

**A LONG-RANGE FINE-SCALE RF POSITIONING SYSTEM USING  
TUNNELING TAGS**

A Dissertation  
Presented to  
The Academic Faculty

By

Cheng Qi

In Partial Fulfillment  
of the Requirements for the Degree  
Doctor of Philosophy in the  
School of Engineering  
Department of Electrical and Computer Engineering

Georgia Institute of Technology

May 2021

© Cheng Qi 2021

# **A LONG-RANGE FINE-SCALE RF POSITIONING SYSTEM USING TUNNELING TAGS**

Thesis committee:

Dr. Gregory Durgin  
School of Electrical and Computer Engineering  
*Georgia Institute of Technology*

Dr. Andrew Peterson  
School of Electrical and Computer Engineering  
*Georgia Institute of Technology*

Dr. David Taylor  
School of Electrical and Computer Engineering  
*Georgia Institute of Technology*

Dr. Billy Kihei  
School of Electrical and Computer Engineering  
*Kennesaw State University*

Dr. Ying Zhang  
School of Electrical and Computer Engineering  
*Georgia Institute of Technology*

Date approved: Apr 16, 2021

To Maggie, my beloved wife,  
who makes my world full of miracles.

## ACKNOWLEDGMENTS

I would like to express my deepest and sincere gratitude to my advisor, Prof. Gregory Durgin, for inviting me to the Propagation Group in 2015 at the Georgia Tech Shenzhen campus. He guided me through all the difficulties in my research and life, taught me both skills as a researcher and integrity as a good man.

I am extremely grateful to my committee members, Prof. David Taylor, Prof. Ying Zhang, Prof. Andrew Peterson, and Prof. Billy Kihei, for providing invaluable feedback and approving my dissertation.

I am highly thankful to my colleagues in the Propagation Group, Francesco Amato, Mohammad Al-Hassoun, Mike Varner, Bashir Akbar, and Qian Yang for their friendship and support. Special thanks to Francesco Amato, Billy Kihei, and Joshua Griffin for working with me and guiding me as professional researchers.

I greatly appreciate all the excellent ECE faculty and staff, Sharon Pugh, James Steinberg, Kevin Pham, and Daniela Staiculescu, for their kind help and support throughout my study.

I would also like to say thank you to all my friends: Yiliang Guo, Yuanzheng Zhu, Scott Murphy, Marion Murphy, Dennis Schauer, Melynda Schauer, David Rau, Anna Rau, Qianli Feng, Yinzhi Zhang, Zhe Tang, Jiahao Zhu, Xinyu Wei, Muliang Zhu, Fanpeng Kong, and Rui Zhang, who made my time at Georgia Tech very fun and memorable for me.

There are no words to express my deep gratitude to my parents, Xuliang Qi and Xin Liu. Also, I want to say thank you to my entire family, who genuinely cared about and encouraged me during this adventure.

Last but not least, my special appreciation goes to my beloved wife, Yuming Maggie Zou, without whom this dissertation would not be possible. She is the brightest star in my night and lights up my sky.



## TABLE OF CONTENTS

<b>Acknowledgments</b> . . . . .	iv
<b>List of Tables</b> . . . . .	xi
<b>List of Figures</b> . . . . .	xii
<b>List of Acronyms</b> . . . . .	.xviii
<b>Summary</b> . . . . .	xxi
<b>Chapter 1: Introduction and Background</b> . . . . .	1
1.1 RFID System Overview . . . . .	4
1.2 The Tunneling Effect . . . . .	6
1.3 RSP-Based Positioning . . . . .	8
1.3.1 RSP-based Ranging Method . . . . .	8
1.3.2 Trilateration approach . . . . .	9
1.4 Document Organization . . . . .	10
<b>Chapter 2: Literature Survey</b> . . . . .	11
2.1 Overview of Positioning Systems . . . . .	11
2.2 RFID Frequency Bands and Range Limits . . . . .	12
2.3 Overview of RFID Positioning Techniques . . . . .	14

2.3.1	RSS-Based RFID Localization Techniques . . . . .	15
2.3.2	RSP-Based RFID positioning Techniques . . . . .	16
2.3.3	Hybrid RFID positioning Technique . . . . .	17
2.4	Accuracy and Range of RFID-based Positioning Techniques . . . . .	18
<b>Chapter 3: Frequency Hopping RFID system at 5.8 GHz for Space Sensing Mission and Terrestrial Applications . . . . .</b>		<b>20</b>
3.1	Introduction . . . . .	20
3.2	System Overview . . . . .	21
3.3	Reader Design . . . . .	23
3.3.1	RFID reader Architecture . . . . .	23
3.3.2	Antennas . . . . .	25
3.3.3	Frequency Hopping Design . . . . .	28
3.3.4	Power Breakdown . . . . .	30
3.3.5	Link Budget . . . . .	31
3.4	Backscatter Communication . . . . .	32
3.4.1	Test Setup . . . . .	32
3.4.2	Results . . . . .	33
3.5	RF Tag Design . . . . .	35
3.5.1	RF Tag Architecture . . . . .	35
3.5.2	Antennas . . . . .	37
3.5.3	Power Consumption . . . . .	37
3.5.4	Link Budget . . . . .	38
3.5.5	Charge Pump . . . . .	38

3.5.6	RF Tag Integration . . . . .	39
3.6	Tag Operation without power management IC . . . . .	40
3.6.1	Test Setup . . . . .	40
3.6.2	Results . . . . .	41
3.7	Tag Operation with DC Power Management . . . . .	45
3.7.1	Test Setup . . . . .	45
3.7.2	Results . . . . .	45
3.8	On-orbit Data . . . . .	46
3.9	Conclusion . . . . .	52
<b>Chapter 4: Long-range Sub-meter Scale Ranging with Tunneling RFID Tags . .</b>		<b>53</b>
4.1	Introduction . . . . .	53
4.2	Rationale . . . . .	55
4.2.1	RSP-based Distance Estimation . . . . .	55
4.2.2	Distance and Error Estimation . . . . .	58
4.3	Multipath . . . . .	58
4.3.1	Multipath Channel Modeling . . . . .	58
4.3.2	Evidence of Multipath Channel . . . . .	61
4.4	The Experimental Setup . . . . .	63
4.5	Experimental Results . . . . .	65
4.5.1	Exploiting RSP Data . . . . .	65
4.5.2	RSS- vs RSP-based Method . . . . .	68
4.5.3	Calibration with Reference Measurements . . . . .	71

4.6	Conclusions . . . . .	73
<b>Chapter 5:</b>	<b>Fine-scale Ranging Using Tunneling RFID Tags in NLoS Scenarios . . . . .</b>	<b>75</b>
5.1	Introduction . . . . .	75
5.2	Rationale . . . . .	78
5.2.1	Backscatter Communication with Tunneling Tags . . . . .	78
5.2.2	RSP-based Positioning in Real World . . . . .	79
5.2.3	Measurement Offsets and Errors . . . . .	80
5.2.4	System Calibration . . . . .	82
5.3	Experimental Setup . . . . .	83
5.3.1	Through-obstruction NLoS Setup . . . . .	83
5.3.2	Through-wall NLoS Setup . . . . .	84
5.4	RSS in LoS and NLoS Conditions . . . . .	86
5.4.1	Through-obstruction NLoS vs LoS . . . . .	86
5.4.2	Through-wall NLoS vs LoS . . . . .	87
5.5	Ranging Accuracy in NLoS . . . . .	89
5.5.1	Ranging accuracy for Through-obstruction NLoS . . . . .	89
5.5.2	Ranging accuracy for Through-Wall NLoS . . . . .	91
5.6	Dwell-time vs Accuracy . . . . .	92
5.7	Conclusions . . . . .	95
<b>Chapter 6:</b>	<b>A Real-time RFID Positioning System Using Tunneling Tags . . . . .</b>	<b>96</b>
6.1	Introduction . . . . .	96
6.2	Rationale . . . . .	97

6.2.1	2D Localization with RSP-based Ranging Method . . . . .	97
6.2.2	Real-time Software Defined Radio-based Reader Design . . . . .	98
6.2.3	SDR Implementation . . . . .	99
6.3	Measurements . . . . .	102
6.3.1	Experimental Setup . . . . .	102
6.3.2	Experimental Results . . . . .	102
6.4	Conclusion . . . . .	106
<b>Chapter 7: A Backscatter Channel Sounder Using Tunneling RFID Tags . . . .</b>		<b>108</b>
7.1	Introduction . . . . .	108
7.2	Rationale . . . . .	109
7.2.1	Channel Sounding Reader Design . . . . .	109
7.2.2	RSP-based Ranging Method . . . . .	112
7.2.3	Channel Sounding Technique Using Tunneling Tags . . . . .	113
7.3	Measurements . . . . .	115
7.3.1	Experimental Setup . . . . .	115
7.3.2	Channel Modeling . . . . .	117
7.3.3	Distance Estimation . . . . .	119
7.4	Conclusion . . . . .	122
<b>Chapter 8: Future Work . . . . .</b>		<b>124</b>
<b>Appendices . . . . .</b>		<b>126</b>
Appendix A: Circuit design . . . . .		127

Appendix B: Reader Setup . . . . .	132
Appendix C: Data and Relevant Code . . . . .	133
<b>References . . . . .</b>	<b>147</b>
<b>Vita . . . . .</b>	<b>156</b>

## LIST OF TABLES

3.1	Hopping Sequence [62] . . . . .	29
3.2	Hop Set Statistical Properties [62] . . . . .	29
3.3	The power consumption and price of major components in the RFID reader. The price of the components for purchasing a single chip and 1000 units are listed. . . . .	31
4.1	Idealized centroids and RMS widths of multipath distributions in delay for one- and two-way channels, with power or envelope delay spectra. . . . .	60
4.2	Specifications of the Experimental Setup . . . . .	65
5.1	Summary of Error Sources . . . . .	81
5.2	Specifications of the Experimental Setups . . . . .	85
5.3	Average distance estimation error for Semi-passive and tunneling tags in LoS and NLoS(o) scenarios. . . . .	91
5.4	Average distance estimation error for Semi-passive and tunneling tags in LoS and through-wall NLoS(w) scenarios. . . . .	92
6.1	Specifications of the reader setup for outdoor 2D positioning . . . . .	100
6.2	Statistics of 1D and 2D location estimations . . . . .	106
7.1	Specifications of the outdoor long range experimental setup. . . . .	116
7.2	Statistics of distance estimations . . . . .	123

## LIST OF FIGURES

1.1	Illustration of two different uses of real-time RFID positioning systems. (a) <i>asset tracking</i> mode: fixed readers collect data from one or more tunneling tags to locate and track assets; (b) <i>navigation</i> mode: a mobile, low-powered reader grabs data from multiple anchor points for accurate contact tracing. .	3
1.2	The RFID backscatter system . . . . .	4
1.3	Elements of the RF tag reader operating at 5.8GHz. . . . .	6
1.4	a) Microstrip line structure of the tunneling reflection amplifier as in [16]; b) the measured IV curve [1] of tunnel diode model MBD5057 c) The block diagram of the tunneling tag. . . . .	7
1.5	In the trilateration approach the location is estimated by intersection of the three or more circles formed by evaluation of the target object's distance using its received signal phase. . . . .	9
2.1	Overview and classification of positioning systems. . . . .	13
2.2	Overview and classification of RFID positioning systems. . . . .	14
2.3	RFID positioning and tracking techniques, state-of-the-art and prediction of what will be obtained by combining Tunneling Tags (TT) and RSP-based positioning approaches. Comparisons were made in terms of reported distance errors and maximum ranges. . . . .	19
3.1	RFTSat with the RF tag separated from its mounting position to show the reader transmitter and receiver patch antennas. The tag will harvest energy from the RF tag reader and send sensor data to the reader using modulated backscatter. . . . .	21
3.2	RFTSat with the RF tag separated from its mounting position to show the tag's backscatter and energy harvesting antennas. . . . .	22



3.3	The RF tag reader mounted between the two metal plates. The different boards of the RF tag reader as well as the reader transmit and receive antennas are shown. . . . .	22
3.4	A backside view of the RF tag reader boards showing the location of the transitter's band pass filter. . . . .	23
3.5	Elements of the RFID reader operating at 5.8 GHz . . . . .	24
3.6	The front side of the transmit-receive E-shaped patch antenna pair and a microstrip patch array (a), and the ground plane of the antenna pair (b). . .	27
3.7	The isolation between the transmit and receive port by using a circulator and a pair of E-shaped patch antenna with solid ground plane and slitted ground plane. The slitted ground plane has 10 dB more isolation than the circulator at 5.8 GHz and 8 dB more than the solid ground plane. . . . .	27
3.8	Hopping Sequence for all 77 frequencies in the 5.8 GHz band [62]. . . . .	30
3.9	The experimental setup with antenna on the open-air, rooftop antenna range at Georgia Tech. . . . .	33
3.10	The eye diagram of the received signal when bistatic (a) and monostatic (b) antenna configuration are used. . . . .	33
3.11	An example of ADC-sampled received data packets (single channel) for bistatic and monostatic antenna configurations. . . . .	34
3.12	Elements of the RF tag operating at 5.8 GHz. . . . .	35
3.13	The profile of the harvesting antenna. . . . .	37
3.14	The schematic of a a) conventional one-stage Dickson charge pump and b) two-stage Dickson charge pump. . . . .	40
3.15	The schematic of a one-stage Dickson charge pump with a class-F load. . .	40
3.16	Fabricated a) one-stage Dickson charge pump and b) two-stage Dickson charge pump with matching networks and class-F loads. . . . .	41
3.17	The simulation and measurement results of the a) DC output voltage and b) RF-DC power conversion efficiency of the one-stage charge pump at different input power levels when connected to a 3000 $\Omega$ load resistor. . . .	42

3.18	The simulation and measurement results of the a) DC output voltage and b) RF-DC power conversion efficiency of the two-stage charge pump at different input power levels when connected to a $3000\ \Omega$ load resistor. . . .	43
3.19	The measured DC output voltage of the one-stage charge pump at different input power levels when connected to the RF tag circuit . . . . .	44
3.20	The initial tantalum capacitor charging process of the power management circuit. The total time it takes to charge from 0 V to 3 V is 140 s when the input power is 1 dBm. . . . .	46
3.21	The operating/recharging duty cycle of the power management circuit when the input power is 1 dBm. The operating period lasts for 3 s and the recharging period takes 4.6 s. . . . .	47
3.22	The sampled, baseband I and Q waveforms received from the RF tag on orbit beginning on August 07, 2019 at 16:42 (UMT). The waveform consists of a header, two copies of the RF tag's temperature, and two copies of the burst counter. Samples are missing from the I channel, but were estimated using the corresponding samples from the Q channel. . . . .	48
3.23	Recorded temperature in Celsius over time in orbital period. The points in the yellow region were taken at the portion of an orbital period when RFTSat was in sunlight, and those in the grey region were taken at the portion when RFTSat was in darkness. . . . .	50
4.1	Received signal from semi-passive and tunneling tags. . . . .	56
4.2	Solid line: 2-way envelope delay spectrum of the multipath-rich indoor environment (time span: 100 ns, distance $d$ : 3 m between reader and tag antennas). The LoS and the multipath effects are highlighted. Stem plot: the CLEAN algorithm reconstruction of the 2-way envelope delay spectrum. The average time delay $\bar{\tau} = 25.0$ ns, due to multipath corresponds. Inset: setup used to estimate the multipath effects of the indoor scenario. VNA settings: center frequency 5.8 GHz; span 2 GHz; $d = 3$ m; # of points 1601; avg.: 16. . . . .	62
4.3	a) Reader and tag configuration used for indoor and outdoor measurements. $G_{tx} = G_{rx} = 7.5$ dBi, $G_t = 9$ dBi, $P_T = 3$ dBm, $d \in [5, 35]$ m. Photos of the b) indoor and c) outdoor setups used for long range tests. . . . .	64

4.4	The IQ constellation points in the 5.8 GHz band (5.751 to 5.763 GHz) for both the semi-passive and the tunneling tags measured indoor at a distance of 5 m from the reader. The tunneling tag provides a higher level of backscattered power. . . . .	65
4.5	a) Phases, and b) phase-differences between 13 adjacent channels measured indoor at 5 meters away from the reader for both the semi-passive ( $\circ$ ) and the tunneling tags ( $\square$ ). . . . .	66
4.6	a) Indoor, and b) outdoor calculated (dashed) and measured (solid) $P_{RSS}$ values. Data points are for both semi-passive ( $\circ$ ), and tunneling tags ( $\square$ ). . .	68
4.7	a indoor, and b) outdoor distance estimates $\hat{d}$ using RSS-based method (dashed) and RSP-based method (solid). Data points are for both semi-passive ( $\circ$ ), and tunneling tags ( $\square$ ). . . . .	69
4.8	a) Indoor, and b) outdoor distance errors $\epsilon$ for RSS-based (dashed) and RSP-based (solid) methods with calibration at 5 meters. Data points are for both semi-passive ( $\circ$ ), and tunneling tags ( $\square$ ). . . . .	70
4.9	Estimated errors $\epsilon$ and averages $\epsilon_{avg}$ with and without calibrations in a) indoor, and b) outdoor environments for the tunneling tag ( $\square$ ). . . . .	73
5.1	Schematic representations of RFID positioning system setups: (a) LoS in ideal case; (b) LoS with scattering and reflections; (c) diffraction due to an obstacle; and (d) propagation through a wall, or a floor. . . . .	77
5.2	(a) The experimental setup seen from the above. (b) Photo of the setup with the the tag at 5 m from the reader in LoS. (c) The cinder block in front of the tag for NLoS(o) conditions. . . . .	84
5.3	(a) Overview of the experimental setup in: (b)-(c) through-wall (NLoS(w)), and (d) LoS conditions. . . . .	85
5.4	$P_{RSS}$ values for semi-passive ( $\circ$ ) and tunneling tags ( $\square$ ) in LoS (dashed) and through-obstruction NLoS(o) (solid). . . . .	86
5.5	$P_{RSS}$ values for semi-passive ( $\circ$ ) and tunneling tags ( $\square$ ) in LoS (dashed) and through-wall NLoS(w) (solid). . . . .	87
5.6	Calibrated estimation errors in (a) meters, and (b) percent for LoS (dashed) and NLoS(o) (solid) conditions for the Semi-passive and tunneling tags. . .	88

5.7	Calibrated estimation errors in (a) meters, and (b) percent for LoS (dashed) and NLoS(w) (solid) conditions for the semi-passive and tunneling tags. . . . .	90
5.8	Calibrated estimation errors in percentage (left), and meters (right) in LoS and NLoS(o) conditions for the semi-passive and tunneling tags when using a slow hopping mode (top) or a fast hopping mode (bottom). The x-axis represents the estimation error in either meter or percentage, while the y-axis represents the CDF probability of the estimation error. . . . .	93
5.9	Calibrated estimation errors in percentage (left), and meters (right) in LoS and NLoS(w) conditions for the semi-passive and tunneling tags when using a slow hopping mode (top) or a fast hopping mode (bottom). The x-axis represents the estimation error in either meter or percentage, while the y-axis represents the CDF probability of the estimation error. . . . .	94
6.1	In the trilateration approach the location is estimated by intersecting three or more circles that identify the distance of an object from a target. The distance is here computed through the received signal phase. . . . .	97
6.2	Block diagram of the 5.8 GHz frequency hopping reader. The reader was placed on a mobile cart. . . . .	99
6.3	(a) GNU radio implementation and (b) logic flow diagram for data processing and frequency hopping in the real-time 2D positioning system. . . . .	101
6.4	(a) Experimental setup for the real-time RFID positioning system with three fixed tags and a mobile reader. (b) Fixed positions of the tags (used as anchor points) ( $\bigcirc$ ) and actual positions of the moving reader ( $\square$ ). . . . .	103
6.5	Empirical CDF of distance errors $\epsilon$ for RSP-based methods with calibration, including 120 data points for the reader-to-tag distance estimation error (1D error) CDF and 40 data points for the position estimation error (2D error) CDF. . . . .	104
6.6	Location estimates vs true reader locations for the 2D positioning system having three fixed tags and a moving reader. Fixed positions of the tags (used as anchor points) ( $\times$ ); actual positions of the moving reader ( $\square$ ); and measured positions of the reader ( $\times$ ). . . . .	105
7.1	Block diagram of the RFID reader used as channel sounder. . . . .	110

7.2	How channel sounding can be used to detect both LoS and multipath components in an RFID system. a) The transmitted, b) backscattered, and c) post-processed signals are shown. . . . .	111
7.3	The experimental setup seen (a) from the above and (b) from the reader with the tag placed at 100 m away. Photos of the (c) frequency hopping reader and (d) the tunneling tag. . . . .	115
7.4	Delay profile calculated using the IDFT of the a) normalized received signal ( <i>IDFT norm</i> ) and b) un-normalized received signal ( <i>IDFT un-norm</i> ) in frequency domain. The additional RSS information of un-normalized received signals can increase the detection accuracy of multipath components. . . . .	118
7.5	The RSS values of slow hopping mode in the frequency domain. The dips are caused by pedestrians and vehicles momentarily obstructing the LoS. . . . .	119
7.6	Empirical Cumulative Distribution Function (CDF) measured with different methods in a) slow hopping (dwell time = 10 ms) and b) fast hopping (dwell time = 2 ms) configurations. . . . .	120
7.7	Mean Estimation Errors measured with using different methods in a) slow hopping (dwell time = 10 ms) and b) fast hopping (dwell time = 2 ms) configurations from 20 m to 100 m. . . . .	122
A.1	The circuit schematic diagram of the reader's receive board. A IQ down-converter (Analog Device HMC951b) and a low-noise amplifier (Analog Device HMC902) are used in this design. . . . .	127
A.2	The schematic diagram of the DSP's emulator board. This design is based on the reference design available in [102]. . . . .	128
A.3	The circuit schematic diagram of the DSP. A DSP chip (Texas Instrument Piccolo F28027) is used in this design. The reference design is available in [102]. . . . .	129
A.4	The circuit schematic diagram of the base-band amplifier board. Operational amplifiers (Texas Instrument OPA2626) are used in this design. . . . .	130
A.5	The circuit schematic diagram of the 5.8 GHz conventional tag board. A microcontroller (Texas Instrument MSP430f2132) and a RF switch (Analog Device HMC8038) are used in this design. . . . .	131
B.1	Photo of the reader setup. . . . .	132

## LIST OF ACRONYMS

<b>ADC</b>	Analog-to-Digital Converter
<b>AoA</b>	Angel of Arrival
<b>BPSK</b>	Binary Phase Shift Keying
<b>CDF</b>	Cumulative Distribution Function
<b>CDMA</b>	Code Division Multiple Access
<b>CFR</b>	Code of Federal Regulations
<b>COTS</b>	Commercial Off-The-Shelf
<b>DBN</b>	Deep Brief Network
<b>DC</b>	Direct Current
<b>DFT</b>	Discrete Fourier Transform
<b>DSP</b>	Digital Signal Processor
<b>EIRP</b>	Equivalent Isotropically Radiated Power
<b>FCC</b>	Federal Communications Commission
<b>FDMA</b>	Frequency Division Multiple Access
<b>FFT</b>	Fast Fourier Transform
<b>GLONASS</b>	Global Navigation Satellite System
<b>GNSS</b>	Global Navigation Satellite Systems
<b>GPS</b>	Global Positioning System
<b>HF</b>	High-Frequency
<b>HIMR</b>	Hibrid Inertial Microwave Relectometry
<b>I</b>	In-phase
<b>IC</b>	Intergrated Circuits

**IDFT** Inverse Discrete Fourier Transform

**INS** Inertial Navigation System

**IoT** Internet of Things

**ISM** Industrial, Scientific and Medical

**L-VIRT** Localization of RFID tags with Virtual Reference Tags

**LANDMARC** Location Identification Based on Dynamic Active RFID Calibration

**LEO** Low-Earth Orbit

**LF** Low-Frequency

**LNA** Low-Noise Amplifier

**LO** Local Oscillator

**LoS** Line-of-Sight

**NLoS** Non-Line-of-Sight

**NSL** Near Space Launch

**OOK** On-Off Keying

**PA** Power Amplifier

**PCB** Printed Circuit Boards

**PDoA** Phase Difference of Arrival

**PLL** Phase-Lock Loop

**Q** Quadrature

**RDMA** Range Division Multiple Access

**RFID** Radio Frequency Identification

**RFTSat** Radio Frequency Tag Satellite

**RMS** Root-Mean-Square

**RSP** Received Signal Phase

**RSS** Received Signal Strength

**RSSI** Received Signal Strength Indicator

**Rx** Receive

**SDMA** Space Division Multiple Access

**SDR** Software-Defined Radio

**SFCW** Stepped-Frequency Continuous-Wave

**SHF** Super-High-Frequency

**SIR** Signal-to-Interference Ratio

**SNR** Signal-to-Noise Ratio

**SPI** Peripheral Interface Bus

**SpT** Semi-passive Tag

**TDMA** Time Division Multiple Access

**TDOA** Time Difference of Arrival

**ToA** Time of Arrival

**TT** Tunneling Tag

**Tx** Transmit

**UHF** Ultra-High-Frequency

**USRP** Universal Software Radio Peripheral

**VIRE** Active RFID-based Localization Using Virtual Reference Elimination

**VNA** Vector Network Analyzer



## SUMMARY

Fine-scale positioning systems using inexpensive, low-power, and reliable smart tags enables numerous commercial and scientific applications. Internet of Things (IoT) applications, such as asset tracking, contact tracing, and autonomous driving, require wireless technologies with both the long ranges of conventional wireless links and the low power consumption of passive and semi-passive Radio Frequency Identification (RFID) tags [1, 2]. Results in [3] have shown how a 5.8 GHz Tunneling RFID tag can significantly increase the range of backscatter radio links while consuming very low power.

This dissertation proves that using the Received Signal Phase (RSP)-based positioning method along with tunneling backscatter communication at 5.8 GHz breaks the range limit of fine-scale RFID positioning systems. A frequency hopping reader operating in the 5.8 GHz Industrial, Scientific and Medical (ISM) band is designed and implemented in this work. Experimental results yield a one-dimensional distance estimation error of less than 1% at ranges of 100 m when a clear Line-of-Sight (LoS) is available in indoor and outdoor environments. Compared to Received Signal Strength (RSS)-based positioning techniques, the average positioning accuracy is improved by a factor of 51 at ranges of tens of meters. In Non-Line-of-Sight (NLoS) scenarios, the proposed system achieves an estimation error of less than 1.9%. Experimental results also demonstrate that the RSP-based positioning technique allows estimating a mobile reader's two-dimensional position with an average error of 0.17 m in an outdoor environment. A channel sounder is also implemented using the same hardware configuration, which further increases the accuracy in multipath environments. Calculation based on the system specifications projects a sub-meter level accuracy at ranges of more than 1 km is feasible using the proposed method.

# **CHAPTER 1**

## **INTRODUCTION AND BACKGROUND**

Ultra-precise wireless positioning could revolutionize smartphone applications, augmented reality experiences, asset tracking, and autonomous vehicle navigation, as well as opening up entirely new use cases for Internet of Things (IoT) devices. A qualified system that can apply to drone delivery, inventory tracking, and contact tracing requires devices with at least the following features: long battery life, low cost, high tracking accuracy, and long communication range. However, a solution that satisfies all of these requirements is not available in the IoT industry yet. For instance, Global Positioning System (GPS) drains battery life and have low accuracy in urban and indoor environments [4] [5]; Bluetooth and WiFi require a dense RF infrastructure to cover indoor areas [6]; while passive Radio Frequency Identification (RFID) tags have short ranges [7].

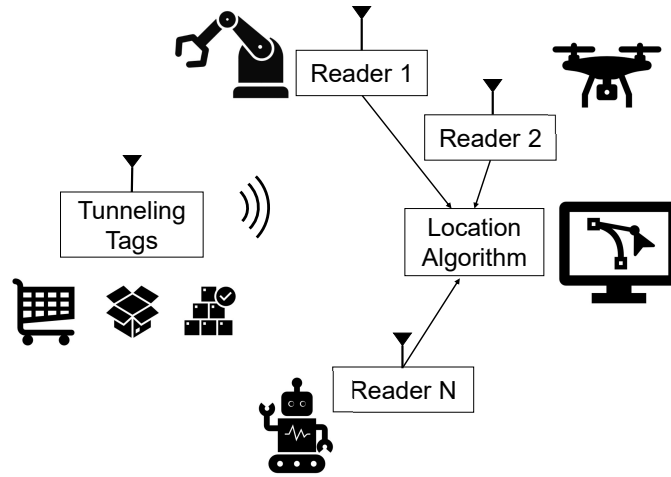
RFID, the most commonly seen backscatter communication technology, relies on passive reflection and modulation of an incident electromagnetic wave. RFID systems typically find applications for identifying objects because of their simplicity and low-power characteristics [8]. RFID readers perform fully coherent detection of the backscattered signal, which can utilize the Received Signal Phase (RSP) of backscattered signals to calculate the position and velocity of a tagged object [9].

The rapid development of the IoT and RFID industry is witnessing an increasing demand for systems that can identify people and objects together with their locations. Nevertheless, some classical wireless positioning approaches cannot be effectively applied to passive Ultra-High-Frequency (UHF) RFIDs because of their short-range (up to 10 m) and narrow bands (26 MHz) characteristics, which do not allow readers to operate in the short pulse mode required for Time Difference of Arrival (TDOA) methods [9]. Fundamental limitations (e.g., communication range and positioning accuracy) in RFID-based

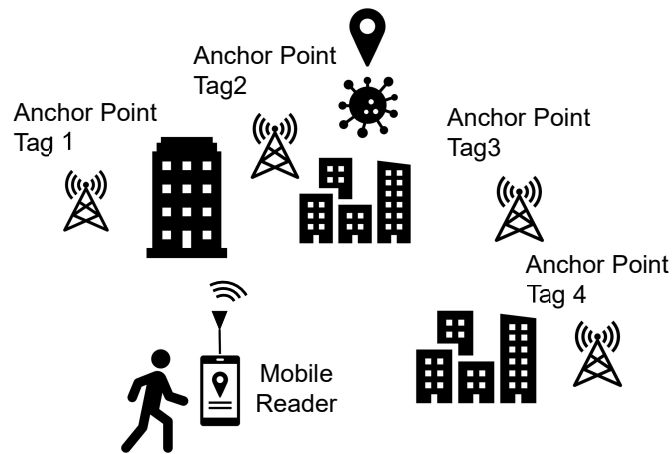
positioning techniques hampered the massive deployment of RFID-based positioning systems. Consequently, RFID technology to date is only a short-range wireless communication technique.

The objectives of this work are to overcome fundamental limits in RFID technology and enable new wireless technologies for IoT applications that require the long ranges of conventional wireless links, the low power consumption of passive and semi-passive RFID tags, and accurate location estimations not achievable using conventional RFID localization systems. Results in this dissertation show that a low-powered tunneling tag, operating at 5.8 GHz Industrial, Scientific and Medical (ISM) band, can significantly increase the range of backscatter radio links and providing fine-scale position estimation accuracy using phase-based methods at long distances. Identifying the real-time position of both objects and people without a clear Line-of-Sight (LoS) is another key feature for versatile sensing applications. Rescuers, task forces, and security staff can benefit from a positioning technology that would protect them from unpredictable threats in unknown buildings and environments. In this work, the proposed phase-based method is also studied in Non-Line-of-Sight (NLoS) environments.

As shown in Figure 1.1, long-range RFID positioning systems can provide accurate item locations in a large area for precise asset tracking. Tunneling tags mounted on vehicles, people, or goods will assist driver-less cars, facilitate intelligent drone delivery, and monitor the transportation of goods in real-time. Sports analysts could capture the movements and collisions of sports players during a match for scientific, medical, or entertainment purposes by tracking helmets equipped with tunneling tags. Moreover, a mobile device equipped with an RFID reader can communicate with tunneling tags deployed at known locations as anchor points to obtain its real-time position. As one use case, a drone equipped with a low-power and lightweight RFID reader can navigate itself using anchor tags in the warehouse for inventory management. People with the reader built-in their smartphones can also receive notification and location updates for contact tracing purposes



(a)



(b)

Figure 1.1: Illustration of two different uses of real-time RFID positioning systems. (a) *asset tracking* mode: fixed readers collect data from one or more tunneling tags to locate and track assets; (b) *navigation* mode: a mobile, low-powered reader grabs data from multiple anchor points for accurate contact tracing.

during pandemics.

The results from this work could disrupt existing positioning approaches for IoT applications – which have severe range and environmental limitations – by using hardware already available in every smartphone. Today’s smartphones are already equipped with RF

transceivers, RF switches, and microwave antennas. By adding long-range precise localization capabilities, an entirely new class of low-powered positioning systems would become available for the next-generation cellular networks [10] [11].

## 1.1 RFID System Overview

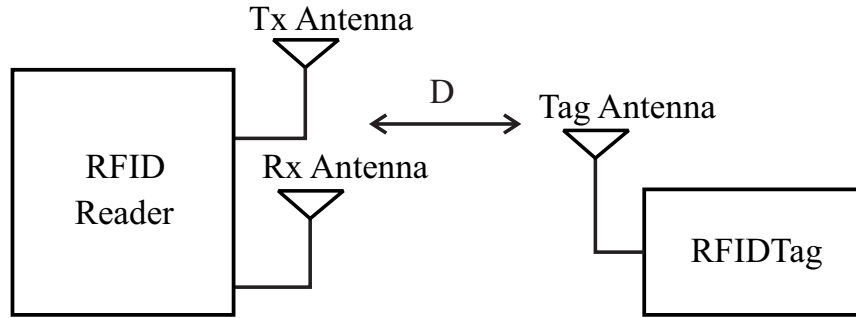


Figure 1.2: The RFID backscatter system

Figure 1.2 presents a conventional RFID backscatter system, including an RFID reader and tag. The RFID reader is usually an RF transceiver that acts as an interrogator in most commercialized RFID systems. The tag, acting as a transponder, is placed at a certain distance ( $D$ ) from the reader. The reader's Transmit (Tx) antenna transmits continuous electromagnetic waves at the operating frequency and irradiates the tag's antenna. The modulator integrated with the tag antenna modulates these waves using load modulation and backscatter modulated waves back to the Receive (Rx) antenna of the reader. RFID tags provide a means of very low-power sensing and communication for a wide variety of applications, including RFID for intelligent transportation systems [12], structural health monitoring [13, 14], and orientation sensing[15]. Based on their power sources, RFID tags can be divided into three categories: passive, semi-passive, and active tags. Passive RFID tags utilize simple and energy-efficient circuitry without batteries, which rely on harvesting energy from the incident electromagnetic field. Semi-passive tags, also known as battery-assisted tags, are usually powered by small coin batteries, which provide the tags chances

of implementing peripheral sensor circuitry and operating at longer ranges than passive tags.

In chapter 3, a low-power, compact frequency hopping RFID reader is introduced, which has great potential for use in sensing applications, including structural health monitoring, asset tracking, inventory management, and sensitive field measurements. Figure 1.3 illustrates a simplified block diagram of the RFID reader based on direct conversion configuration, which reduces the complexity, the size of the antenna, and the number of components. The RF output signal is generated by the Local Oscillator (LO) operating the 5725-5875 MHz frequency ISM band, amplified by a power amplifier (optional), then radiated out by the Tx antenna. The reader utilizes a Rx antenna and a Low-Noise Amplifier (LNA) to receive and amplify the backscattered signal. A downconverter is then used to output both In-phase (I) and Quadrature (Q) channel baseband signal. The baseband signal is then sampled by a digital signal processor with a built-in Analog-to-Digital Converter (ADC) or a Software-Defined Radio (SDR) platform (e.g. Universal Software Radio Peripheral (USRP) N210). The sampled signal can be processed using SDR or saved in the local drive for post-processing in MATLAB.

The RFID reader proposed in chapter 3 has been launched into low-earth orbit aboard the Radio Frequency Tag Satellite (RFTSat) and served as a demonstration of backscatter communications in space. On 26 July 2019, a Falcon 9 rocket launched the CRS SpX-18 (Dragon) mission to resupply the international space station. As part of its obligatory CubeSat payload, RFTsat was launched to test a new space-certified, ultra-low-power 5.8 GHz microwave RFID reader. A 5.8 GHz passive RF tag was energized at a distance by the reader; the tag backscattered temperature sensor data to the RFID reader.

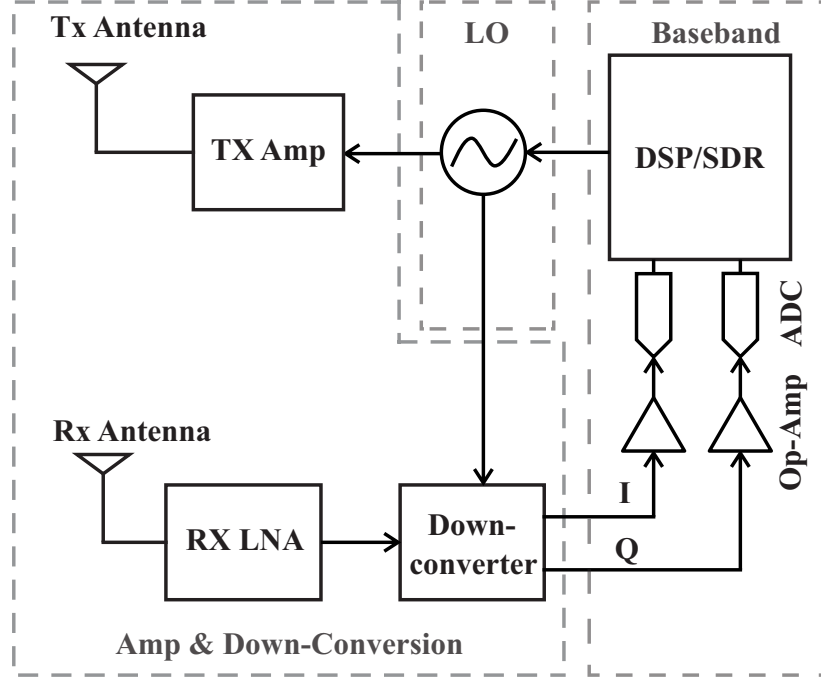


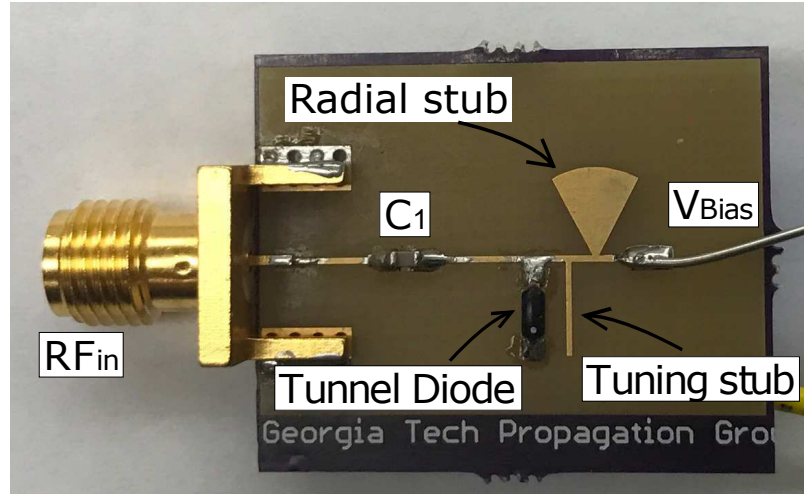
Figure 1.3: Elements of the RF tag reader operating at 5.8GHz.

