	Square grid with Honeycomb pattern and rectenna aperture overlap	$n^2 + (n+1)^2$ TNR, value has been deduced from their work. Authors have mentioned in their work that to harvest power from scattered RF waves the developed panel has an extra row and column than the required size. So, value of n used for TNR calculation is $n+1$	**Grid-2**, as rectenna placement pattern is same.
[87]	0.5 λ	Square grid with Honeycomb pattern and rectenna aperture overlap	$n^2 + (n+1)^2$ TNR, value has been deduced from their work. Authors have mentioned in their work that to harvest power from scattered RF waves the developed panel has an extra row and column than the required size. So, value of n used for TNR calculation is $n+1$.	**Grid-2**, as rectenna placement pattern is same.
This work Design, Grid-2heteo	Derived from rectenna **effective aperture**	Hexagonal grid structure with rectenna placement on vertices of equilateral triangle.	From equation (4-12) and (4-13)	Not required

The important findings for comparative validation are listed below:

1) Square grid pattern used by authors of [85] matches with this work Grid-1 design. Authors of this paper have experimentally verified that if rectenna spacing is more than 0.7λ than the rectenna panel efficiency degrades. The equation (4-4), presented

in this Chapter for calculating non-overlap rectenna spacing abides by their experimental results. Also as per experimentation, for Grid2_NO CCT is more compared to single row rectenna panel. Even though for Grid_2NO rectenna spacing is ~0.4λ, it is certain that with further increase in rectenna spacing rectenna performance will degrade.

2) The honeycomb panel pattern with aperture overlap used by authors in [86], [87], is comparable to Grid-2 layout described in this Chapter. The pattern used in these works has not been experimentally compared with any other rectenna panel design. Grid-2 pattern of this work corresponds to P7 pattern of Observation-1. Based on experimental evaluation, aperture overlap degrades the panel performance.

3) Even though the honeycomb pattern discussed in literature appears to be same as hexagonal grid proposed in this work, their developed panel is a **square-shaped grid** with a **honeycomb** pattern. While optimized Grid-2hetero is **hexagonal shape grid**, it eliminates all the unused rectenna present at the corners of the square shape grid.

With this validation study, it can be concluded that the mathematical formulation developed in this work can be used to design rectenna panel of any size. Moreover, the proposed optimized Grid-2hetero is optimal from existing designs used in the literature concerning the total number of rectenna, rectenna utilization, and power void elimination.

4.5 INTEGRATED TESTING OF DEVELOPED SECURED BACKSCATTER TAG WITH RECTENNA PANEL

The power consumption of developed secured backscatter based WSN (SBWSN) node and backscatter tag during continuous active and switching mode operation is shown in Table 4-12. The switching mode cycle repeats after every one

second and during this mode, the SBWSN is made active for 10ms to transmit its data and then remains in power down state until next cycle begins. As mentioned in Chapter 3, for development purpose the controller used for SBWSN node design is LPC1768. Even though the power consumption of LPC1768 is high during active mode (3V@50mA), its current consumption during power down mode is very low, 530nA. Considering the SBWSN power consumption, integrated testing with rectenna and optimized rectenna panel was performed. The various experiments performed are explained in following subsections.

Table 4-12: Power requirement for secured backscatter WSN (SBWSN) node and its major components

Type of Device	Continuous active mode	Switching mode
Backscatter tag	4.8mW	3μW
LPC1768 controller	150.0mW	1.5mW
SBWSN node	154.8mW	1.503mW

4.5.1 Interfacing of Backscatter Tag with Rectenna

As discussed in Chapter 3, the developed backscatter tag is capable to generate DC power when connected to RF to DC converter. Hence, to quantify the amount of power generated during idle mode of backscatter tag feature, the tag was interfaced with the developed rectenna as shown in Figure 4-19. Even though the rectenna interfaced with backscatter tag was designed for 915MHz, it was able to generate the DC power from 2.45GHz RF signal. The RF signal losses due to cable and impedance mismatch were not accounted in this testing. For this testing, controller of SBWSN node was not powered by the power generated from backscatter coupled rectenna. The SBWSN node was able to backscatter the data when its tag was having sufficient

power. Table 4-13, displays the data transmission interval for rectenna powered SBWSN node.

Table 4-13: SBWSN node, data transmission interval for rectenna powered tag

Rectenna powered SBWSN node distance from RF source (m)	SBWSN node data transmission interval
0.3	10min
1	~1hr