## 1.2 The Tunneling Effect

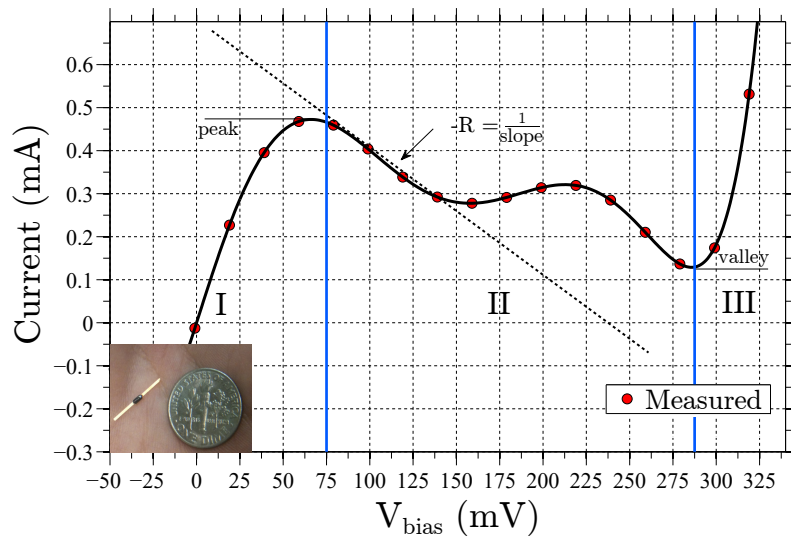
The well known link budget equation of a backscattering system:

$$P_r = P_T G_{tx} G_{rx} G_t^2 \left( \frac{\lambda}{4\pi d} \right)^4 M, \quad (1.1)$$

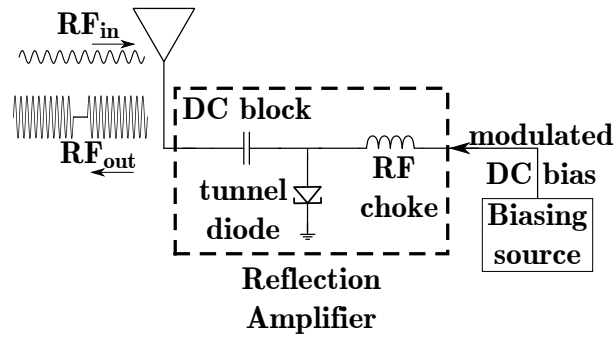
can involve one tag with gain  $G_t$ , and one co-located bistatic reader with transmitting and receiving antenna gains  $G_{tx}$  and  $G_{rx}$ , respectively [17]. It suggests that a system engineer can operate on some parameters to improve the reading distance  $d$  between the reader and the transponder. For example, a modulation factor  $M = \frac{1}{4} |\Gamma_1 - \Gamma_2|^2$  [17] can achieve values greater than 1 when active loads are used. In particular, a tunneling reflection amplifier based on tunnel diodes and mounted on a tunneling tag (Figure 1.4, [1] [18]) is an efficient way to obtain a modulation factor  $M > 1$  with very low biasing power (21.32  $\mu$ W at 80 mV [19]). The tunneling tag exploits the *tunneling effect* that, as shown in the region **I** of Figure 1.4b, takes place for extremely low reverse and forward biasing voltages



a)



b)



c)

Figure 1.4: a) Microstrip line structure of the tunneling reflection amplifier as in [16]; b) the measured IV curve [1] of tunnel diode model MBD5057 c) The block diagram of the tunneling tag.



applied to a tunnel diode. When the forward biasing voltage slightly increases, the tunneling effect fades and the device displays a negative resistance  $-R_L$ . The corresponding amplitude of the reflection coefficient  $|\Gamma| = \left| \frac{Z_L - Z_{ant}}{Z_L + Z_{ant}^*} \right| = \frac{-R_L - Z_{ant}}{-R_L + Z_{ant}^*}$  can be made greater than one ( $|\Gamma| > 1$ , hence  $M > 1$ ) by matching the value of  $-R_L$  with a properly matched antenna impedance  $Z_{ant}$ . Therefore, the on/off biasing of the tunneling diode can modulate, backscatter, and amplify an impinging RF signal and enhance the backscattering link range.

### 1.3 RSP-Based Positioning

#### 1.3.1 RSP-based Ranging Method

The transmitter and receiver of an RFID reader usually share the same local oscillator, giving it the capability of near-perfect phase coherence detection. The demodulated complex received signal  $\tilde{S}(f_c)$  at frequency  $f$  can be express by:

$$\tilde{S}(f_c) = A(f_c) \exp [-j (\varphi_{ps}(f_c) + \varphi_m(f_c) + \varphi_0(f_c))], \quad (1.2)$$

where  $A(f_c)$  is the magnitude of the received signal at the carrier frequency  $f_c$ ,  $\varphi_{ps}(f_c) = \frac{4\pi f_c d}{c}$  is the phase shift due to the propagated distance  $d$ ,  $\varphi_0(f_c)$  is the phase offset caused by the propagation within hardware (e.g. cables, antennas, tag modulation, and other reader components), and  $\varphi_m(f_c)$  is the phase offset caused by the multipath channel.

With an RSP-based method, the estimated distance  $\hat{d}$  between a reader and a tag can be calculated using the received signal phase [20]:

$$\hat{d} = \frac{\lambda_e}{4\pi N} \sum_{n=1}^{N-1} (\varphi_{n+1}(f_n + 1) - \varphi_n(f_n)), \quad (1.3)$$

with  $\varphi_n$  and  $\varphi_{n+1}$  being the measured phases of the received signals obtained by the reader at carrier frequencies  $f_n$  and  $f_{n+1}$ , respectively;  $N$  being the number of the frequency

channels; and  $\lambda_e = \frac{c}{\Delta f}$  the equivalent wavelength obtained when a uniform frequency step,  $\Delta f = f_{n+1} - f_n$ , is used. It is important to highlight that the maximum detection range  $\hat{d}_{max}$  of the RSP-based method is determined by the minimum frequency step  $\Delta f$  of the reader:  $\hat{d}_{max} = \frac{c}{2\Delta f} = \frac{\lambda_e}{2}$ .

### 1.3.2 Trilateration approach

To obtain the two-dimensional position of a target tag, multiple readers collaborate to localize the tag by using the trilateration approach. Figure 1.5 illustrates the trilateration approach that finds the position of a tagged object in a coplanar scenario. At least three readers at known positions and three measurements of distance are required in this case. The location of the target tag can be determined using the intersection of the circles centered at the known reader locations with radius estimated using the phase-based method. For non-coplanar or three-dimensional scenarios, at least four readers and distance readings are necessary to find the intersection point.

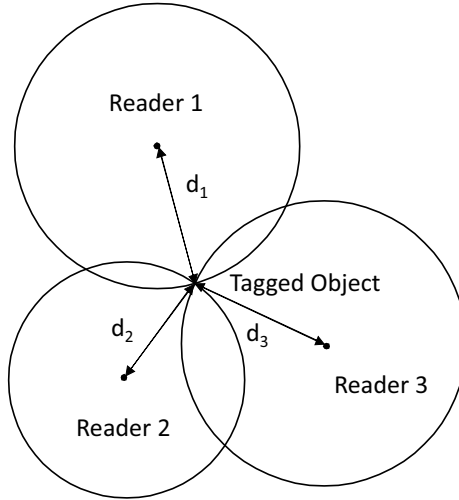


Figure 1.5: In the trilateration approach the location is estimated by intersection of the three or more circles formed by evaluation of the target object's distance using its received signal phase.

## 1.4 Document Organization

The goal of this dissertation is to demonstrate how a novel 5.8 GHz RSP-based RFID positioning system achieves long-range and high-precision positioning using tunneling tags.

This dissertation is organized as follows:

- Chapter 1 introduces the background of backscatter communication using tunneling tags and how RSP-based positioning works for conventional semi-passive tags and tunneling tags;
- Chapter 2 discusses the state-of-art of RF and RFID-based positioning, which illustrates the range and accuracy advantage of RSP-based positioning using tunneling tags over other techniques;
- Chapter 3 presents the 5.8 GHz RF backscatter system architecture, including the design of the RF transceiver, semi-passive tag, energy harvesting tag, and the space mission utilizing the system;
- Chapter 4 demonstrates the RSP-based ranging technique and tunneling tags for extending the range and accuracy of RFID positioning;
- Chapter 5 analyzes the positioning performance of RSP-based positioning technique and tunneling tags in NLoS environments;
- Chapter 6 describes the design of a real-time 2D RSP-based positioning system using tunneling tags and shows the positioning accuracy of it in an outdoor environment;
- Chapter 7 proves that the proposed system can also be used as a channel sounding, and the channel sounding algorithm improves the ranging accuracy at long distances in realistic environments;
- Chapter 8 summarizes the achievements in this dissertation and discusses the future work.

## **CHAPTER 2**

### **LITERATURE SURVEY**

In the past few decades, the rapid development of the IoT and wireless communication industry motivates increasing demands for versatile systems that can accurately identify and localize people and objects in realistic environments. In this chapter, a literature survey is presented in the following sections: (1) Overview of positioning systems; (2) RFID frequency bands and range limits; (3) Overview of RFID positioning techniques; (4) Accuracy and range of RFID-based localization techniques.

#### **2.1 Overview of Positioning Systems**

Numerous position tracking solutions have been developed to determine the absolute or relative location within a coordinate system of people and objects [21]. In general, positioning systems can be classified in various ways based on different criteria that depend on the purpose, coverage area, and infrastructures. Positioning systems can be classified into two major categories, Global Navigation Satellite Systems (GNSS) and terrestrial positioning systems, as shown in Figure 2.1 [4].

GNSS, GPS, Global Navigation Satellite System (GLONASS), Galileo, and BeiDou systems have been effectively demonstrated for many outdoors navigation applications across the world. Relying on multiple Earth-orbiting satellites, GNSS-enabled devices can track their latitude, longitude, and altitude, which determines their locations on earth. Even though GNSS has provided reliable outdoor location service since the early 1980s, they are not yet capable of accurate enough positioning inside of buildings and in clustered environments due to signal attenuation and multipath interference [4].

In contrast, terrestrial positioning systems estimate the location of targeted objects by collecting information from sensory devices, transponders, and local RF base stations on

earth. Commonly used terrestrial positioning systems can be divided into three categories by their techniques: (1) Device-less, (2) Inertial Navigation System (INS) (inertial navigation systems), and (3) RF-based position tracking system [4, 11]. The taxonomy of location and tracking systems are present in Figure 2.1. Device-less positioning systems do not require any sensors or transponders on the targeted object, like vision-based tracking systems and radar systems. INS uses sensory data (e.g., gyroscopes and accelerometers) to track the position, velocity, and orientation and the target relative to a known initial state. RF-based positioning systems track the location of targeted objects by using RF transponders and interrogators to collect information via RF communication links. Most of the terrestrial positioning systems have better accuracy in indoor and clustered environments than GNSS, but are usually limited by their range for outdoor navigation. RFID positioning systems, as other RF-based positioning systems, have the advantage of lower power and less complexity on the tag side, but usually are considered shorter range than other RF-based techniques (e.g. WLAN, Bluetooth, Zigbee, etc.). This work uses backscatter communication, frequency hopping RFID reader, and tunneling tags to achieve long-range RFID positioning. Therefore, this chapter focuses on RFID-based positioning systems and techniques used by them, as highlighted in Figure 2.1.

## **2.2 RFID Frequency Bands and Range Limits**

Backscatter tags have been used in a wide variety of low-power sensing and communication applications, including RFID for intelligent transportation systems [12], structural health monitoring [13, 14], indoor vehicle localization [22], and orientation sensing [15]. Positioning an RFID tag with high accuracy at a long distance in a realistic environment remains challenging. The RFID industry employs frequencies from around 100 kHz to over 5 GHz for various RFID systems. Instead of operating across the whole frequency spectrum, RFID systems are usually concentrated in narrow bands that have been made available by regulators. The most commonly used RFID bands are 125/134 KHz, 13.56 MHz, 433 MHz,

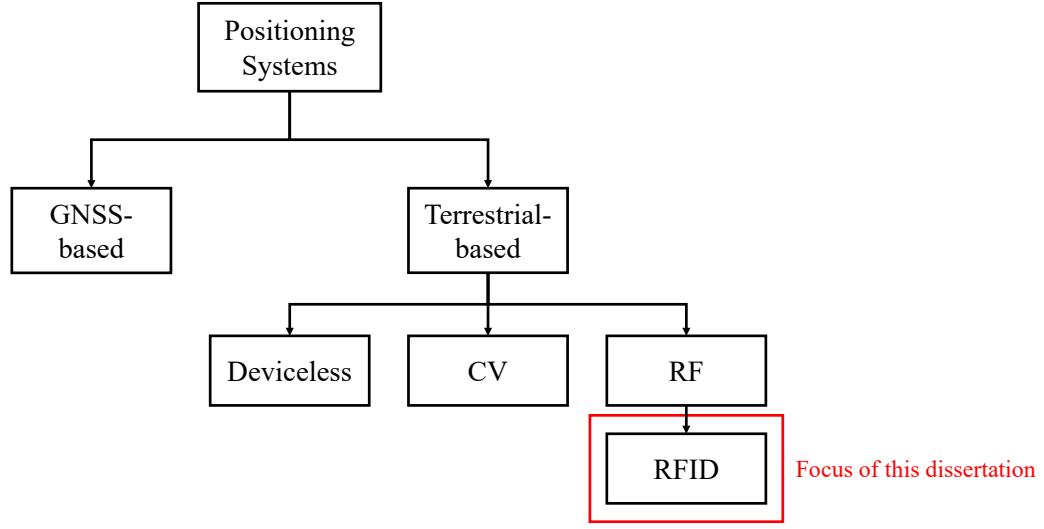


Figure 2.1: Overview and classification of positioning systems.

860-960 MHz, 2.4-2.45 GHz, and 5.8 GHz. For RFID positioning systems, range and accuracy are two of the most significant characteristics, usually directly related to the frequency band and the corresponding wavelength.

The earliest RFID systems operate at 125/134 KHz frequency band, which is also known as the Low-Frequency (LF) band. LF band RFID system relies on inductive coupling by direct contacting. RFID systems operate at High-Frequency (HF) band (13.56 MHz) also utilize inductive coupling but provide higher ranges than LF band RFID systems. However, both LF and HF band RFID systems have insufficient ranges and do not support accurate positioning due to long wavelength. Readers and tags that operate from 433 MHz to 2.45 GHz are all classified as the UHF band RFID systems. Most RFID positioning systems and well-known RFID localization techniques operate at this frequency band due to its longer range and shorter wavelength than LF and HF RFID systems. Recently, Super-High-Frequency (SHF) band, as known as microwave band, and THz/mm-wave band are brought up for the next generation of RFID systems. SHF band devices usually operate around 5 GHz. THz band devices use frequency bands that are higher than 20 GHz.

### 2.3 Overview of RFID Positioning Techniques

The objective of RFID positioning systems is to estimate the position of RFID-tagged objects by using one or multiple RFID readers that gather information from tags. A low-power RFID system that can identify and localize the tagged item simultaneously is a competitive tool for location services in an IoT application. RFID readers, with coherent detection capability, collect various backscattered signal characteristics from the targeted tags, including Received Signal Strength (RSS), RSP, and additional sensory information. RFID positioning systems can be divided into three categories based on the characteristics and approaches utilized by their localization techniques: 1) RSS-based techniques, 2) RSP-based techniques, and 3) Hybrid techniques [11]. Figure 2.2 shows the classification of RFID positioning systems based on the proposed method.

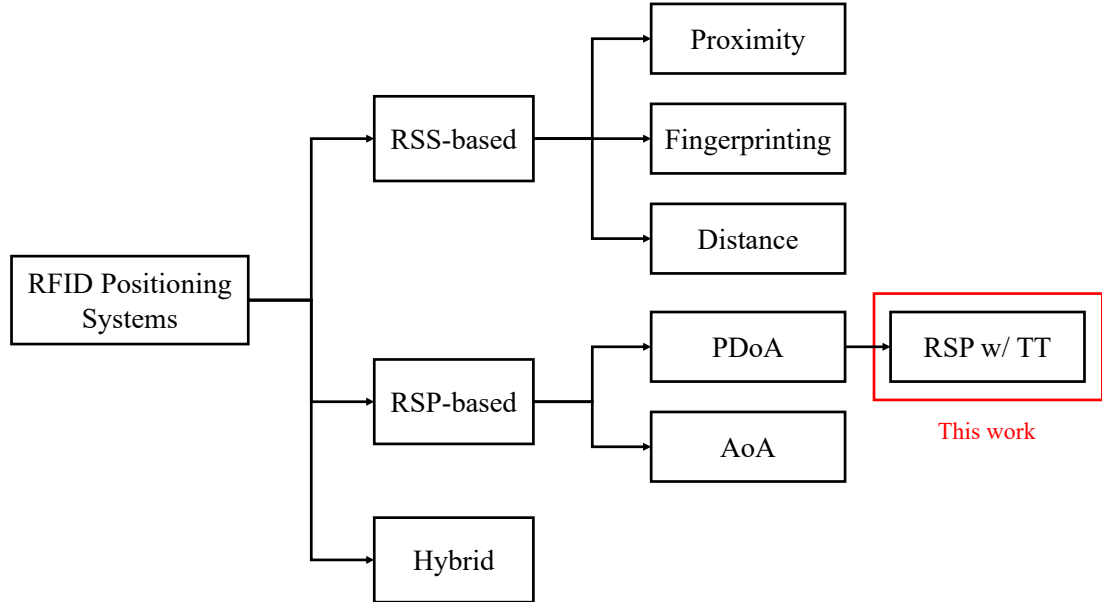


Figure 2.2: Overview and classification of RFID positioning systems.

### 2.3.1 RSS-Based RFID Localization Techniques

The most common RFID positioning and tracking systems estimate the reader-to-tag distances using the RSS. They are classified into proximity-based techniques [23, 24]; RF fingerprint techniques [25, 26, 27, 28]; and distance-based techniques [29, 30, 31, 32]. However, RSS-based methods suffer from poor accuracy, especially when the target is far away from the reader. Therefore, complicated RF infrastructure is required to achieve reasonable accuracy in a large area when using RSS-based techniques.

Proximity and RF fingerprint techniques require a set of reference tags or reference readers as markers. Proximity approaches deploy reference tags/readers in a grid with known positions and use the readability of the object identity to determine its position in the area of interest. RSS or Received Signal Strength Indicator (RSSI) can be used to narrow down the location estimation to a single grid. The localization accuracy of proximity approaches is influenced by the hardware implementation, and localization algorithms [23, 24].

Although RF-fingerprint techniques also require pre-installed reference tags/readers, they estimate the location of target objects by comparing radio transmission characteristics, also known as RF-fingerprint, to the information pre-stored in the system. RF characteristics like RSS or RSSI are usually measured in advance as the RF fingerprints. The most well-known and cited RF-fingerprint approaches are Location Identification Based on Dynamic Active RFID Calibration (LANDMARC) [25, 27], Active RFID-based Localization Using Virtual Reference Elimination (VIRE) [33], and Localization of RFID tags with Virtual Reference Tags (L-VIRT) [26]. Although RF-fingerprint techniques can track the location of the target in indoor environments reliably, the major issue of these approaches is the high cost due to the vast number of reference tags/readers and high implementation complexity.

RSS is also widely used by a variety of distance-based positioning techniques in a broad frequency spectrum from HF to UHF [29, 30, 31]. In distance-based RFID positioning sys-



tems, RSS is measured to estimate the distance between tagged objects and readers by using the path loss equation given in Equation 1.1 [17]. Despite its simplicity, RSS measurements suffer from poor accuracy caused by shadowing and multipath effects. Although Time of Arrival (ToA), TDOA, and Phase Difference of Arrival (PDoA) are utilized to obtain the distance in many other RF positioning systems, TOA and TDOA cannot be effectively applied to HF or UHF RFID positioning systems because their short-range and narrow frequency bands do not allow readers to operate in the short-pulse mode with enough time resolution [9].

### 2.3.2 RSP-Based RFID positioning Techniques

Recent papers have demonstrated that *Received Signal Phase* (RSP)-based RFID localization systems can achieve high ranging accuracy by using various techniques[9] [34] [20]. Nikitin *et al.* summarize RFID positioning techniques based on Phase Difference of Arrival (PDoA), including TD (Time Domain), FD (Frequency Domain), and SD (Spatial Domain) PDoA methods [9]. Povalac *et al.* applied PDoA ranging method to UHF RFID tags and achieved a mean absolute estimation error of 0.14 m at 2.5 m. Cnaan-on *et al.* demonstrate multi-channel backscatter communication and ranging using active backscatter RF tags [34]. Zhou *et al.* proposed and characterized a dual-frequency phase-based ranging technique for backscatter RF tags. Results in [9] also show that the TD-PDoA method performs more robustly in multipath environments compared to FD-PDoA, due to the narrow bandwidth in the UHF band (26 MHz). A phase-based localization method combined with sensory data for tracking mobile nodes equipped with a UHF RFID system was demonstrated in [35].

Angle of Arrival (AoA) techniques also utilize RSP, allowing RFID of readers with active antenna arrays to find the direction of arrival of the incident wave [36, 37]. However, the accuracy of the AoA techniques highly depends on the number of elements in the antenna array used by the RFID reader. AoA-based RFID positioning systems have to

make trade-offs between complicated and expensive reader infrastructures with angular resolution and accuracy.

### 2.3.3 Hybrid RFID positioning Technique

Researchers have developed many hybrid RFID localization techniques to increase the accuracy of conventional RFID-based positioning techniques, combining various other positioning techniques with RFID-based systems, including heterogeneous techniques and post-processing approaches. Heterogeneous approaches take advantage of another RF or non-RF positioning technique, such as computer vision [38, 39], WLAN [40], and Zigbee [41], to mitigate the shadowing, interference, and multipath effect.

Akbar et al. developed a new INS-assisted RFID localization tracking scheme with cm-level to decimeter-level tracking accuracy, Hibrid Inertial Microwave Relectometry (HIMR), at 5.8 GHz ISM band[10, 11]. HIMR scheme estimated the velocity and position of the tag by measuring the received signal RSP and RSS and combined them with the reflected inertial acceleration data from a tag-mounted, 9-axis inertial accelerator in data post-processing. The HIMR scheme did not require reference tags or an external system for localization.

Other post-processing techniques improve the hybrid technique using Kalman filter and machine learning, which may further mitigate environmental dependant factors like multipath fading, interference in dynamic environments, and measurement errors. Chai, et al. integrated robust support vector regression and Kalman filter to improve the localization accuracy of a reference-based RFID tracking system [42]. Simulation results in [43] showed that by using various versions of the Kalman filter, the tracking accuracy of HIMR scheme could be further improved. Zhang et al. proposed a 3D structure prediction system based on the combination of Deep Brief Network (DBN), computer vision, and conventional reference-based RFID positioning system, and reduced the tracking error to 0.168 m [44].

## 2.4 Accuracy and Range of RFID-based Positioning Techniques

Most RFID-based IoT applications require reliable communication between readers and tags in various environments at different distances. Two significant challenges involved in designing RFID positioning systems are improving the accuracy and range. Usually, the accuracy of the same positioning system is degraded when tagged objects are close to the maximum reading range. Multiple factors also affect the precision and coverage of positioning systems, such as the frequency band used by the RFID system, the sensitivity of the RFID reader, antenna gain, localization techniques used by the system, environmental factors, and the availability of clear LoS between tags and readers.

Although researches have improved the accuracy, few techniques have been proposed to improve distance estimation accuracy at long distances. Many researchers have built RSS-based or RSP-based positioning systems at higher frequency bands (e.g., 5.8 GHz) to achieve higher accuracy brought by the shorter wavelength and broader bandwidth. Nonetheless, higher frequencies bring shorter communication ranges due to the higher path loss. Therefore, positioning an RFID tag with high accuracy and a long distance in a multipath-rich environment remains challenging. In the last few years, researchers have proposed solutions to overcome the range limits of passive and semi-passive RFID tags [1, 2]. Experimental results in [3] have shown how a 5.8 GHz RFID tunneling tag can significantly increase the range of backscatter radio links while consuming very low power. Authors in [45, 46, 47, 2] have suggested equipping RFID tags with Van Atta-based Arrays [48] to increase the communication range further while maintaining a wide field-of-view.

A summary of the state-of-the-art is shown in Figure 2.3 where the errors (in %) are calculated as the ratio between the mean error at the maximum distance and the maximum distance itself<sup>1</sup>. In this dissertation, a mean error of 0.45% is observed when the tunneling tag is placed at 20 m to 100 m by using a channel sounding method in chapter 7. Projected results can be given by increase the transmit power and reader's sensitivity. In the 5.8 GHz

---

<sup>1</sup>When this mean error is not reported, an average error is calculated among all the achieved distances.

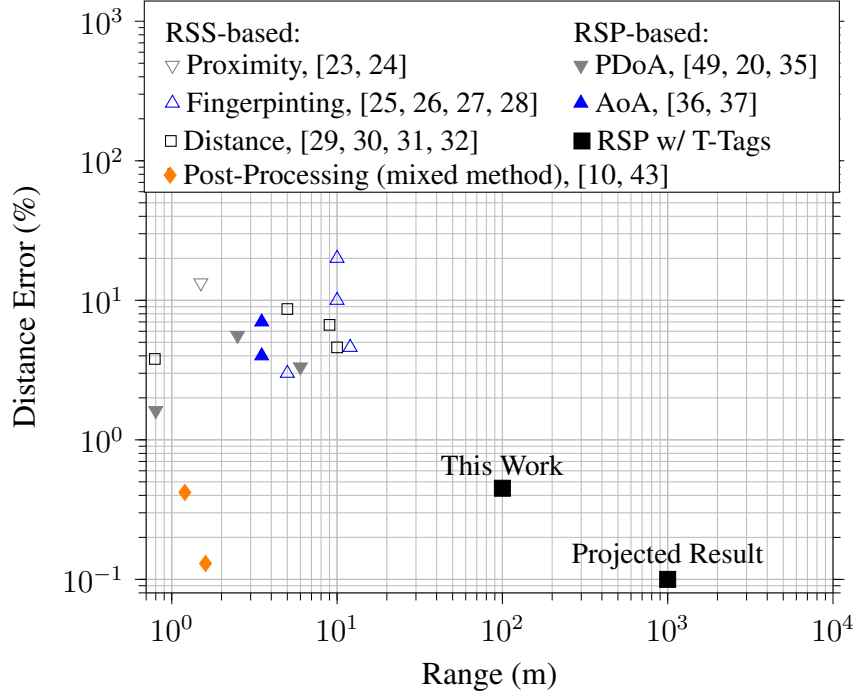


Figure 2.3: RFID positioning and tracking techniques, state-of-the-art and prediction of what will be obtained by combining Tunneling Tags (TT) and RSP-based positioning approaches. Comparisons were made in terms of reported distance errors and maximum ranges.

ISM band, a 150 MHz bandwidth is available, giving a ranging resolution of 1 m (0.1% at 1000 m).

## **CHAPTER 3**

### **FREQUENCY HOPPING RFID SYSTEM AT 5.8 GHZ FOR SPACE SENSING MISSION AND TERRESTRIAL APPLICATIONS**

#### **3.1 Introduction**

This chapter presents the design of a frequency hopping RFID reader at 5.8 GHz ISM band. Because of the low-power consumption and small profile, our RFID backscatter system can operate in RFTSat, a 3U nanosatellite (10 x 10 x 34 cm) designed by undergraduate students at Northwest Nazarene University (NNU). The RFTSat mission is to demonstrate the use of 5.8 GHz distributed sensor tags deployed from a CubeSat in a Low-Earth Orbit (LEO). RFTSat derives its power operating power from solar cells and stores energy in lithium-ion batteries, which limits the power consumption of the reader system under 4 W. On 26 July 2019, a Falcon 9 rocket launched the CRS SpX-18 (Dragon) mission to resupply the international space station. As part of its obligatory CubeSat payload, RFTsat was launched to test a new space-certified, ultra-low-power 5.8 GHz microwave RFID reader. This reader and tag combo was designed and built entirely by the team at Georgia Tech [50]. A 5.8 GHz passive transponder tag was energized at a distance by the reader; the tag backscattered temperature and other sensor data to the RFID reader.

Although radio transmissions in space are not governed by Federal Communications Commission (FCC) Part 15 regulations, this reader was designed to comply with Part 15 rules to allow it to operate in both the space and terrestrial environments. Therefore, the reader must incorporate spread spectrum communications to mitigate interference as outlined in the Code of Federal Regulations, Title 47, Part 15, sub-part C.247. Schematics of the proposed reader and semi-passive tag are available in Appendix A.

### 3.2 System Overview

RFTSat is composed of hardware provided by Near Space Launch (NSL) [51], NNU, and Georgia Tech. The satellite bus (i.e., solar panels, electrical power supply, satellite frame, and downlink radio) was supplied by NSL, the 5.8 GHz backscatter system including a RFID reader and a passive RF tag was developed by Georgia Tech, and the payload control hardware was developed by NNU. A rendering of RFTSat is shown in Figure 3.1 and Figure 3.2. All the satellite subsystems (except the RF tag) are powered by the solar panels installed on the three sides of the satellite. On the fourth side of the satellite, the RF tag is mounted, facing inward towards the reader's transmitter and receiver antennas. The distance between the reader and tag antennas is approximately 3-4 cm. The tag communicates the sensor data to the RF tag reader by modulating the portion of the continuous wave transmitted by the RFID reader and backscattering it to the RFID reader. The sensor data will then be relayed to a network of ground stations using the GlobalStar satellite constellation. The NNU team will access the data from RFTSat using an online portal. RFTSat was launched into a LEO, coordinated through the NASA CubeSat Launch Initiative, in 2019.

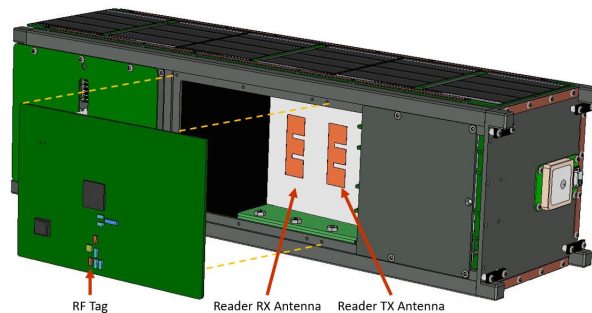


Figure 3.1: RFTSat with the RF tag separated from its mounting position to show the reader transmitter and receiver patch antennas. The tag will harvest energy from the RF tag reader and send sensor data to the reader using modulated backscatter.

Figure 3.3 and Figure 3.4 show the RFID reader boards and antennas. The RF tag, reader boards, and antennas are designed to fit between two metal plates that allow the entire unit to be easily removed for testing. Due to the limited size of the nanosatellite, the

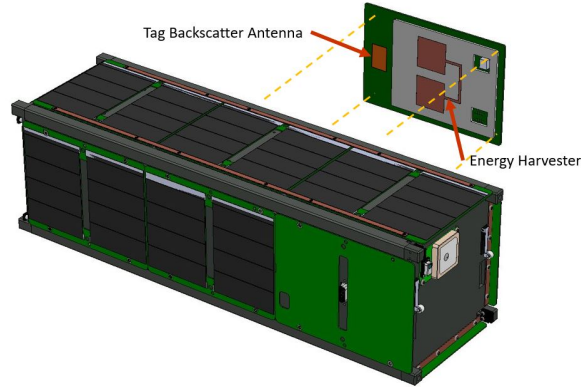


Figure 3.2: RFTSat with the RF tag separated from its mounting position to show the tag's backscatter and energy harvesting antennas.

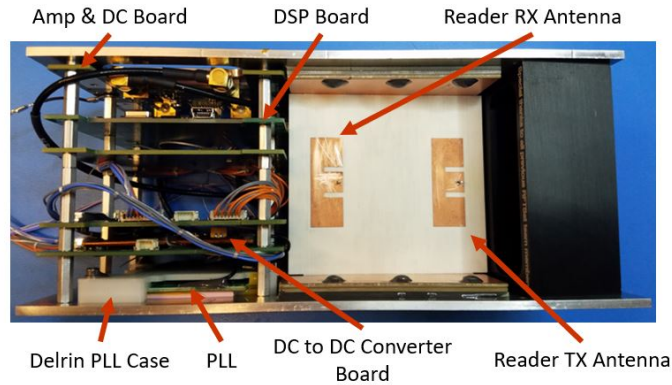


Figure 3.3: The RF tag reader mounted between the two metal plates. The different boards of the RF reader as well as the reader transmit and receive antennas are shown.

RF reader was designed on multiple Printed Circuit Boards (PCB) to fill the available space (the reader and payload control circuitry fit in an approximately 10 cm cube). RF coaxial cables are used to connect the boards and reader antennas internally. Since the Phase-Lock Loop (PLL) board is a commercial, Commercial Off-The-Shelf (COTS) evaluation board without mounting holes, it was secured directly to the lower plate with a custom plastic (Delrin) case (i.e., plastic mounting clamp). The RF portion of reader including the transmit RF power amplifier, LNA, and the I/Q downconverter are allocated to the same board which is placed at the top of the board stack (labeled “Amp & DC Board”). The baseband processing board is located just below it in the stack (“DSP board”). The PLL is thermally connected to the metal slider plates. Figure 3.4 shows the transmitter bandpass

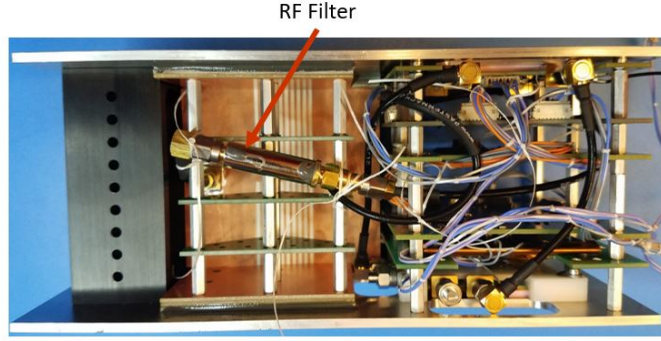


Figure 3.4: A backside view of the RF tag reader boards showing the location of the transmitter's band pass filter.

filter mounted on the back of the board stack. The other boards in the stack (not labeled in Figure 3.3) are the payload control boards and a temperature sensing board. The details of the reader design are presented in section 3.3.

In this chapter, a semi-passive tag (assisted by a coin battery) will be used to demonstrate the backscatter communication capability of the RFID reader and the frequency hopping algorithm will be presented for use in terrestrial applications. An energy harvesting tag is then designed and implemented for the final space mission. The data collected during the space mission is present to demonstrate the overall system.

### 3.3 Reader Design

#### 3.3.1 RFID reader Architecture

Figure 3.5 illustrates the comprehensive block diagram of the RFID reader with the details on the specs. Similar to most UHF RFID readers extensively used in the industry [52][53], the RFID reader in this chapter uses the homodyne architecture, also known as direct conversion architecture. Direct conversion receiver architecture reduces the complexity and power consumption; meanwhile, it avoids the problem of images [7]. However, direct conversion receivers contend with other challenges including lacking IF gain and saturated RF power amplifier because of the Direct Current (DC) offset and leakage from the transmit antenna [54][52].



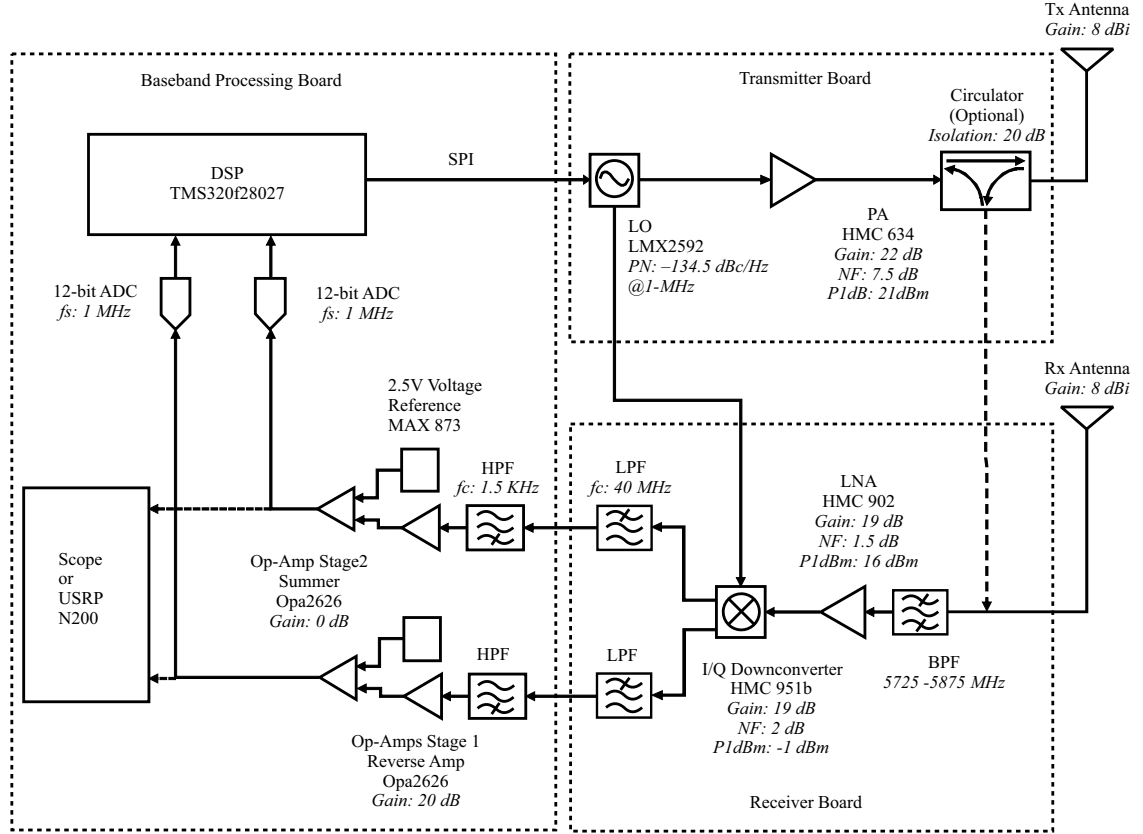


Figure 3.5: Elements of the RFID reader operating at 5.8 GHz

The nexus of the reader is a Digital Signal Processor (DSP) which digitally controls the synthesizer via Serial Peripheral Interface Bus (SPI) in single-frequency mode for space application and frequency-hopping mode for terrestrial applications. The DSP samples the in-phase and quadrature-phase outputs from the receiver demodulation block simultaneously using on-chip 12-bit ADC. The synthesizer is a PLL evaluation board and contains a Texas Instrument LMX2592 chip. It provides the  $g_{slo}$  used in the reader. The Power Amplifier (PA) amplifies the output of the synthesizer (3 dBm) by 20 dB and transmits 23 dBm RF power to the transmit antenna.

Unlike most commercial UHF RFID readers that use monostatic antenna configuration, the proposed RFID reader uses the bistatic antenna configuration. A major reason to use monostatic antenna configuration for commercial UHF RFID readers is that the reader size

mainly depends on the antenna size. And circulators at 915 MHz usually have 30 dB isolation to ensure relatively little of the transmitted signal leaks into the receiver. However, commercial circulators at 5.8 GHz have no more than 20 dB isolation, which may cause the amplifiers in the receiver to be saturated by the transmission leakage. The transmit-receive leakage also leads to significant residual colored noise in the received signal, which accumulates significantly more power density at lower frequencies [54]. The overall size of antennas shrinks as operating frequency increases. Therefore, two antennas on a single board can coexist while creating higher isolation between two antennas than that of a circulator at 5.8 GHz frequency ISM band. The transmit antenna and receive antenna are designed to have an identical gain of 8 dB with 30 dB isolation, which gives the reader the ability to transmit up to 31 dBm of Equivalent Isotropically Radiated Power (EIRP).

The receiver consists of a low noise amplifier (LNA), an in-phase/quadrature (I/Q) downconverter, filters, and baseband amplification circuits. The LNA can be used to increase the reader sensitivity when higher isolation between transmit antenna and receive antenna is achievable. When not saturated, the downconverter has 13 dB conversion gain with 2 dB noise figure. The high pass filter eliminates the DC offsets due to self-mixing and multi-path reflection. Operational amplifiers (Op-Amps) are used for both I and Q channel with adjustable gain determined by the target communication distance. The voltage reference generator adds 1.8 V DC offset to the received signal sampled by the 12-bit ADC to utilize the most bits of the ADC result registers.

### 3.3.2 Antennas

An E-shaped patch antenna, first proposed by Yang, et al., is a conventional patch antenna with two slots in parallel, like a capital letter "E" shown in Figure 3.6a [55]. Like conventional microstrip patch antennas typically used in sensing networks, the E-shaped patch antenna has the same advantages: low profile, low cost, and conformable for planar surfaces. Furthermore, the E-shaped antenna typically has 2-3 dB gain more than that of a

conventional microstrip antenna [56]. A microstrip antenna array shown in Figure 3.6a is used to increase the gain of the system. By using the E-shaped antenna, we can avoid using the feeding network to reduce the overall size of a transmit-receive antenna pair and obtain more separation between the transmitting and receiving antenna. Therefore, the E-shaped antenna is a better choice for this application, in which the total size of the transmit antenna and receive antenna (on single 2-layer board) has to be smaller than 8 cm by 8 cm, and the isolation between two antennas has to be as high as possible.

For a longer communication distance and a smaller profile, the transmitting and receiving antenna are implemented to be co-polarized on one substrate, which causes 20-30 dB more mutual coupling than a cross-polarized configuration [57]. Many self-jamming cancellation approaches were used to achieve higher isolation for monostatic antenna configuration [58] [59]. Although these methods can usually achieve 25 dB more isolation than a single circulator, they require multiple RF couplers and extra control units (e.g. DSP units) that take more space and consume more power. To achieve higher isolation between the co-polarized transmitting and receiving antennas without exceeding the size and power constraints of the cubesat, a slitted structure can be used on the ground plane between the transmitting and receiving antennas[60]. Figure 3.6b shows the shape of the structure used between the antennas.

Figure 3.7 illustrates the isolation between two E-shaped antennas with a slitted ground plane and a solid ground plane between each other, along with the isolation of a commercial circulator. The reflection coefficient of the antenna is optimized at 5.8 GHz and the gain is optimized to be 8 dBi. The slitted ground plane increases the isolation between the two E-shaped patch antennas with conventional solid ground plane from 21 dB to 29 dB on average within the 5.8 GHz frequency band. Compare to a commercial circulator with 19 dB isolation, the E-shaped antenna pair has 10 dB more isolation, which means less leakage from the transmitter and improves the receiver sensitivity without adding any hardware to the reader. The isolation can be further increased for other applications in which the size

of the antenna pair is not a constraint or using cross polarized TX/RX reader antennas.