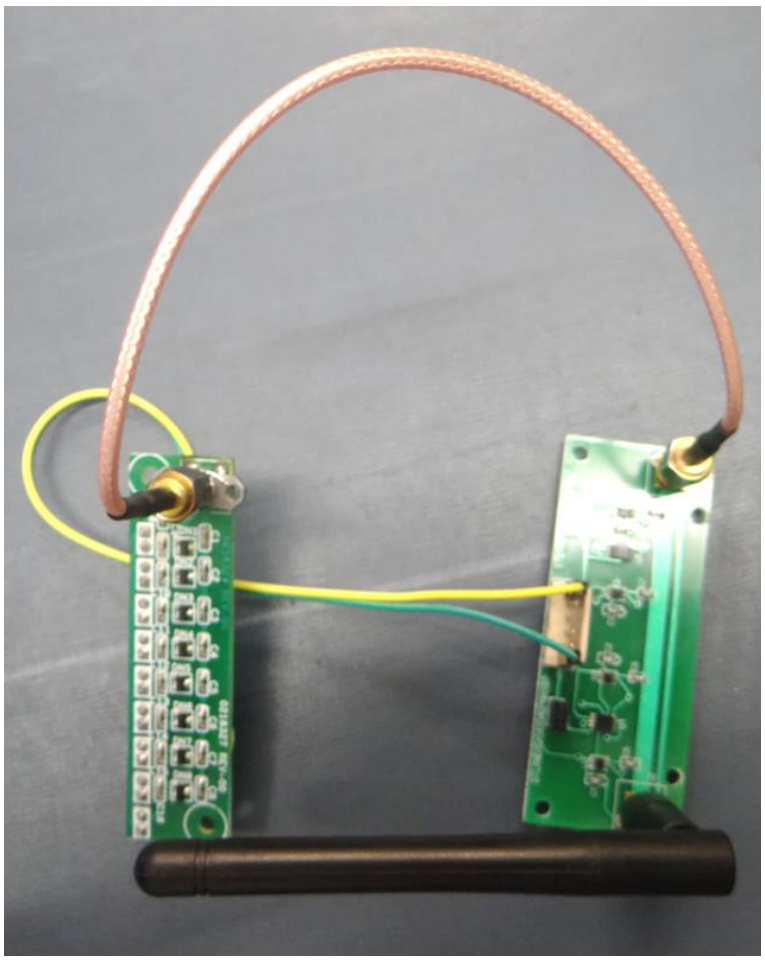

Figure 4-19: Interfacing of backscatter tag with rectenna

The inference drawn from this testing is that the he developed backscattered tag with rectenna setup is able to operate in dual mode, i.e. it can backscatter the data and generate DC power. The data transmission interval can be reduced if rectenna and tag layout are integrated on same PCB with proper impedance matching.

4.5.2 Interfacing of Backscatter Tag with Rectenna Panel

For this experiment, only the backscatter tag of SBWSN node was powered with rectenna panel while its controller was operating with mains operated 12V regulated DC power supply. For this testing, the SBWSN node was placed at the distance of 120m indoor from RF source. The observation made are tabulated in Table 4-14.

Table 4-14: SBWSN node, data transmission interval for rectenna panel powered tag

SBWSN node operation mode	SBWSN node data transmission interval
Switching at 1sec interval for 10ms	1sec
Continuous switching	10min

The SBWSN node is able to transmit the data at its defined switching rate when optimized Grid_2hetero panel is powering the tag. Further, the analysis was extended to optimize the rectenna size for optimized Grid_2hetero variant-1& 2. As shown in Table 4-15, the SBWSN node was able to operate with its defined switching rate even for reduced panel size consisting of 10 rectennas (O_P1 and O_P2 of Table 4-15). However, with further reduction of size, delay in data transmission interval was observed (O_P3 and O_P4 of Table 4-15).

Table 4-15: Rectenna panel size optimization for backscatter tag

Optimized panel	Rows	Columns										SBWSN node data transmission interval
		C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	
O_P1 Optimized Grid_2hetero Variant- 1	**M_R3**	×	×	×	×	×	×	×	×	×	×	1sec
	S_R2	×	√	×	×	√	×	×	√	×	×	
	M_R2	√	×	×	√	×	×	√	×	×	√	
	S_R1	×	√	×	×	√	×	×	√	×	×	
	M_R1	×	×	×	×	×	×	×	×	×	×	
O_P2 Optimized Grid_2hetero variant -2	**M_R3**	×	×	√	×	√	×	√	×	×	×	1sec
	S_R2	×	×	×	×	×	×	×	×	×	×	
	M_R2	×	√	×	√	×	√	×	√	×	×	
	S_R1	×	×	×	×	×	×	×	×	×	×	
	M_R1	×	×	√	×	√	×	√	×	×	×	
O_P3 Optimized Grid_2hetero Variant- 1	**M_R3**	×	×	×	×	×	×	×	×	×	×	5sec
	S_R2	×	×	×	×	√	×	×	√	×	×	
	M_R2	×	×	×	√	×	×	√	×	×	√	
	S_R1	×	×	×	×	√	×	×	√	×	×	
	M_R1	×	×	×	×	×	×	×	×	×	×	
O_P4 Optimized Grid_2hetero variant -2	**M_R3**	×	×	×	×	√	×	√	×	×	×	5sec
	S_R2	×	×	×	×	×	×	×	×	×	×	
	M_R2	×	×	×	√	×	√	×	√	×	×	
	S_R1	×	×	×	×	×	×	×	×	×	×	
	M_R1	×	×	×	×	√	×	√	×	×	×	

4.5.3 Interfacing of Secured Backscatter based WSN Node with Rectenna Panel

This experiment was performed for SBWSN node configured with sleep state. The sleep cycle was of 1sec with wake up period of 10ms for transmitting the backscattered data. In this experiment, the optimized rectenna panel powered both controller and tag. As shown in Table 4-16, the SBWSN node was able to transmit at its defined rate when placed at the distance of 70m from RF source. With increase of distance to 120m, delay in data transmission rate was observed. Hence, a SBWSN node designed with an ultra-low power controller will be able to operate at the distance of 120m.

Table 4-16: SBWSN node, data transmission interval for rectenna powered node

Rectenna powered SBWSN node distance from RF source (m)	SBWSN node data transmission interval
70	1sec
120	>1min

4.6 SUMMARY

This Chapter explores the capabilities of RF wave to wirelessly power the WSN node. Considering the poor RF energy density, it is highlighted that with reduction of WSN node power requirement, the rectenna panel based technique should be used for wireless power application. To design the efficient rectenna panel, the methodology for optimizing rectenna panel parameters has been developed. Further, the developed methodology has been validated by experimental evaluation. The integrated testing of the developed secured backscatter based WSN node with optimized rectenna panel has also been performed.

The important findings of this Chapter are enumerated below:

1) The hexagonal shape pattern designed with triangulation placement and rectenna spacing is governed by the effective aperture of antenna, then the rectenna panel will be able to intercept maximum RF signal with minimum number of rectenna. Also, the cost of rectenna panel, which is directly proportional to rectenna count, is governed by the tradeoff between storage CCT and rectenna arrangement pattern.

2) This work demonstrates that rectenna panel can be used for network sustenance, if its storage capacitor are not allowed to discharge below its threshold. The power demand for resource constrained devices are in microwatt scale, which can be easily delivered though wireless power in couple of seconds. A completely drained 3F

super capacitor take more than 10hrs to charge to 2V at the distance of 120m far-field while to boost 300mV for partially charged capacitor it take less than 1hr time.

3) The SBC based WSN node is able to transmit the data at the interval of 1sec when wirelessly powered through hexagonal shape rectenna panel consisting of only 10 rectennas. The RF source was placed at the distance of 70m indoor from SBWSN node and was radiating 4W. The radiated power is within the emission limit defined by ICNIRP.