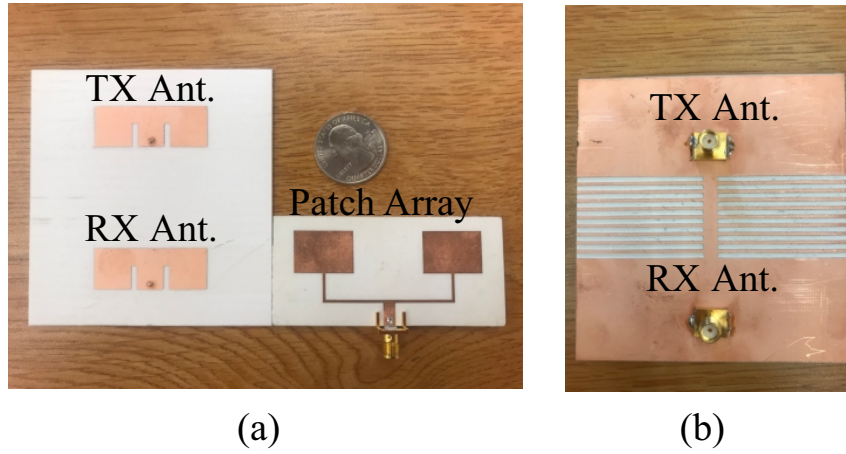


Figure 3.6: The front side of the transmit-receive E-shaped patch antenna pair and a microstrip patch array (a), and the ground plane of the antenna pair (b).

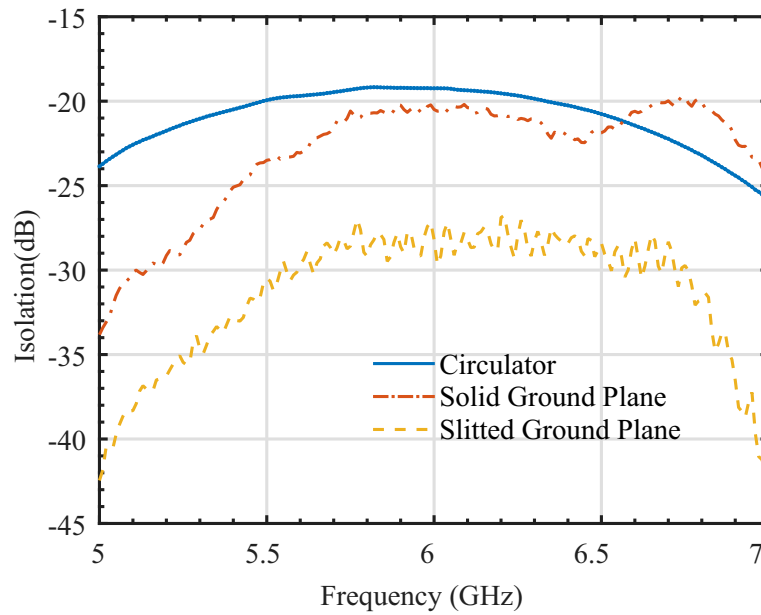


Figure 3.7: The isolation between the transmit and receive port by using a circulator and a pair of E-shaped patch antenna with solid ground plane and slitted ground plane. The slitted ground plane has 10 dB more isolation than the circulator at 5.8 GHz and 8 dB more than the solid ground plane.

### 3.3.3 Frequency Hopping Design

The frequency hopping design has three components: the hop set, the hopping sequence, and the hop rate. The hop set is the set of frequencies the system will use while the hopping sequence is the specific order of those frequencies. The hop rate, or hop duration, is the amount of time the system will spend on a single frequency before hopping to the next one in the sequence. The RFID reader derives its frequency hopping criteria from 47 Code of Federal Regulations (CFR) Part 15.247 for RF devices operating in the 5.8 GHz ISM band, which provides 125 MHz of bandwidth,  $W$ , for the hop set. The frequency hopping design must use at least 75 frequencies with a hop duration,  $T_h$ , of no more than 400ms in a thirty-second period and a hopping pattern based on a pseudo-randomly ordered list that uses each frequency equally. [61]

The RFID reader maximizes the hop duration and channel bandwidth to create a hopping pattern that is as close to single frequency communication as possible. Hardware limitations restrict the transmitter's output frequency resolution to 0.2 MHz increments of even decimal fractions. Dividing the 125 MHz bandwidth into 75 or more frequencies to the nearest even decimal fraction led to a hop set of 77 frequencies each with 1.6 MHz bandwidth,  $B$ , and guard bands of 0.8 MHz and 1.0 MHz at the bottom and top of the band, respectively. [62]

The hop sequence used a three-step process to ensure adequate randomness in the hopping pattern. The first step used a random number generator to produce a value for each frequency and then the list of frequencies sorted according to their random value. [62] The list of frequencies was then divided into seven sub-hop sets of eleven frequencies each and each frequency compared to its two adjacent neighbors to ensure they did not share the same sub-hop set. [62] Any frequency within two hops of a frequency in the same sub-hop set was switched with a frequency near its location in the sequence until all frequencies had two-hop neighbors from a different sub-hop set. [62]

The final randomization step ensured that the last and first couple of frequencies in ad-

Table 3.1: Hopping Sequence [62]

Seq	f (MHz)	Seq	f (MHz)	Seq	f (MHz)	Seq	f (MHz)
1	5824.2	21	5734.6	41	5809.8	61	5825.8
2	5745.8	22	5769.8	42	5744.2	62	5797.0
3	5830.6	23	5819.4	43	5838.6	63	5753.8
4	5779.4	24	5790.6	44	5792.2	64	5795.4
5	5805.0	25	5771.4	45	5845.0	65	5816.2
6	5750.6	26	5843.4	46	5763.4	66	5777.8
7	5813.0	27	5728.2	47	5808.2	67	5811.4
8	5787.4	28	5793.8	48	5782.6	68	5739.4
9	5733.0	29	5822.6	49	5742.6	69	5761.8
10	5773.0	30	5737.8	50	5835.4	70	5829.0
11	5848.2	31	5837.0	51	5758.6	71	5768.2
12	5803.4	32	5747.4	52	5781.0	72	5798.6
13	5760.2	33	5806.6	53	5817.8	73	5840.2
14	5785.5	34	5736.2	54	5755.4	74	5741.0
15	5821.0	35	5789.0	55	5833.8	75	5776.2
16	5726.6	36	5749.0	56	5814.6	76	5752.2
17	5827.4	37	5729.8	57	5765.0	77	5774.6
18	5731.4	38	5841.8	58	5846.6		
19	5766.6	39	5801.8	59	5757.0		
20	5800.2	40	5832.2	60	5784.2		

jacent sub-hop sets had sufficient separation. Each sub-hop set has a bandwidth of 17.6 MHz; therefore, adjacent frequencies were compared to ensure they had at least 17.6 MHz separation between them. [62] Any frequency within a sub-hop set bandwidth of its neighbor was switched with a frequency nears its location in the sequence until all frequency hops were greater than the 17.6 MHz sub-hop set bandwidth. Table 3.1 lists all seventy-seven frequencies according to their order in the hopping sequence, and Table 3.2 provides basic statistical properties of the hopping sequence.

Table 3.2: Hop Set Statistical Properties [62]

Smallest hop	19.2 MHz
Largest hop	115.2 MHz
Average hop	53.5 MHz
Median hop	46.4 MHz
Most Frequent (mode)	25.6 MHz

The final component of the frequency hopping design is the hop rate. Due to the 77-

frequency hop set, the RFID reader must use a 390ms or less hop duration to ensure it does not occupy a single frequency for longer than 400ms in a thirty-second period. Figure 3.8 provides the final hopping sequence for the RFID reader.

The RFID reader uses slow frequency hopping, so it must account for situations in which the reader reaches the end of its 390ms hop duration but is still receiving a transmission. Should this occur, the reader will add a 1ms hop duration extension, with a maximum of ten 1ms extensions, to the standard 390ms duration until the incoming transmission is complete at which point it will hop to the next frequency in the hop set. [62] If the incoming transmission takes longer than 10ms to complete, the reader will hop to its next frequency so comply with the 400ms maximum occupancy restriction. [62]

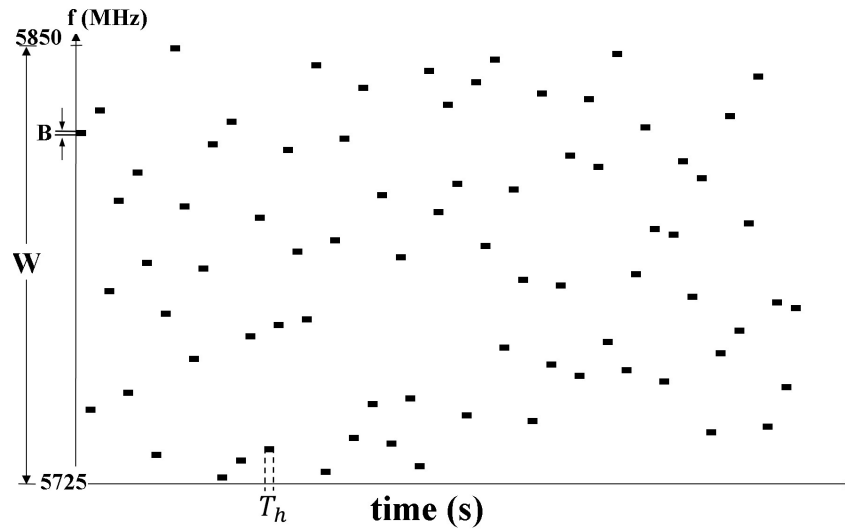


Figure 3.8: Hopping Sequence for all 77 frequencies in the 5.8 GHz band [62].

### 3.3.4 Power Breakdown

In the space sensing application, the solar panel of the cube satellite can provide our RFID system with limited power supply. Consequently, we have to trade off between an optimized performance and the power consumption. In this design, we use the most energy efficient on-shelf components we can find in the market to make use of the amount of power

we have. A total power consumption of 3.78 W is achieved by this design as listed in Table 3.3 along with the power consumption of each part. The cost of the first-run prototype in this project totaled \$114.60 per reader using price quotes for purchases of 1,000 units. When purchasing only one unit for each required component, the total price increases to \$175.44. Table 3.3 lists the critical components of the reader unit including the synthesizer, RF amplifiers, and the I/Q downconverter, which are the most expensive units and are crucial for determining the overall cost per unit. Reader size is another important consideration in the project and was aimed to be kept as small as possible. Ideally, the reader unit should be two boards that slide into the cube satellite. A rough size of approximately 7 x 7 cm was estimated for the complete reader PCB. This size can be further reduced by closely spacing the ICs and removing the RF connector space. The total power consumption and size can be even further reduced by integration onto a single Intergrated Circuits (IC) chip [53].

Table 3.3: The power consumption and price of major components in the RFID reader. The price of the components for purchasing a single chip and 1000 units are listed.

Part	Component	Price (\$)	Price/1k (\$)	Power (W)
LO	LMX2592	30.49	26.16	1.48
PA	HMC634LC4	63.11	51.65	0.90
LNA	HMC902LP3E	35.71	25.54	0.25
I/Q Downc.	HMC951BLP3E	31.98	26.52	0.59
Op-Amp	OPA2626	6.58	3.10	0.11
ADC/DSP	TMS320F28027	7.57	5.35	0.45
Total		175.44	112.16	3.78

### 3.3.5 Link Budget

To derive the amount of power received by the receiver, a link budget calculation is necessary. Griffin, et al. summarized the link budget equation for various types of backscatter communication systems [17]. For a bistatic RFID reader, the received modulated backscat-



ter power,  $P_r$ , is given by

$$P_r = P_t + G_T + G_R + 2G_t + M + 40\log(\lambda/4\pi D) \quad (3.1)$$

where  $P_t$  is the transmitted power of the reader,  $G_t$  and  $G_r$  are the gain of the transmit and receive antenna,  $G_t$  is the gain of the tag antenna,  $\lambda$  is the wavelength at 5.8 GHz,  $D$  is the distance between the RFID reader and tag,  $M$  is the modulation factor, which is measured to be  $-6$  dB in our case. All parameters in equation Equation 3.1 are in dB scale. Identical antennas are used for the transmitter, receiver, and tag, therefore, equation Equation 3.1 can be further simplified into

$$P_r = P_t + 4G + M + 40\log(\lambda/4\pi D) \quad (3.2)$$

where  $G = G_T = G_R = G_t$  is the gain of the E-shaped antenna used for the transmitter, receiver and tag respectively.

### 3.4 Backscatter Communication

#### 3.4.1 Test Setup

In practice, the reader will connect to transmitting and receiving antennas for wireless backscatter communication. To validate the performance of our reader under wireless conditions, we complement the RFID reader with antennas and place the RF tag 1.2 m away from the reader, present in Figure 3.9. The tag modulates the incoming RF signal based on BPSK and scatters data packets back to the receiver. The data packets use preambles as packet headers to help the receiver recognize the beginning of the data packets. After the demodulation, amplification, and sampling, the matched filter processes the received signal and stores the decoded data packet in the flash memory of the DSP. To compare the performance of the RFID reader based on bistatic and monostatic antenna configuration,

we use an oscilloscope to sample the output of the baseband amplifiers. Eye diagrams are generated by the oscilloscope as an indicator of the quality of signals the received signal when different antenna configurations are used.

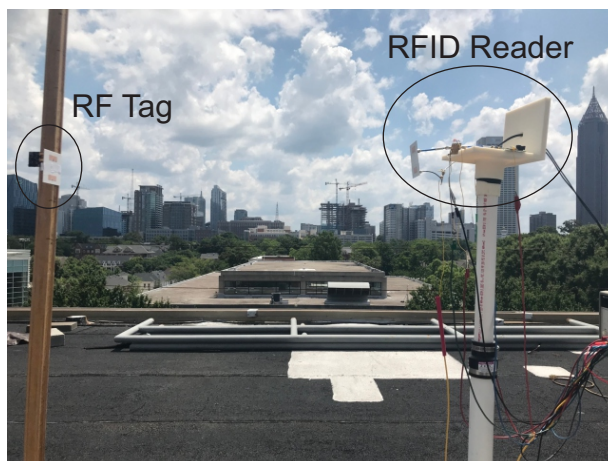


Figure 3.9: The experimental setup with antenna on the open-air, rooftop antenna range at Georgia Tech.

### 3.4.2 Results

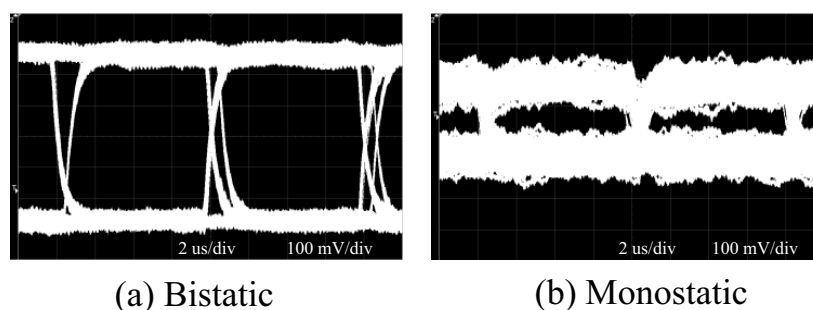


Figure 3.10: The eye diagram of the received signal when bistatic (a) and monostatic (b) antenna configuration are used.

An eye diagram, also known as eye pattern, gives a quick glance at the amplitude and time distortion of the signal that degrade the BER, which indicates the quality of the received signal. An eye diagram can be generated by properly configuring an oscilloscope with higher persistence. Figure 3.10a and Figure 3.10b represent the eye diagram of the

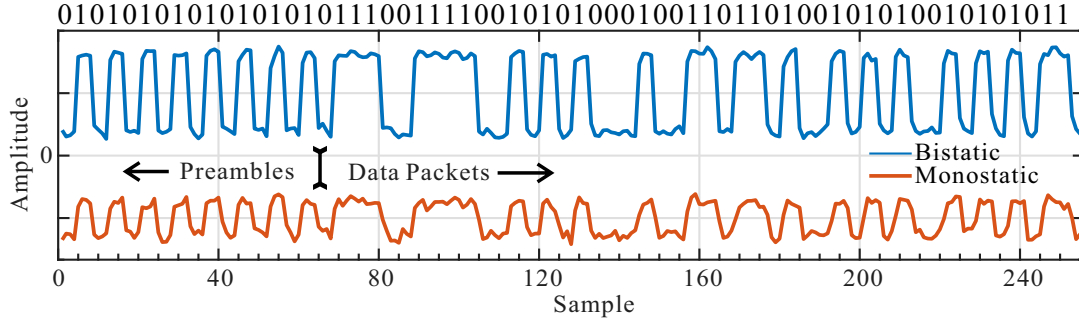


Figure 3.11: An example of ADC-sampled received data packets (single channel) for bistatic and monostatic antenna configurations.

received signal when bistatic and monostatic antenna configurations are used, respectively. In an eye diagram, the eye-opening, which is the distance between higher level and bottom level, indicates the Signal-to-Noise Ratio (SNR) of the received signal. The bistatic reader has higher SNR than that of the monostatic reader, clearly shown in Figure 3.10, which leads to lower BER. Note that the jitter noise in the eye diagrams for both for bistatic and monostatic readers implies a potential timing error when decoding the backscattered symbol. In this design, this problem does not occur because of a shorter symbol. Many wireless communication systems implement late-early timing recovery to prevent problems caused by timing errors for simplicity, which can be implemented in the future when using longer data packets.

An example of the signal sampled by the ADC for both bistatic and monostatic antenna configurations is present in Figure 3.11. In accordance with the eye diagram, the sampled symbol of the bistatic reader has a higher amplitude and less noise than that of the monostatic reader. The reader demodulated and recorded the backscattered data packets lead by preambles, which demonstrates the feasibility of using this RFID reader to achieve backscatter communication with both antenna configurations. However, based on the better performance of the bistatic antenna configuration, it is the recommended option for all RFID readers that require higher isolation between the transmitter and receiver.

### 3.5 RF Tag Design

#### 3.5.1 RF Tag Architecture

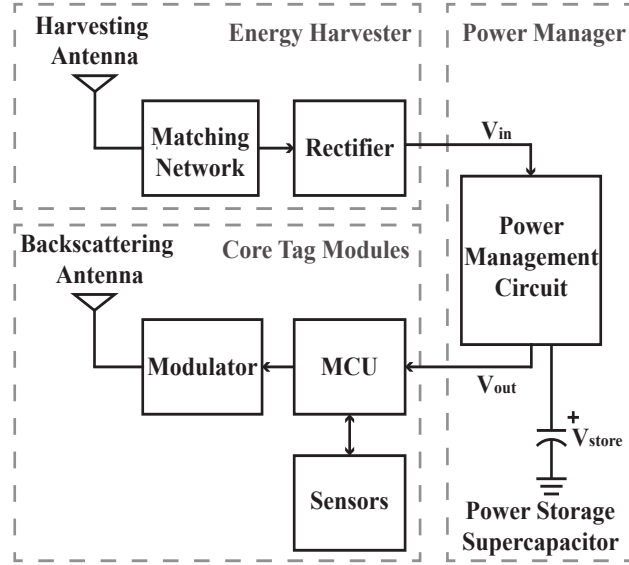


Figure 3.12: Elements of the RF tag operating at 5.8 GHz.

Figure 3.12 illustrates the comprehensive block diagram of the batteryless RF tag. The RF tag consists of three major parts: the energy harvester, the power manager, and the core tag block. The initial RF energy harvester, a single stage Dickson charge pump, converts the RF power at 5.8 GHz received by the harvesting antenna to a DC voltage. The charge pump is matched to the  $50\ \Omega$  microstrip patch antenna array to reduce the reflection loss. The Avago HSMS-286C zero-bias Schottky diodes are used for their high-detection sensitivity at microwave frequencies. As the next stage, the power management circuit (BQ25570) boosts the output voltage of the charge pump and stores the DC power in a 1.5 mF tantalum capacitor. The minimum required input voltage for the power management IC to start charging is 0.35 V, known as the cold start voltage. Once the power received by the tag is sufficient to turn-on the power management IC, it begins accumulating charge in the tantalum capacitor. When the voltage accumulated in the tantalum capacitor exceeds 3 V, the power management IC releases the power to the RF tag. The output voltage of the power

management IC is programmable to be 1.5 V to 5 V determined by external resistors. In this application, the output voltage is set to be 1.8 V because the TI MSP430F2132 MCU requires a minimum supply voltage of 1.8 V.

The TI MSP430F2132 MCU is the central hub of the core tag module, which uses the on-board 10-bit analog-to-digital converter to read the built-in temperature sensor. Meanwhile, it digitally controls the RF modulator via SPI to modulate and backscatter the data to the RF reader. Once a sufficient voltage is obtained, the MCU and sensors start operating in active mode, utilizing the energy stored in the tantalum capacitor. As the supercapacitor discharges, the output voltage remains 1.8 V until the stored voltage decreases to 2.8 V. Then the power management IC disconnects the MCU and sensors from the tantalum capacitor to recharge the voltage of the supercapacitor to 3 V again. The period of the operating/recharging duty cycle is determined by the output power level of the charge pump, the efficiency of the power management IC, and the capacitance of the tantalum capacitor.

The duty cycle and DC-DC booster based approach is often used in low-power applications [63] [64]. A major reason to use such a configuration is the limited received power by the tag and insufficient RF-DC conversion efficiency of the charge pump. The situation is worse at higher frequencies, in which the free space path loss is higher and the conversion efficiency of charge pumps are lower. For example, the free space path loss at 5.8 GHz is 16 dB higher than at 915 MHz. Furthermore, the energy harvester at 5.8 GHz usually has lower efficiency, which further reduces the available DC power [65]. By introducing the power management IC and the operating/recharging duty cycle, the required turn-on power of the tag was reduced and the communication range of the tag increased far beyond what would be possible by simply increasing the efficiency of the one-stage Dickson charge pump. Of course, the trade-off is that the tag may not be able to operate continuously at low power levels.

### 3.5.2 Antennas

A microstrip patch antenna array is used to increase the received power of the RF power harvester. Microstrip patch antennas, typically used in many sensing networks, have the following advantages: low profile, low cost, and conformable for planar surfaces. Furthermore, microstrip antennas can be easily made into a two-element antenna array with typically 2-3 dB more realized gain. For the RFTSat mission, nearly no polarization mismatch occurs if the microstrip antennas used by the reader and tag are properly aligned. In this circumstance, the microstrip patch antenna array is a better choice to increase the RF power received by the RF tag. Figure 3.13 presents the outline of the harvesting antenna. The highest realized gain of this antenna array is 10.3 dBi in the normal direction without polarization mismatch.

### 3.5.3 Power Consumption

In the space sensing application, an external accelerometer, a radiation sensor, and a built-in temperature sensor inside the MCU are used to gather various kinds of information. Meanwhile, the modulator, as an RF switch, also requires power supply to accomplish the backscatter communication. Both sensing and backscatter communication require a sufficient amount of voltage, current, and time to remain operating in active mode. Consequently, we have to select a large enough tantalum capacitor that can accumulate sufficient charge to satisfy the power consumption over enough time to complete initialization, read sensors, and communicate with the RF reader. In this design, the total minimum power

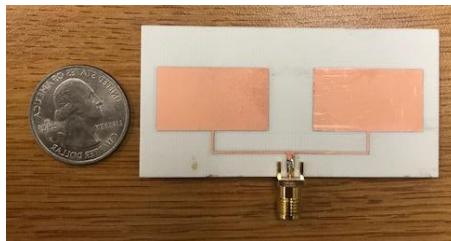


Figure 3.13: The profile of the harvesting antenna.

consumption of the tag (including the microcontroller, RF switch, radiation sensor, and accelerometer) totaled  $559 \mu\text{W}$ . A  $1.5 \text{ mF}$  tantalum capacitor made by AVX is used in this design.

#### 3.5.4 Link Budget

The amount of power received by the RF tag can be derived by a link budget calculation. Griffin, *et al.* first proposed the link budget equation for various types of backscatter communication systems [17]. Usually, the maximum communication distance between the RF reader and the passive RF tag is determined by the amount of power received by the RF tag, which is given by the down-link budget:

$$P_r = P_t + G_T + G_t + 20\log(\lambda/4\pi D) \quad (3.3)$$

where  $P_t = 23 \text{ dBm}$  is the transmitted power of the reader,  $G_t = 8 \text{ dBi}$  is the gain of the transmit antenna of the RF reader,  $G_r = 10.3 \text{ dBi}$  is the gain of the tag harvesting antenna,  $\lambda$  is the wavelength at  $5.8 \text{ GHz}$ ,  $D = 0.75 \text{ m}$  is the maximum distance between the RF reader and tag. Consequently, the power received by the charge pump  $P_r = -4.21 \text{ dBm}$ , which is approximately  $0.3793 \text{ mW}$ .

#### 3.5.5 Charge Pump

Figure 3.14 a) shows the schematic of a single-stage Dickson charge pump circuit, consisting of two capacitors and two Schottky diodes. Although an ideal Dickson charge pump has 100% efficiency, in reality, the conversion efficiency is demolished due to impedance mismatch, material loss, and output voltage harmonics[66][67]. Wang, *et al.* increased the conversion efficiency of a conventional single-stage Dickson charge pump by replacing C2 in Figure 3.14 with a class-F load as shown in Figure 3.15 [67]. The class-F load creates an RF ground for the Schottky diode D2 and shorts the first and third harmonic of the output

voltage to ground. Furthermore, it also performs as parallel plate capacitor that can replace C2 with higher capacitance [67]. A similar structure is used in this chapter to maximize the conversion efficiency of the charge pump for lower input power at 5.8 GHz. Figure 3.16 a) presents the manufactured charge pump used in this chapter. The performance of this charge pump with and without power management IC are measured and compared in Section section 3.6 and Section section 3.7.

Figure 3.14 b) shows the schematic of the two-stage Dickson charge pump circuit. This topology utilizes four capacitors and four Schottky diodes. Conversion efficiency of this device is reduced due to diode losses, mismatch in traces and connections, and output voltage harmonics. The purpose of the second stage is to double the output voltage produced by the one stage charge pump, operating at higher input power level than one-stage Dickson charge pump. While the second stage does introduce higher losses to the system, the higher output voltage allows the device to be useful in higher power applications without damaging the diodes by operating at higher voltage than the reverse break-down voltage of the diode. A similar matching network and class-F load is used for both stages to achieve higher output voltage and conversion efficiency, as shown in Figure 3.16 b). Both charge pumps are built on a 2-layer antenna grade laminate (RO4725JXR) made by Rogers Corporation with a dielectric constant of 2.55 and a loss tangent of 0.0022 measured at 2.5 GHz. The output voltage and efficiency into a 3000 Ohm load are presented in Section section 3.6.

### 3.5.6 RF Tag Integration

Two separate boards are manufactured to implement the RF tag. The RF components, consisting of an energy harvesting antenna and one-stage Dickson charge pump, are built using the same 2-layer laminate (RO4725JXR). The antenna and energy harvester are placed on the top layer and the bottom layer is used as the ground plane. The backscattering antenna, core tag modules, and the power manager are distributed on a 4-layer FR-4 print



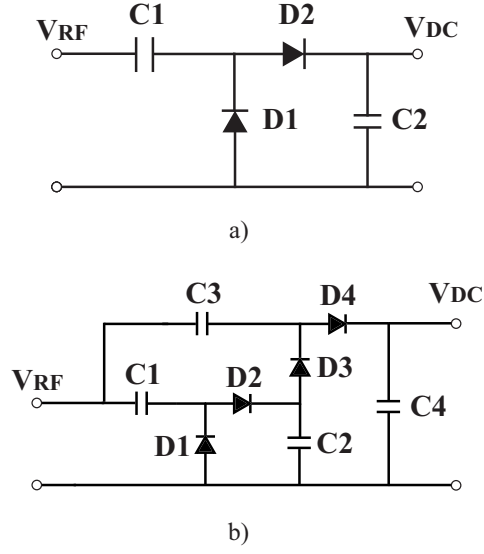


Figure 3.14: The schematic of a a) conventional one-stage Dickson charge pump and b) two-stage Dickson charge pump.

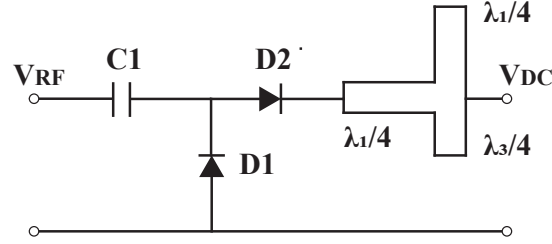


Figure 3.15: The schematic of a one-stage Dickson charge pump with a class-F load.

circuit board (PCB). In the launch mission, the harvester board and tag board will be glued together and mounted to the boom. The operation and data transmission of this tag are presented in Section section 3.7.

### 3.6 Tag Operation without power management IC

#### 3.6.1 Test Setup

The conversion efficiency and output voltage are the most important specs for a Dickson charge pump. To investigate the conversion efficiency of the RF tag at different distances from the RF reader, we connect the charge pump to an RF signal generator. The output voltage of the one- and two-stage charge pump across a load resistor ( $R_L = 3000 \Omega$ ) are

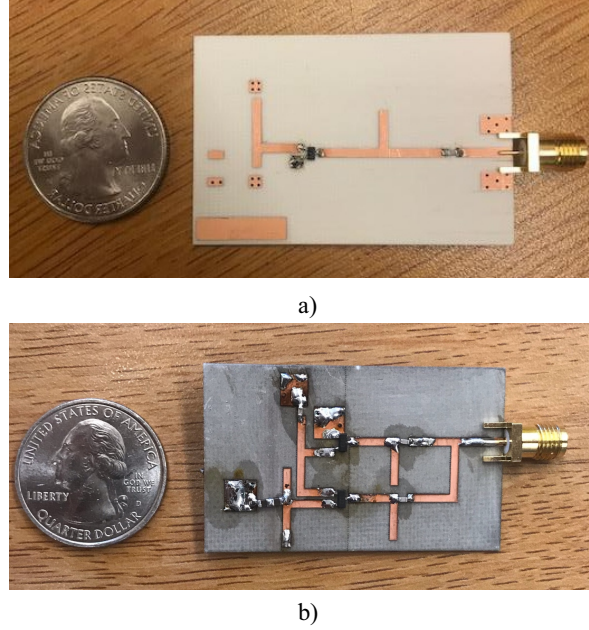
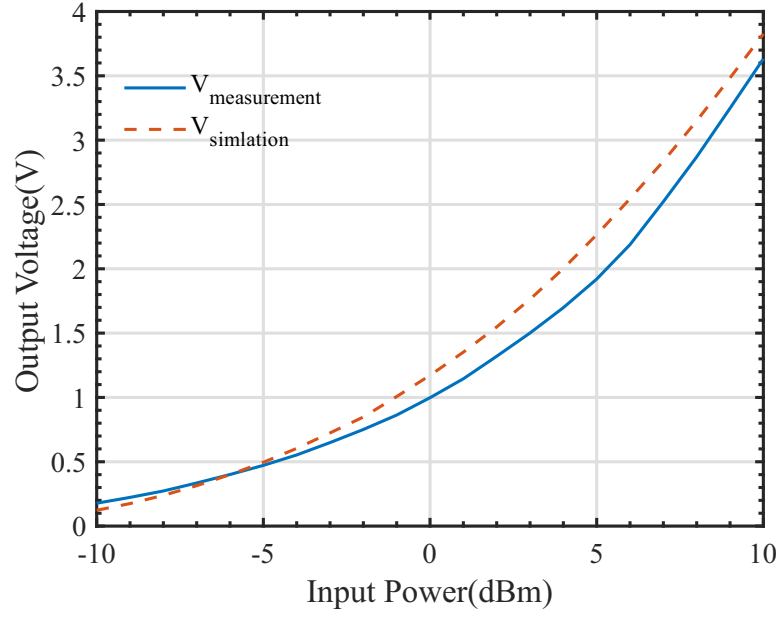


Figure 3.16: Fabricated a) one-stage Dickson charge pump and b) two-stage Dickson charge pump with matching networks and class-F loads.

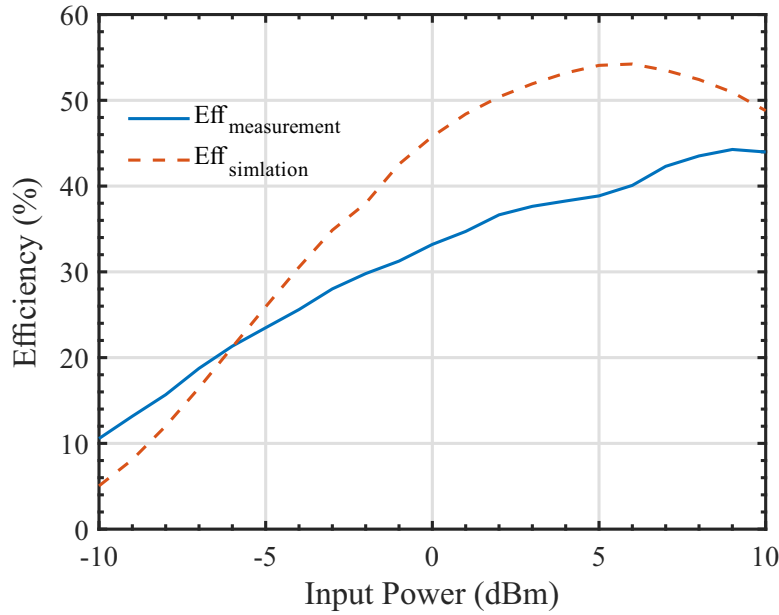
measured at different input power levels. The voltages when the charge pump is connected to the MCU is also measured to investigate the possibility of using the charge pump as the power supply for the RF tag.

### 3.6.2 Results

As a demonstration of how the one-stage Dickson charge pump performs, Figure 3.17 a) presents the output voltage of the tag at different levels of input power. Knowing the resistance of the load resistor ( $R_L = 3000 \Omega$ ), we can derive the efficiency of the charge pump at different input power levels, as shown in Figure 3.17 b). The peak efficiency is around 44% when the input power is 9 dBm, and the efficiency of 25% is obtained at -4 dBm input power level. Figure 3.18 a) shows a comparison of the theoretical and measured output voltage of the two-stage Dickson charge pump with a 3000 Ohm load. At -4dBm this shows a voltage of only 15 mV which proves that the single stage is a much better device for low power applications than the two stage. At higher powers, the output voltage peaks at 10.2 V at the max input power of 25 dBm. This shows that the two-stage



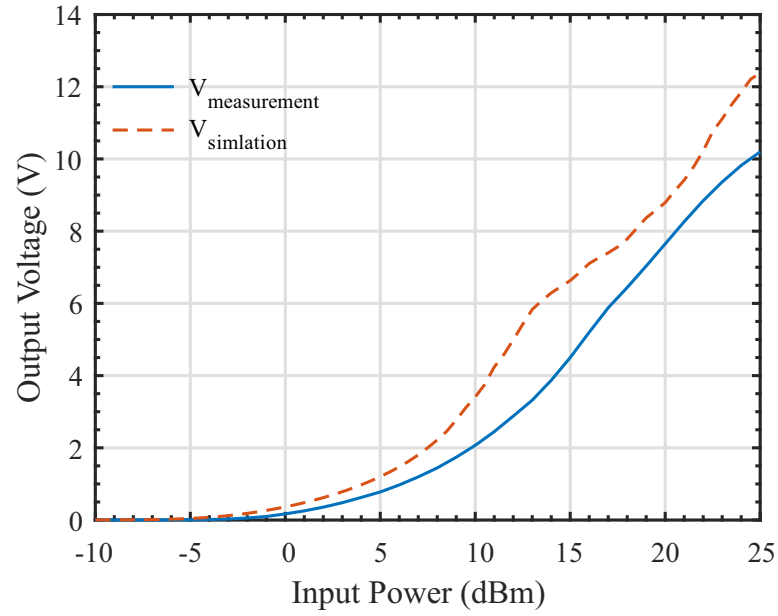
a)



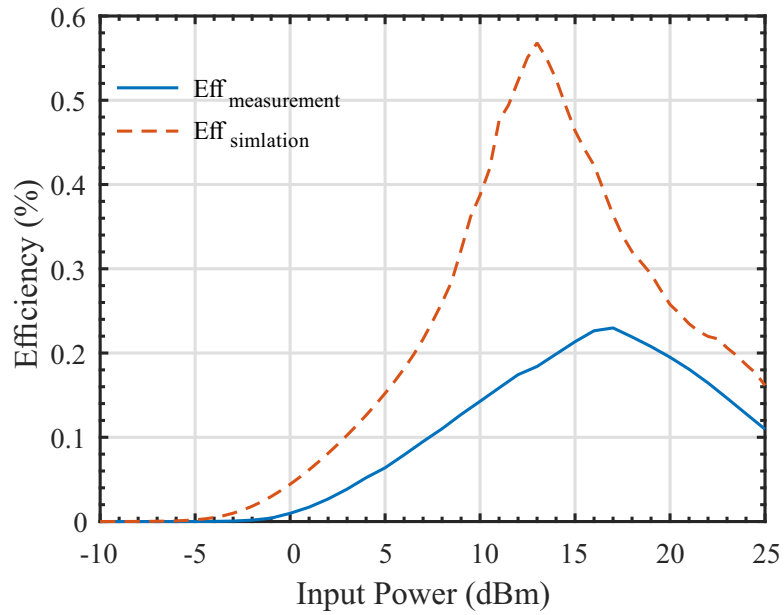
b)

Figure 3.17: The simulation and measurement results of the a) DC output voltage and b) RF-DC power conversion efficiency of the one-stage charge pump at different input power levels when connected to a  $3000\ \Omega$  load resistor.

device is much better for higher power applications since the single stage charge pump is not able to handle output voltages of this magnitude. Figure 3.18 b) shows the output



a)



b)

Figure 3.18: The simulation and measurement results of the a) DC output voltage and b) RF-DC power conversion efficiency of the two-stage charge pump at different input power levels when connected to a 3000  $\Omega$  load resistor.

efficiency of the two-stage charge pump with a 3000 Ohm Load. The peak efficiency of 23 % occurs at around 17 dBm. The simulation shows a theoretical peak efficiency of

up to 60 % showing large room for improvement of this device in future iterations. The device shows operation at near peak efficiency at powers up to 20 dBm showing that it is much better suited for high power applications, while the single stage charge pump will get damaged due to higher output voltage than the reverse break-down voltage of the diode.

In practice, the charge pump needs to provide power for the RF tag instead of a resistor, including the MCU and sensors. Figure 3.19 illustrates the output voltage of the charge pump when it supplies power to the MCU. According to Figure 3.19, the output voltage reaches 1.8 V when the input power is 2 dBm. However, the RF tag only receives -4 dBm RF power when the deployable boom is fully extended to 75 cm from the satellite frame, which means that the charge pump itself is not sufficient to provide power for the RF tag over the entire boom range. Furthermore, as shown in Figure 3.19, the output voltage can increase to more than 4 V when the input power is larger than 9 dBm. Before the boom is fully extended, the RF tag receives more power as it is closer to the reader. For example, when the RF tag is 15 cm away from the transmitting antenna, the received power of the charge pump is around 10 dBm. At this input power level, the excessive output voltage may damage the core tag circuit if no power management circuit is applied.

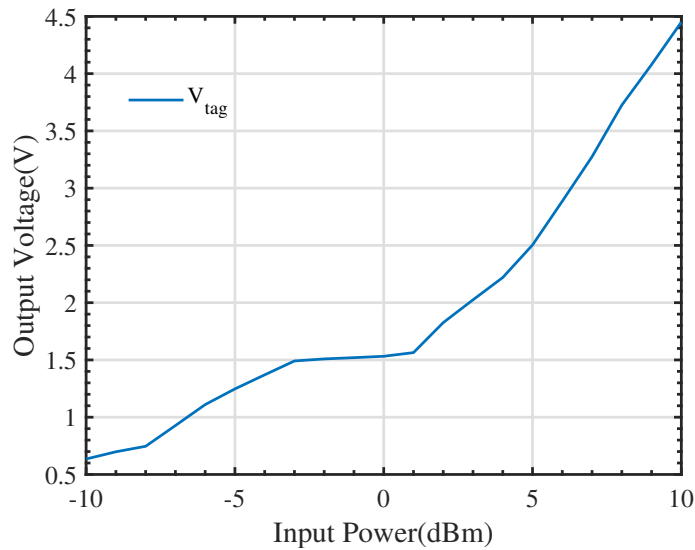


Figure 3.19: The measured DC output voltage of the one-stage charge pump at different input power levels when connected to the RF tag circuit

### **3.7 Tag Operation with DC Power Management**

#### 3.7.1 Test Setup

As shown in the previous section, the energy harvester cannot power up the tag properly when the input power is higher than 9 dBm or lower than 2 dBm. Therefore, the use of the power management IC is necessary for the RFTSat mission. To validate the performance of our RF tag enhanced by the power management IC under realistic conditions, we complement the RF power harvester with the power management circuit and load its output with the core tag module. The input of the charge pump is connected to a RF signal generator. The charging process and operational duty cycle are investigated at different input power levels to obtain the minimum turn-on power required by the enhanced RF tag.

#### 3.7.2 Results

Figure 3.20 shows the initial tantalum capacitor charging process of the power management circuit as an example. The input power is set to 1 dBm to show multiple cycles in one plot. According to Figure 3.20, if the RF tag starts charging from 0 V, it can build up the voltage to 3 V within 140 s. Once the voltage stored in the capacitor exceeds the operating point, which is set to be 3 V here, the power management IC transitions the MCU from idle mode to active mode. As shown in Figure 3.21, the operating period lasts for 3 s until the stored voltage drops to 2.8 V. Then the power management IC starts to recharge by disconnecting the tantalum capacitor and the MCU. The recharging period is 4.6 s, as presented in Figure 3.21. The operating/recharging duty cycle is eventually determined by the power received by the RF tag. When the received power decreases, the recharging time increases and the operating time decreases. When the received power exceeds 4 dBm, the recharging time decreases to 0 and the MCU keeps operating. Because the output voltage is locked to 1.8 V, the tag is protected from excessive supply power when at the proximity of the RF reader. The minimum received power to turn-on the RF

tag is -8 dBm. Once the received power is under -8 dBm, the power management IC stops accumulating charge in the tantalum capacitor to trigger the operating mode. Therefore, the turn-on power requirement of the RF tag is -8 dBm, and the continuously operating power requirement of the RF tag is 4 dBm.

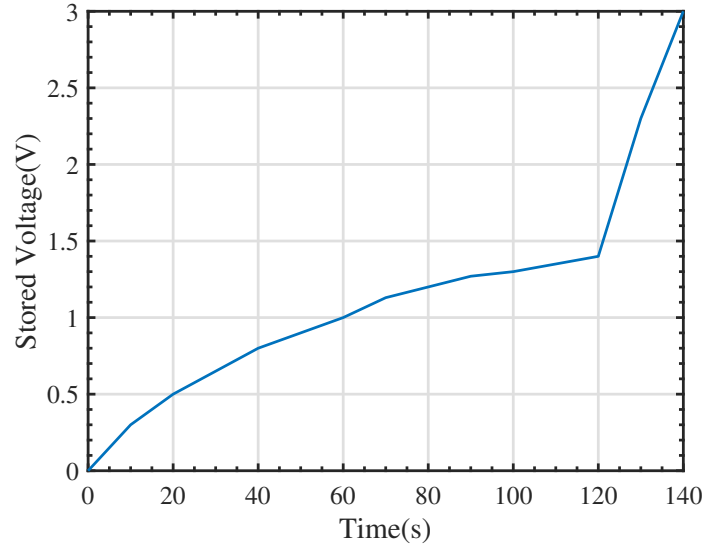


Figure 3.20: The initial tantalum capacitor charging process of the power management circuit. The total time it takes to charge from 0 V to 3 V is 140 s when the input power is 1 dBm.

In the final mission, the implemented tag will be used to harvest energy wirelessly. To prove the concept, we placed the tag at about 75 cm away from the RF reader, where the RF tag expects an input power around -4 dBm. The time for charging the 1.5 mF super capacitor from 0 V to 3 V increased to 600s. The operating time decreased to 300 ms, and the recharging time increased to about 10 s. During the operating time, the RF tag collects data from the temperature sensor and radiation sensor and backscatters multiple data packets back to the RF tag reader.

### 3.8 On-orbit Data

As mentioned previously, technical difficulties and schedule constraints forced the team to remove the extendable boom, mount the tag to the side of the satellite, and reduce the

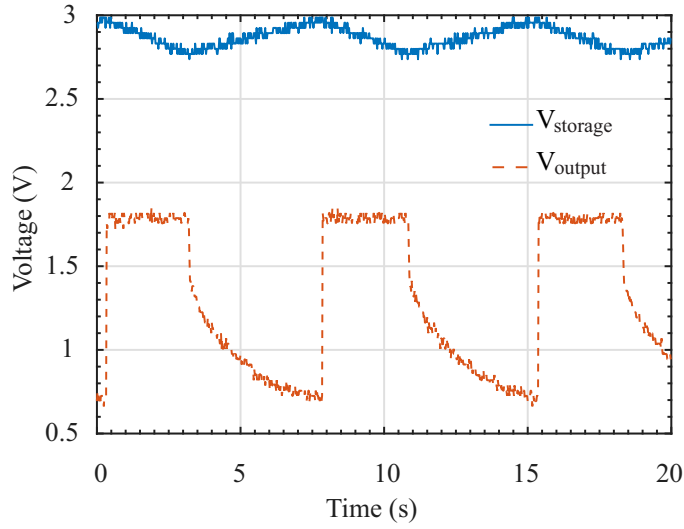


Figure 3.21: The operating/recharging duty cycle of the power management circuit when the input power is 1 dBm. The operating period lasts for 3 s and the recharging period takes 4.6 s.

number of sensors. Sections section 3.3 through section 3.7 of this chapter discussed the RF tag system designed for the original plan; this section reports on-orbit results with no boom and the tag operating only a temperature sensor.

RFTSat began operating its RF tag system approximately 30 minutes after being placed into orbit. The RF tag system was powered on and the RF tag was read approximately every 16 hours. Immediately after receiving data from the RF tag, the sampled I/Q baseband waveform from the RF tag was down-linked to Earth and a copy of the same waveform was downlinked eight hours later (i.e., new tag data or a copy of tag data was downlinked every 8 hours).

Each time the RF tag was to be read, the reader transmitter 1) output a 5.8 GHz CW signal for 2 minutes while backscatter from the RF tag data was ignored, 2) was then powered off for four seconds and 3) was powered back on while sampling of the down-converted backscatter signal was started. This approach avoided a problem receiving reliable data from the tag when its energy harvesting circuitry was completely uncharged. A simple edge-detecting state machine was used to detect the beginning of the RF tag waveform and



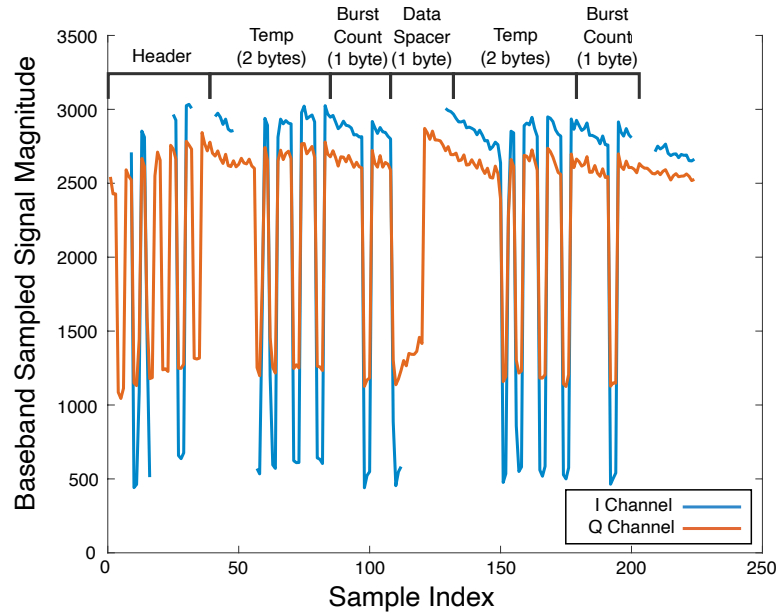


Figure 3.22: The sampled, baseband I and Q waveforms received from the RF tag on orbit beginning on August 07, 2019 at 16:42 (UMT). The waveform consists of a header, two copies of the RF tag’s temperature, and two copies of the burst counter. Samples are missing from the I channel, but were estimated using the corresponding samples from the Q channel.

begin storing the I/Q baseband samples.

Each time that the energy harvesting circuit on the RF tag stored adequate energy from the incident 5.8 GHz reader signal, the tag’s MSP430 microcontroller powered on, read its internal temperature sensor, and began to modulate the backscattered signal using an RF switch. The data from the tag was backscattered as a packet containing a 2-byte header (0xAAAA) used for synchronization and timing recovery by the reader, the 2-byte temperature data, a 1-byte burst counter, a fixed byte or data spacer (0xF0) for synchronization, followed by second copy of the temperature data and burst counter. A set of sampled, baseband I and Q waveforms received from RFTSat on August 7, 2019 is shown in Figure 3.22. As can be seen, the waveforms exhibit little noise, but some samples are missing. The source of the missing samples is missing data packets that were lost either in communication between the RF tag system and the RFTSat down-link radio or downlink packets lost after being transmitted from the RFTSat down-link radio (the latter is the primary source

of lost samples).

It is estimated that only 30-36% of the RF tag system's data packets were received. The uncertainty in percent packets received is related to the method used to estimate the total number of packets that should have been received from the satellite. The missing packets significantly complicated processing the satellite's data.

Data was processed using a combination of Python and Matlab scripts. First, since two copies of each temperature measurement waveform were downlinked, all identifiable waveform copies were combined to form a single I and Q waveform set with any missing samples replaced from the copy. Second, if any missing samples remain after combining the waveform copies, the missing samples were estimated if at least one sample was received on either the I or Q channel. For example, if a sample was missing on the I channel of a waveform, the value of the I channel sample was interpolated from the corresponding Q channel sample. Although the estimated amplitude is not exact, it was adequate to make a bit decision. Third, the sampled waveforms were interpolated to increase the number of samples per bit. Fourth, each waveform was normalized and each sample limited to either a high or low value, based on the average of the entire signal. For the waveforms with a complete header, the average number of samples per bit was estimated from the waveform header, and the subsequent bits were sequentially estimated by searching for bit transitions and estimating runs of 1s or 0s using the estimated number of samples per bit. The same procedure was executed on the waveforms without a complete header, except that the number of samples per bit was extrapolated from the waveforms with a complete header. This approach allowed bits to be effectively identified even when waveform samples were missing. Once the waveform samples were processed into bits, the bits were manually examined. A total of 44 valid temperature readings were recovered from the RFTSat data, shown in Figure 3.23. A temperature measurement was determined to be valid if the data related to the measurement was self-consistent. In other words, even if bits were missing, the data was considered valid if the data present did not contradict what was expected or

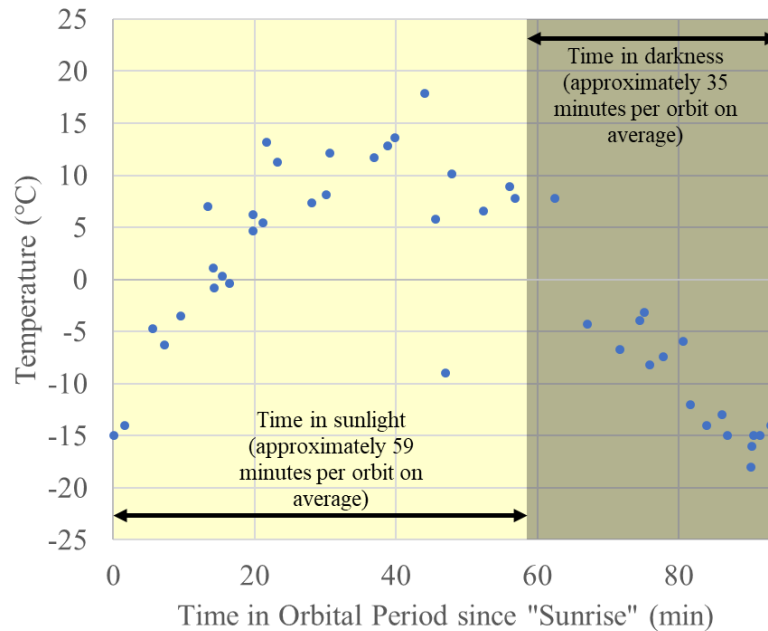


Figure 3.23: Recorded temperature in Celsius over time in orbital period. The points in the yellow region were taken at the portion of an orbital period when RFTSat was in sunlight, and those in the grey region were taken at the portion when RFTSat was in darkness.

observed in other measurements and if multiple copies of the burst counter, data spacer, or temperature data were present in a measurement waveform, the copies did not contradict each other.

To produce Figure 3.23, the time of each temperature measurement was referenced to the start of an orbital day; here, the start of an orbital day is considered the time when the satellite exits Earth's shadow and first passes into sunlight. Using the Analytical Graphics Inc.'s Systems Tool Kit (STK), the position of the satellite at specific instances in time (latitude, longitude, and altitude) can be visualized. STK provides the ability to visualize the satellite's continuous orbital path and sunlight penumbra light/dark boundaries at a specified altitude above Earth's surface (essentially the boundary of Earth's projected shadow upon any orbital path a specific height above Earth's surface). Therefore, it is possible to visualize the relative total time in sunlight or darkness for a satellite's orbital period (looking at the approximate differences in time between dark-to-light and light-to-dark crossover events).

For this procedure, an altitude of 478 km was used to plot the sunlight penumbra boundary and determine crossover events. This 478 km value was the average altitude of the satellite during the evaluated mission period, having a periapsis of 469 km, and apoapsis of 487 km. With sunlight penumbra plotting available, the time and position of when each temperature measurement was made was compared to the time and position of when the most recent crossover event occurrence took place. By knowing the time difference between when a temperature measurement was taken, and when the most recent crossover event was made, the temperature measurement's relative placement in an orbital day was determined. The collection of temperature measurements were then processed and placed into their appropriate time positions within an orbital day, as shown in Figure 3.23.

In general, Figure 3.23 shows the expected result that the longer the satellite is in sunlight, the higher the recorded temperature and the longer the satellite is in darkness, the lower the recorded temperature. The purpose of Figure 3.23 is to show a general correlation between the recorded temperature and the time in sunlight/darkness; attempts to infer more detailed conclusions from Figure 3.23 should be avoided because several assumptions were made to create the plot. First, the time recorded for each measurement is the time at which the first data packet was received by the GlobalStar satellite constellation, not the time that the temperature measurement was taken. Second, the altitude of the satellite was assumed to be 478 km; the time spent in sunlight/darkness varies with the altitude of the satellite. Third, Figure 3.23 shows that the average time in sunlight and darkness is 59 and 35 minutes, respectively. These times are average because they vary with each orbit of the satellite. Fourth, the temperature analysis in Figure 3.23 does not account for variations caused by rotation of the satellite; sometimes the RF tag's temperature sensor faced the sun and sometime it did not. In conclusion, Figure 3.23 suggests that RFTSat's RF tag system reported valid temperature measurements by showing that the measurements generally follow the expected sunlight/darkness trend.

### **3.9 Conclusion**

In this chapter, we propose the design of a frequency hopping RF reader and a power harvesting RF tag enhanced by a power management IC operating at the 5725-5850 MHz ISM frequency band for space and terrestrial sensing applications. A bi-static antenna configuration is used to increase the isolation between the transmit and received antenna of the RF reader for better sensitivity. The recharging speed and operating time of this RF tag are measured at different levels of received power. By introducing the power management circuit to a one-stage Dickson charge pump, we reduce the turn-on power requirement of the passive RF tag from 2 dBm to -8 dBm, which results in twice the communication distance (assuming that backscatter communication is down-link limited). The power management module also protects the RF tag from excessive supply voltage, enabling the backscatter communication at shorter distances. Furthermore, the data received from RFTSat on orbit is reported and shown to generally match expected trends.

### **Acknowledgment**

This work is sponsored by Northwest Nazarene University and through a NASA Undergraduate Student Instrument Project (USIP) Student Flight Research Opportunity (SFRO) grant (NNX16AI77A) awarded to the university.

## **CHAPTER 4**

### **LONG-RANGE SUB-METER SCALE RANGING WITH TUNNELING RFID TAGS**

This chapter demonstrates the ability to extend the positioning range of low-powered RFID tags to distances usually not achievable with other wireless or conventional RFID technologies. The technique is performed through a Received Signal Phase (RSP)-based method on a 5.8 GHz backscatter Tunneling Tag (TT), in multipath-rich indoor and outdoor environments, at distances up to 35 meters from the reader. Distance errors as low as 0.1% of the total reader-to-tag distance were observed with average errors of 0.8% and 0.6% for indoor and outdoor environments, respectively. Compared to Received Signal Strength (RSS)-based techniques, the average distance estimation accuracy is improved by a factor of 51 and 38 for indoor and outdoor environments, respectively. Moreover, an Effective Isotropic Radiated Power (EIRP) of only 10.5 dBm and a biasing power for the tunneling tag of only  $21.3 \mu\text{W}$  at 80 mV promise a low-power, long-range sub-meter scale positioning technique with a projected maximum range over 1 km. The reader setup and MATLAB code used in this chapter are available in Appendix B and C.1.

#### **4.1 Introduction**

The rapid development of the Internet-of-Things and RFID industry is witnessing an increasing demand for systems that can identify people and objects together with their locations. A highly accurate wireless positioning system, in fact, could revolutionize smartphone applications, augmented reality experiences, and autonomous vehicle navigation with the RFID technology being the key player in their development. In fact, RFID readers perform coherent detection that allows to gather both RSS, and coherent RSP that can be used to locate and track an RFID tag. Yet, fundamental limitations in wireless localization

and positioning techniques remain: fine-scale accuracy, particularly at the fringe of coverage for both short- and long-range radios, is extremely difficult to achieve. Multiple factors affect the coverage and the accuracy of localization: the frequency bandwidth used by the RFID system, the sensitivity of the RFID reader, the antenna gain, the localization techniques, the environmental factors, the availability of clear LoS between tags and readers, multipath, and propagation losses.

Starting from early results described in [19], this chapter presents how to break the range limit of RFID positioning by combining RSP-based positioning methods with tunneling tags. It exploits both the full-coherent signal and the multiple phase data that a single RFID reader receives from a tag operating at the 5.8 GHz ISM band (5.725 GHz to 5.975 GHz). A tunneling tag amplifies the signal strength of a backscattered signal and preserves its phase allowing for accurate estimates of position and/or orientation at long distances. Through both indoor and outdoor reader-to-tag distance measurements, this article demonstrates how long-range LoS positioning is possible with tunneling tags; it compares the achieved accuracy with that of a conventional RSS-based technique; and it introduces an effective calibration method that can further increase the accuracy. Finally, all the results obtained with the Tunneling Tag (TT) are compared with those achieved through a conventional Semi-passive Tag (SpT).

With respect to the state-of-the-art of RFID positioning systems (summarised in chapter 2), the proposed technology gives lower positioning errors (below 0.8%) than state-of-the-art solutions at above-average backscattering ranges (35 meters, and more). Traditional positioning techniques tend to have percentage distance errors that worsen when the ranges increase. With this work, instead, the lowest percentage errors are reported despite longer distances are involved.

Since multiple readers can be used for accurate positioning applications both in 2- and 3-dimensional spaces, this new technique enables real-time, low-powered, and long-range precise positioning of objects such as pallets, vehicles, animals, and goods. For instance,

RFID readers equipped in smart warehouses could monitor goods while handling ground traffic of forklifts and staff equipped with tunneling tags. Finally, by operating at microwave frequencies, this system could be integrated within handheld devices or drones and communicate with future 5G networks.

## 4.2 Rationale

### 4.2.1 RSP-based Distance Estimation

The coherent detection performed by RFID readers allows the recovery of both amplitudes and phases of the received signals to perform spatial identification, such PDoA, of an RFID tag. Upon demodulation and after filtering out the DC component of a backscattered RFID signal (Figure 4.1), the RSS and the RSP can be expressed as:

$$P_{RSS} = \frac{I_{rx}^2 + Q_{rx}^2}{Z_0}, \quad (4.1)$$

$$\varphi_{RSP} = \arctan\left(\frac{Q_{rx}}{I_{rx}}\right) \in [0, 2\pi), \quad (4.2)$$

where  $I_{rx}$  and  $Q_{rx}$  are the amplitudes of the In-phase ( $I$ ) and Quadrature ( $Q$ ) channels of the received signal; and  $Z_0$  is the input impedance of the receiving antenna ( $50 \Omega$ ).

In free space, when no multipath reflections occur, the unwrapped phase offset  $\varphi_{ps}$  caused by the LoS round-trip propagation can be written as [9]:

$$\varphi_{ps} = -\frac{4\pi f_c d}{c}, \quad (4.3)$$

where  $c$  is the speed of light in free-space;  $d$  is the distance between the reader and the target tag; and  $f_c$  is the carrier frequency of the RFID reader.

The overall  $\varphi_{RSP}$  in (Equation 4.2) with presence of multipath can then be expressed



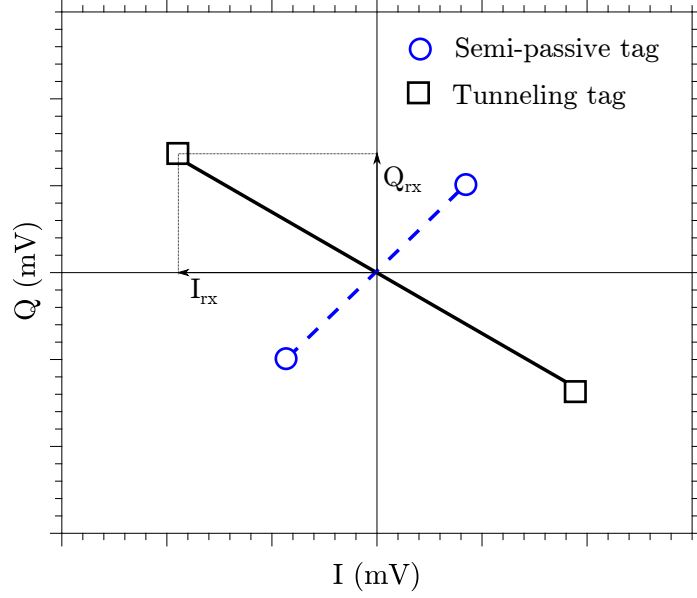


Figure 4.1: Received signal from semi-passive and tunneling tags.

also as:

$$\varphi_{RSP}(f_c) = \varphi_{ps}(f_c) + \varphi_0(f_c) + \varphi_m(f_c) + \varphi_t, \quad (4.4)$$

where the dependency on the carrier frequency  $f_c$  is highlighted. In (Equation 4.4),  $\varphi_0$  is the phase offset caused by the system and due to cables, antennas, tag modulation, and other reader components;  $\varphi_m$  is the phase offset caused by the multipath channel; and  $\varphi_t$  is the phase error due to the thermal noise, the Local Oscillator (LO), the IQ imbalance, the transmit-to-receive leakage [54], and other random interference such as a person passing by.

An RSP-based method [20] can be used to estimate the distance  $\hat{d}$  between a reader and a tag. The method consists in subtracting the phases,  $\varphi_{RSP}$ , of two signals received at two adjacent frequency channels and in averaging those differences over a specific band:

$$\hat{d} = \frac{c}{4\pi N} \sum_{n=1}^{N-1} \left| \frac{\varphi_{RSP_n} - \varphi_{RSP_{n+1}}}{f_n - f_{n+1}} \right|. \quad (4.5)$$

With  $\varphi_{RSP_n}$  and  $\varphi_{RSP_{n+1}}$  being the measured phases of the received signals obtained

through (Equation 4.2) at the reader carrier frequencies  $f_n$  and  $f_{n+1}$ , respectively; and  $N$  being the number of the frequency channels.

Through a uniform frequency step  $\Delta f = f_{n+1} - f_n$ , the equivalent wave length  $\lambda_e = \frac{c}{\Delta f}$  can be defined. Therefore, (Equation 4.5) becomes:

$$\hat{d} = \frac{\lambda_e}{4\pi N} \sum_{n=1}^{N-1} |\varphi_{RSP_n} - \varphi_{RSP_{n+1}}| = \frac{\lambda_e}{4\pi} \overline{\Delta\varphi}, \quad (4.6)$$

with

$$\overline{\Delta\varphi} = \frac{1}{N} \sum_{n=1}^{N-1} |\varphi_{RSP_n} - \varphi_{RSP_{n+1}}|, \quad (4.7)$$

being the average phase offset caused by both the system and by the multipath environment. Since the received wrapped signal phase  $\varphi_{RSP}$  is equal to the unwrapped phase  $\varphi_{ps}$  only when  $|\varphi_{RSP_n} - \varphi_{RSP_{n+1}}| \geq 2\pi$ , then, the maximum detection range  $\hat{d}_{max}$  of the phase-based method is determined by the minimum frequency step  $\Delta f$  of the reader:

$$\hat{d}_{max} = \frac{c}{2\Delta f} = \frac{\lambda_e}{2}. \quad (4.8)$$

Although most conventional positioning techniques for RFID tags use distance-dependent path loss models based on RSS, they are usually severely affected by both the propagation environment and the properties of the tagged objects. Therefore, RSS-based positioning techniques cannot be universally applied, and absolute calibration is rather difficult. Moreover, unlike a conventional backscatter RFID tag that has a constant modulation factor  $M$ , the gain of the tunneling tag fluctuates between 5 dB to 38 dB for impinging powers ranging between -55 dBm and -80 dBm [3], respectively. The nonlinear relationship between the gain and the impinging power makes the calibration of RSS-based localization for tunneling tag even more difficult. However, the phase offset of the backscatter signal caused by the tunneling tag modulation is a constant that is independent of the impinging power and does not affect phase-based positioning techniques.

### 4.2.2 Distance and Error Estimation

To achieve good accuracy, system calibration is usually necessary for most positioning techniques before performing any measurements. For the RSP-based method, the ground-truth distance  $d$  between a reader and a tag is affected by distance errors  $\epsilon$  such that the estimated distance  $\hat{d}$  in (Equation 4.6):

$$\hat{d} = d + \epsilon, \quad (4.9)$$

includes the distance errors  $\epsilon$ :

$$\hat{d} = d + \epsilon_0 + \epsilon_m + \epsilon_t; \quad (4.10)$$

where  $\epsilon_0$  is the distance error brought by the phase delay due to wave traveling within the RF cables and traces in the reader and tag;  $\epsilon_m$  is the error brought by multipath; and  $\epsilon_t$  is the error due to the thermal noise, the phase noise of the LO, the IQ imbalance, the transmit-to-receive leakage [54], and other interference sources such as a person passing by. Finally, by comparing the ground-truth distance  $d$  with the estimated  $\hat{d}$ , it is possible to define the percentage error as:

$$\epsilon_{\%} = \frac{\hat{d} - d}{d} \cdot 100\% \quad (4.11)$$

## 4.3 Multipath

### 4.3.1 Multipath Channel Modeling

Any terrestrial, non-laboratory radio channel will contain multipath components due to the reflection, diffraction, and scattering of electromagnetic waves. Multipath introduces numerous delayed copies of the original signal, which distort time-of-flight measurements. Wireless engineers often model the multipath channel as a collection of discrete multipath

components constituting a *power delay profile*,  $p(\tau)$ , as a function of delay  $\tau$ :

$$p(\tau) = \sum_i p_i \delta(\tau - \tau_i) \approx \frac{P_o}{\sigma_{\text{RMS}}} \exp\left(-\frac{\tau}{\sigma_{\text{RMS}}}\right) u(\tau) \quad (4.12)$$

where  $p_i$  is the power of the  $i$ th multipath component, arriving at delay  $\tau_i$ ,  $u(\tau)$  is the unit step function. Delays for this analysis have been normalized relative to the first arriving multipath component at  $\tau = 0$ . The power delay profile generally consists of a first-arriving LoS component that also is usually the strongest in terms of power. Subsequent components generally, but not strictly, decay as the arrival time increases its delay. For this reason, radio engineers early capture the overall shape of typical power delay profiles with an exponential distribution of power vs delay, as indicated in (Equation 4.12), which depends only on the Root-Mean-Square (RMS) delay spread,  $\sigma_{\text{RMS}}$  [68].

The exponential model for power-delay-profile is a helpful guide for the dispersive nature of a radio channel. The RMS delay spread, in particular, is often enough to completely characterize the *coherence bandwidth* of a radio channel – the bandwidth over which the channel appears essentially “flat”. For an exponentially decaying distribution of power in delay, the mean delay (as referenced from  $\tau = 0$  in (Equation 4.12)) *and* the RMS width (second centered moment) of the distribution are both given by  $\sigma_{\text{RMS}}$ . RMS delay spread has been measured extensively for indoor and outdoor one-way channels and is typically calculated from spatial-averaging of at least several, local area power impulse responses to remove small-scale fading effects.

If the beginning of a power delay profile marks the arrival of a first LoS component, then the absolute delay of this first component can be used for precise positioning. However, if a narrowband signal is probing the channel phase as a function of frequency, then *all* multipath components will contribute to this aggregate measurement – not simply the first arriving component. Thus, we would expect the *centroid* of the distribution to introduce a consistent bias in phase change as a function of frequency (causing a positioning

algorithm to *overestimate* the distance between transmitter and receiver). Likewise, the *RMS width* (delay spread) of the distribution will influence the variability of instantaneous phase measurements about the average, biased range estimate.

For the purposes of backscatter positioning with narrowband phase measurements, we should not simply consider the 1-way power delay profile. First, it is more natural to measure an *envelope profile* in signal processing with units proportional to *voltage* rather than power. Fortunately, the envelope distribution of the one-way channel should follow naturally from the square root of the power delay profile and will also be exponential. The centroid and RMS width of the envelope profile will differ, though, as summarized in Table 4.1.

Table 4.1: Idealized centroids and RMS widths of multipath distributions in delay for one- and two-way channels, with power or envelope delay spectra.

Delay Spec.	Profile, $\tau > 0$	Centroid	RMS Width
1-way Power	$\frac{\exp\left(\frac{-\tau}{\sigma_{\text{RMS}}}\right)}{\sigma_{\text{RMS}}}$	$\sigma_{\text{RMS}}$	$\sigma_{\text{RMS}}$
1-way Env.	$\frac{\exp\left(\frac{-\tau}{2\sigma_{\text{RMS}}}\right)}{2\sigma_{\text{RMS}}}$	$2\sigma_{\text{RMS}}$	$2\sigma_{\text{RMS}}$
2-way Power	$\frac{\tau^2 \exp\left(\frac{-\tau}{\sigma_{\text{RMS}}}\right)}{2\sigma_{\text{RMS}}^3}$	$3\sigma_{\text{RMS}}$	$\sqrt{3}\sigma_{\text{RMS}}$
2-way Env.	$\frac{\tau \exp\left(\frac{-\tau}{2\sigma_{\text{RMS}}}\right)}{4\sigma_{\text{RMS}}^2}$	$4\sigma_{\text{RMS}}$	$2\sqrt{2}\sigma_{\text{RMS}}$

If the radio channel is measured in a simple, monostatic backscatter configuration, the radio signal must travel through the channel twice. For a single-antenna RFID tag with load modulation, the effective channel is the *convolution* of a one-way channel with itself. A channel that follows a conventional exponential decay of power as a function of delay will have an envelope spectrum of the generic form  $\tau \exp(-\tau)$  in the two-way link. Furthermore, the power delay spectrum of the two-way link would naturally follow the square of the envelope delay spectrum, leading to a generic  $\tau^2 \exp(-\tau)$  distribution. Table 4.1 contains the profile shape for each type of spectrum and link, with the appropriate scaling constants to normalize the area under the distribution to 1.

The fine structure of the discrete multipath channel model will cause deviations from the ideal centroids and RMS widths of Table 4.1. Even ignoring this complexity, a conventional RMS delay spread of  $\sigma_{\text{RMS}}$ , could reasonably lead to 1, 2, 3, or 4 times the actual offset error, depending on how the radio channel is measured and processed. The preliminary measurements and analysis in this chapter use the centroid error corresponding to the two-way channel envelope profile. This appears to match the error best for the specific, measured backscatter links.

#### 4.3.2 Evidence of Multipath Channel

Indoor settings are characterized by a multipath-rich environment where the  $\varphi_m$  in (Equation 4.4) contributes significantly to the measured phase  $\varphi_{RSP}$  and may significantly affect the correct estimation of the actual tag position, especially at short distances. To calibrate out the error added by the multipath propagation ( $\epsilon_m$ ), the multipath-rich wireless channel is investigated by using the setup shown in the inset of Figure 4.2 having two antennas at a distance of 3 m from each other. Both the reader and the tag antennas were connected to a Vector Network Analyzer (VNA) to record the S-parameters and measure the channel frequency response from 4.8 GHz to 6.8 GHz. The 2-way envelope delay spectrum of the multipath channel can be derived by:

$$P_{rx}(\tau) = \int_{-\infty}^{+\infty} S_{21}(f)S_{12}(f)e^{2j\pi f\tau}df, \quad (4.13)$$

where  $P_{rx}(\tau)$  is the magnitude of the 2-way envelope delay spectrum. Five measurements were taken to average out the impact of small scale fading whose effect is depicted by the solid line in Figure 4.2.

In Figure 4.2 both the LoS and the multipath components that generate the delay profile of an indoor environment are highlighted. To obtain a high-resolution multipath channel model required for an accurate estimation of tag location, a deconvolution algorithm, called the CLEAN algorithm [69, 70, 71] was used to obtain the discrete 2-way envelope delay

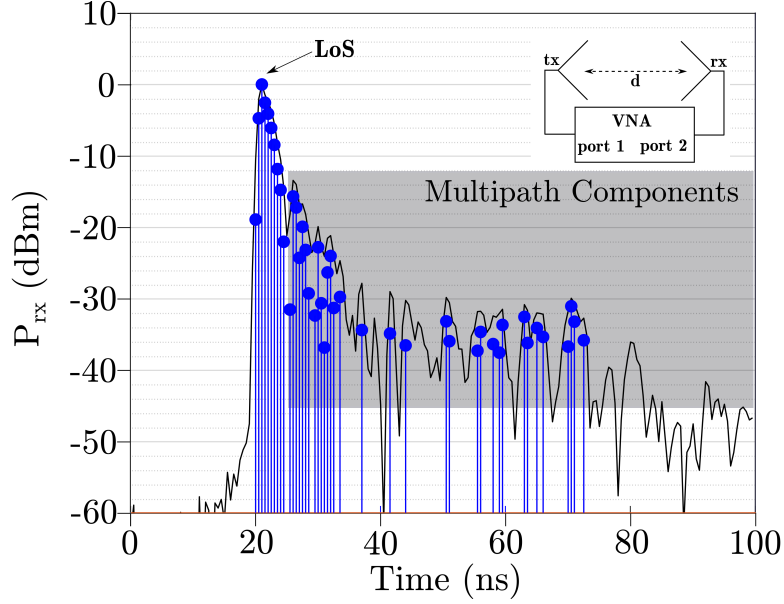


Figure 4.2: Solid line: 2-way envelope delay spectrum of the multipath-rich indoor environment (time span: 100 ns, distance  $d$ : 3 m between reader and tag antennas). The LoS and the multipath effects are highlighted. Stem plot: the CLEAN algorithm reconstruction of the 2-way envelope delay spectrum. The average time delay  $\bar{\tau} = 25.0$  ns, due to multipath corresponds. Inset: setup used to estimate the multipath effects of the indoor scenario. VNA settings: center frequency 5.8 GHz; span 2 GHz;  $d = 3$  m; # of points 1601; avg.: 16. spectrum. The distorted clean pulse used by the deconvolution algorithm is measured by connecting the two ports of the VNA directly [71]. The amplitude  $A(\tau)$  of the delay profile after deconvolution, at time delay  $\tau$ , is shown by the stem plot in Figure 4.2. The received signal at the reader,  $\tilde{R}(\tau)$ , can be written as:

$$\begin{aligned}\tilde{R}(\tau) &= \sum_n A_n(\tau) \\ &\approx R_o \exp(-j\bar{\Delta\varphi}) \exp(-j2\pi f\tau).\end{aligned}\tag{4.14}$$

The mean delay  $\bar{\tau}$  of the multipath channel can be calculated by:

$$\bar{\tau} = \frac{\int_0^\infty \tau A(\tau)}{\int_0^\infty A(\tau)}.\tag{4.15}$$

Although in a multipath-free environment a time delay  $\tau$  of 20 ns is expected at 3 m,

as the leading pulse implies, the presence of multipath adds further delays that shift the average  $\bar{\tau}$  to 25.0 ns as computed through (Equation 4.15) and shown in Figure 4.2. This corresponds to a positioning error of 37.5 cm according to Table 4.1. Multipath, in fact, is one of the major sources of error, its procedures are not practical for realistic applications because of its complexity and because its accuracy is prone to every environmental changes. Nonetheless, its effects can be mitigated by calibrating the system with measurements at distances above the meter (*e.g.*: at 5 m, subsection 4.5.3) so that the effects of multipath are taken into account and lower distance estimation errors occur.

#### 4.4 The Experimental Setup

subsection 4.2.1 has described a positioning method that uses the received signal phase to estimate, through (Equation 4.6), the distance  $\hat{d}$  between the reader and the tag. An experimental setup (Figure 4.3a) has been used to test how the phase-based method improves the estimation of tag positioning both for short and long-ranges in indoor and outdoor environments. The benefits of system calibrations are also investigated.

As shown in Figure 4.3b and Figure 4.3c, indoor and outdoor experiments were done while using both semi-passive ( $M \leq 1$ ) and tunneling tags ( $M > 1$ ). The RF reader (described in [72, 73]) was programmed to operate at 5.8 GHz ISM band, hopping between 50 pre-programmed frequency channels and connected to transmit and receive microstrip patch antennas with a gain  $G_{tx,rx} = 7.5$  dBi and located 1.14 meters above the ground. The transmit power of the reader,  $P_T$ , was set to 3 dBm to trigger enough gain in the tunneling tag [3]. The detailed reader setup is available in Appendix B. The signal received by the reader was demodulated and down-converted to base-band, but no base-band amplification was used. The received signal was processed in GNU Radio and MATLAB to extract the phase and amplitude of the received square wave. An Fast Fourier Transform (FFT) filter increases the signal to noise ratio and mitigates the errors due to both phase and thermal noises. A summary of the experimental setups is reported in Table 4.2.



Both indoor and outdoor tests were performed. For fair comparison the same patch antenna array with  $G_t = 9$  dBi<sup>1</sup> was used on both tags and the LoS distance  $d$  from the reader was changed from 5 to 35 meters, with a step width of 5 meters. The reader was programmed for hopping between 50 frequency channels (from 5.75 GHz to 5.8 GHz) with a dwell time of 2 seconds at uniform intervals of 1 MHz ( $d_{max} = 150$  m). The semi-passive tag was modulated by Binary Phase Shift Keying (BPSK) with a maximum modulation factor  $M$  of -6 dB<sup>2</sup>, while the tunneling tag used On-Off Keying (OOK) and, through tunneling, it amplified the backscattered signal ( $M > 5$  dB).

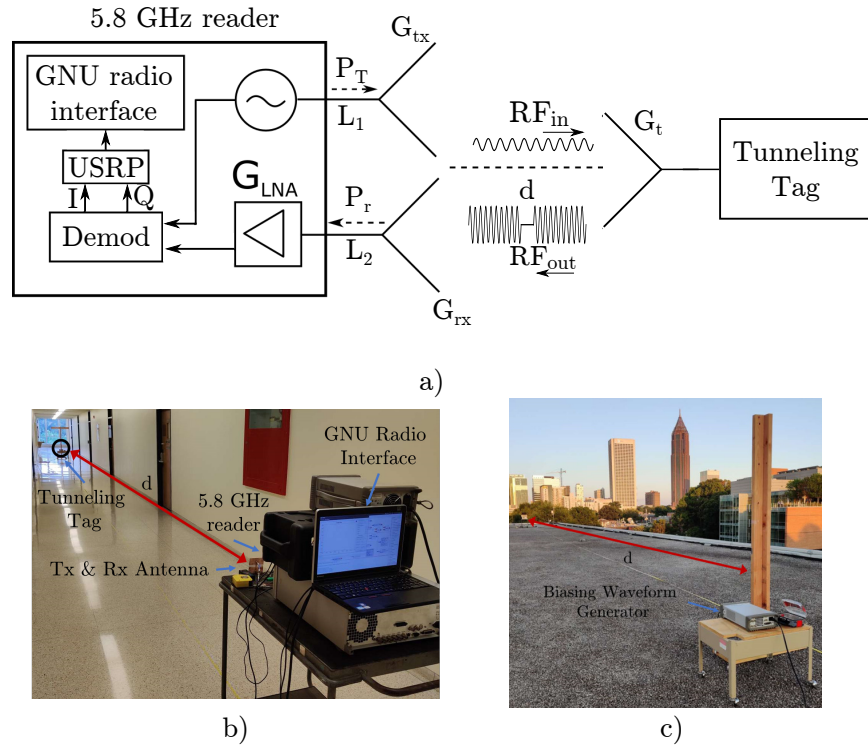


Figure 4.3: a) Reader and tag configuration used for indoor and outdoor measurements.  $G_{tx} = G_{rx} = 7.5$  dBi,  $G_t = 9$  dBi,  $P_T = 3$  dBm,  $d \in [5, 35]$  m. Photos of the b) indoor and c) outdoor setups used for long range tests.

<sup>1</sup>An array antenna was chosen to allow the Semi-passive tag to backscatter from longer distances and enable a comparison with the long-range backscattering of the tunneling tag.