CHAPTER 5

Conclusion & Future Works

The present chapter summarizes the research work carried out for sustainable secure wireless monitoring system design. The conclusions derived from this study are briefly outlined. Further, the scope for future works in this field is also highlighted.

5.1 CONCLUSION

The past few years have seen dramatic growth in wireless-based monitoring in military, industrial and health sector. However, the growth of secured wireless monitoring for inaccessible zone/scenario faces three pressing challenges: security, power consumption, and battery energy density. The compute-intensive cryptographic based security protocols demand high processing and power from resource-constrained WSN device. Wireless communication consumes more energy than computation, storage or sensing. Hence, integration of security with radio communication in battery-operated WSN is a bottleneck for sustainable secure wireless monitoring required for long-lived inaccessible zone monitoring.

This research aimed to identify and implement novel strategies for designing a secured wireless monitoring network for resource-constrained applications. In this work, the domain of underutilized secure backscatter communication (SBC) has been explored for WSN inaccessible zone monitoring applications. Considering the ad-hoc nature of WSN, a novel obfuscation technique for M-ary spread spectrum (MaSS) has been proposed. For establishment of backscatter communication in WSN technology, a novel quad phase keying backscatter tag has been designed and developed. This tag

backscatters the incoming RF signal with desired phase by allowing the short-circuit load to float over the straight-line microstrip track. Further, to leverage the battery issue, a rectenna panel-based approach has been introduced to power the nodes wirelessly.

Following are the significant contributions of this work:

1) The developed WSN security technique waives off the computation overhead of the cryptographic algorithms and hardware overhead of existing physical layer security techniques. This work proposes an outstanding technique for implementing the obfuscated MaSS. It highlights that by obfuscating mapping sequence of MaSS, eavesdropping can be inhibited. The proposed technique demands a single security key per node. Even though the key length required for this obfuscation scheme is not 128bit long, its mapping attribute disguises the eavesdroppers to accept invalid packet as valid detection (Figure 2-5,Table 2-7, Table 2-8). This advantage is expected to revive the future of MaSS based PHY security, which got buried in literature due to the requirement of M secret keys per device.

2) In the domain of backscatter technology, the noteworthy contribution made by this research is that it resolves the pressing issue in backscatter technology, which demands tradeoff between energy harvesting and wireless communication data rate. The floating load based straight-line microstrip transmission line used for phase modulation does not work in power split mode for establishing communication and generating energy. The developed microstrip track is dual port transmission line, this facilitates to receive incoming RF and backscatter it from the first port while other port is used for RF harvesting during active and idle mode of the tag. The non-reflected RF signal governed by switching-off of RF switches due to frequency

translation scheme is utilized for energy harvesting during active mode. During idle mode, i.e. absence of backscatter switching, all the incoming power is utilized by harvesting circuit. In addition, the developed backscatter tag consumes 5000 times less power than conventional WSN transmitter and it can be used as a frequency router (Table 3-4) between networks operating at different channel frequency. The developed WSN BT tag is able to mitigate in-band interference, maintain the compatibility and desired throughput without incurring power penalty.

3) RF power disperses in space as it propagates, thus, to aggregate the dispersed RF power, rectenna panel-based spatial RF power sampling has been introduced to power the WSN nodes wirelessly. In the domain of RF power generation, for the first time, this work presents a novel methodology for efficient panel design. The developed model optimizes the rectenna spacing, count, and arrangement pattern, further it proposes a hexagonal shape rectenna panel for wireless power generation (Figure 4-12,Figure 4-13). The panel design framework presented in this work is generic and can be used for any application that requires a far-field wireless power solution. Further, experimentally it has been verified that far-field wireless power generated through optimized RF rectenna panel is sufficient for sustenance of SBC based WSN monitoring extending up to the distance of 70m from RF source (Table 4-16).

Overall, the wirelessly powered secure backscatter based WSN approach presented in this thesis, facilitates the wireless power generation in far field, and allows the sensor device to backscatter its data securely without violating the radiation emission limits set by the International Commission on Non-Ionizing Radiation Protection (ICNIRP).

5.2 SOCIETAL IMPACT OF THIS WORK

The vision of this thesis was to propose a sustainable secure wireless monitoring system for inaccessible are monitoring in the domain of healthcare sector, nuclear sector and disaster management. The wirelessly powered secure backscatter communication based WSN is capable of meeting the requirements of inaccessible area monitoring technically has been demonstrated in this work. However, for healthcare application, a miniaturized device with body-friendly materials needs to be designed. Whereas for the nuclear sector applications, radiation hardening of the developed hardware is required. For the scenario of disaster management, a commercial product developed based on the designs and methodology presented in this work will suffice the application requirement. Above all, concerning health safety, the significant impacts of the developed system on the society are enumerated below:

1) In the domain of health sector, the zero overhead security scheme presented in this work will be very much useful, to ensure the security of wireless implants. The implants equipped with the SBWSN node, can perform their desired medical functioning without being detected inadvertently. These SBWSN implants will transmit their parameter status only when triggered by external RF source. Even though the unauthorized RF signal is transmitted to them, SBWSN will transmit the PHY obfuscated frame. In addition, considering the body attenuation factor of 0.5dB/cm to 2.9dB/cm [131] and round trip loss for backscattered signal the SNR received by eavesdropper will be less than -1dB. Hence, it is difficult for an attacker to eavesdrop the implant data.

2) In the domain of nuclear sector, concerning the adverse effects of ionizing radiation, human based process monitoring is prohibited in the zones that involve high radiation dose. For illustration, after Fukushima Daiichi Nuclear Power Station

accident, machinery survey was required for primary containment vessel. The entrance towards machinery zone had the radiation level of 20mSv/hr. However, 20mSv is the allowable dose for operational worker for a year, hence, considering the human safety factor the maintenance was performed though human assisted robotic device. In that scenario, it was ensured human does not stay in that high radiation zone for more than 3minutes. However, safety was at risk. Thus, in such application or for various long-term fuel-processing tasks, human exposure to radiation dose can be eliminated by deploying the wirelessly powered SBWSN. By integrating the control action with SBWSN, these battery-less devices can be used for any monitoring and maintenance task.