<sup>2</sup>Due to internal losses within the on-board RF switch.

Table 4.2: Specifications of the Experimental Setup

$G_t$ (dBi)	9
$d$ (m)	[5:5:35]
$P_T$ (dBm)	3
$G_{tx,rx}$ (dBi)	7.5
Freq. hopping (GHz)	5.75:5.8
Freq. step $\Delta f$ (MHz)	1

## 4.5 Experimental Results

### 4.5.1 Exploiting RSP Data

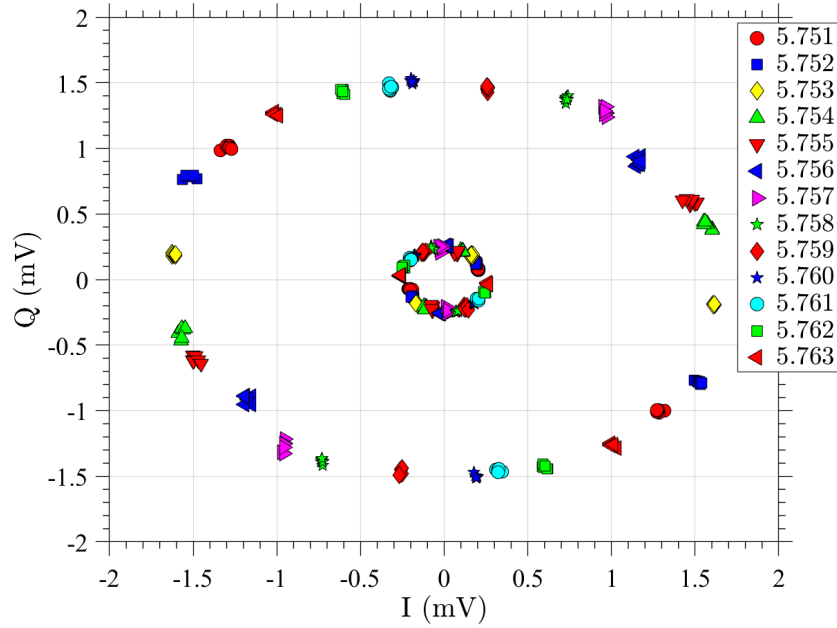
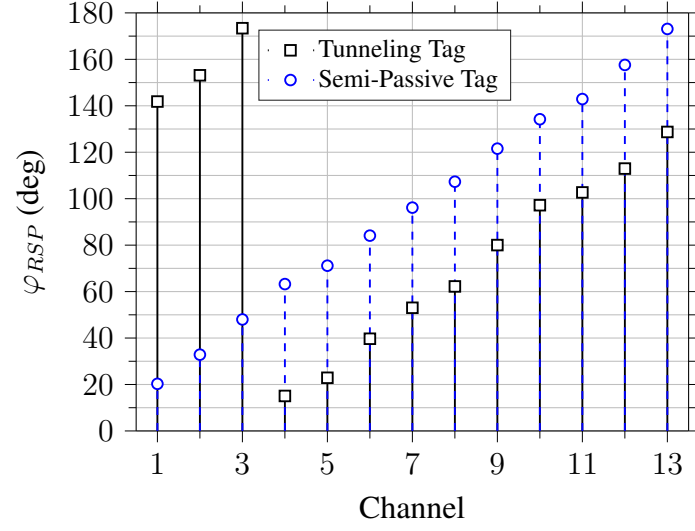
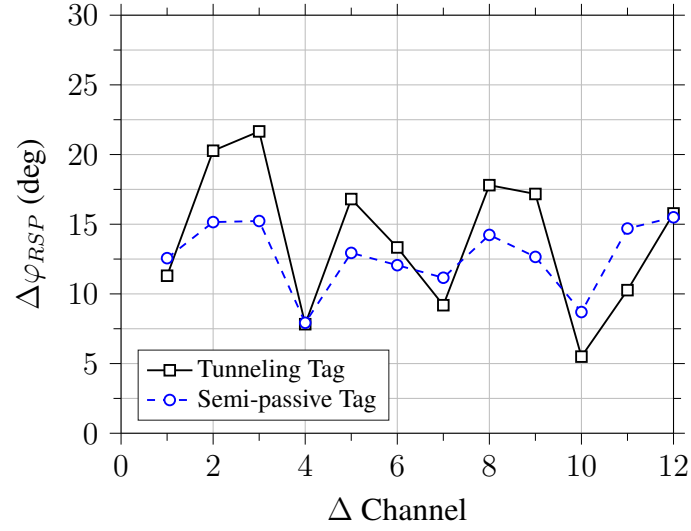


Figure 4.4: The IQ constellation points in the 5.8 GHz band (5.751 to 5.763 GHz) for both the semi-passive and the tunneling tags measured indoor at a distance of 5 m from the reader. The tunneling tag provides a higher level of backscattered power.

The experimental setup detailed in section 4.4 collected the IQ constellations of the received signals for both the semi-passive and the tunneling tags at a distance of 5 m away from the reader (impinging power on tag of -42.20 dBm). Figure 4.4 shows the received



(a)



(b)

Figure 4.5: a) Phases, and b) phase-differences between 13 adjacent channels measured indoor at 5 meters away from the reader for both the semi-passive ( $\circ$ ) and the tunneling tags ( $\square$ ).

$I_{rx}$  and  $Q_{rx}$  values of 13 out of 50 adjacent channels for both the semi-passive and the tunneling tags; it highlights that the  $P_{RSS}$  of the former is 20 dB below the  $P_{RSS}$  of the latter. Considering that the tunneling tag has higher gains when the impinging power decreases (especially below -60 dBm), intelligible received powers  $P_r$  are expected at longer distances [3].

Figure 4.5a illustrates the absolute wrapped phases  $\varphi_{RSP}$  of the received signals while

the phase differences between adjacent channels,  $\Delta\varphi_{RSP_n} = |\varphi_{RSP_n} - \varphi_{RSP_{n+1}}|$ , are shown in Figure 4.5b. When a tag is 5 meters away from the reader, the expected phase difference between two adjacent channels is  $\Delta\varphi_{RSP_0} = \frac{4\pi d}{\lambda_e} = 0.21 \text{ rad}$  ( $12^\circ$ ), with  $\lambda_e = \frac{c}{\Delta f} = 300 \text{ m}$ . Nevertheless, Figure 4.5b shows that the phase differences between adjacent channels are generally higher than  $12^\circ$  in both tags due to the combined effects of multipath and wave propagation within the reader. In fact, computing (Equation 4.7) over all the available 50 channels, returns an average phase differences  $\overline{\Delta\varphi}$  of  $13.27^\circ$  and  $14.33^\circ$  to which corresponds, through (Equation 4.6), estimated distances  $\hat{d}_{SpT} = 5.53 \text{ m}$  and  $\hat{d}_{TT} = 5.97 \text{ m}$ , for a semi-passive Tag and a tunneling Tag, respectively.

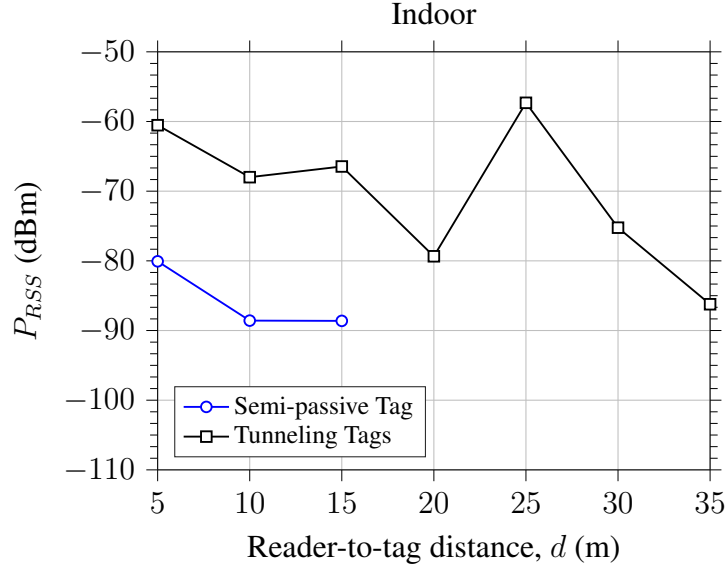
Among the three error sources in (Equation 4.10), the one caused by RF cables ( $\epsilon_0$ ) is universal across all distances when using the same hardware setup. Thus, it can be calibrated out by using one or more reference measurements. As reference, therefore, the measurements done on the rooftop (Figure 4.3c) were used for both the semi-passive and the tunneling tags. If the measurement at 1 m is used as reference, then the signal-to-noise ratios are high enough to allow neglecting  $\epsilon_t$  brought by the thermal noise. Moreover, both the open environment and the short distance allow to neglect the effects of multipath  $\epsilon_m$ . The total distance error at 1 m thus becomes:

$$\epsilon_{1m} = \epsilon_0 = \hat{d} - d. \quad (4.16)$$

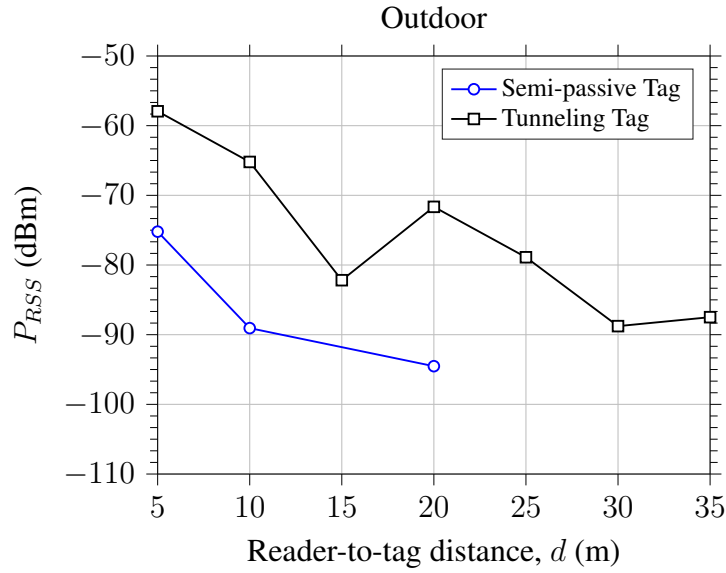
If the reference measurement is taken at 5 m instead, all the error sources can be taken into account, thus giving:

$$\epsilon_{5m} = \epsilon_0 + \epsilon_m + \epsilon_t = \hat{d} - d. \quad (4.17)$$

Calibration at distances higher than 1 m should, therefore, be able to take into account more error sources and provide better accuracy.



(a)

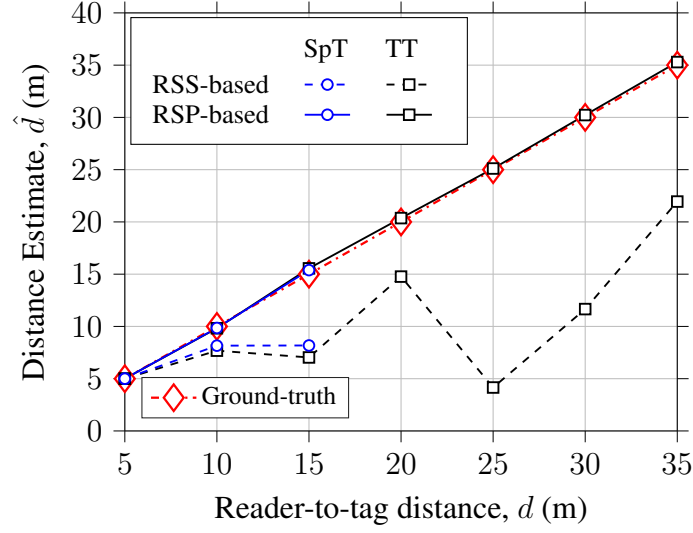


(b)

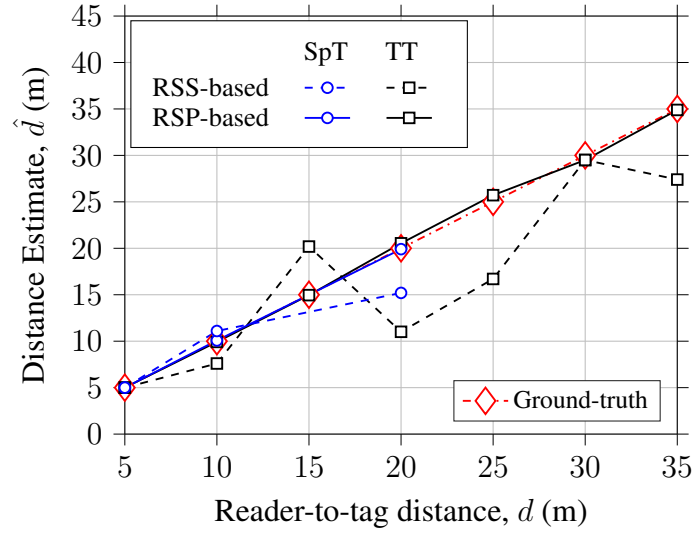
Figure 4.6: a) Indoor, and b) outdoor calculated (dashed) and measured (solid)  $P_{RSS}$  values. Data points are for both semi-passive ( $\circ$ ), and tunneling tags ( $\square$ ).

#### 4.5.2 RSS- vs RSP-based Method

Using the experimental setup described in section 4.4, the  $P_{RSS}$  of both the semi-passive and the tunneling tags were measured, through (Equation 4.1), when changing their distance  $d$  from the reader. Figure 4.6a and Figure 4.6b compare the RSS when using a



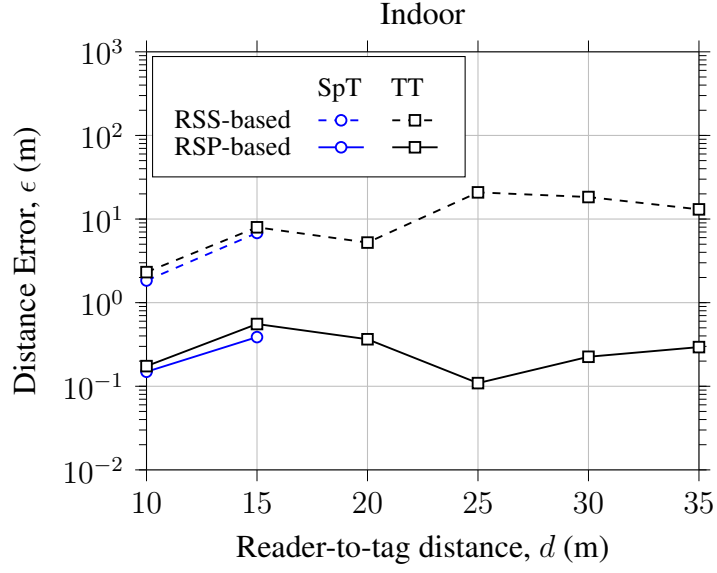
(a)



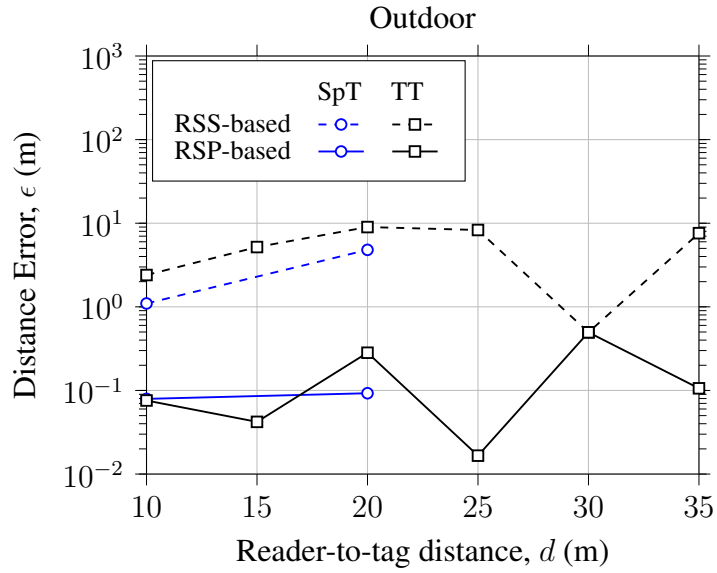
(b)

Figure 4.7: a) indoor, and b) outdoor distance estimates  $\hat{d}$  using RSS-based method (dashed) and RSP-based method (solid). Data points are for both semi-passive ( $\circ$ ), and tunneling tags ( $\square$ ).

semi-passive and a tunneling tag; the results clearly show that a semi-passive tag cannot be detected for distances above 15 meters (indoor) and 20 meters (outdoor), while the tunneling tag can still be read at 35 meters, or more, from the reader. Moreover, the measured  $P_{RSS}$  of the tunneling tag show a non-linear relationship with the distances because the actual reflection gain depends both on the biasing voltage level, the operating frequency,



(a)



(b)

Figure 4.8: a) Indoor, and b) outdoor distance errors  $\epsilon$  for RSS-based (dashed) and RSP-based (solid) methods with calibration at 5 meters. Data points are for both semi-passive ( $\circ$ ), and tunneling tags ( $\square$ ).

and the impinging RF power level [1].

RSS-based methods estimate the distance from the reader by inverting the free-space link budget equation in (Equation 1.1) and by substituting  $P_r$  with the measured  $P_{RSS}$ .

Figure 4.7a and Figure 4.7b show the estimated distance  $\hat{d}$  for the two types of tags<sup>3</sup> in indoor and outdoor environments and compare them with the estimations obtained through the RSP-based method in (Equation 4.6) *when using measurements taken at 5 meters as calibration data*. The figures highlight how the accuracy of the RSS-based method worsen when the distances increase since multipath significantly affects the received signal power level  $P_{RSS}$ . The RSP-based method, on the other hand, significantly improves the positioning accuracy for both semi-passive tags and tunneling tags that operate at longer distances.

Finally, Figure 4.8a and Figure 4.8b show the distance errors  $\epsilon$  of both RSS- and RSP-based methods for semi-passive and tunneling tags. In both indoor and outdoor measurements, the RSS-based method does not give an accurate estimation when the distance increases, while the RSP-based method provides more accurate results at any distance. For both tags, the RSP-based method can reduce the estimation distance error by at least an order of magnitude at all distances. In fact, the RSS-based method, combined with tunneling tags, gives an average distance error  $\bar{\epsilon}$  of 40.6% (9.68 m) and 22.9% (4.71 m) indoor and outdoor, respectively. The proposed RSP-based method, instead, gives a mean error  $\bar{\epsilon}$  of 0.8% (0.25 m) and 0.6% (0.15 m) indoor and outdoor, respectively. Thus, it increases the accuracy by a factor of 51 and 38 for the two scenarios.

#### 4.5.3 Calibration with Reference Measurements

It is interesting to compare the effects of calibration on the final results of the proposed RSP-based method. For this purpose, Figure 4.9a and Figure 4.9b are used to compare the distance errors  $\epsilon$  for indoor and outdoor cases when either i) no calibration; or ii) calibration at 1 m; or iii) calibration at 5 m are applied. For each set of data, the average distance error  $\bar{\epsilon}$  associated with positioning of the tunneling tag decreases from 1.17 m (no calibration) to 0.65 m (calibration at 1 meter), and up to 0.25 m (calibration at 5 meters) for the indoor

---

<sup>3</sup>Since the gain of the tunneling tag is difficult to predict at a specific distance, its distance from the reader using the link budget equation was computed by assuming a uniform gain ( $\approx 18$  dB) across all the considered positions.

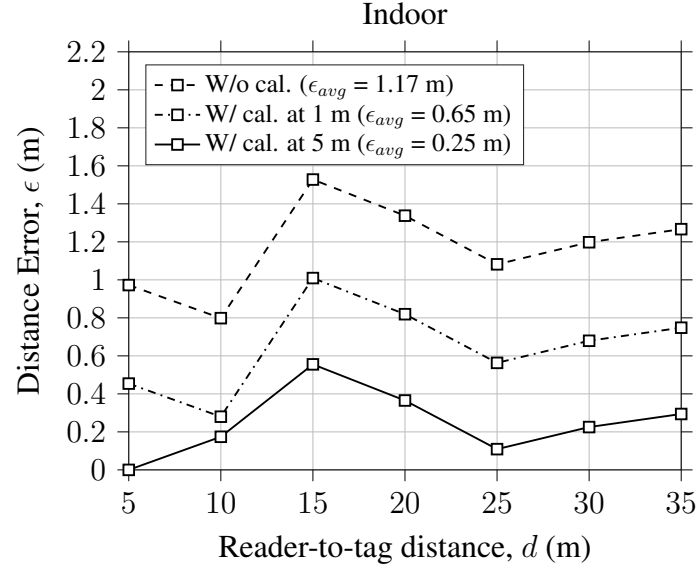


tests. It decreases from 0.67 m (no calibration) to 0.22 m (calibration at 1 meter) and up to 0.15 m (calibration at 5 meters) for the outdoor tests. Indoor, the estimated distance errors differ by 40 cm according to the type of calibration used (at 1 m vs 5 m) since multipath is taken more into account at 5 m. Outdoor, instead, the estimated distance errors differ by only 7 cm.

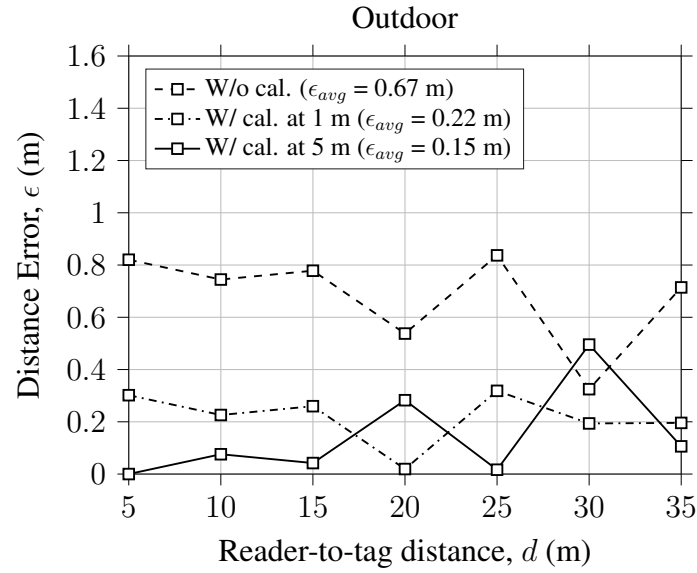
Positioning within a 35-meter range gives an uncalibrated average distance error  $\overline{\epsilon}_{\%}$  of 8.0% and 5.5%, for indoor and outdoor scenarios, respectively. Finally, calibration with reference measurement at 5 m reduces the mean errors to 0.8% and 0.6%, respectively.

Overall,  $\epsilon$  tends to be constant over the distance with a slight fluctuation in the indoor case where the multipath ( $\epsilon_m$ ) is more significant. The calibration at 5 m applied in an outdoor scenario reduces the average distance error  $\bar{\epsilon}$  only from 0.22 m to 0.15 m because of the reduced effect of multipath. The beneficial effect of calibrating the setup at long distances is evident especially for indoor measurements; outdoor, instead, short-range calibrations already provide good accuracy that can be further enhanced by using calibrations at longer ranges.

Considering that an EIRP of 10.5 dBm is used in this work, the maximum reading range can be easily extended up to 1 km by further increasing the EIRP (*e.g.*: an EIRP of 36 dBm used in many unlicensed ISM bands) and by adding base-band amplification in the receiver chain [3]. Since the estimation error does not increase with distance (Figure 4.9), a frequency-hopping step  $\Delta f$  of 150 kHz, would increase the maximum range to 1000 m while keeping similar absolute error. Given the  $\bar{\epsilon}$  is expected to be less than 1 m, the percentage error  $\overline{\epsilon}_{\%}$  at 1000 m can be below 0.1% (Figure 2.3). At this distance, the range correlation may degrade the phase noise of the LO by maximum 6 dB rather than improving it like at shorter distances [74]. However, after degradation, the LO phase noise of a disciplined commercial oscillator will still satisfy the phase noise requirements of an RFID reader [75].



(a)



(b)

Figure 4.9: Estimated errors  $\epsilon$  and averages  $\epsilon_{avg}$  with and without calibrations in a) indoor, and b) outdoor environments for the tunneling tag ( $\square$ ).

## 4.6 Conclusions

An RSP-based positioning technique has been described and validated for long-range backscattering. Since tunneling tags allow long communication distances, they have been used to prove the proposed method. With appropriate calibration, correct positioning is possible

even in a multipath-rich indoor environment. Comparisons with RSS-methods have shown how the RSP-method improves the accuracy by a factor of up to 51. All the results were compared with those of a conventional semi-passive tag; despite the accurate estimation of its position, it proved to have a shorter detectable range than the tunneling tag. Finally, the low-power consumption and an EIRP of only 10.5 dBm confirms how tunneling tags can extend RFID positioning ranges with lower powers and higher accuracy than any other RFID-based positioning techniques.

## **CHAPTER 5**

### **FINE-SCALE RANGING USING TUNNELING RFID TAGS IN NLOS SCENARIOS**

Tunneling Tags (TTs) have already shown their long-range capability for communications and localization in Line of Sight (LoS) with a reader operating in the 5.8 GHz band. In this chapter, a received signal phase-based positioning method is investigated using semi-passive and tunneling RFID tags in various non-line-of-sight (NLoS) environments. Experimental results show that a tunneling tag achieves gains above 18.6 dB and 19.6 dB when communicating through a cinder block and a plaster wall, respectively. When using the tunneling tag, with proper calibration, an average distance estimation accuracy of 1.33% and 2.2% is achieved in the hallway and classroom with clear LoS. An average estimation error of 1.02% and 1.9% is observed in through-obstruction and through-wall NLOS conditions, respectively. The code used in this chapter is available in Appendix C.2.

#### **5.1 Introduction**

Fine-scale localization technology in realistic environments enables numerous commercial and scientific applications that can be key for the development of versatile wireless sensing applications. Rescuers, task forces, and security staff would all benefit from a tracking technology that can, for example, protect from unpredictable threats in unknown buildings or environments [56][76].

RF sensing is a popular choice for localizing people in NLoS conditions because of its ability to sense movements through obstructions and smoke, independently from lighting conditions [77][78]. Prior research has demonstrated how radio tomographic imaging (RTI) and through-wall radars provide solutions for imaging, identification, and motion tracking accross walls and buildings [77, 78, 79, 80, 56, 76]. However, obstacles significantly impair

most radio-based localization techniques due to low signal strength and multipath effects.

Research has recently focused on improving the accuracy to localize RFID tags in non-line-of-sight (NLoS) scenarios using both RSS and RSP methods [81, 82, 83, 84]. Ma *et al.* proposed a joint iterative phase reconstruction and weighted localization algorithm based on convex optimization achieving an average accuracy of 2.8997 m [81]. Simulation and experimental results in [83] and [84] by Kledoye *et al.* showed that a multidimensional scaling (MDS) based positioning technique with fixed nodes can provide an average error as low as 2.51 m for estimating NLoS tag locations. Yet, fundamental limitations in wireless localization and positioning techniques remain: cm-scale precision, particularly at the fringe of coverage for even short-range radios, is extremely difficult to achieve due to losses and multipath.

A novel class of long-range RFID tags utilizing the tunneling effect were proposed in [3, 1]. Experiments showed that, at 5.8 GHz, the backscattering properties of Tunneling RFID Tags provide much longer communication ranges than traditional RFID tags. Meanwhile, [19, 85] have proved that long-range positioning of tunneling tags is feasible through RSP-based techniques for indoor and outdoor scenarios in LoS. However, performances of the RSP-based method using tunneling tags in NLoS remain unexplored.

Obstacles and walls cause various electromagnetic effects that degrade the localization accuracy of RFID tags, especially with RSS-based techniques [56]. This work applies the RSP-based positioning technique introduced in [19] and [85] to through-obstruction and through-wall NLoS conditions and compares the results that can be obtained when using either a conventional Semi-passive Tag (SpT) or a Tunneling Tag (TT) operating at the 5.8 GHz band. The experimental results show that the phase-based localization of tunneling RFID tags can both maintain high Signal-to-Noise Ratio (SNR) in NLoS conditions and perform counterintuitively *better* in ranging than LoS operations (21.3 cm LoS vs 16.6 cm through-obstruction NLoS average error; 13.5 cm LoS vs 11.3 cm through-wall NLoS average error.).

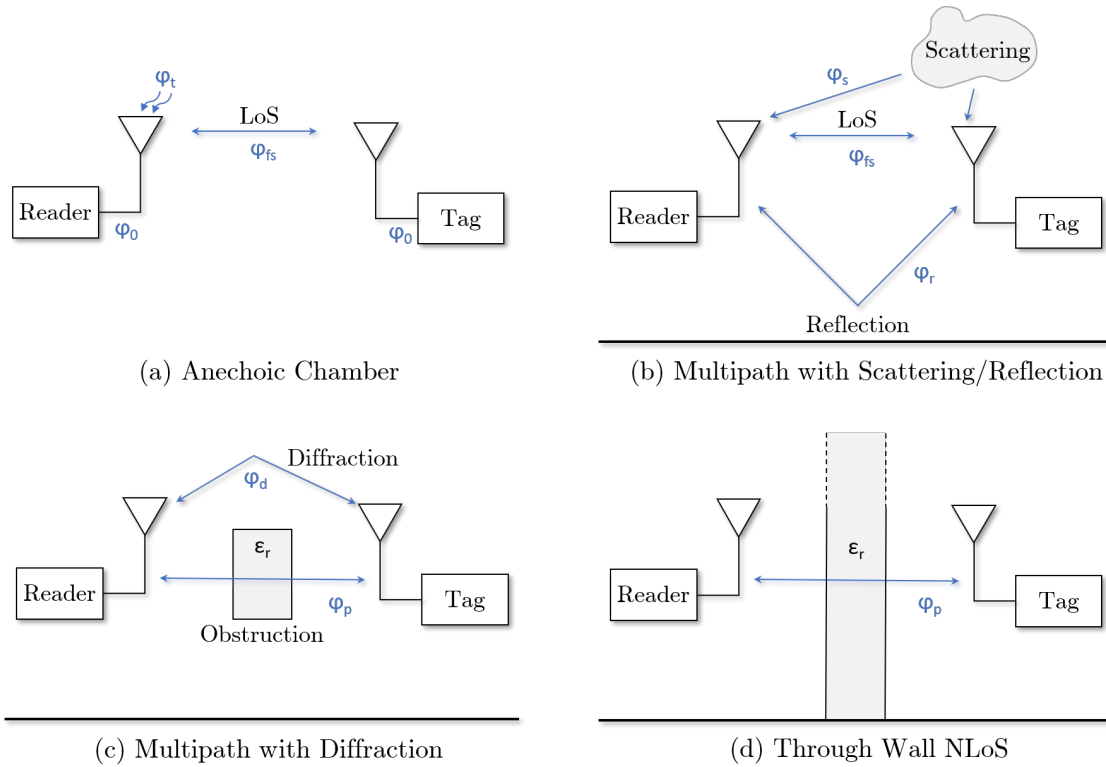


Figure 5.1: Schematic representations of RFID positioning system setups: (a) LoS in ideal case; (b) LoS with scattering and reflections; (c) diffraction due to an obstacle; and (d) propagation through a wall, or a floor.

## 5.2 Rationale

### 5.2.1 Backscatter Communication with Tunneling Tags

The reader described in [85] is used in this paper to study the phase and amplitude of a signal. The down-converted backscatter received signal is digitized and sampled by a Universal Software Radio Peripheral (USRP, model N200). A Geortzel filter is used to improve the signal-to-noise ratio of the received signal for accurate phase detection. The RSS and the RSP can be expressed as:

$$P_{RSS} = \frac{I_{rx}^2 + Q_{rx}^2}{Z_0}, \quad (5.1)$$

$$\varphi_{RSP} = \arctan\left(\frac{Q_{rx}}{I_{rx}}\right) \in [0, 2\pi), \quad (5.2)$$

where  $I_{rx}$  and  $Q_{rx}$  are the amplitudes of the in-phase ( $I$ ) and quadrature ( $Q$ ) channels of the received signal; and  $Z_0$  is the input impedance of the receiving antenna ( $50 \Omega$ ). The RSS received by the RFID reader can be expressed by the link budget equation of a backscattering system [17]:

$$P_r = P_T G_{tx} G_{rx} G_t^2 \left(\frac{\lambda}{4\pi d}\right)^4 M, \quad (5.3)$$

where  $M$  is the modulation factor given by  $M = \frac{1}{4} |\Gamma_1 - \Gamma_2|^2$ ,  $G_t$  is the gain of the tag, and  $G_{tx}$  and  $G_{rx}$  are transmitting and receiving antenna gains of a co-located bistatic reader, respectively. tunneling tags have shown their potential in extending the reading distance  $d$  between the reader and the tag [1] through the *tunneling effect*. In fact, a modulation factor  $M > 1$  can be achieved by a tunneling tag with very low biasing power ( $21.32 \mu\text{W}$  at  $80 \text{ mV}$  [3]), while the modulation factor for a semi-passive tag is always less than 1.

### 5.2.2 RSP-based Positioning in Real World

In an ideal environment, *e.g.*: the anechoic chamber, an RFID reader communicates directly with the tag at distance  $d$  in LoS without interacting with any other objects (Figure 5.1a).

The measured RSP consists then of three components:

$$\varphi_{RSP_{Ideal}}(f_c) = \varphi_{fs}(f_c) + \varphi_0(f_c) + \varphi_t, \quad (5.4)$$

where  $\varphi_{fs} = \frac{4\pi f_c d}{c} \bmod 2\pi$  is the wrapped phase shift due to the wave propagation in free space [20];  $\varphi_0$  is the phase offset caused by wave traveling within cables and other reader components, antennas, and tag modulation; and  $\varphi_t$  is the phase error caused by thermal noise and other random interference such as a person passing by. The dependency on the carrier frequency  $f_c$  is highlighted.

Nevertheless, readers and tags, although still in LoS, are usually placed near objects and obstacles that scatter and reflect electromagnetic waves creating multiple propagation paths (Figure 5.1b). Already in these cases, the  $P_{RSS}$  is unpredictable due to, among others, nonuniform antenna gains at different directions, antenna polarization mismatch, and small scale fading, while the RSP has the following components:

$$\varphi_{RSP_{LOS}}(f_c) = \varphi_{RSP_{Ideal}}(f_c) + \varphi_m(f_c), \quad (5.5)$$

where  $\varphi_m = \varphi_s + \varphi_r$  is the phase offset caused by the multipath channel, including reflection and scattering.

In some other multipath scenarios, the direct path is partially or completely blocked by an obstacle (Figure 5.1c) or a wall (Figure 5.1d). When waves travel within a dielectric material, the phase shift increases due to shorter wave length within the material itself. Moreover, when the materials are unknown, it becomes harder to predict and calibrate the RSS. In NLoS conditions, therefore, knowing the amount of the additional phase shift



added to  $\varphi_{RSP_{LoS}}$  can help in modeling the relationship between  $\varphi_{RSP_{NLoS}}$  and distances:

$$\varphi_{RSP_{NLoS}}(f_c) = \varphi_{RSP_{LoS}}(f_c) + \varphi_d(f_c) + \varphi_p(f_c), \quad (5.6)$$

where the additional phase offset components  $\varphi_d$  and  $\varphi_p$  are due to the diffraction and propagation within dielectric materials, respectively.

An RSP-based method can be used to estimate the distance  $\hat{d}$  between a reader and a tag [19, 85] using the measured RSP:

$$\begin{aligned} \hat{d} &= \frac{\lambda_e}{4\pi N} \sum_{n=1}^{N-1} (\varphi_{RSP_n}(f_n) - \varphi_{RSP_{n+1}}(f_{n+1})) \\ &= \frac{\lambda_e}{4\pi N} \sum_{n=1}^{N-1} \Delta\varphi_{RSP}(f_n), \end{aligned} \quad (5.7)$$

with  $\varphi_{RSP_n}$  and  $\varphi_{RSP_{n+1}}$  being the measured phases of the received signals obtained through (Equation 5.2) at the reader carrier frequencies  $f_n$  and  $f_{n+1}$ , respectively;  $N$  being the number of the frequency channels; and  $\lambda_e = \frac{c}{\Delta f}$  the equivalent wave length obtained when an uniform frequency step,  $\Delta f = f_{n+1} - f_n$ , is used. It is important to highlight that the maximum detection range  $\hat{d}_{max}$  of the phase-based method is determined by the minimum frequency step  $\Delta f$  of the reader:  $\hat{d}_{max} = \frac{c}{2\Delta f} = \frac{\lambda_e}{2}$ .

### 5.2.3 Measurement Offsets and Errors

To achieve good accuracy, it is usually necessary for most positioning techniques to identify the sources and characteristics of errors. According to (Equation 5.4) - (Equation 5.6), the measured phases contain both the phase shifts due to wave propagation in free-space between the reader and tag antennas and the phase offsets due to other factors. Reflections, scattering, diffraction, and propagation within dielectric materials cause higher phase-shifts. Therefore, when using (Equation 5.7) to measure distances, the estimation offsets,  $\epsilon$

*i.e.* errors, must be included:

$$\hat{d} = d \pm \epsilon, \quad (5.8)$$

where  $\hat{d}$  is the the estimated distance defined in (Equation 5.7);  $d$  is the ground truth between reader and tag. The distance estimation offset  $\epsilon$  has the following LoS and NLoS components due the corresponding phase offsets:

$$\epsilon = \epsilon_0 + \epsilon_m + \epsilon_t + \epsilon_d + \epsilon_p, \quad (5.9)$$

where  $\epsilon_0$ , related to the hardware setup and design, is the error brought by the phase delay of waves traveling within the RF cables and traces in the reader and tag and can be easily averaged out;  $\epsilon_m$  is the multipath error that does not significantly change if the environment stays the same; and  $\epsilon_t$  is due to thermal noise and other interference sources such as a person passing by. In NLoS scenarios, the additional components  $\epsilon_d$ , caused by the diffraction paths, is negligible when the distance is long and the obstacle is small. Although the presence of walls and big obstacles introduces an extra  $\epsilon_p$ , which is determined by the thickness of the wall, it also suppresses the amplitude of multipath reflection and scattering from broader angles, reducing  $\epsilon_m$ . The overall impact of NLoS due to a wall may be neutralized, which will be investigated in the following section. Table 5.1 summarizes the sources of the measured RSP offsets and the corresponding estimation errors.

Table 5.1: Summary of Error Sources

Source of RSP Offset	RSP Offset	Error
Internal propagation	$\varphi_0$	$\epsilon_0$
Scattering and Reflection	$\varphi_m = \varphi_s + \varphi_r$	$\epsilon_m$
Diffraction	$\varphi_d$	$\epsilon_d$
Penetrating Materials	$\varphi_p$	$\epsilon_p$
Thermal Noise	$\varphi_t$	$\epsilon_t$

By comparing the ground truth distance  $d$  with the estimated one  $\hat{d}$ , it is possible to define the percentage error as:

$$\epsilon_{\%} = \frac{\hat{d} - d}{d} \cdot 100\% \quad (5.10)$$

Although  $\epsilon_t$  is not always positive as a zero-mean Gaussian distributed random variable, it is possible to average out the phase errors due to the hardware,  $\epsilon_0$ , by using multiple frequency channels.

#### 5.2.4 System Calibration

Although the exact value of each error from various sources listed in Table 5.1 is unknown, it is not necessary to quantify it. In fact, by performing a calibration procedure, the offsets can be removed. A method of measuring RSP offsets caused by multipath has been introduced in [19, 85], however, this method is impracticable without laboratory equipment such as a Network Vector Analyzers and it only applies to the environment where the test is held. Fortunately, most of the errors in the RSP-based positioning system do not significantly vary in the same environment. Therefore, reference measurements are usually a simple and effective calibration method to estimate the overall estimation offset  $\epsilon$ . For a reference measurement at a chosen distance  $\bar{d}$ , the measured estimation offset  $\bar{\epsilon}$  at  $\bar{d}$  can be calculated through the estimated distance  $\hat{\bar{d}}$  using:

$$\bar{\epsilon} = \hat{\bar{d}} - \bar{d}. \quad (5.11)$$

Assuming the measurement errors are the same for any other measurement in the same environment, the system can be calibrated by subtracting  $\bar{\epsilon}$  from any other estimated distance  $\hat{d}$ ; therefore, the calibrated estimated distance ( $\hat{d}_{cal}$ ) can be written as:

$$\hat{d}_{cal} = \hat{d} - \bar{\epsilon}. \quad (5.12)$$

### 5.3 Experimental Setup

The RSP-based positioning method was validated in [19, 85] using a reader and tags in LoS, both in indoor and outdoor settings. This paper focuses on new experiments to validate the RSP-based method in NLoS conditions, including through-obstruction and through-wall experiments shown in Figure 5.1c and Figure 5.1d. Preliminary results of this work were presented in [86]. When there is an obstruction between the reader and a tag, errors due to diffraction  $\epsilon_p$  must be taken into account while they can be neglected in through-wall experiments.