5.3 FUTURE WORK

The thesis has provided experimental insight on the design of the sustainable secure wireless monitoring system, but for deployment of such a system, further research needs to be pursued in the following aspects:

1) The strength of a security protocol depends on its implementation approach and key management technology. RF channel impairment-based key generation technology is gaining importance in wireless cryptography. The mentioned key generation approach generates a unique key for every link. If such link dependent key generation technique is used for obfuscating the spread spectrum, it would increase the complexity of eavesdropper. Hence, implementation and integration of PHY based key generation technique with the developed PHY security scheme will be an interesting research problem. Further, analysis and quantification of the eavesdropper complexity can be carried out to evaluate the security capacity of the developed scheme.

2) The developed backscatter tag can translate the frequency channel. This feature of the tag can be explored for frequency band translation. Band translation feature will be useful against most aggressive physical layer attack, such as jamming attack. On detection of the powerful jamming signal, the legitimate nodes can translate and backscatter the jamming signal for attack indication or data communication.

3) The investigations carried out on wireless power generation were done with the assumption that an intentionally radiated RF source is present in space. In the absence of intentionally radiated directional RF source, ambient radiations can be considered as an anisotropic source; hence, further study to design a rectenna panel for such scenario can be taken up.

REFERENCES

[1] C. Buratti, A. Conti, D. Dardari, and R. Verdone, "An overview on wireless sensor networks technology and evolution," *Sensors*, vol. 9, no. 9, pp. 6869–6896, 2009.

[2] A. Ali, Y. Ming, S. Chakraborty, and S. Iram, "A comprehensive survey on real-time applications of WSN," *Futur. Internet*, vol. 9, no. 4, 2017.

[3] H. Ghayvat, S. C. Mukhopadhyay, X. Gui, and J. Liu, "Enhancement of WSN based smart home to a smart building for assisted living: Design issues," *Proc. - 2015 5th Int. Conf. Commun. Syst. Netw. Technol. CSNT 2015*, pp. 219–224, 2015.

[4] S. Oh, "The vehicle location tracking system using wireless network," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 4352 LNCS, no. PART 2, pp. 651–661, 2007.

[5] A. Baggio, "Wireless Sensor Network in Precision Agriculture," in *Workshop on Real-World Wireless Sensor Networks. REALWSN'05*, 2005, vol. Stockholom.

[6] L. Ruiz-Garcia, L. Lunadei, P. Barreiro, and J. I. Robla, "A review of wireless sensor technologies and applications in agriculture and food industry: State of the art and current trends," *Sensors (Switzerland)*, vol. 9, no. 6, pp. 4728–4750, 2009.

[7] R. I. Gomaa, I. A. Shohdy, K. A. Sharshar, A. S. Al-Kabbani, and H. F. Ragai, "Real-time radiological monitoring of nuclear facilities using ZigBee technology," *IEEE Sens. J.*, vol. 14, no. 11, pp. 4007–4013, 2014.

[8] M. Nishimura *et al.*, "Gateway Vectors for Plant Genetic Engineering: Overview of Plant Vectors, Application for Bimolecular Fluorescence Complementation (BiFC) and Multigene Construction," *Genet. Eng. - Basics, New Appl. Responsib.*, vol. 2, p. 64, 2012.

[9] C. L. Lowe, C. J. Kiger, D. N. Jackson, and D. M. Young, "Implementation of Wireless Technologies in Nuclear Power Plants ' Electromagnetic Environment Using Cognitive Radio System," pp. 385–393, 2018.

[10] H. M. Hashemian, C. J. Kiger, G. W. Morton, and B. D. Shumaker, "Wireless sensor applications in nuclear power plants," *Nucl. Technol.*, vol. 173, no. 1, pp. 8–16, 2011.

[11] I. Priyadarshinee, K. Sahoo, and C. Mallick, "Flood Prediction and Prevention through Wireless Sensor Networking (WSN): A Survey," *Int. J. Comput. Appl.*, vol. 113, no. 9, pp. 30–36, 2015.

[12] M. Sheik Dawood, J. Suganya, R. Karthika Devi, and G. Athisha, "A Review on

Wireless Sensor Network Protocol for Disaster Management," *Int. J. Comput. Appl. Technol. Res.*, vol. 2, no. 2, pp. 141–146, 2013.

[13] A. Mangla Amit Kumar Bindal Devendra Prasad, "Disaster Management in Wireless Sensor Networks: a Survey Report," *Int. J. Comput. Corp. Res. ISSN (Online*, vol. 6, no. September, pp. 2249–54, 2016.

[14] E. Cañete, J. Chen, M. Díaz, L. Llopis, A. Reyna, and B. Rubio, "Using wireless sensor networks and trains as data mules to monitor slab track infrastructures," *Sensors (Switzerland)*, vol. 15, no. 7, pp. 15101–15126, 2015.

[15] S. Ul Islam *et al.*, *Implanted Wireless Body Area Networks: Energy Management, Specific Absorption Rate and Safety Aspects*, 1st ed. Elsevier Inc., 2016.

[16] T. Zhang, "Radioactive Target Detection Using Wireless Sensor Network," in *Computer, Informatics,Cybernetics and Application, Lecture Notes in Electrical Engineering*, vol. 107, 2012, pp. 659–664.

[17] A. Laikari, "Wireless in Nuclear applications," in *ENERGIFORSK NUCLEAR SAFETY RELATED I&C – ENSRIC*, 2018.

[18] A. Gomez, M. F. Lagadec, M. Magno, and L. Benini, "Self-powered wireless sensor nodes for monitoring radioactivity in contaminated areas using unmanned aerial vehicles," in *2015 IEEE Sensors Applications Symposium (SAS)*, 2015, pp. 1–6.

[19] T. Sakaue, S. Yoshino, K. Nishizawa, and K. Takeda, "Survey in Fukushima Daiichi NPS by combination of human and remotely-controlled robot," *SSRR 2017 - 15th IEEE Int. Symp. Safety, Secur. Rescue Robot. Conf.*, pp. 7–12, 2017.