Moreover, further temporary source of errors can appear in a real-world scenario that can occasionally make phase measurements inaccurate *e.g.*: interference caused by Wi-Fi access points; people moving in the hallway and nearby rooms. To avoid the impact of abnormally high and low phase shifts, upon reception, the measured differential phases are sorted from lowest to highest; the lowest 10% and highest 10%, are discarded and only the remaining data are used to estimate the distance  $\hat{d}$  (Equation 5.7).

#### 5.3.1 Through-obstruction NLoS Setup

Figure 5.2 shows the experimental setup for the through-obstruction tests, NLoS(o). The reader was placed at one end of the hallway, while the tag was moved from 5 m to 35 m away from the reader. Both semi-passive tags (SpTs) and tunneling tags (TTs) are used in the distance measurements for comparison. Figure 5.2b is a photo of the experimental setup, taken from the reader side. In NLoS tests, a cinder block is placed roughly 1 m away from the tag (as shown in Figure 5.2c) to investigate the diffraction effect on RSP-based method. The cinder block was placed in front of the tag and completely covered the reader from its view.

The reader operates from 5.725 GHz to 5.875 GHz with a dwell time of 200 ms and step frequency of 0.5 MHz. Two conventional patch antennas ( $G_{tx,rx} = 6$  dBi) are used for

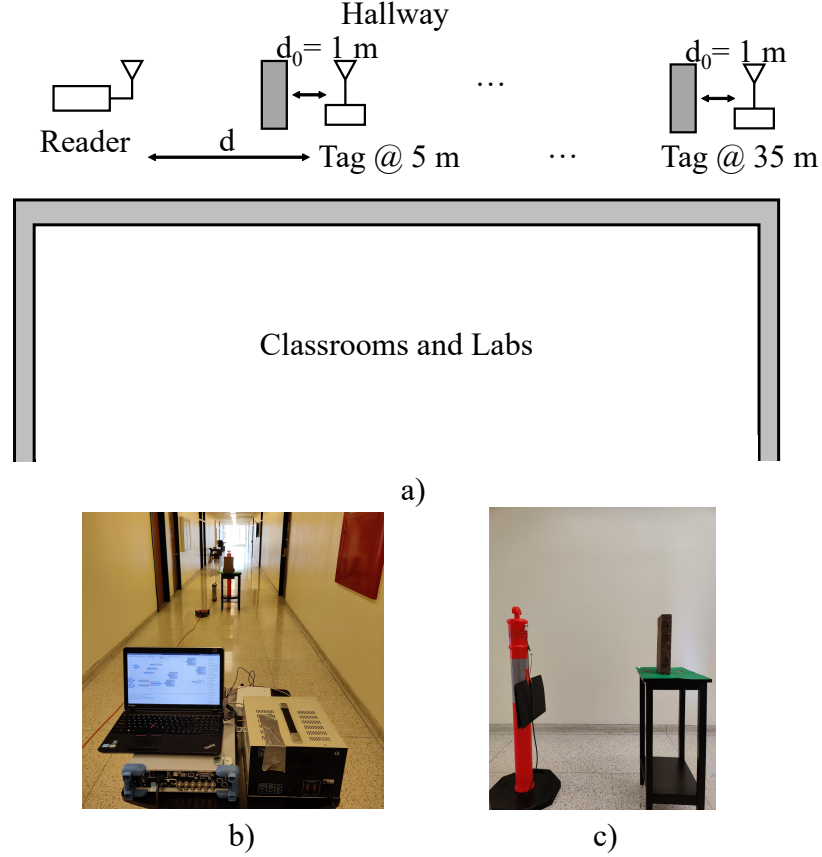


Figure 5.2: (a) The experimental setup seen from the above. (b) Photo of the setup with the tag at 5 m from the reader in LoS. (c) The cinder block in front of the tag for NLoS(o) conditions.

transmitting and receiving, while a patch array ( $G_t = 8$  dBi) is used by both the SpT and the TT. The transmit power  $P_T$  is 3 dBm for all measurements to avoid over-saturating the TT. The detailed reader setup is available in Appendix B. A summary of the experimental setup is listed in Table 5.2

### 5.3.2 Through-wall NLoS Setup

Figure 5.3a illustrates the experimental setup for the through-wall tests, NLoS(w). The reader was placed in a hallway at 1.75 meters away from a 15 cm-thick plaster wall (Figure 5.3b), while the tag was located inside an adjacent classroom (Figure 5.3c). The distance  $d$  between the tag and the reader was changed from 3 to 9 meters. LoS measurements, with both the reader and the tag inside the classroom (Figure 5.3d), were also performed

Table 5.2: Specifications of the Experimental Setups

$P_T$ (dBm)	3
$G_{tx,rx}$ (dBi)	6
$G_t$ (dBi)	8
$d$ (m)	[3:1:9] - NLoS(o) [5:5:35] - NLoS(w)
Calibrating distance $\bar{d}$ (m)	5 - NLoS(o) 3 - NLoS(w)
Freq. hopping (GHz)	5.725:5.875
Freq. step $\Delta f$ (MHz)	0.5
Channel dwell time (s)	0.2

for comparison with NLoS(w) results. A summary of the experimental setup is listed in Table 5.2.

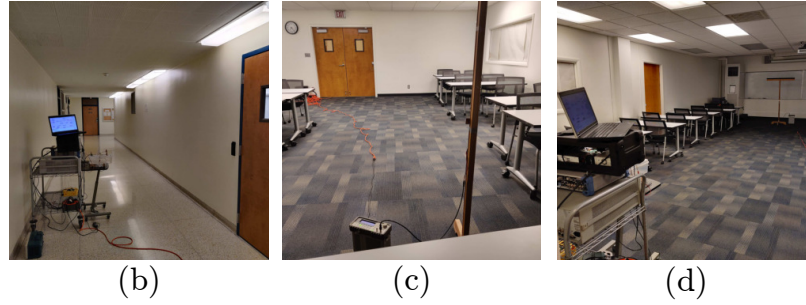
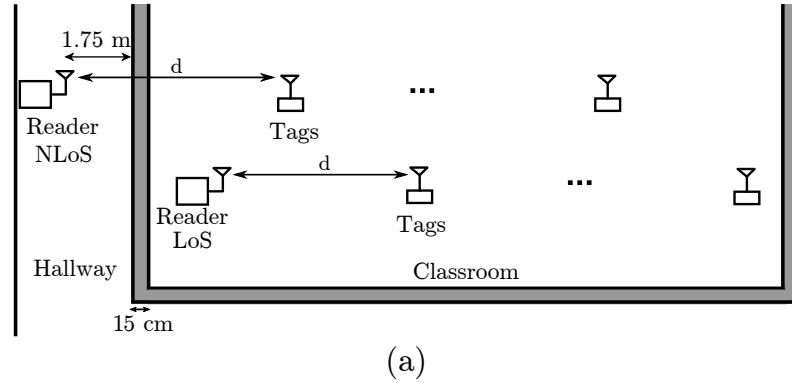


Figure 5.3: (a) Overview of the experimental setup in: (b)-(c) through-wall (NLoS(w)), and (d) LoS conditions.

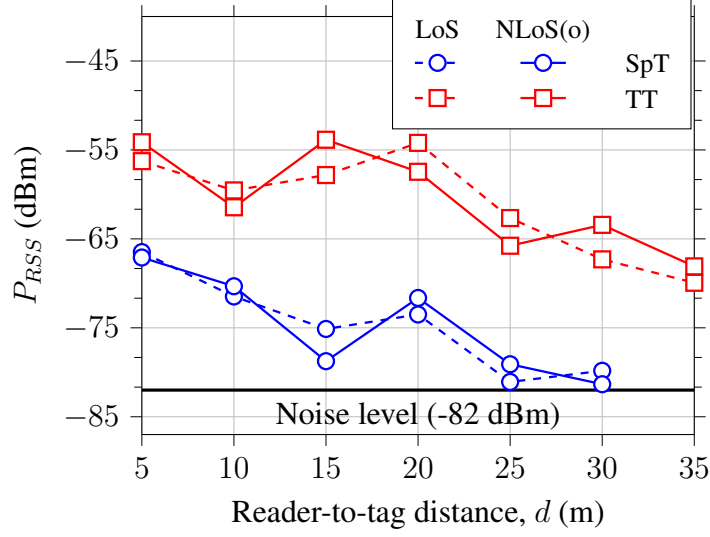


Figure 5.4:  $P_{RSS}$  values for semi-passive ( $\circ$ ) and tunneling tags ( $\square$ ) in LoS (dashed) and through-obstruction NLoS(o) (solid).

## 5.4 RSS in LoS and NLoS Conditions

### 5.4.1 Through-obstruction NLoS vs LoS

To properly estimate the phase from a tag, adequate RSS and SNR are required by an RFID reader. However, the RSS alone is not adequate for a precise estimation of the distance. Figure 5.4 shows the average received strength of all frequency channels for both tags in LoS and NLoS(o) conditions. The presence of the obstruction at 1 m away from the tag does not always reduce the RSS, due to diffraction. In LoS conditions, the RSS backscattered from the SpT drops below the noise level when the tag is placed at more than 30 m away from the reader, while the TT amplifies the RSS by 10 dB to 30 dB compared to using SpT, and tends to have higher gain when the impinging power is lower when the tag is placed further away from the reader.

With the presence of the cinder block, the diffraction around it changes the RSS by constructively or destructively interfering with the backscattered signal, which makes it more difficult to estimate the distance accurately using merely RSS. Therefore, a more accurate method is required for fine-scale indoor positioning systems in this scenario.

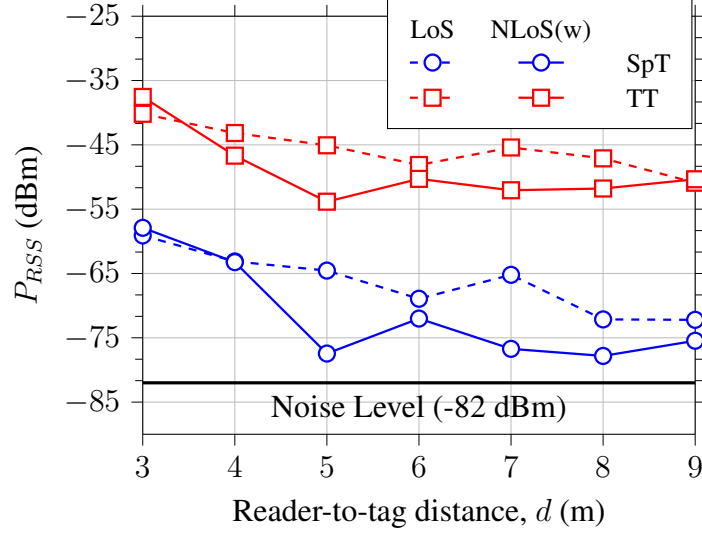


Figure 5.5:  $P_{RSS}$  values for semi-passive ( $\circ$ ) and tunneling tags ( $\square$ ) in LoS (dashed) and through-wall NLoS(w) (solid).

#### 5.4.2 Through-wall NLoS vs LoS

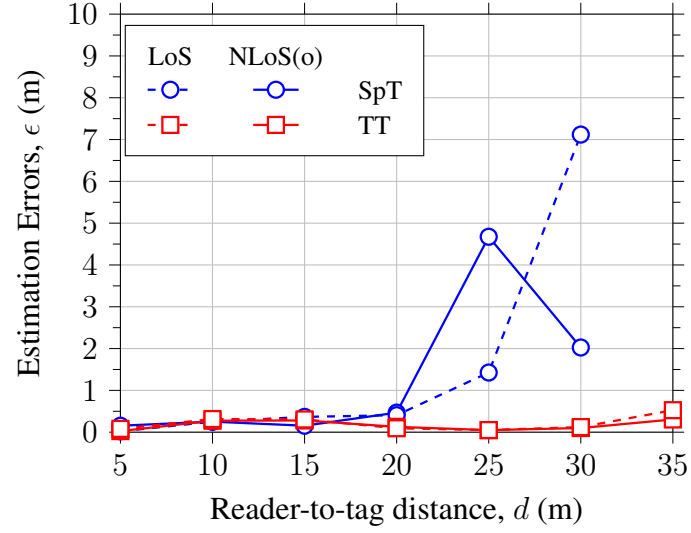
Figure 5.5 shows the RSS values obtained both in LoS and through-wall NLoS(w) from the SpT and the TT. In LoS conditions, the RSS from the TT is amplified from 18.9 dB to 25.0 dB depending on the impinging power on the tag. Moreover, its gain increases when it is further away from the reader due to the nature of tunneling diodes [3]. In through-wall NLoS conditions, a gain of 19.6 dB to 25.1 dB is observed when using the TT.

The round-trip attenuation due to the presence of the wall can be defined as:  $\Delta P_{loss} = P_{RSS_{LOS}} - P_{RSS_{NLoS}}$ . The measured RSS is affected by both blockage and multipath (*e.g.*: reflection from the wall, ground, and metal poles inside the wall), therefore the NLoS RSS is not always lower than the LoS RSS as it can be observed in the measurement at 3 m shown in Figure 5.5.

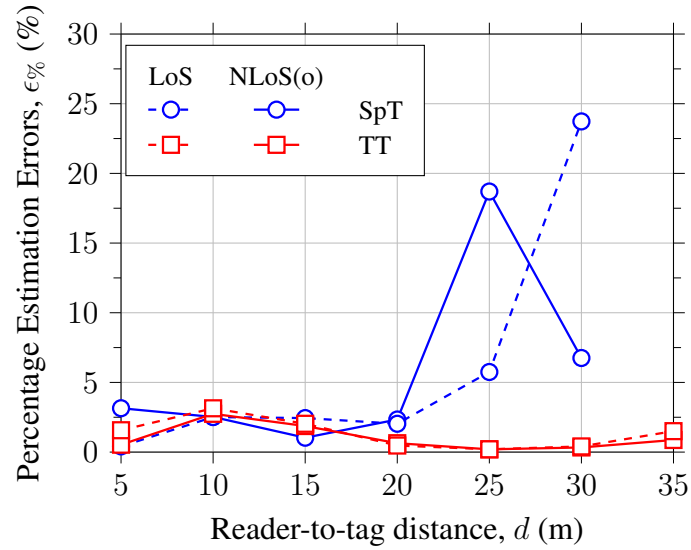
Overall, the wall introduces an average attenuation of 2.52 dB and 5.05 dB in one-way and round-trip links, respectively. Assisted by the tunneling effect, instead, the attenuation with a TT is reduced to 1.62 dB and 3.23 dB in one-way and round-trip links, respectively. The experimental results also confirm that, at longer distances, the gain of the TT significantly reduces the path losses. To jeopardize the backscatter communication between a TT



and a reader, at least 6-7 plaster walls are required. Due to the metal bars in the plaster wall and multipath such as ground reflections, the calculation of attenuation brought by the plaster wall is not very accurate, however, the TT could at least communicate through multiple walls before becoming undetectable [87].



(a)



(b)

Figure 5.6: Calibrated estimation errors in (a) meters, and (b) percent for LoS (dashed) and NLoS(o) (solid) conditions for the Semi-passive and tunneling tags.

## 5.5 Ranging Accuracy in NLoS

To investigate the positioning performance of RSP-based method in LoS and NLoS scenarios for both tags, the reader-to-tag distance are estimated by using the RSP-based method described in subsection 5.2.2. To reduce the thermal noise, data received over a 10 ms time frame were recorded for each frequency channel (total dwell time in each channel is 200 ms) to calculate  $\varphi_{RSP_n(f_n)}$  and  $\Delta\varphi_{RSP(f_n)}$  in (Equation 5.7). Since the estimated RSP is not always accurate due to multipath, 10% of the lowest and highest RSP shifts were discarded and not used to calculate the average RSP shift.

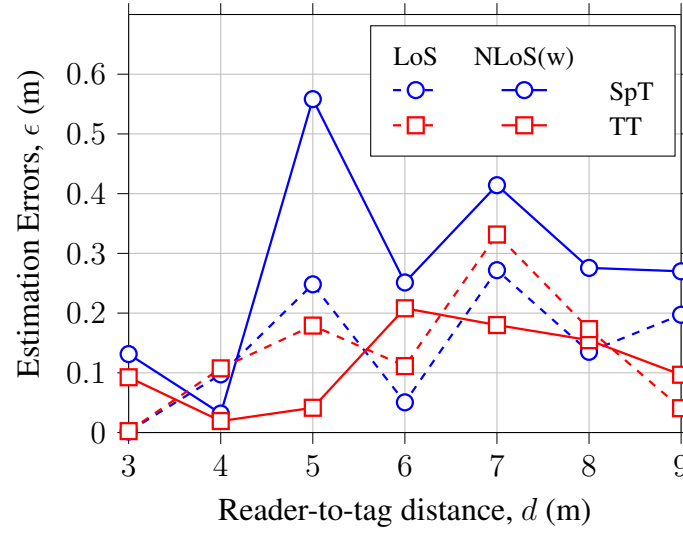
### 5.5.1 Ranging accuracy for Through-obstruction NLoS

The distance estimates are calibrated by using a reference measurement at a chosen distance  $\bar{d}$ , as discussed in subsection 5.2.3. In this paper,  $\bar{d} = 5$  m in LoS was chosen as reference and the offset  $\bar{\epsilon}$  was calculated using (Equation 5.11) to calibrate out the other data points. Figure 5.6 summarizes calibrated estimation errors both in meters ( $\epsilon$ ) and percentage ( $\epsilon\%$ ), for both tags in LoS and NLoS(o) conditions, by using (Equation 5.8) and (Equation 5.10), respectively.

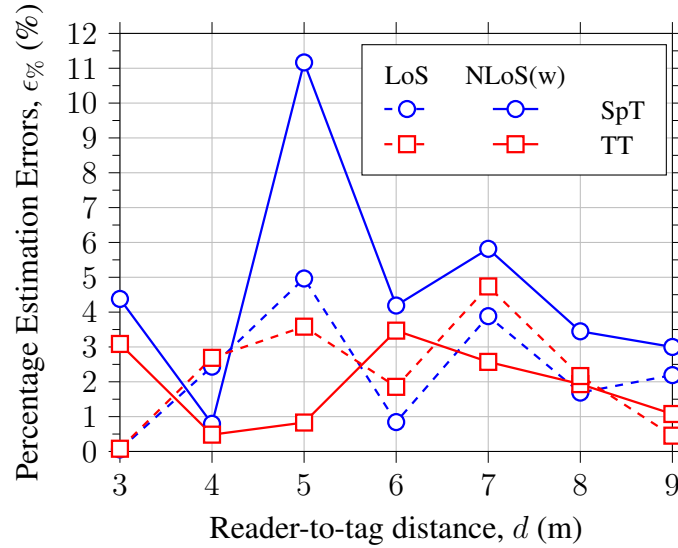
As it is shown in Figure 5.6, when the SpT and TT are placed at 20 m or closer from the reader, the estimation error is below 4% in both LoS and NLoS(o) conditions; however, the estimated distance for the SpT at 25 m and above has a much higher error due the insufficient SNR. The highest error observed when using SpT is above 7.88 m (26.3%) when the tag is placed at 35 m from the reader. On the other hand, when locating the TT, the percentage estimation errors remain under 3.14% over all distances resulting from the amplification brought by the reflection amplifier [1] of the TT. Estimation errors  $\epsilon$  as low as 4.46 cm ( $\epsilon\% = 0.18\%$ ) and 4.96 cm ( $\epsilon\% = 0.20\%$ ) are observed when the TT is placed at 20 m from the reader both in LoS and NLoS(o) scenarios, respectively.

The average errors  $\epsilon_{av}$  and average percentage errors  $\epsilon\%_{av}$  are summarized in Table 5.3.

By using the TT, the average distance estimation error is significantly reduced from 1.60 m (6.14%) to 0.213 cm (1.33%) and from 1.289 m (5.75%) to 0.166 m (1.02%), in LoS and NLoS(o), respectively. The added estimation error due to the diffraction is not significant especially at long distances, where the noise and multipath contribute more to the errors. The results show that fine-scale ranging is feasible in both LoS and through-obstruction scenarios using the RSP-based method proposed in subsection 5.2.2.



(a)



(b)

Figure 5.7: Calibrated estimation errors in (a) meters, and (b) percent for LoS (dashed) and NLoS(w) (solid) conditions for the semi-passive and tunneling tags.

Table 5.3: Average distance estimation error for Semi-passive and tunneling tags in LoS and NLoS(o) scenarios.

	$\epsilon$ (m)		$\epsilon_{\%}$ (%)	
	SpT	TT	SpT	TT
LoS	1.600	0.213	6.14	1.33
NLoS(o)	1.289	0.166	5.75	1.02

### 5.5.2 Ranging accuracy for Through-Wall NLoS

Accurate distance estimation in through-wall NLoS conditions is feasible using the RSP-based method. The same RSP-based technique and reference-based calibration method used previously in NLoS(o) are applied in this demonstration. The measured reader-to-tag distance at 3 m in the classroom is used as reference to calibrate out the measurement offset  $\bar{\epsilon}$  using (Equation 5.11) for the other data points.

Figure 5.7 shows the calibrated estimation errors for both tags in LoS and NLoS(w) scenarios, by using (Equation 5.8) and (Equation 5.10), respectively. In LoS, the estimation error is relatively low for both SpT and TT. However, when locating the SpT through a wall, the RSS and SNR are dramatically reduced by 5 dB on average, causing the increase of estimation errors. When measuring the reader-to-tag distance for SpT in NLoS(w), the estimation error can be as high as 55.8 cm (11.2%), when the tag is placed at 5 m, where the highest attenuation is observed. In contrast, when locating the TT, the estimation errors remain under 33 cm (4.7%) over all distances due to the higher SNR brought by the reflection amplifier [1] of the TT (the major source of error is multipath reflections and scattering). An estimation error  $\epsilon$  of 4.1 cm ( $\epsilon_{\%} = 0.45\%$ ) and 9.6 cm ( $\epsilon_{\%} = 1.07\%$ ) are observed when the TT is placed at 9 m from the reader in LoS and NLoS(w) conditions, respectively.

The average errors  $\epsilon_{av}$  and average percentage errors  $\epsilon_{\%av}$  are summarized in Table 5.4. By using the TT, the total average distance estimation error is significantly reduced from

14.3 cm (2.3%) to 13.5 cm (2.2%) and from 27.6 cm (4.7%) to 11.3 cm (1.9%), in LoS and NLoS(w), respectively. When locating the SpT in NLoS(w), the error is increased due to the reduced SNR, while the accuracy for the TT is not affected by the presence of the wall. This observation also validates the hypothesis that the wall compensates the additional equivalent travel distance by suppressing the multipath.

Table 5.4: Average distance estimation error for Semi-passive and tunneling tags in LoS and through-wall NLoS(w) scenarios.

	$\epsilon$ (m)		$\epsilon_{\%}$ (%)	
	SpT	TT	SpT	TT
LoS	0.143	0.135	2.3	2.2
NLoS(w)	0.276	0.113	4.7	1.9

## 5.6 Dwell-time vs Accuracy

A real-time positioning system demands an accurate estimation and a short processing time. Though the measurements used a long dwell time of 200 ms for each frequency, 10 ms of the acquired data in each frequency were used to estimate the distance between the reader and the tag. This approach allows us to investigate the impact of dwell time on the distance estimation accuracy using the estimation error statistics.

In Section section 5.5, 10 ms of data sampled during the dwell time in each channel was used to measure the RSP and RSS (*slow hopping mode*). To study the impact of dwell time on ranging accuracy, the same estimation algorithm was used on only 2 ms of data (*fast hopping mode*) for both the LoS and NLoS scenarios. The empirical CDF of the estimation errors for both the slow and fast hopping modes are shown in Figure 5.8 and Figure 5.9 for SpT and TT in through-obstruction and through-wall tests (NLoS(o), NLoS(w)) and compared with LoS tests.

For the experiment in the hallway, the estimation error with the SpT at 25 m and above is high due to insufficient SNR and missing channels, as shown in Fig Figure 5.6. Therefore,

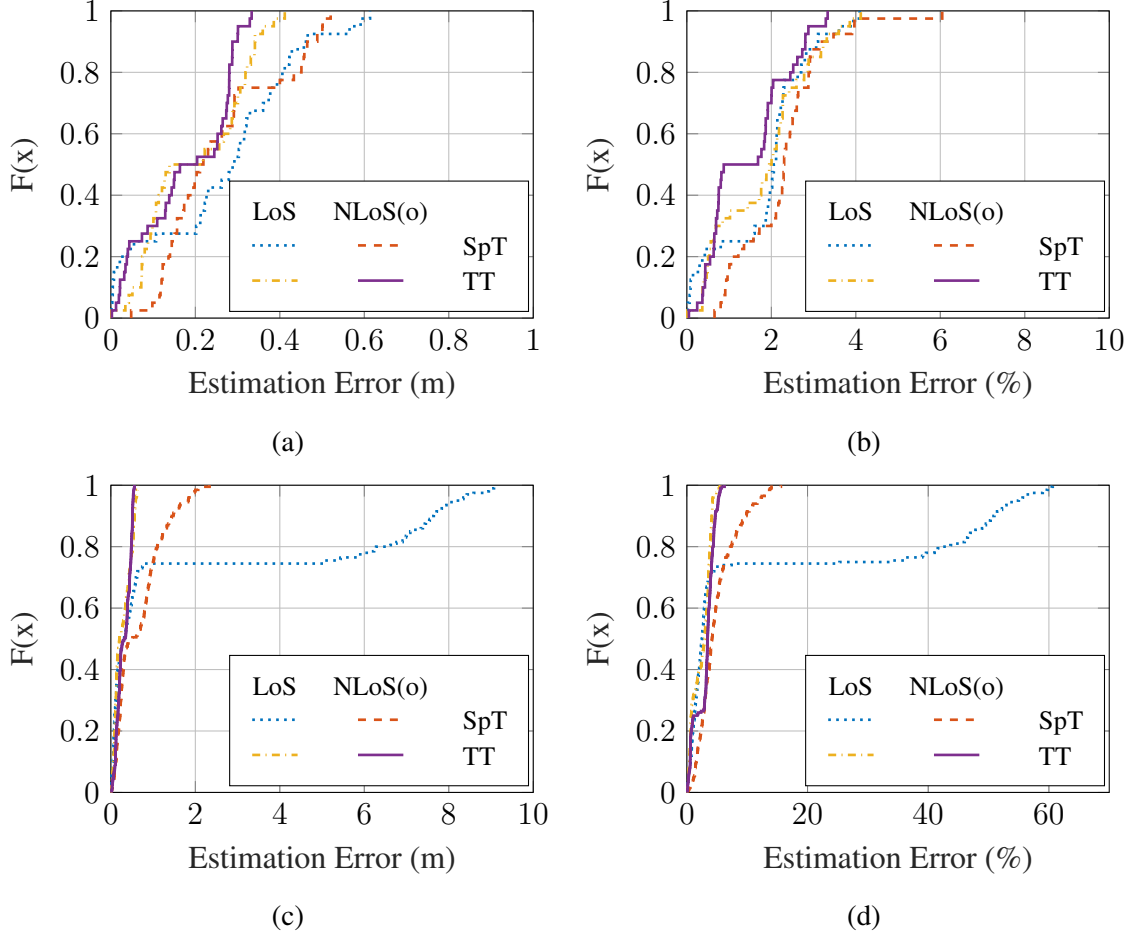


Figure 5.8: Calibrated estimation errors in percentage (left), and meters (right) in LoS and NLoS(o) conditions for the semi-passive and tunneling tags when using a slow hopping mode (top) or a fast hopping mode (bottom). The x-axis represents the estimation error in either meter or percentage, while the y-axis represents the CDF probability of the estimation error.

only estimation error for measurements under 20 m are used to plot the error distribution in Figure 5.9. When using *slow hopping mode*, although the TT outperforms the SpT in the estimation errors (absolute and percentage), both tags show good estimation accuracy with an estimation error of less than 0.5 m (3%) in 90% of the cases. When using *fast hopping mode*, the localization of the SpT starts to suffer from increased estimation error due to its low SNR and higher thermal noise when located at 15 m. This results in a high estimation error caused by thermal noise when the RSS is low, as Figure 5.8d and Figure 5.8c show. However, the thermal noise plays a less significant role when locating the TT due to the

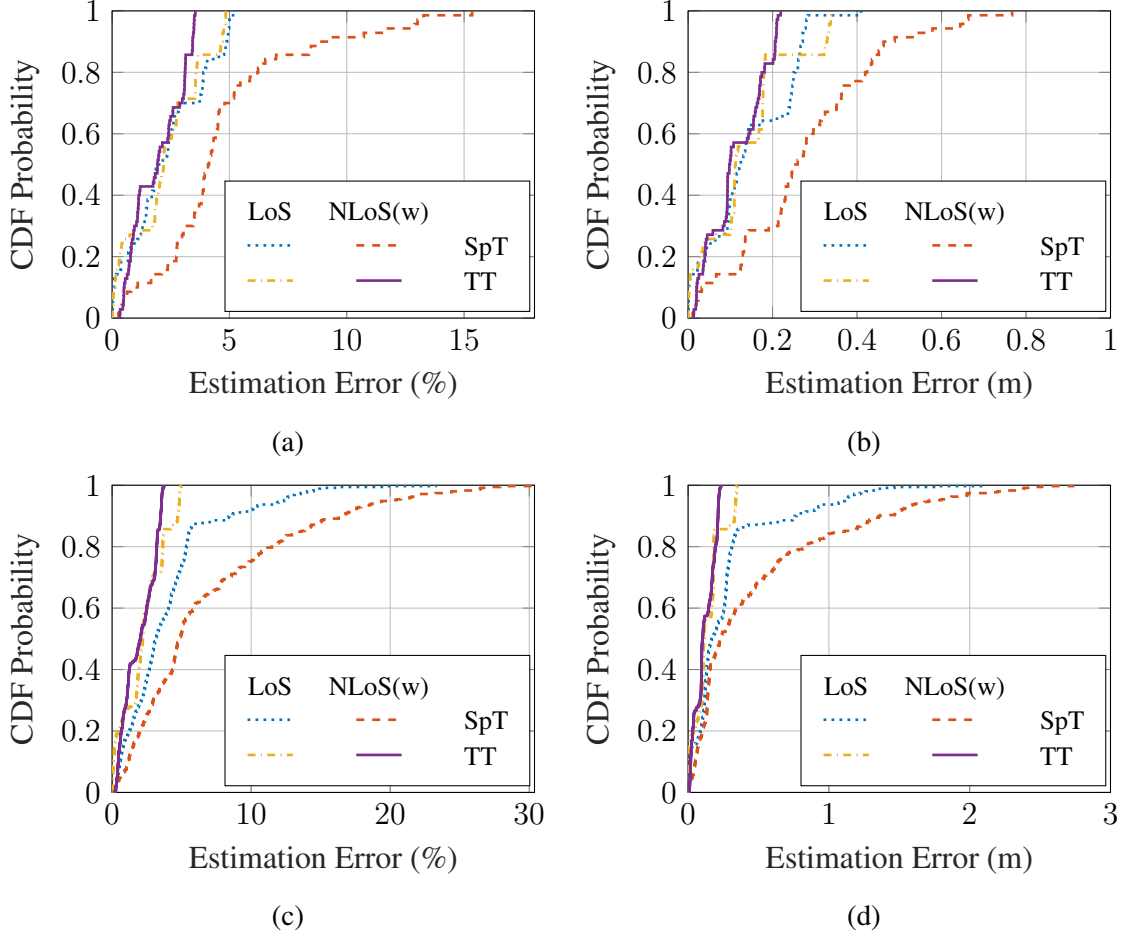


Figure 5.9: Calibrated estimation errors in percentage (left), and meters (right) in LoS and NLoS(w) conditions for the semi-passive and tunneling tags when using a slow hopping mode (top) or a fast hopping mode (bottom). The x-axis represents the estimation error in either meter or percentage, while the y-axis represents the CDF probability of the estimation error.

amplification. The TT maintains less than 5% estimation error when using *fast hopping mode* in both LoS and through-obstruction NLoS(o) conditions.

As shown in Figure 5.9, reducing the dwell time does not have significant impact on the error distribution of TT in both LoS and through-wall NLoS(w). However, similarly with the through-obstruction measurements, the error dramatically increases in both LoS and NLoS(w) with the SpT because of a low SNR. By using the TT, a fast and accurate positioning system is possible with RSP-based ranging technique in both LoS, through-obstruction, and through-wall NLoS conditions.

## 5.7 Conclusions

In this paper, the RSP-based positioning technique proposed in [19] was investigated in indoor LoS and NLoS environments. The sources of errors in various scenarios and their impacts were discussed and validated. It has been verified that, with appropriate calibration, accurate localization is possible even through a wall and a cinder block. The RSP-based positioning technique allows reader-to-tag distance estimation for a tunneling tag with a total average error of 1.02% and 1.9%, over a range of 5-35 m in through-obstruction NLoS, and 3-9 m in through-wall NLoS, respectively. A conventional semi-passive tag was also tested and correctly localized, however, total average errors of 5.75% and 4.7% were observed, over a range of 5-35 m in through-obstruction NLoS, and 3-9 m in through-wall NLoS, respectively. Compared to the semi-passive tag, the tunneling tag provides both longer communication range and better estimation accuracy in both LoS and various NLoS environments.



## CHAPTER 6

### A REAL-TIME RFID POSITIONING SYSTEM USING TUNNELING TAGS

This chapter proposes a new type of real-time decimeter-level RFID positioning system at 5.8 GHz. The system uses received signal phase (RSP)-based positioning techniques and Tunneling Tags (TTs). TTs amplify the signal strength of their backscattered signals while preserving the phases allowing for ultra-precise position estimates at long distances. A proof-of-concept RSP-based real-time frequency hopping reader is implemented on SDR and USRP platform. Experimental results show an average one-dimensional and two-dimensional positioning accuracy of 11 cm and 17 cm, respectively, in outdoor environments.

#### 6.1 Introduction

Identifying the real-time position of both objects and people without a clear LoS is another key feature for versatile sensing applications. Preliminary measurements in the previous chapters have also shown that, by using RSP-based method, tunneling RFID ranging systems can produce a one-dimensional distance estimation with an average error of less than 1% at ranges of 35 m in line-of-sight (LoS) scenarios [85], and 1.4% in non-line-of-sight (NLoS) indoor scenarios [86] when operating at microwave frequencies (5.8 GHz). Experiments have demonstrated how ultra-low-power tunneling tags can reflect their signatures and can be detected at ranges of 1 km [3]. However, a two-dimensional tunneling RFID positioning system using RSP-based method is yet to be demonstrated.

In this chapter, we propose a frequency hopping RFID system operating at 5.8 GHz ISM Band that provides position estimations for tunneling RFID tags with decimeter-level accuracy. This localization technology applies RSP-based positioning [85] to a TT [1]. The TT exploits the Esaki tunneling diode [88] to amplify a backscattered signal and to

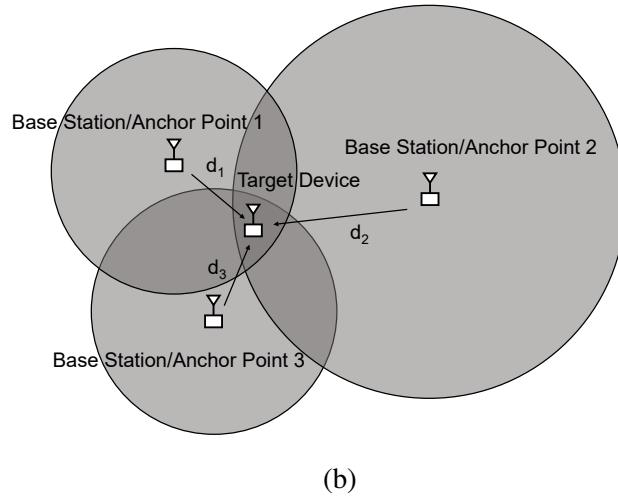
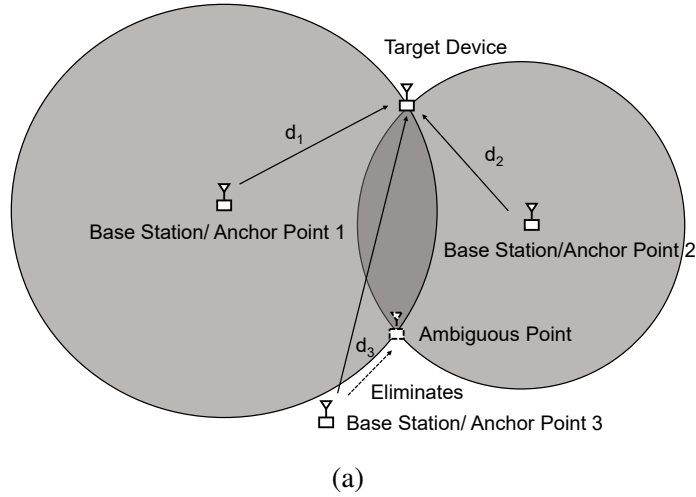


Figure 6.1: In the trilateration approach the location is estimated by intersecting three or more circles that identify the distance of an object from a target. The distance is here computed through the received signal phase.

accurately estimate the position and/or orientation of an RFID tag at long distances while preserving the linear relationship between the reader-to-tag distance and the RSP.

## 6.2 Rationale

### 6.2.1 2D Localization with RSP-based Ranging Method

An RSP-based *ranging system* [86] can be extended to two- and three-dimensions *positioning systems* by using multiple and appropriate frequency hopping readers and tags. By measuring the distances of a tag from three (or four) readers at known locations, its 2D (or

3D) position can be extrapolated using a trilateration approach.

Trilateration is widely used in many well-known real-time positioning systems (*e.g.*: GPS). Once the distance  $\hat{d}$  between a reader and a tag is computed through (Equation 1.3), the tag may be located on a circumference of radius  $\hat{d}$ . To estimate the actual 2D location of the tag, the intersection of at list two circumferences is required, hence the need of at least two readers receiving backscattered data from the same tag. Nonetheless, as shown in Figure 6.1a, the position is still not precise since the tag can be on either of the two intersection points or, in case of estimation errors, anywhere within the area of intersection. One way to eliminate the ambiguous point is adding a third reader (Figure 6.1b). Directional or Van Atta antennas [89] [47] would further increase the position accuracy. In this chapter, the ambiguous point was eliminated by using the directivity of the antennas. The target location was estimated using the spatial average of the three remained intersection points.

Two different use cases are possible with the RSP-based method, depending on whether the reader or the tag is the object being localized. Two configurations can, therefore, be identified: *i) conventional configuration*, when a tag is moving and three or more readers are fixed; and *ii) reverse configuration*, when a reader is moving and three (or more) fixed tags act as anchor points. In this chapter, the positioning system is demonstrated with a mobile reader and multiple custom-made tags (*reversed configuration*); the reader will move both along a straight line and across space for 2D positioning.

### 6.2.2 Real-time Software Defined Radio-based Reader Design

Since the use of microwave frequencies (*e.g.*: the 5.8 GHz ISM band) is still uncommon in the RFID industry, a custom measurement system is necessary to make a real-time frequency hopping coherent reader that extracts the RSP from a received signal, processes the data, and presents the calculated position on a graphical user interface (GUI) in real-time. A Software Defined Radio (SDR)-based reader was realized for this purpose.

Figure 6.2 shows the design architecture of the reader used for 2D real-time position-

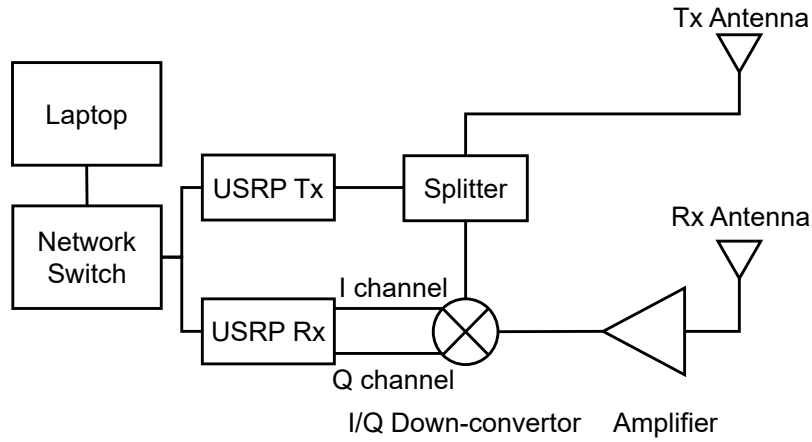


Figure 6.2: Block diagram of the 5.8 GHz frequency hopping reader. The reader was placed on a mobile cart.

ing at 5.8 GHz band. Two Software Defined Radio (USRP) devices (USRP N200 from Ettus Research[90]), are used to transmit the unmodulated carrier frequencies  $f_c$  at the 5.8 GHz ISM band. The output of the transmitter is split to coherently down-convert the I/Q components of the received signals. The I and Q components, in base-band, are then sampled for post-processing. A laptop, connected to the USRPs via network switches, uses GNU-radio [91] to let the user control the system via a GUI, to implement a frequency hopping function, and to process base-band I/Q signals. Table 6.1 lists the specifications of the reader. Although it can use any type of receiving and transmitting antennas, a high isolation between the receiving and the transmitting front-ends is required to achieve good sensitivity, therefore, a co-located bi-static reader configuration is recommended. The frequency bandwidth was chosen to be 101 MHz with 101 evenly distributed channels ( $\Delta f = 1$  MHz).