[20] "Implants and Prosthetics | FDA," *U.S. Food and Drug Adminstration*. [Online]. Available: https://www.fda.gov/medical-devices/products-and-medical-procedures/implants-and-prosthetics.

[21] R. Sobot, "Implantable Technology : History, Controversies, and Social Implications [Commentary]," *IEEE Technol. Soc. Mag.*, vol. 37, no. 4, pp. 35–45, 2018.

[22] American heart Association, "Implantable Medical Devices American Heart Association." .

[23] A. L. Benabid, S. Chabardes, J. Mitrofanis, and P. Pollak, "Deep brain stimulation of the subthalamic nucleus for the treatment of Parkinson's disease," *Lancet Neurol.*, vol. 8, no. 1, pp. 67–81, 2009.

[24] R. G. Hauser, W. T. Katsiyiannis, C. C. Gornick, A. K. Almquist, and L. M. Kallinen, "Deaths and cardiovascular injuries due to device-assisted implantable cardioverter-defibrillator and pacemaker lead extraction.," *Eur. Eur. pacing, arrhythmias, Card. Electrophysiol. J. Work. groups Card. pacing, arrhythmias, Card. Cell. Electrophysiol. Eur. Soc. Cardiol.*, vol. 12, no. 3, pp. 395–401, Mar.

2010.

[25] Tim Newman, “Endoscopy: Types, preparation, procedure, and risks,” *Medical News Today*, 2017. [Online]. Available: https://www.medicalnewstoday.com/articles/153737.php.

[26] “Nuclear Fuel Cycle Overview - World Nuclear Association.” [Online]. Available: http://www.world-nuclear.org/information-library/nuclear-fuel-cycle/introduction/nuclear-fuel-cycle-overview.aspx.

[27] ENS, “Hot Cell,” *European nuclear society*, 2018. [Online]. Available: https://www.euronuclear.org/info/encyclopedia/h/hotcell.htm.

[28] “Hot cell - Wikipedia.” [Online]. Available: https://en.wikipedia.org/wiki/Hot_cell.

[29] A. Bhandekar *et al.*, “New Hot Cell Facility for Post Irradiation Examination,” no. April, pp. 19–26, 2015.

[30] R. I. Da Silva, V. D. D. Almeida, A. M. Poersch, and J. M. S. Nogueira, “Wireless sensor network for disaster management,” *Proc. 2010 IEEE/IFIP Netw. Oper. Manag. Symp. NOMS 2010*, pp. 870–873, 2010.

[31] S. S. Choi and H. S. Lim, “Factors that affect cycle-life and possible degradation mechanisms of a Li-ion cell based on {LiCoO}2,” *J. Power Sources*, vol. 111, no. 1, pp. 130–136, Sep. 2002.

[32] I. Design, O. F. Vented, L. S. Batteries, F. O. R. Nuclear, and P. Plants, “OF VENTED LEAD-ACID STORAGE BATTERIES,” no. February, pp. 2–7, 2007.

[33] P. Musilek, P. Kromer, and M. Prauzek, “Location-specific optimization of energy harvesting environmental monitoring systems,” *IEEE SSCI 2014 - 2014 IEEE Symp. Ser. Comput. Intell. - IES 2014 2014 IEEE Symp. Intell. Embed. Syst. Proc.*, pp. 8–13, 2014.

[34] P. Musilek, M. Prauzek, P. Krömer, J. Rodway, and T. Bartoň, “Intelligent Energy Management for Environmental Monitoring Systems,” in *Smart Sensors Networks: Communication Technologies and Intelligent Applications*, Elsevier, 2017, pp. 67–94.

[35] IEEE Computer Society, “IEEE Standard for Low-Rate Wireless Networks.” IEEE, 2003.

[36] V. Venkatachalam and M. Franz, “Power reduction techniques for microprocessor systems,” *ACM Comput. Surv.*, vol. 37, no. 3, pp. 195–237, 2005.

[37] V. Raghunathan, S. Ganeriwal, and M. Srivastava, “Emerging techniques for long lived wireless sensor networks,” *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 108–114, 2006.

[38] Lin Zhong, “Power Consumption by Wireless Communication,” 2011. [Online]. Available: http://www.ruf.rice.edu/~mobile/elec518/lectures/3-wireless.pdf.

[39] Y. Li, B. Bakkaloglu, and C. Chakrabarti, “A comprehensive energy model and energy-quality evaluation of wireless transceiver front-ends,” *IEEE Work. Signal Process. Syst. SiPS Des. Implement.*, vol. 2005, pp. 262–267, 2005.

[40] V. Daiya, T. S. S. Krishnan, G. S. Rani, J. Ebenezer, S. A. V SatyaMurty, and B. P. C. Rao, “Theoretical analysis on designing Full Functional Device of {WSN} using Wireless Power Transfer,” in *2015 Annual {IEEE} India Conference ({INDICON})*, 2015.

[41] W. Toorisaka, G. Hasegawa, and M. Murata, “Power Consumption Analysis of Data Transmission,” no. c, pp. 75–80, 2012.

[42] N. Van Huynh *et al.*, “Ambient Backscatter Communications : A Contemporary Survey,” *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 2889–2922, 2018.

[43] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, “Ambient Backscatter : Wireless Communication Out of Thin Air,” pp. 39–50, 2013.

[44] C. Xu, L. Yang, and P. Zhang, “Practical Backscatter Communication Systems for Battery-Free Internet of Things: A Tutorial and Survey of Recent Research,” *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 16–27, Sep. 2018.

[45] M. L. Memon, N. Saxena, A. Roy, and D. R. Shin, *Backscatter Communications : Inception of the Battery-Free Era- A Comprehensive Survey*. 2019.

[46] P. Zhang, D. Bharadia, K. Joshi, and S. Katti, “HitchHike : Practical Backscatter Using Commodity WiFi,” in *SenSys’ 16 Stanford,CA,USA*, 2016.

[47] B. Kellogg, A. Parks, S. Gollakota, J. R. Smith, and D. Wetherall, “Wi-Fi Backscatter : Internet Connectivity for RF-Powered Devices,” in *SIGCOMM’14, Chicago, IL, USA*, 2014.