### 6.2.3 SDR Implementation

To collect multiple data in real time from different tags and to do trilateration, a Frequency Division Multiple Access (FDMA) method can be used. Figure 6.3a shows, through a GNU Radio block diagram, how the FDMA method is used in *reverse configuration* (three

Table 6.1: Specifications of the reader setup for outdoor 2D positioning

$P_T$ (dBm)	7
$G_{tx}$ (dBi)	7.5
$G_{rx}$ (dBi)	7.5
Freq. hopping (GHz)	5.725:5.825
Freq. step $\Delta f$ (MHz)	1
Dwell Time (ms)	50
Total Estimation Time (s)	5

fixed tags) to detect the real time position of a moving reader. Three tunneling tags were loaded with a square wave at 500 KHz, 600 KHz, and 700 KHz, respectively. The receiving section collects the three different frequencies backscattered by each tag and discerns them through Goertzel filters [92, 93] with pre-set center frequencies, which act as a single point FFT filter with very narrow bandwidth. The filters extract the RSP from each tag and, when enough data are collected, the position of the moving reader is measured and displayed on the GUI in real-time. Copies of the received raw data output are also saved locally for post processing. The transmitting section, instead, implements the frequency hopping controller that lets the reader to always interrogate the tags at different frequencies.

Figure 6.3b shows the diagram for implementing the real-time frequency hopping in GNU radio. The reader starts by transmitting an unmodulated continuous wave at 5.785 GHz to collect the RSP data from each tag. It dwells on the same frequency channel for 50 ms until it receives 500 samples of backscattered data that are used for extracting an averaged RSP value. After collecting the required samples, the transmit frequency is set to the next adjacent channel ( $\Delta f = 1$  MHz); the process is repeated for 101 different frequency channels after which the reader can calculate its position in space and display it on the graphical user interface. The transmit frequency is then reset to 5.725 GHz and the positioning measure restarts. Each acquired data are also saved on the local hard drive to draw statistical analysis and for post-processing.

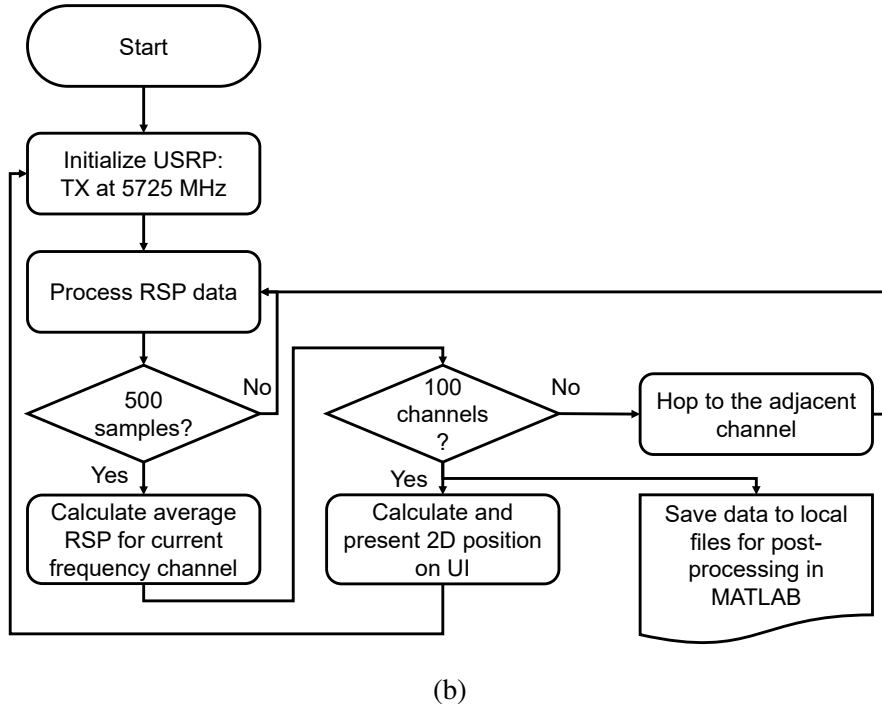
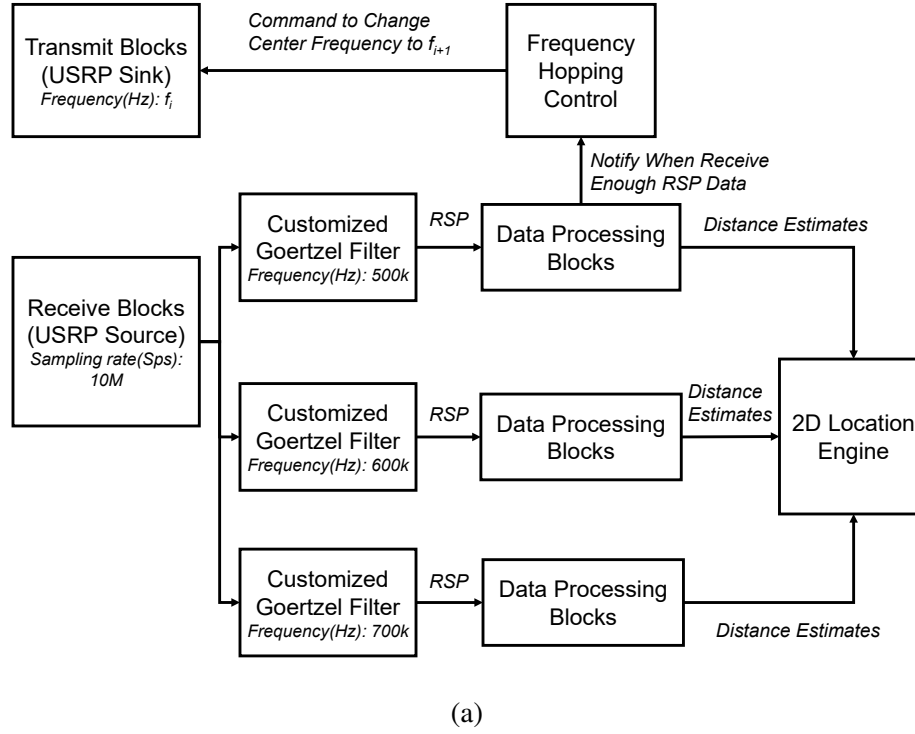


Figure 6.3: (a) GNU radio implementation and (b) logic flow diagram for data processing and frequency hopping in the real-time 2D positioning system.

## 6.3 Measurements

### 6.3.1 Experimental Setup

Figure 6.4a and Figure 6.4b show the experimental setups used to test the real-time positioning system with three fixed tags and a mobile reader (*reverse configuration*). Three tunneling tags are placed at known locations and serve as anchor points; a moving reader measures its real-time distance from each tag and its 2D location is calculated with trilateration. The tunneling tags are biased and modulated with a continuous square wave at different modulating frequencies  $f_m$ . The reader is moved around an area of  $2.15 \times 2.15 \text{ m}^2$ , while transmitting a frequency hopping continuous wave at 7 dBm towards tunneling tags located at 6 m to 8 m away from it.

The tag antennas are placed at 1.5 m away from the ground, while the reader antenna is at 1.0 m. The tags use the same circuit design shown in [85]. The tunneling diodes are biased with a waveform generator of square waves at various frequencies (500 KHz, 600 KHz, and 700 KHz). The minimum voltage is set to 0 while the maximum voltage varies between 115 mV to 137 mV for each tag to have the optimized backscattering gain. The maximum drawn current varies from 0.35 mA to 0.53 mA for a total biasing power ranging between 21.5  $\mu W$  and 30.5  $\mu W$ .

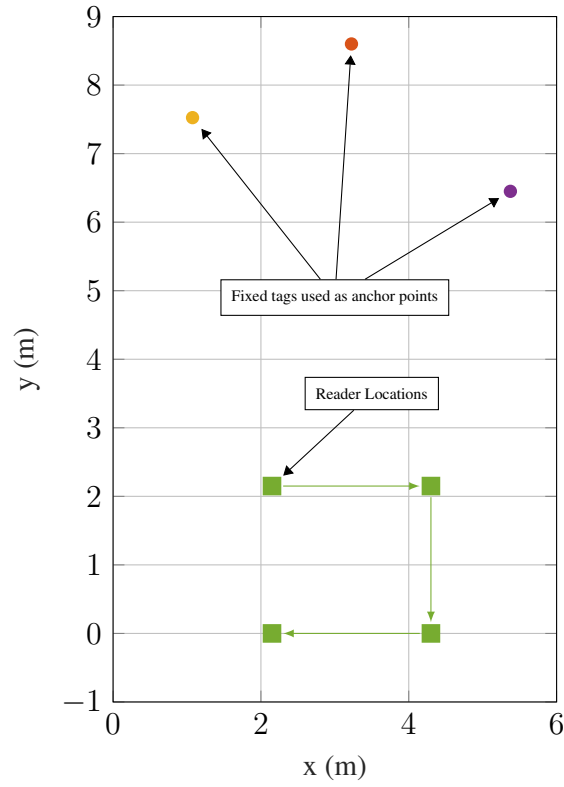
Figure 6.4b illustrates the real-time locations of the moving reader. 10 measurements from each tag are taken at each position before moving to the next one to collect statistics about precision and accuracy of the real-time positioning system. While the reader continuously transmits and estimates its 2D location in real-time, it also records the RSP data for post-processing in MATLAB.

### 6.3.2 Experimental Results

Following the procedures, the reader-to-tag distances are estimated for each reader location. To achieve accurate positioning, proper calibration is required due to the measure-



(a)



(b)

Figure 6.4: (a) Experimental setup for the real-time RFID positioning system with three fixed tags and a mobile reader. (b) Fixed positions of the tags (used as anchor points) ( $\circ$ ) and actual positions of the moving reader ( $\square$ ).



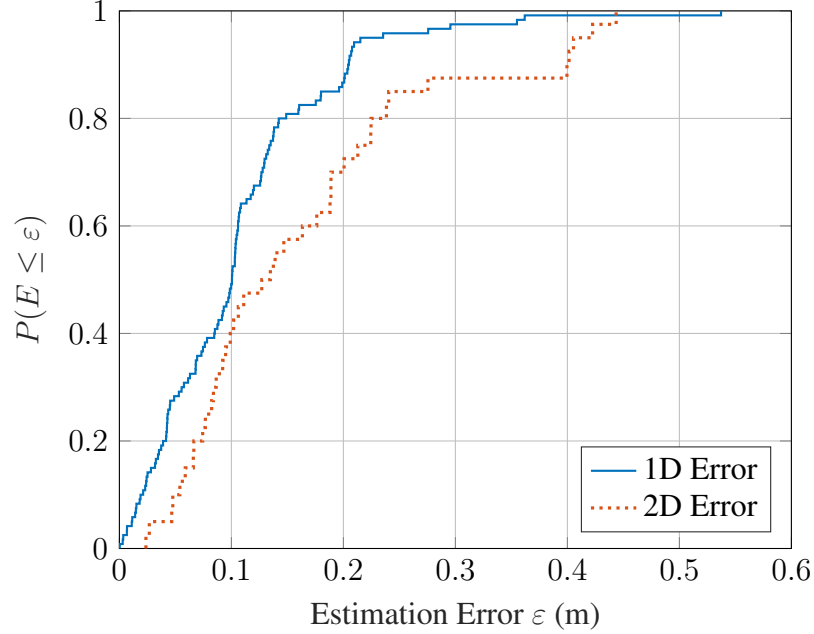


Figure 6.5: Empirical CDF of distance errors  $\epsilon$  for RSP-based methods with calibration, including 120 data points for the reader-to-tag distance estimation error (1D error) CDF and 40 data points for the position estimation error (2D error) CDF.

ment offset caused by internal wave traveling within the RF cables, transmission lines, matching networks, *etc.* Since the same reader is used for all measurements, the offset can be calibrated out by reference measurements. Each tunneling tag performs differently and requires unique impedance matching and separate calibrations due to their manufacture imperfections. Nonetheless, once the offset is measured for a reader and tag pair, the offset does not require re-calibration. In practice, the pre-calibration for a new reader and new tag needs to be done only once using the reference readers and tags. By placing the reader at a known location, the estimated distance  $\hat{d}$  can be used to determine the value of the offset  $d_o$ :

$$d_o = d - \hat{d}, \quad (6.1)$$

where  $d$  is true reader-to-tag distance. Nevertheless, estimation errors caused by time-varying factors (*e.g.*: tag movements due to the windy weather, changing multipath caused by people moving around the reader, *etc.*) also exist, which cannot be calibrated out by

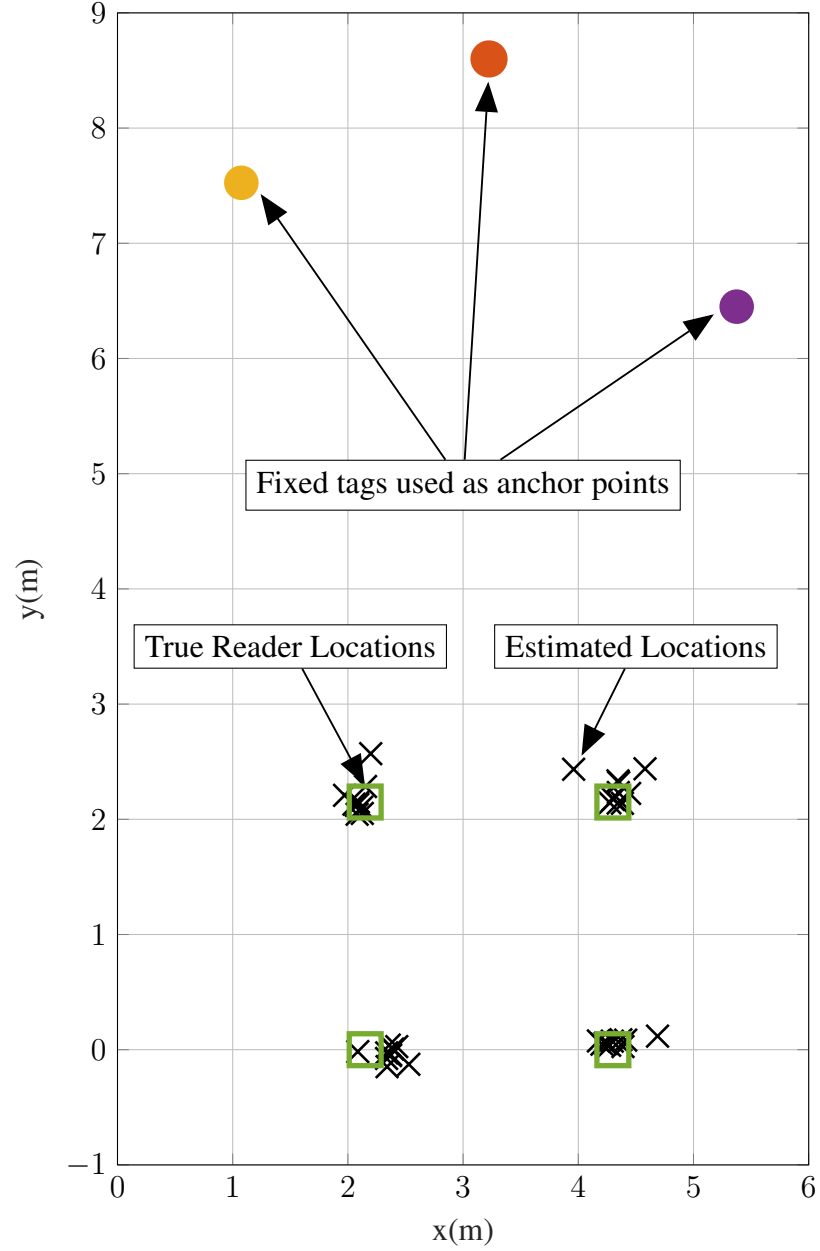


Figure 6.6: Location estimates vs true reader locations for the 2D positioning system having three fixed tags and a moving reader. Fixed positions of the tags (used as anchor points) ( $\times$ ); actual positions of the moving reader ( $\square$ ); and measured positions of the reader ( $\times$ ).

reference measurements.

The first set of measurements at the first known reader location were used to calculate the offset  $d_o$  for each tag as in (Equation 6.1). Figure 6.5 demonstrates the CDF of the estimation errors ( $\varepsilon$ ) after calibration based on 120 and 40 data points for 1D and 2D posi-

Table 6.2: Statistics of 1D and 2D location estimations

Statistics	1D Estimation	2D Estimation
Mean $\varepsilon$ (m)	0.11	0.17
RMS $\varepsilon$ (m)	0.14	0.20
STD (m)	0.08	0.12
$\varepsilon_{90\%}$ (m)	0.20	0.40

tioning, respectively. A mean error and an RMS error of 0.11 m and 0.14 m were observed for 1D estimations. While, in 2D, the calculated positions provide a mean and an RMS error of 0.17 m and 0.20 m, respectively. Table 6.2 summarizes these statistics; the reported 90-th percentile error  $\varepsilon_{90\%}$ , defined as  $P(E < \varepsilon_{90\%}) = 90\%$ , is 0.2 m and 0.4 m for 1D and 2D locations measurements.

Figure 6.6 illustrates the estimated locations along with the ground truth reader and tag locations. Considering the size of the reader’s cart (about 1 m by 0.5 m) and the placement error, the achieved positioning error in this chapter is smaller than the size of the target. Moreover, the estimated position of the reader is both accurate and precise. It is worth mentioning that the distance estimation error remains the same while the reader-to-tag distance increases; therefore the percentage error is expected to be lower at longer ranges [85]. Similar accuracy is expected for using this system in a larger area covered by more tags or readers. Although only the *reverse* positioning system has been shown in this set of experiments, the same performance is expected for the *conventional* configuration, in which multiple fixed readers are used for localizing one or more moving tags.

## 6.4 Conclusion

In this chapter, an RSP-based 2D real-time RFID positioning system using tunneling tags was proposed. GNU Radio and USRPs were used to implement a frequency hopping reader at 5.8 GHz. An FDMA method was used to measure the distance between the moving reader and multiple tags for trilateration. Both good accuracy and precision is achieved

using the proposed system, with a mean and RMS positioning error of 0.17 m and 0.2 m, respectively.

## CHAPTER 7

### A BACKSCATTER CHANNEL SOUNDER USING TUNNELING RFID TAGS

This chapter introduces a backscatter channel sounder technique used for a RFID positioning system at 5.8 GHz. This system applies Received Signal Phase (RSP)-based positioning and channel sounding techniques to a tunneling tag, providing sufficient information to calculate the delay spectrum for accurate positioning in a complicated multipath environment. Ultra-precise (0.45%) position estimates at long distances (100 m) are achieved using the proposed channel sounding techniques. The reader setup is available in Appendix B. An MATLAB code example used in this chapter is available in Appendix C.3.

#### 7.1 Introduction

A versatile fine-scale localization technology in realistic environments enables numerous commercial and scientific sensing applications. Emergency responders, law enforcement field officers, and security staff, in fact, can all benefit from a positioning technology that would protect them from unpredictable threats in unknown buildings and scenarios [5] [6]. Realistic environments have thwarted past attempts at fine-scale radiolocation due to multipath echoes and fading. In this work, however, we demonstrate how the unique properties of a backscatter link can be used to sound the channel with respect to an absolute time scale, thereby allowing the identification and removal of multipath effects from a location estimate.

High-accuracy indoor positioning is typically performed with optical sensors that have limited range, long setup time, and cannot be used under certain circumstances (e.g.: infrared sensors are affected by smoke and cannot work outdoor) [11]. Motion capture technologies require complicated sensors and have ranges limited to few meters [11] [94]. On the other hand, backscattering-radio-based trackers (*i.e.*: RFID - Radio Frequency Identi-

fications *tags*) have smaller sizes, reduced complexity, and low power requirements [11]. Nonetheless, they still require Line-of-Sight (LoS) with an RFID reader, they have limited ranges, and low ranging precision [22].

For stable wireless communication and indoor localization with IoT devices, an accurate propagation channel model is essential [95] [96]. Traditional channel modeling relies on complicated sliding correlator systems or bulky lab equipment such as Vector Network Analyzers (VNAs), Synthesized Sweepers, *etc.* [97]. In practice, local oscillator synchronization is difficult to achieve; often a cable is connected between source and measurement nodes to share a common frequency reference, which greatly limits the range of measurements [98] [99].

In this chapter, we propose a backscatter channel sounder that provides the capability of channel modeling for backscatter communication systems at 5.8 GHz without complicated wired setup and synchronization. Ultra-precise, submeter-scale position estimates at long distances in real-world scenarios can also be achieved using this system, which utilize the *Received Signal Phases* (RSP) of the backscattered signals from a tunneling tag [3]. The tunneling tag utilizes the Esaki tunneling diode [88] for use in amplification of backscattered signals while preserving the linear relationship between the reader-to-tag distance and RSP. Its property allows accurate estimates of the backscatter propagation channel model at long distances, and gives the capability of precise positioning in real-world applications under multipath and external interference.

## 7.2 Rationale

### 7.2.1 Channel Sounding Reader Design

The proposed channel sounder can be viewed as a form of Stepped-Frequency Continuous-Wave (SFCW) radar system, which transmits an unmodulated wave at 5.8 GHz, receives the backscattered signal from any RFID tags, and down-converts it into baseband in-phase (I) and quadrature-phase (Q) signals. Figure 7.1 shows the design diagram of the proposed

channel sounding reader. A Software Defined Radio device (USRP N200 from National Instrument [90]), is used to digitizes and filters the baseband signal for post-processing.

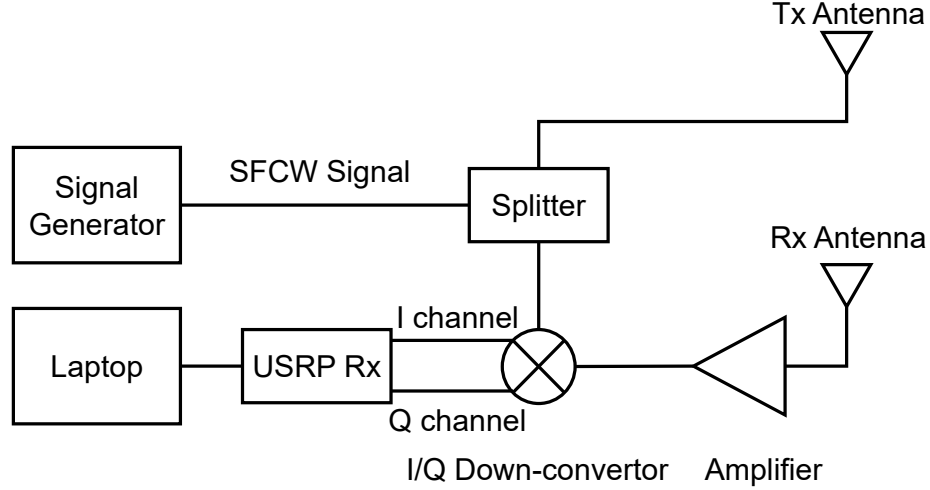


Figure 7.1: Block diagram of the RFID reader used as channel sounder.

The channel sounding reader transmits a frequency-hopping continuous wave at constant output power and hops between each frequency channel upon dwelling for a certain amount of time. Figure 7.2 summarizes the channel sounding procedure showing the transmitted and received signals both in frequency and time domains. The train of transmitted signals is backscattered and modulated by a custom tunneling RFID tag operating at the 5.8 GHz ISM band. The amplitude and phase of the received backscattered signals can be expressed as:

$$P_{RSS}(f) = \frac{I_{rx}(f)^2 + Q_{rx}(f)^2}{Z_0}, \quad (7.1)$$

$$\varphi_{RSP}(f) = \arctan\left(\frac{Q_{rx}(f)}{I_{rx}(f)}\right) \in [0, 2\pi), \quad (7.2)$$

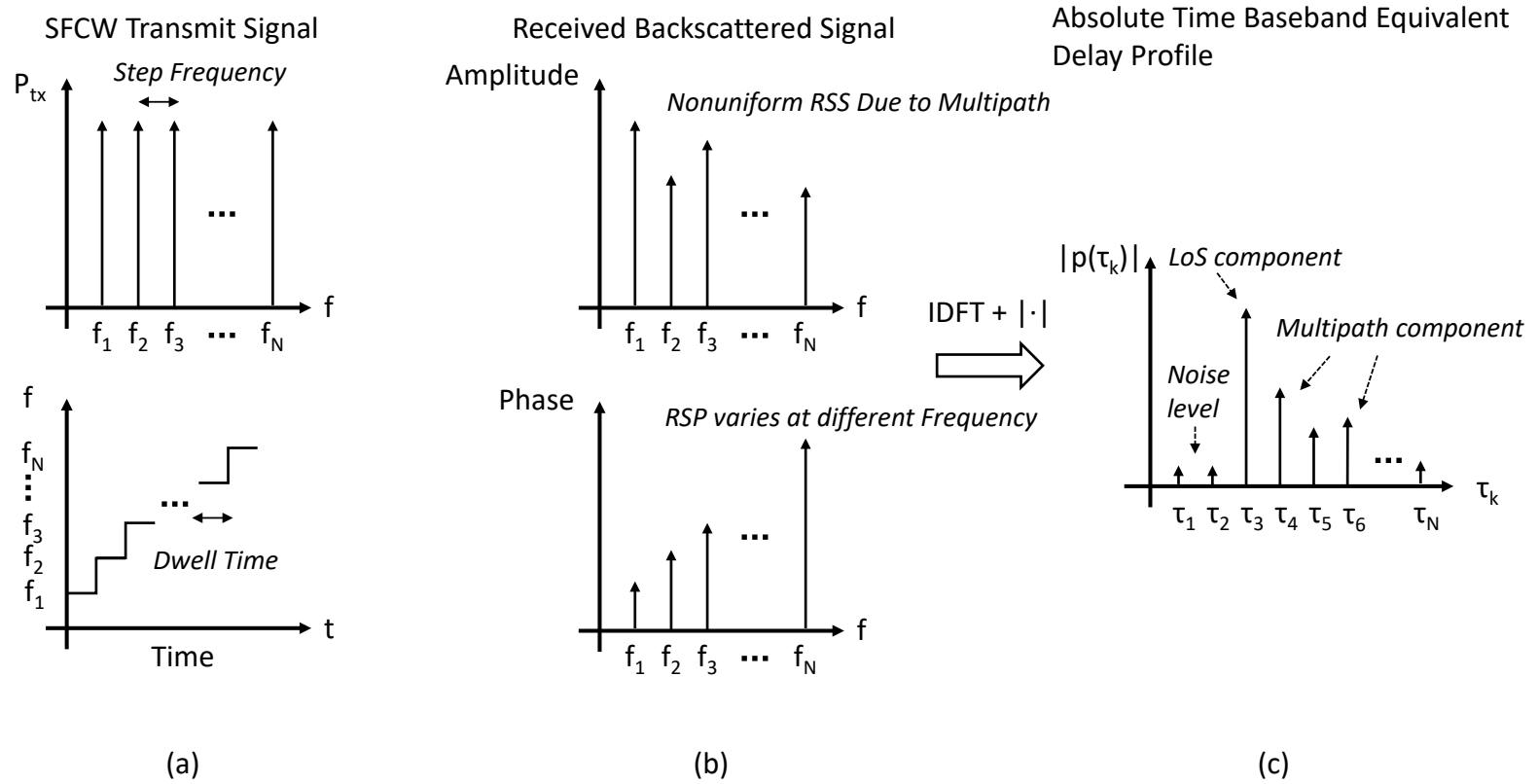


Figure 7.2: How channel sounding can be used to detect both LoS and multipath components in an RFID system. a) The transmitted, b) backscattered, and c) post-processed signals are shown.



where  $Z_0$  is the impedance of the RF circuits,  $f$  is the hopping carrier frequencies of the reader, and  $I_{rx}$  and  $Q_{rx}$  are the received signals in baseband for each carrier. Since the down-converted and the transmitted signals share the same signal generator, the channel sounding reader can perform near-perfect coherent phase detection. Moreover, to increase the , a GNU Radio built-in Geortzel filter [91, 92, 93] is used. Figure 7.2b shows the amplitude, also known as the RSS, and RSP at each frequency channel (from  $f_1$  to  $f_N$ ). Although the transmitted signal is uniform at each channel, the RSS usually changes for each frequency due to multipath, different frequency responses of the system, temporarily blocked LoS, *etc.*

In a multipath free environment, the RSP offset  $\varphi_{ps}$  caused by the LoS round-trip propagation can be written as [9]:

$$\varphi_{ps} = -\frac{4\pi d}{\lambda}, \quad (7.3)$$

where  $\lambda$  is the wavelength at the carrier frequency  $f$ . Therefore, the RSP at different carrier frequencies varies due the difference wavelengths. The RSPs, like the RSSs, are also affected by the environment, therefore the differential RSP between adjacent channels is usually not a constant as (Equation Equation 7.3) suggests.

### 7.2.2 RSP-based Ranging Method

Knowing the RSPs at different frequency channels, the distance  $\hat{d}$  between a reader and a tag can then be estimated using [20] [85]:

$$\hat{d} = \frac{\lambda_e}{4\pi N} \sum_{n=1}^{N-1} (\varphi_{n+1}(f_n + 1) - \varphi_n(f_n)), \quad (7.4)$$

with  $\varphi_n$  and  $\varphi_{n+1}$  being the measured RSP obtained by the reader at carrier frequencies  $f_n$  and  $f_{n+1}$ , respectively;  $N$  being the number of the frequency channels. The maximum detection range  $\hat{d}_{max}$  for the RSP-based method depends on the minimum frequency step

$\Delta f$  used by the reader:  $\hat{d}_{max} = \frac{c}{2\Delta f} = \frac{\lambda_e}{2}$ , with  $\lambda_e = \frac{c}{\Delta f}$ .

### 7.2.3 Channel Sounding Technique Using Tunneling Tags

The multipath channel can be modeled as a set of discrete components that together determine a power delay profile,  $p(\tau)$ , as a function of delay  $\tau$ :

$$p(\tau) = \sum_i p_i \delta(\tau - \tau_i), \quad (7.5)$$

with  $p_i$  being the backscattered signal received at time delay  $\tau_i$ . In frequency domain, the normalized and un-normalized complex received signal can be expressed as:

$$C(n)_{norm} = \sum_{n=1}^N \exp(-j\phi_n), \quad (7.6)$$

$$C(n)_{un-norm} = \sum_{n=1}^N R_n \exp(-j\phi_n), \quad (7.7)$$

where  $R_n$  and  $\phi_n$  are respectively the RSS and RSP at the  $n$ -th frequency channel with  $N$  being the total number of channels determined by the frequency span and step frequency. Given the signal in the frequency domain, the discrete power delay profile in time delay domain,  $p(\tau_k)$ , can be derived using the Inverse Discrete Fourier Transform (IDFT) of the the complex received signal  $C(n)$  in the frequency domain:

$$p(\tau_k) = \frac{1}{N} \sum_{n=1}^N C(n) \exp\left(\frac{-j2\pi n\tau_k}{N}\right) \quad (7.8)$$

where  $\tau_k$  represents the discrete two way travel time delay  $\tau$  in (Equation 7.5). Figure 7.2c shows the delay profile after IDFT, which is represented by a summation of Kronecker delta functions with various amplitudes from  $\tau_1 = 1$  to  $\tau_N = N$ :

$$p(\tau_k) = \sum_{k=1}^N p_k \delta(\tau - \tau_k), \quad (7.9)$$

Both normalized and un-normalized received signals can be used to calculate the delay profile. The former only requires RSP while the latter needs a good estimation of both RSS and RSP. However, tunneling tags have non-uniform gain depending on the impinging power level and its frequency response. Therefore, it is necessary to investigate the delay profile generated using both normalized and un-normalized received signals.

To estimate the distance traveled by the backscattered signal, the discrete time delay  $\tau_k$  in (Equation 7.8) can be converted to one-way travel distance using:

$$d = \frac{c}{2B} \tau_k, \quad (7.10)$$

where  $c$  is the speed of light and  $B$  is the bandwidth. The distance between the reader and tag can then be determined by the travel distance of the first arrival component of the delay profile. The resolution of the discrete one-way travel distance and the ambiguous distance are determined by both the bandwidth and the number of channels, respectively:

$$d_{res} = \frac{c}{2B}, \quad (7.11)$$

and

$$d_{max} = \frac{c}{2B} N. \quad (7.12)$$

Zero-padding is a common technique used to increase the frequency resolution of the Discrete Fourier Transform (DFT). By appending the actual signal in frequency domain to a zero vector of length  $M$ , the resolution of the IDFT in time delay domain can also be improved, resulting in a better distance estimate resolution. The improved distance resolution is written as:

$$d_{res} = \frac{c}{2B} \frac{N}{N + M}. \quad (7.13)$$

## 7.3 Measurements

### 7.3.1 Experimental Setup

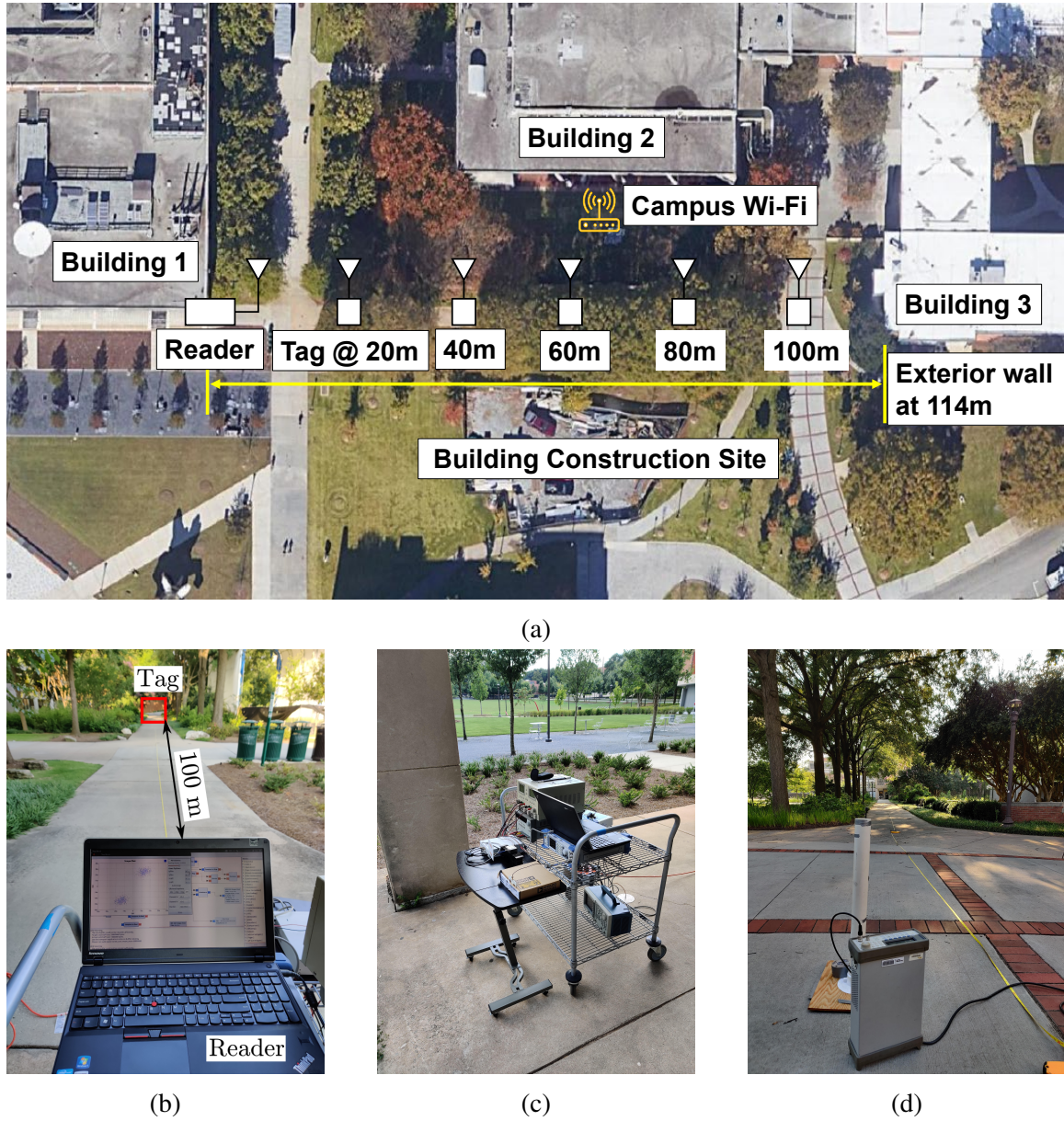


Figure 7.3: The experimental setup seen (a) from the above and (b) from the reader with the tag placed at 100 m away. Photos of the (c) frequency hopping reader and (d) the tunneling tag.

To test the channel sounder and to investigate the impact of multipath and interference, an outdoor environment near multiple buildings and a construction site was chosen.

A custom-made microwave frequency hopping RFID reader was realized (shown in Appendix B); it was used to transmit an unmodulated continuous wave in the 5.8 GHz ISM band at various frequencies, to receive the modulated signals backscattered by one tunneling tag, and to downconvert them into their baseband I and Q components. An E-shaped patch antenna was used on the receiving front-end of the reader while an omnidirectional monopole antenna was used for the tunneling tag. The detailed specifications of the experimental setup are listed in Table 7.1.

Table 7.1: Specifications of the outdoor long range experimental setup.

$G_t$ (dBi)	1.5
$d$ (m)	[20:20:100]
$P_T$ (dBm)	13
$G_{tx}$ (dBi)	8
$G_{rx}$ (dBi)	7.5
Freq. hopping (GHz)	5.725:5.875
Dwell Time ( <i>Slow</i> , ms)	2
Dwell Time ( <i>Fast</i> , ms)	10
Freq. step $\Delta f$ (kHz)	200
Number of Channels (N)	751
Zero-padded IDFT Length (M)	2048
Distance Resolution ( $d_{res}$ , cm)	18.3

As shown in Figure 7.3a, the reader was placed nearby Building 1 with the antennas facing Building 3 at about 114 m away. The tunneling tag was moved every 20 m from the reader and up to 100 m from it with a step of 20 m on a straight path between the two buildings. Along the path, trees and bushes were always near the reader. A Wi-Fi router located on the exterior wall of Building 2 was left powered on despite the possible interference it could have introduced to the system. To estimate the multipath delay spectrum and reader-to-tag distance, the reader hopped from 5.725 GHz to 5.875GHz with a step frequency of 200 KHz for each position of the tag. To study the impact of dwell time on the ranging accuracy, the reader dwells on each channel for 200 ms. In post processing, different lengths

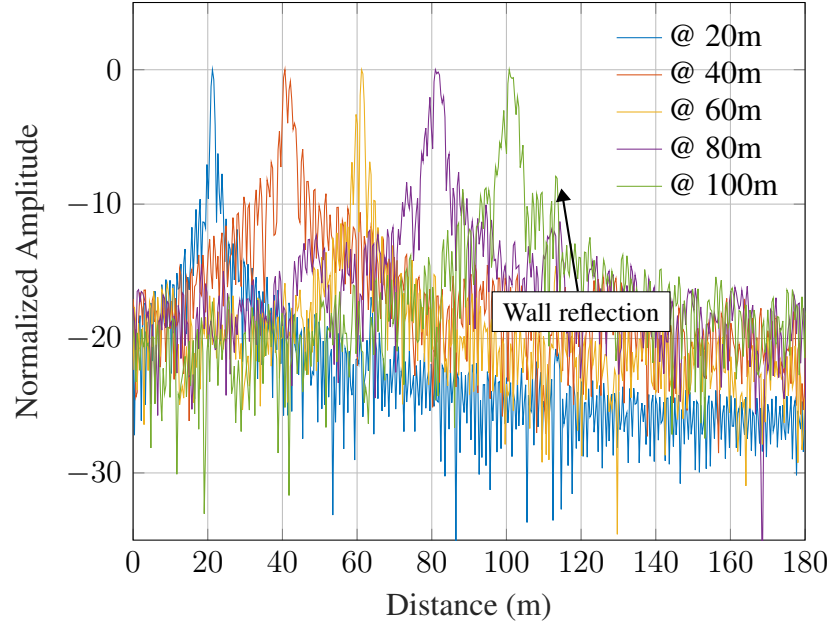
of data were extracted to study the effects of various dwelling times. In particular, two different dwell times were investigated by using part of the digitized received signal of each channel: the slow hopping (10 ms) and the fast hopping (2 ms).