[48] H. Stockman, “Communication by Means of Reflected Power,” *Proc. IRE*, vol. 36, no. 10, pp. 1196–1204, 1948.

[49] D. Bharadia, K. Joshi, M. Kotaru, and S. Katti, “BackFi : High Throughput WiFi Backscatter,” pp. 283–296, 2015.

[50] J. Qian, A. N. Parks, J. R. Smith, F. Gao, and S. Jin, “IoT Communications with M -PSK Modulated Ambient Backscatter: Algorithm, Analysis, and Implementation,” *IEEE Internet Things J.*, vol. 6, no. 1, pp. 844–855, 2019.

[51] B. Kellogg, V. Talla, S. Gollakota, and J. R. Smith, “Passive Wi-Fi : Bringing Low Power to Wi-Fi Transmissions,” in *NSDI*, 2016.

[52] J. Zhang, V. Varadharajan, “Wireless sensor network key management survey and taxonomy,” *J. Netw. Comput. Appl.*, vol. 33, no. 2, pp. 63–75, 2010.

[53] N. Fips, “197: Announcing the advanced encryption standard (AES),” *Adv. ENCRYPTION Stand. (AES),Technology Lab. Natl. Inst. Stand. …*, vol. 2009, pp. 8–12, 2001.

[54] C. W. Hung and W. T. Hsu, “Power consumption and calculation requirement analysis of AES for WSN IoT,” *Sensors (Switzerland)*, vol. 18, no. 6, 2018.

[55] M. J. Chaudhry, S. Murawwat, F. Saleemi, S. Tariq, M. Saleemi, and F. J. Chaudhry, “Power optimized secure bluetooth communication,” *IEEE INMIC 2008 12th IEEE Int. Multitopic Conf. - Conf. Proc.*, pp. 182–188, 2008.

[56] Y.-S. S. Shiu, S. Y. Chang, H.-C. C. Wu, S. C. H. Huang, and H.-H. H. Chen, “Physical layer security in wireless networks: a tutorial,” *{IEEE} Wirel. Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[57] S. Goel and R. Negi, “Guaranteeing Secrecy using Artificial Noise,” *IEEE Trans. Wirel. Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[58] Y. Tang, J. Xiong, D. Ma, and X. Zhang, “Robust Artificial Noise Aided Transmit Design for MISO Wiretap Channels with Channel Uncertainty,” *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2096–2099, Nov. 2013.

[59] A. Mukherjee and A. L. Swindlehurst, “Robust Beamforming for Security in MIMO Wiretap Channels With Imperfect CSI,” *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[60] C. Jeong, I. Kim, and D. I. Kim, “Joint Secure Beamforming Design at the Source and the Relay for an Amplify-and-Forward MIMO Untrusted Relay System,” *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.

[61] L. Zheng, D. N. C. C. Tse, Z. Lizhong, and D. N. C. C. Tse, “Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels,” *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1073–1096, May 2003.

[62] Y. Zou, X. Wang, and W. Shen, “Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[63] Y. Hwang and H. C. Papadopoulos, “Physical-layer secrecy in AWGN via a class of chaotic DS/SS systems: Analysis and design,” *IEEE Trans. Signal Process.*, vol. 52, no. 9, pp. 2637–2649, 2004.

[64] A. Yener and S. Ulukus, “Wireless Physical-Layer Security: Lessons Learned from Information Theory,” *Proc. IEEE*, vol. 103, no. 10, pp. 1814–1825, 2015.

[65] G. Chopra, R. K. Jha, and S. Jain, “RBA: Detection and Protection Analysis Using Region-Based Algorithm in Ultra-Dense Networks,” *IEEE Access*, vol. 7, pp. 52997–53011, 2019.

[66] W. Liu, X. Zhou, S. Durrani, and P. Popovski, “Secure Communication with a

Wireless-Powered Friendly Jammer," *IEEE Trans. Wirel. Commun.*, vol. 15, no. 1, pp. 401–415, 2016.

[67] N. Romero-Zurita, D. McLernon, and M. Ghogho, "Physical layer security by robust masked beamforming and protected zone optimisation," *IET Commun.*, vol. 8, no. 8, pp. 1248–1257, 2014.

[68] D. Abbasi-Moghadam, V. T. Vakili, and A. Falahati, "Combination of Turbo Coding and Cryptography in NONGEO Satellite Communication Systems," in *IEEE International Symposium on Telecommunications*, 2008, pp. 666–669.

[69] S. Sedaghatnejad and M. Farhang, "Detectability of Chaotic Direct-Sequence Spread-Spectrum Signals," *IEEE Wirel. Commun. Lett.*, vol. 4, no. 6, pp. 589–592, 2015.

[70] T. T. Li *et al.*, "Physical layer built-in security analysis and enhancement of CDMA systems," in *MILCOM 2005 - 2005 IEEE Military Communications Conference*, 2005, vol. 2005, pp. 956-962 Vol. 2.

[71] B. Muntwyler, V. Lenders, F. Legendre, and B. Plattner, "Obfuscating IEEE 802.15.4 communication using secret spreading codes," *2012 9th Annu. Conf. Wirel. On-Demand Netw. Syst. Serv. WONS 2012*, vol. 4, pp. 1–8, 2012.

[72] S. Soderi, L. Mucchi, M. Hamalainen, A. Piva, and J. Iinatti, "Watermark-based secure communications in safety-related scenarios," *Int. Symp. Med. Inf. Commun. Technol. ISMICT*, vol. 2016-June, 2016.

[73] A. K. Nain and P. Rajalakshmi, "A reliable covert channel over IEEE 802.15.4 using steganography," in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, 2016, pp. 711–716.

[74] H. Sun, "An Enhanced Rectenna Using Differentially-Fed Rectifier for Wireless Power Transmission," *IEEE Antennas Wirel. Propag. Lett.*, vol. 15, pp. 32–35, 2016.

[75] N. Degrenne, V. Marian, C. Vollaire, F. Buret, J. Verdier, and B. Allard, "Voltage reversal in unbalanced rectenna association," *IEEE Antennas Wirel. Propag. Lett.*, vol. 11, pp. 941–944, 2012.

[76] V. Marian, C. Vollaire, J. Verdier, and B. Allard, "Potentials of an Adaptive Rectenna Circuit," *IEEE Antennas Wirel. Propag. Lett.*, vol. 10, pp. 1393–1396, 2011.

[77] B. Mukherjee, P. Patel, and J. Mukherjee, "Hemispherical Dielectric Resonator Antenna loaded with a Photonic Band Gap structure for wideband and high gain applications," *2014 31th URSI Gen. Assem. Sci. Symp. URSI GASS 2014*, no. 1, pp. 3–6, 2014.

[78] B. Mukherjee, P. Patel, and J. Mukherjee, "Hemispherical dielectric resonator antenna loaded with a novel sierpinski carpet fractal based photonic band gap

structure for wireless applications," in *2014 Asia-Pacific Microwave Conference Proceedings, APMC 2014*, 2014, pp. 1279–1281.

[79] M. Sinha, V. Killamsetty, and B. Mukherjee, "Near field analysis of RDRA loaded with split ring resonators superstrate," *Microw. Opt. Technol. Lett.*, vol. 60, no. 2, pp. 472–478, 2018.

[80] N. Shinohara and H. Matsumoto, "Experimental study of large rectenna array for microwave energy transmission," *IEEE Trans. Microw. Theory Tech.*, vol. 46, no. 3, pp. 261–268, Mar. 1998.

[81] U. Olgun, C. C. Chen, and J. L. Volakis, "Investigation of rectenna array configurations for enhanced RF power harvesting," *IEEE Antennas Wirel. Propag. Lett.*, vol. 10, pp. 262–265, 2011.

[82] A. Massa, G. Oliveri, F. Viani, and P. Rocca, "Array Designs for Long-Distance Wireless Power Transmission: State-of-the-Art and Innovative Solutions," *Proc. {IEEE}*, vol. 101, no. 6, pp. 1464–1481, Jun. 2013.

[83] B. R. Marshall, C. R. Valenta, and G. D. Durgin, "DC power pattern analysis of N-by-N staggered pattern charge collector and N2rectenna array," *2013 IEEE Wirel. Power Transf. WPT 2013*, pp. 115–118, 2013.

[84] D. V. Gretskih, A. I. Luchaninov, A. V. Gomozov, Y. M. Penkin, M. V. Nesterenko, and V. A. Katrich, "Mathematical Model of Large Rectenna Arrays for Wireless Energy Transfer," *Prog. Electromagn. Res. B*, vol. 74, pp. 77–91, 2017.

[85] M. Otsuka *et al.*, "Relation between spacing and receiving efficiency of finite rectenna array," *Electron. Commun. Japan (Part I Commun.*, vol. 74, no. 2, pp. 88–96, Feb. 1991.

[86] B. Strassner and K. Chang, "Highly efficient C-band circularly polarized rectifying antenna array for wireless microwave power transmission," *IEEE Trans. Antennas Propag.*, vol. 51, no. 6, pp. 1347–1356, Jun. 2003.

[87] K.-M. Huang, B. Zhang, X. Chen, W. Huang, and C.-J. Liu, "Study on an S-Band Rectenna Array for Wireless Microwave Power Transmission," *Prog. Electromagn. Res.*, vol. 135, pp. 747–758, 2014.

[88] J. E. Ferguson and A. D. Redish, "Wireless Communication with implanted medical devices using the Conductive Properties of the Body," *NIH Public Access, Expert Rev Med. Devices*, vol. 8, no. 4, pp. 427–433, 2011.

[89] H. Park and M. Ghovanloo, "Wireless communication of intraoral devices and its optimal frequency selection," *IEEE Trans. Microw. Theory Tech.*, vol. 62, no. 12, pp. 3205–3215, 2014.

[90] Y. H. Liu, C. L. Li, and T. H. Lin, "A 200-pJ/b MUX-based RF transmitter for implantable multichannel neural recording," *IEEE Trans. Microw. Theory Tech.*,

vol. 57, no. 10, pp. 2533–2541, 2009.

[91] P. Zhang, M. Rostami, P. Hu, and D. Ganesan, “Enabling Practical Backscatter Communication for On-body Sensors,” in *SIGCOMM*, 2016, pp. 22–26.

[92] D. Vasisht, G. Zhang, O. Abari, H.-M. Lu, J. Flanz, and D. Katabi, “In-Body Backscatter Communication and Localization,” in *ACM SIGCOMM*, 2018, p. 15.

[93] K. Agarwal, R. Jegadeesan, Y. X. Guo, and N. V. Thakor, “Wireless Power Transfer Strategies for Implantable Bioelectronics,” *IEEE Rev. Biomed. Eng.*, vol. 10, pp. 136–161, 2017.

[94] L. R. Varshney, “Transporting information and energy simultaneously,” *IEEE Int. Symp. Inf. Theory - Proc.*, pp. 1612–1616, 2008.

[95] C. Camara, P. Peris-Lopez, and J. E. Tapiador, “Security and privacy issues in implantable medical devices: A comprehensive survey,” *J. Biomed. Inform.*, vol. 55, pp. 272–289, 2015.

[96] L. Wu *et al.*, “Wireless sensor network based solution for nuclear radiation detection,” *ICIST 2014 - Proc. 2014 4th IEEE Int. Conf. Inf. Sci. Technol.*, pp. 397–400, 2014.

[97] Y. Shikaze *et al.*, “Field test around Fukushima Daiichi nuclear power plant site using improved Ce:Gd 3 (Al,Ga) 5 O 12 scintillator Compton camera mounted on an unmanned helicopter,” *J. Nucl. Sci. Technol.*, vol. 53, no. 12, pp. 1907–1918, 2016.

[98] D. Jha, S. Dahal, S. Shukla, B. Shahi, and P. G. Student, “Radioactive Contamination Detection in Water Using Wireless Sensor Network,” *IJARIIE*, vol. 1, no. 5, pp. 2395–4396, 2016.

[99] M. Shimura, H. Kobayashi, H. Kitahara, H. Kobayashi, and S. Okamoto, “Radiation Area Monitoring by wireless-communicating Area Monitor with Surveillance Camera,” *J. Nucl. Sci. Technol.*, vol. 41, pp. 271–274, 2004.

[100] P. Constantinou *et al.*, “An energy supply unit for an autonomous remote sensor system monitoring stored nuclear waste,” *Sensors Actuators, A Phys.*, vol. 166, no. 1, pp. 52–65, 2011.

[101] J. Wei, “Capacity Analysis of Frequency Shift Based Backscatter Communication System,” *2018 3rd Int. Conf. Comput. Commun. Syst.*, pp. 353–357, 2018.

[102] F. Jameel, T. Ristaniemi, I. Khan, and B. M. Lee, “Simultaneous harvest-and-transmit ambient backscatter communications under Rayleigh fading,” *Eurasip J. Wirel. Commun. Netw.*, vol. 2019, no. 1, 2019.

[103] Z. Ma *et al.*, “Time- and Power-Splitting Strategies for Ambient Backscatter System,” *IEEE Access*, vol. 7, pp. 40068–40077, 2019.

[104] W. Saad, X. Zhou, Z. Han, and H. V. Poor, “On the Physical Layer Security of Backscatter Wireless Systems,” *IEEE Trans. Wirel. Commun.*, vol. 13, no. 6, pp. 3442–3451, 2014.

[105] H. Song and Y. Gao, “A Distinctive Method to Improve the Security Capacity of Backscatter Wireless System,” pp. 272–276, 2017.

[106] X. Wang, Z. Su, and G. Wang, “Relay selection for secure backscatter wireless communications,” *Electron. Lett.*, vol. 51, no. 12, pp. 951–952, 2015.

[107] L.-G. Tran, H.-K. Cha, and W.-T. Park, “RF power harvesting: a review on designing methodologies and applications,” *Micro Nano Syst. Lett.*, vol. 5, no. 1, p. 14, Dec. 2017.

[108] R. Diwan and D. Vaishnav, “Interaction of solar power satellite with the space and atmosphere environment,” vol. 6, no. 1, pp. 51–56, 2014.

[109] W. ~C. Brown, “The History of the Development of the Rectenna,” in *Solar Power Satellite Microwave Power Transmission and Reception*, 1980, vol. 2141, p. 271.

[110] J. Gavan and S. Tapuchi, “MW WPT for HAPS and SPS: Concepts, EMI and biological hazards issues,” *2011 30th URSI Gen. Assem. Sci. Symp. URSIGASS 2011*, pp. 3–6, 2011.

[111] L. Choong and L. Angeles, “Multi-Channel IEEE 802.15.4 Packet Capture Using Software Defined Radio,” 2009.

[112] N. B. Truong, “Investigating Latency in GNU Software Radio with USRP Embedded Series SDR Platform,” 2013.

[113] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, *How Realistic is the Threat?*, vol. 11. 2011.

[114] T. Goodspeed, S. Bratus, R. Melgares, R. Speers, and S. W. Smith, “Api-do: Tools for exploring the wireless attack surface in smart meters,” *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 2133–2140, 2012.

[115] J. Teubner and L. Woods, *Teubner, Woods - 2013 - Data Processing on FPGAs.pdf*, 2(1). Morgan Claypool Publishers & PVLDB, 2009.

[116] “GNU Radio.” [Online]. Available: https://wiki.gnuradio.org/index.php/Main_Page.

[117] Ettus Research, “USRP B200/B210 Specification Sheet,” *Ettus Res.*, p. 2, 2014.

[118] Ettus Research, “USRP Hardware Driver and USRP Manual.” [Online]. Available: https://files.ettus.com/manual/page_usrp_b200.html.

[119] J. Aspnes, C. Scheideler, A. Arora, and S. Madden, Eds., *Distributed Computing*

in Sensor Systems, vol. 4549. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007.

[120] G. S. Rani, T. S. S. Krishnan, V. Daiya, J. Ebenezer, and S. A. V. S. Murty, "Performance analysis of Wireless Sensor Network," in *Souvenir of the 2014 IEEE International Advance Computing Conference, IACC 2014*, 2014, pp. 282–287.

[121] V. Daiya, T. S. S. Krishnan, J. Ebenezer, K. Madhusoodanan, S. A. V. Satyamurty, and B. Rao, "Dynamic architecture for Wireless Sensor Network-implementation & analysis," in *Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2016*, 2016.

[122] DIGI, "XBee®/XBee-PRO S2C Zigbee® User Guide." DIGI, 2019.

[123] NXP Semiconductors, "LPC1769/68/67/66/65/64/63 Product Datasheet," no. May, 2018.

[124] R. Environment, "µVision ® IDE," 2018. [Online]. Available: http://www2.keil.com/mdk5/uvision/.

[125] T. Instruments, "SmartRF Protocol Packet Sniffer - PACKET-SNIFFER - TI Software Folder ," vol. 2012, no. 2/28/2012. .

[126] NXP Semiconductors, "Arm® Cortex®-M0+ Kinetis® KW21Z 2." .

[127] SAMD20 datasheet, "SAMD20 family," *2017*. [Online]. Available: http://ww1.microchip.com/downloads/en/DeviceDoc/60001504B.pdf.

[128] AT86RF233 datasheet, "Atmel AT86RF2333," 2014. [Online]. Available: http://ww1.microchip.com/downloads/en/devicedoc/atmel-8351-mcu_wireless-at86rf233_datasheet.pdf.

[129] H. T. Friis, "A Note on a Simple Transmission Formula," *Proc. IRE*, vol. 34, no. 5, pp. 254–256, 1946.

[130] R. Bansal, *Antenna theory; analysis and design*, Third., vol. 72, no. 7. Wiley India Pvt. Ltd., 2008.

[131] S. Gabriel, R. W. Lau, and C. Gabriel, "The dielectric properties of biological tissues: II. Measurements in the frequency range 10 Hz to 20 GHz," *Phys. Med. Biol.*, vol. 41, no. 11, pp. 2251–2269, 1996.