### 7.3.2 Channel Modeling

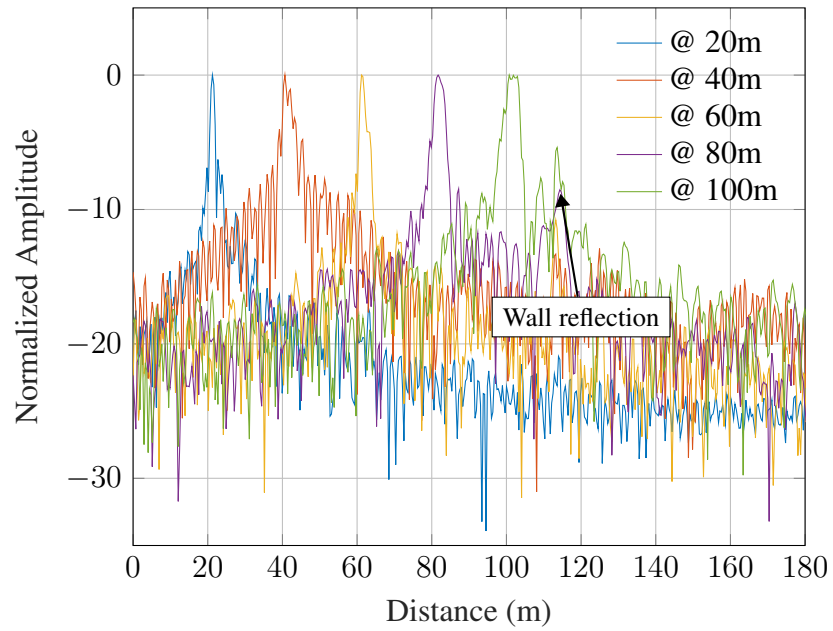
Figure 7.4a and Figure 7.4b demonstrate the delay profile calculated using the IDFT of the normalized (Equation 7.6) and un-normalized (Equation 7.7) received signals through (Equation 7.8), referred to as *IDFT norm* and *IDFT un-norm* in the rest of this chapter. The slow hopping configuration (dwell time of 10 ms) was used to calculate the average RSP for each frequency channel. Both normalized and un-normalized delays provide enough data to estimate the LoS components of the backscatter signals. However, with un-normalized delays, the reflections from the wall (about 114 m away from the reader) can be better distinguished from the noise floor at each set of measurements.

Figure 7.5 shows the RSS at all frequency channels for the tunneling tag located at various distances from the reader when using the E-shaped patch antenna on the receiving front-end of the reader. The ditches are caused by temporary absence of LoS due to pedestrians and vehicles passing by. The reflective gain of the tunneling tag at lower impinging power levels [3] influences the the predictions on tag position based only on RSS causing an increase of the estimation error.

It is worth highlighting that the measurements are done under the interference caused by the campus Wi-Fi at 5.8 GHz band. A router with antenna array pointing to the measurements was found on the exterior wall of building 2 as shown in Figure 7.3a. A strong interference between 5.755 GHz and 5.575 GHz was observed in most measurements. When the tag is placed at 40 m, the combined impinging power from the reader and the strong interfering WiFi saturate the tunneling tag and reduce its reflective gain. As shown in Figure 7.5, the RSS at 40 m is at the same level as the one at both 60 m and 80 m at some frequencies, causing a high noise level.



(a)



(b)

Figure 7.4: Delay profile calculated using the IDFT of the a) normalized received signal (*IDFT norm*) and b) un-normalized received signal (*IDFT un-norm*) in frequency domain. The additional RSS information of un-normalized received signals can increase the detection accuracy of multipath components.

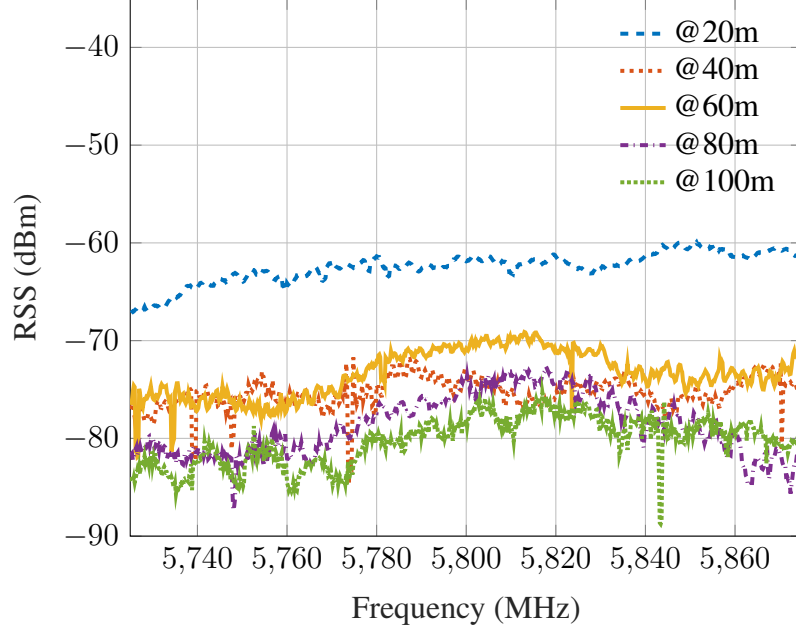
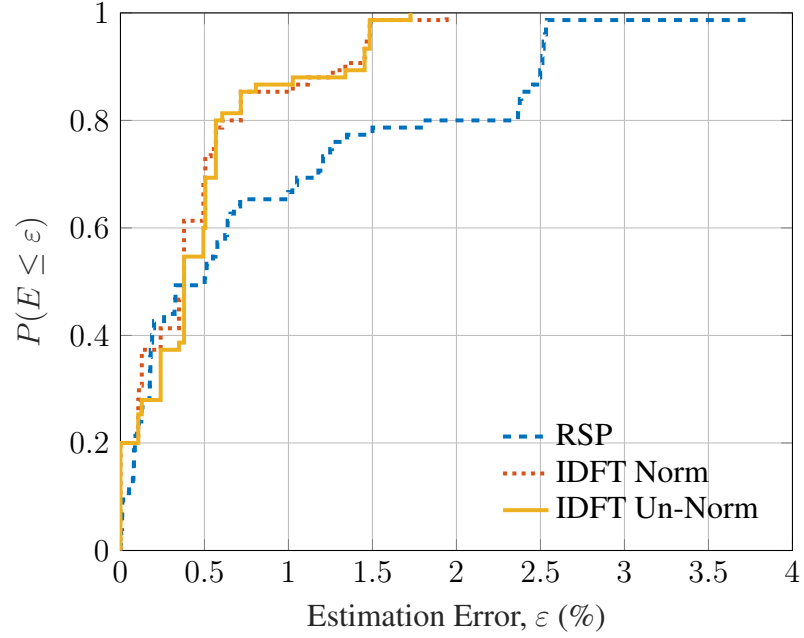


Figure 7.5: The RSS values of slow hopping mode in the frequency domain. The dips are caused by pedestrians and vehicles momentarily obstructing the LoS.

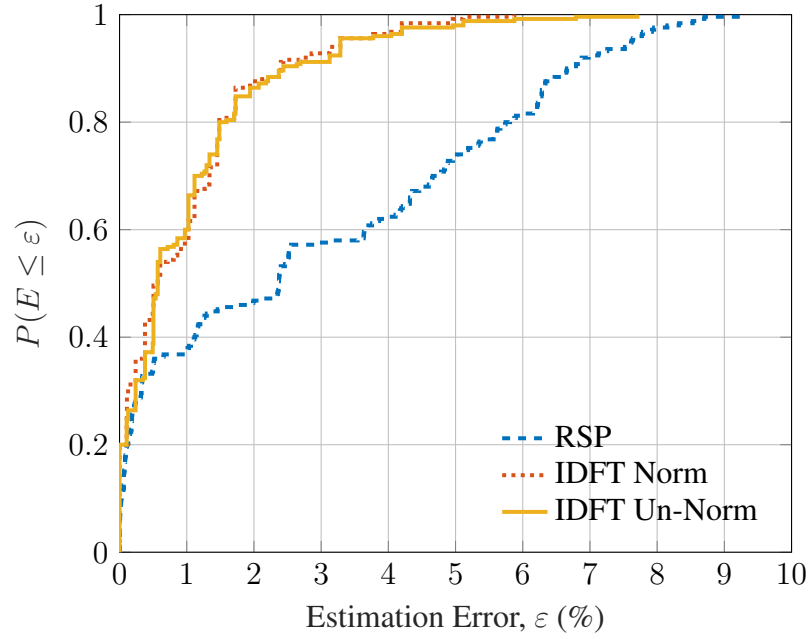
### 7.3.3 Distance Estimation

The proposed channel sounding method can also be used to estimate the position of a tag by looking at the received LoS components of the backscattered signal, while in [85] the reader-to-tag distance is estimated using (Equation 7.4) with only the differential RSP. The measured reader-to-tag distances include distance travelled by the wave within cables and circuits. This distance is constant and can be calibrated out by using the first measurement at 20 m as a reference. Figure 7.6a compares the empirical Cumulative Distribution Function (CDF) of the percentage estimation errors ( $\varepsilon$ ), calculated using the absolute error over the true reader-to-tag distance, when using two different methods with a slow hopping reader (dwell time of 10 ms). With the RSP-based method, a mean error, an RMS error, and the 90th percentile error ( $\varepsilon_{90\%}$ , defined as  $P(E \leq \varepsilon_{90\%}) = 0.9$ ) of 0.86%, 1.28%, and 2.50%, respectively, are observed. The IDFT method reduces the 90-th percentile error to 1.34% (by 46.4%), while the normalization does not significantly change the distance estimation accuracy. Both IDFT methods with or without normalization have a mean error





(a)



(b)

Figure 7.6: Empirical CDF measured with different methods in a) slow hopping (dwell time = 10 ms) and b) fast hopping (dwell time = 2 ms) configurations.

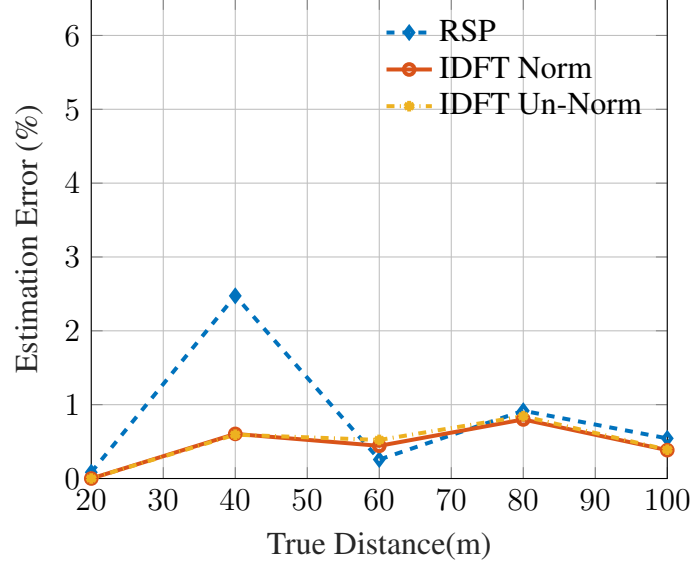
lower than 0.47%, and an RMS error lower than 0.65%.

The distance estimation accuracy also depends on many other factors, such as the dwell time, the number of frequency channels, the existence of interference, and thermal noise.

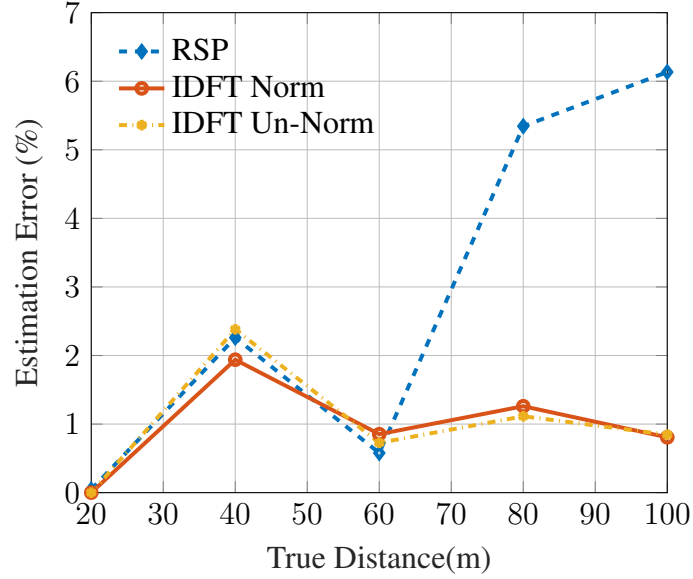
The dwell time determines how fast the system can estimate the location of the tag. Although it is always beneficial to have faster prediction times, taking average RSP of more data when using a slower hopping reader can reduce the impact of the thermal noise and give a more accurate estimation of the RSP when the SNR is low. Figure 7.6b shows the empirical CDF of the estimation errors for fast hopping reader (dwell time of 2 ms). Compared to the RSP-based method, the IDFT methods perform significantly better in terms of both mean error (reduced from 2.87% to less than 1.01%) and 90-th percentile error (reduced from 6.67% to less than 2.44%).

Signal-to-Noise Ratio (SNR) and Signal-to-Interference Ratio (SIR) are also critical factors for accurate estimation. The campus Wi-Fi operating at the same frequency band not only suppresses the gain of the tunneling tag but also causes distance estimation offsets. Figure 7.7a shows the mean estimation error at each distance when using a slow hopping reader. When the tag is placed at 40 m, it receives the highest level of interference, causing dramatic increase in the estimation error. This is also reflected in the higher 90-th percentile error for RSP-based method in Figure 7.6a. When using fast hopping mode, the accuracy of both RSP- and IDFT-based methods decrease at most distances. As shown in Figure 7.7b, the RSP-based method suffers from higher estimation error due to low SNR at longer distances (at 80 m and 100 m), while IDFT methods remains highly accurate ( $< 1.26\%$ ) at such distances.

Table 7.2 summarizes the statistics of distance estimations, which implies that the IDFT methods for distance estimation outperform the RSP-based method. In particular, there is an improvement in the RMS  $\varepsilon$ , respectively by a factor of 2 and 2.7, for the slow and the fast hopping normalized IDFT methods when compared with the RSP-based one. In addition, the extra RSS information in the un-normalized IDFT method does not further improve the accuracy compared to the normalized IDFT method based on RSP.



(a)



(b)

Figure 7.7: Mean Estimation Errors measured with using different methods in a) slow hopping (dwell time = 10 ms) and b) fast hopping (dwell time = 2 ms) configurations from 20 m to 100 m.

## 7.4 Conclusion

This chapter has shown an easy-to-setup long-range RFID channel sounding system that provides coherent channel measurements at 5.8 GHz ISM band. The system estimates the

Table 7.2: Statistics of distance estimations

	<b>Slow Hopping</b>			<b>Fast Hopping</b>		
Statistics	RSP	IDFT Norm.	IDFT un-Norm.	RSP	IDFT Norm.	IDFT un-Norm.
Mean $\varepsilon$ (%)	0.86	0.45	0.47	2.87	0.97	1.01
RMS $\varepsilon$ (%)	1.28	0.64	0.65	3.94	1.48	1.59
$\varepsilon_{90\%}$ (%)	2.50	1.34	1.45	6.67	2.40	2.44

delay profile of multipath environments which characterizes the backscatter communication channel for RFID tags (tunneling tags in this chapter for extended range). Compared to conventional systems, the proposed channel sounder can be easily configured without specialized equipment such as VNAs, pulse generators, and oscilloscopes. The measured delay profile can be also used for positioning purposes, giving higher accuracy compared to conventional RSS- and RSP-based methods, especially in low SIR and SNR scenarios. A mean and a 90-th percentile distance estimation accuracy of 0.45% and 1.34% are observed, respectively, when using the proposed channel sounding technique in slow hopping. When using the fast hopping setup, instead, the channel sounding technique reduces the mean distance estimation error from 2.87% to less than 1.01%, compared to the conventional RSP-based method.

## CHAPTER 8

### FUTURE WORK

This thesis demonstrates the potential of using tunneling tags and the RSP-based localization technique in various real-world applications, including long-range positioning, through-obstruction ranging, and two-dimension localization. The proposed technique can still be improved in many aspects (e.g., range, scalability, tracking capability, etc.). A low-power, flexible, and real-time capable frequency hopping reader operating at 5.8 GHz was designed and implemented. The highest reading and ranging distance of 100 m are tested with a mean distance estimation error of less than 0.97%.

The range in the current proof-of-concept is limited by the low reader transmit power set to 15 dBm only. For comparison, a 5 GHz indoor Wi-Fi router transmits 23 dBm<sup>1</sup>. Therefore, the range can further be improved by increasing the output power (*i.e.*: an RFID reader can transmit up to 30 dBm). The projected ranging results suggest that this positioning method opens up to long-range, low-powered, and highly precise applications for IoT devices. Measurements at ultra-long distances (more than 1 km) using high transmit power (EIRP = 36 dBm) can be performed to study the limit of this system in practice.

The range of the proposed technique can be further improved using retro-directive arrays. Authors in [45, 46, 47, 2] have suggested equipping RFID tags with Van Atta-based Arrays [48] to further increase the communication range while maintaining a wide field-of-view.

In this work, when locating the reader using multiple tags, FDMA was used to distinguish the tags. In traditional RFID systems, readers read hundreds of tags per minute by using a form of Time Division Multiple Access (TDMA). In many IoT applications, the capability of simultaneously identifying and locating thousands of tags is a key factor.

---

<sup>1</sup>[metis.fi/en/2017/10/txpower](http://metis.fi/en/2017/10/txpower)

Multiple access schemes like Code Division Multiple Access (CDMA), or Space Division Multiple Access (SDMA), or Range Division Multiple Access (RDMA) schemes can be studied in the future work. IQ-subspace techniques are another direction for multiple access with great potential in the future.

Although this dissertation shows the potential of using the RSP-based ranging technique in various NLoS environments for locating tunneling tags with sub-meter accuracy. A comprehensive quantitative study to assess the impact of factors such as multipath, diffraction, reflection, and penetrating dielectric materials in different environments (including LoS and NLoS) can be pursued as future work. Researches show that the channel statistics provided by the channel sounding method can be used to achieve improved location accuracy in NLoS environments [100].

The ability to track moving targets at long distances enables many IoT applications using tunneling tags. Hybrid Inertial Microwave Reflectometry (HIMR) based on a 5.8 GHz backscatter tunneling tag with a 6-axis accelerometer and gyroscope sensors can be developed [10]. Although the tunneling tag in this work relied on an external power supply, the extremely low biasing voltage and current requirements would allow using a local solar cell [101] that, at long distances from the reader, will provide enough power. Finally, both 2-D and 3-D tunneling location tracking systems can be implemented by using multiple readers [11].

# **Appendices**

## APPENDIX A

### CIRCUIT DESIGN

This appendix shows the circuit schematic diagrams of the reader and the semi-passive tag. The schematics diagrams are designed based on the reference designs provided by the chip manufacturers.

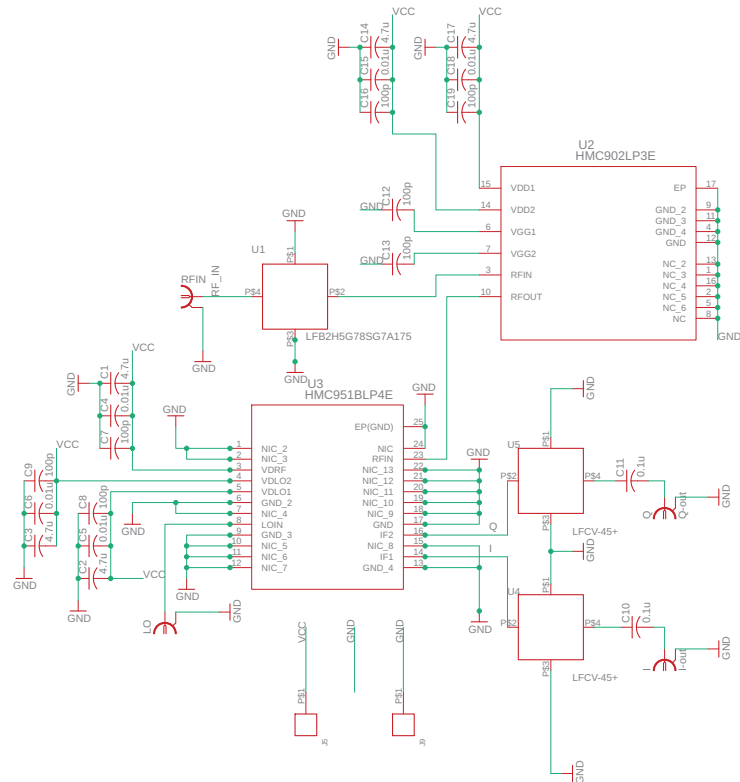


Figure A.1: The circuit schematic diagram of the reader's receive board. A IQ down-converter (Analog Device HMC951b) and a low-noise amplifier (Analog Device HMC902) are used in this design.



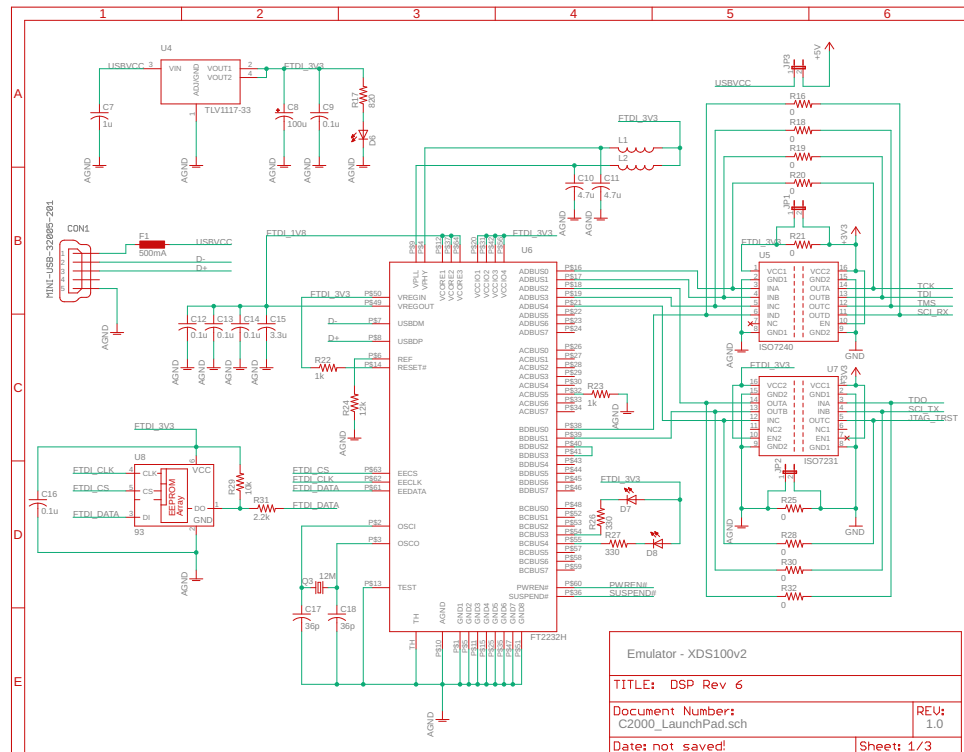


Figure A.2: The schematic diagram of the DSP's emulator board. This design is based on the reference design available in [102].

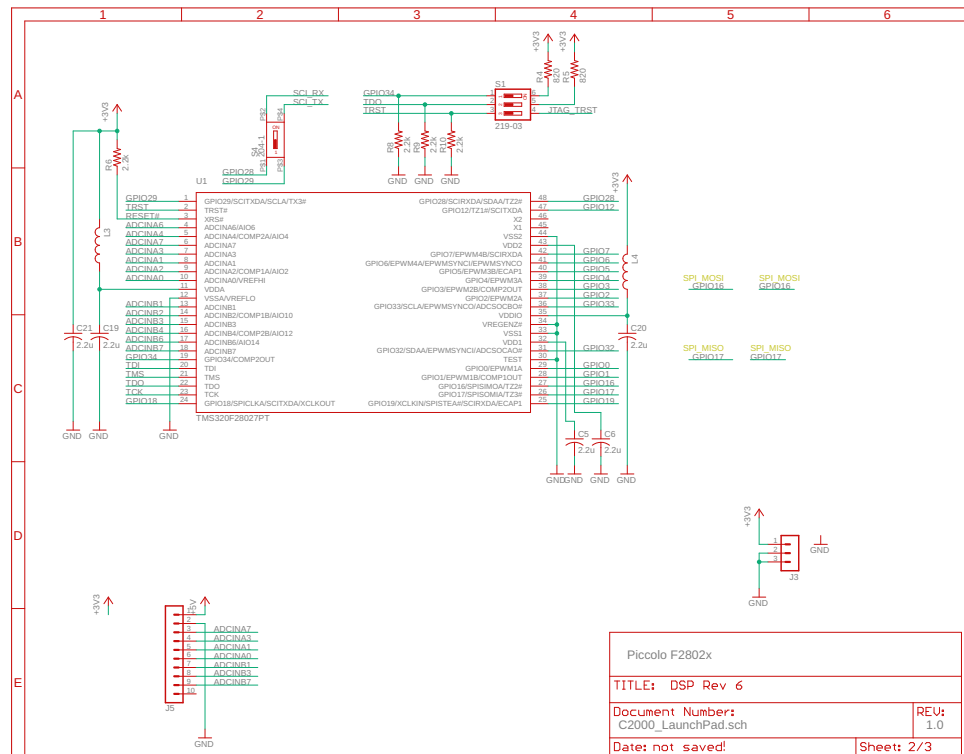


Figure A.3: The circuit schematic diagram of the DSP. A DSP chip (Texas Instrument Piccolo F28027) is used in this design. The reference design is available in [102].

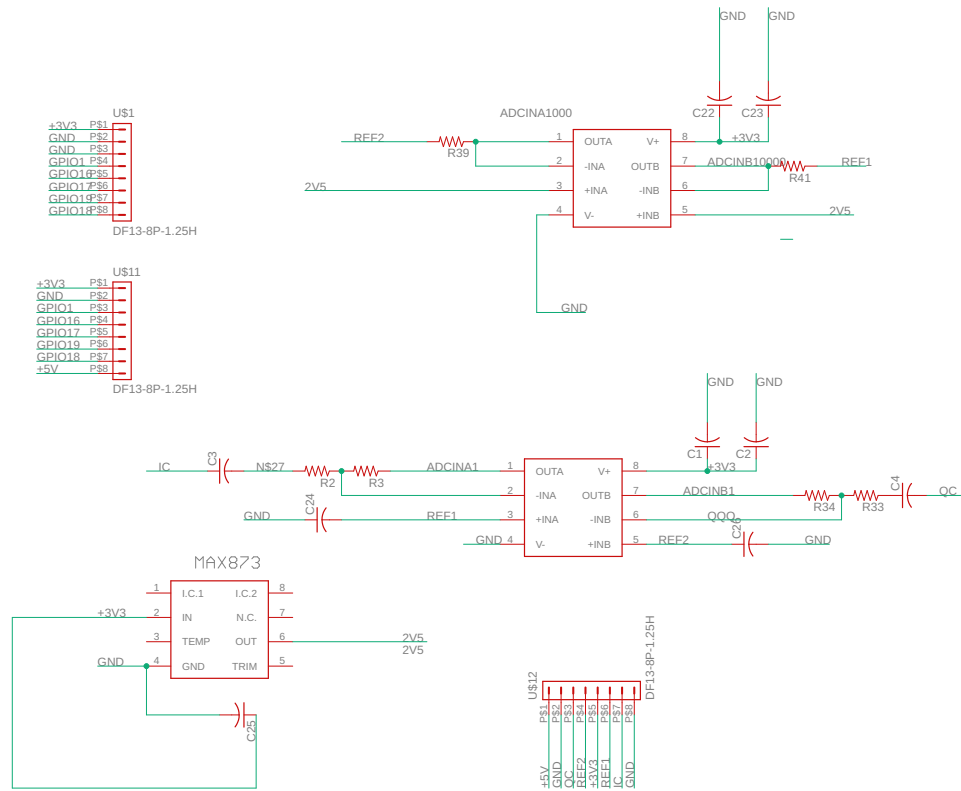


Figure A.4: The circuit schematic diagram of the base-band amplifier board. Operational amplifiers (Texas Instrument OPA2626) are used in this design.



## APPENDIX B

### READER SETUP

This appendix presents the reader setup used for data collection. The required equipment include: i) a microwave signal generator (R&S SMB100A in Figure B.1), ii) a power supply, iii) an Ettus USRP N200 [90], and iv) a receive board introduced in Figure A.1. The devices used in the reader setup slightly vary in different use cases. In Chapter 4, another signal generator model (Agilent E8247C) is used. In Chapter 6, the signal generator is replaced by a second USRP. In Chapter 5 and Chapter 7, two E-shaped patch antennas with separate ground plane are used.

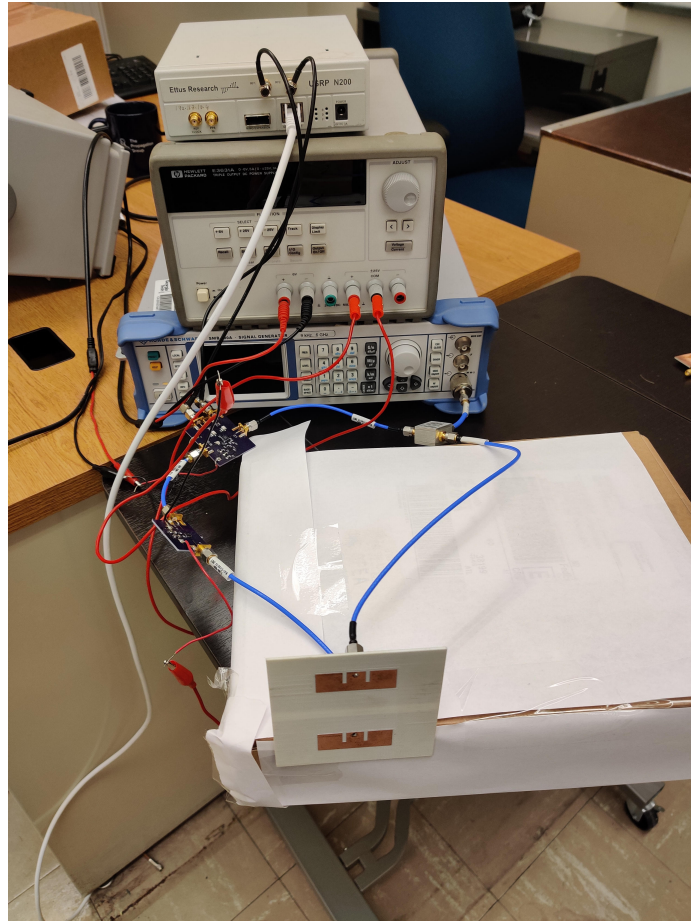


Figure B.1: Photo of the reader setup.

## APPENDIX C

### DATA AND RELEVANT CODE

The data used in this dissertation from Chapter 4 to Chapter 7 are publicly available on the Github repository[103]. Some MATLAB code examples used to process the data are listed below and included in the Github repository [103]. For questions, please send an email to chengqi9335@gmail.com.

#### C.1 MATLAB Code Example for Chapter 4

```
1 clc;clear all;close all
2 %% Frequency sweep from 5820MHz to 5870MHz, each frequency step is 1MHz
3 data_15m_qto1=read_complex_binary ("5m_nt_3v_121_1.bin", 400000,28470);
4 %scatterplot(data_15m_qto1)
5 plot(angle(data_15m_qto1))
6 %% Clean the transition between frequency steps and plot the IQ ...
   constellation
7 for i=1:51
8     data_15m_qto((i-1)*1000+1:i*1000)= ...
9     data_15m_qto1((i-1)*5082+1001:(i-1)*5082+2000);
10 end
11 figure(1)
12 scatterplot(data_15m_qto)
13 figure(2)
14 % Plot the phase of data in the upper-half complex plane
15 data_15m_qt_0=data_15m_qto(angle(data_15m_qto)<0)/2/pi*360;
16 figure(3)
17 plot(angle(data_15m_qt_0))
```

```

18 %% Calculate the received signal phase of each measurements in degree
19 angle_15m_qt_f=angle(data_15m_qt_0)/2/pi*360;
20 %calculate the received signal strength of each measurements
21 magnitude_10m_qt_f=20*log10(mean(abs(data_15m_qt_0))-10*log10(50));
22 RSSI_15m_qt_f=20*log10(abs(data_15m_qt_0));
23 RSSI_5m_nt=mean(RSSI_15m_qt_f(1:500));
24 figure(5)
25 plot(angle_15m_qt_f)
26 for j=1:50
27     mean_mag_15m_qt(j)= ...
28     20*log10(mean(abs(data_15m_qt_0((j-1)*500+1:j*500))));
29 end
30 figure(7)
31 plot(mean_mag_15m_qt)
32 %% Data cleaning and range estimation
33 % Manually clean the phase data when wrapping happens
34 for k=8500:9000
35     if angle_15m_qt_f(k) ≥ -80
36         angle_15m_qt_f(k)=angle_15m_qt_f(k)-180;
37     end
38 end
39 plot(angle_15m_qt_f)
40 mean_angel_15m_qt=zeros(1,120);
41 for j=1:50
42     mean_angel_15m_qt(j)=mean(angle_15m_qt_f((j-1)*500+1:j*500));
43 end
44 figure(6)
45 stem(mean_angel_15m_qt+180)
46 diff_angel_15m_qt=zeros(1,49);
47 for n=1:49
48     diff_angel_15m_qt(n)=mean_angel_15m_qt(n+1)-mean_angel_15m_qt(n);
49     if diff_angel_15m_qt(n) ≤ 0
50         diff_angel_15m_qt(n)=diff_angel_15m_qt(n)+180;

```

```

51     end
52 end
53 figure(7)
54 plot(diff_angel_15m_qt)
55 distance_5m_nt= ...
56 (180-mean(diff_angel_15m_qt))/720*300; % Distance Estimation
57 error_5m_nt=distance_5m_nt/5-1; %Estimation error

```

## C.2 MATLAB Code Example for Chapter 5

```

1  clc;clear all;close all;
2  start_id(1,:)=[93073,102268,10963,11029,46804,8175,7349];
3  start_id(2,:)=[15310,7099,9545,31410,20542,16237,9356];
4  start_id(3,:)=[16810,7553,8479,8100,14375,11379,7629];
5  start_id(4,:)=[25268,12993,19982,9321,21300,59106,10521];
6  distance_ground_truth=linspace(3,9,7);
7  data_len=100;
8
9  %% Data Processing
10 for data_num=1:4
11     for ii = 1:10
12         for nm=1:7
13             if data_num == 1
14                 filename = ...
15                 sprintf('%s%d%s','0228_los_',distance_ground_truth(nm), ...
16                 '_6dbm_tt140.bin');
17             end
18             if data_num == 2
19                 filename = ...
20                 sprintf('%s%d%s','0227_wnlos_',distance_ground_truth(nm), ...
21                 '_6dbm_tt140.bin');

```



```

22 end
23 if data_num == 3
24     filename = ...
25     sprintf('%s%d%s','0228_los_',distance_ground_truth(nm), ...
26     '_6dbm_spt.bin');
27 end
28 if data_num == 4
29     filename = ...
30     sprintf('%s%d%s','0227_wnlos_',distance_ground_truth(nm), ...
31     '_6dbm_spt.bin');
32 end
33 data_15m_qt01=read_complex_binary(filename, ...
34 10000000,start_id(data_num,nm));
35 %% Data Extraction
36 for i=1:300
37     data_15m_qt_0((i-1)*data_len+1:i*data_len)= ...
38     data_15m_qt01((i-1)*2000+data_len*ii+1: ...
39     (i-1)*2000+data_len*(ii+1));
40
41 end
42 angle_15m_qt_f=angle(data_15m_qt_0)/2/pi*360;
43 %% Data cleaning and range estimation
44 mean_angle_15m_qt=zeros(1,300);
45 for j=1:300
46     if max(angle_15m_qt_f((j-1)*data_len+1:j*data_len)) ...
47     -min(angle_15m_qt_f((j-1)*data_len+1:j*data_len)) >170
48         for k =1:data_len
49             if angle_15m_qt_f((j-1)*data_len+k) <90
50                 angle_15m_qt_f((j-1)*data_len+k)= ...
51                 angle_15m_qt_f((j-1)*data_len+k)+180;
52             end
53         end
54     end

```

```

55     mean_angel_15m_qt(j)= ...
56     mean(angle_15m_qt_f((j-1)*data_len+1:j*data_len));
57 end
58 for j=1:300
59     mean_mag_15m_qt(j)= -10*log10(50)+ ...
60     20*log10(mean(abs(data_15m_qt_0((j-1)*data_len+1:j*data_len))));
61     % measured received signal phase
62 end
63 for j=1:300
64     mag_f(j,nm,data_num)= -10*log10(50)+ ...
65     20*log10(mean(abs(data_15m_qt_0((j-1)*data_len+1:j*data_len))));
66     % measured received signal strength
67 end
68 diff_angel_15m_qt=zeros(1,299);
69 distance_25m_qt=zeros(1,299);
70 for m = 1:299
71     diff_angel_15m_qt(m)=mean_angel_15m_qt(m+1)-mean_angel_15m_qt(m);
72     if diff_angel_15m_qt(m) ≤ -100
73         diff_angel_15m_qt(m)=diff_angel_15m_qt(m)+180;
74     end
75 end
76 diff_angel_15m_qt=sort(diff_angel_15m_qt);
77 distance_uncal_los(data_num,nm,ii)= ...
78 2*mean(diff_angel_15m_qt(15:285))/720*300;
79 end
80 end
81 end
82 %% Show the RSS
83 figure(3)
84 for kk = 1:4
85     mean_mag(kk,:)=mean(mag_f(100:200,:,kk))+30;
86
87 end

```

```

88 plot(distance_ground_truth, mean_mag(1,:)+30,'--','Linewidth',1.5)
89 hold on
90 plot(distance_ground_truth, mean_mag(2,:)+30,'--','Linewidth',1.5)
91 plot(distance_ground_truth, mean_mag(3,:)+30,'--','Linewidth',1.5)
92 plot(distance_ground_truth, mean_mag(4,:)+30,'--','Linewidth',1.5)
93 mag_diff_tt= mean(mean_mag(1,:)-mean_mag(2,:));
94 mag_diff_spt= mean(mean_mag(3,:)-mean_mag(4,:));
95 ylabel('RSS (dBm)')
96 xlabel('distance (m)')
97 set(gca, 'fontsize', 14);
98 set(gca, 'XMinorTick', 'on');
99 set(gca, 'XGrid', 'on');
100 set(gca, 'YMinorTick', 'on');
101 set(gca, 'YGrid', 'on');
102 set(gca, 'LineWidth', .5);
103 legend('tt-los','tt-nlos','spt-los','spt-nlos')
104 lgd.Location = 'northeast';
105 lgd.Color='none';
106 lgd.FontSize=12;
107 lgd.Box='off';
108 lgd.NumColumns=2;
109 matlab2tikz('rss_ep.tex');
110 %% Calculate and show the measured distance error
111 for num=1:4
112     for ii = 1:10
113         if num == 1
114             perror_RSP_los(num,ii,:)=(abs(distance_uncal_los(num,:,ii)...
115             -distance_ground_truth-distance_uncal_los(1,1,1)+3)) ...
116             ./distance_ground_truth;
117             derror_RSP_los(num,ii,:)=(abs(distance_uncal_los(num,:,ii)...
118             -distance_ground_truth-distance_uncal_los(1,1,1)+3));
119         end
120     if num == 2

```

```

121         perror_RSP_los(num,ii,:)=(abs(distance_uncal_los(num,:,ii)...
122         -distance_ground_truth-distance_uncal_los(1,1,1)+3)) ...
123         ./distance_ground_truth;
124         derror_RSP_los(num,ii,:)=(abs(distance_uncal_los(num,:,ii)...
125         -distance_ground_truth-distance_uncal_los(1,1,1)+3));
126     end
127     if num == 3
128         perror_RSP_los(num,ii,:)=(abs(distance_uncal_los(num,:,ii)...
129         -distance_ground_truth-distance_uncal_los(3,1,1)+3)) ...
130         ./distance_ground_truth;
131         derror_RSP_los(num,ii,:)=(abs(distance_uncal_los(num,:,ii)...
132         -distance_ground_truth-distance_uncal_los(3,1,1)+3));
133     end
134     if num == 4
135         perror_RSP_los(num,ii,:)=(abs(distance_uncal_los(num,:,ii)...
136         -distance_ground_truth-distance_uncal_los(3,1,1)+3)) ...
137         ./distance_ground_truth;
138         derror_RSP_los(num,ii,:)=(abs(distance_uncal_los(num,:,ii)...
139         -distance_ground_truth-distance_uncal_los(3,1,1)+3));
140     end
141 end
142 end
143
144 perror_tt_los = reshape(mean(100.*perror_RSP_los(1,:,:)),1,7);
145 perror_tt_b = reshape(mean(100.*perror_RSP_los(2,:,:)),1,7);
146 perror_spt_los = reshape(mean(100.*perror_RSP_los(3,:,:)),1,7);
147 perror_spt_b = reshape(mean(100.*perror_RSP_los(4,:,:)),1,7);
148 derror_tt_los = reshape(mean(derror_RSP_los(1,:,:)),1,7);
149 derror_tt_b = reshape(mean(derror_RSP_los(2,:,:)),1,7);
150 derror_spt_los = reshape(mean(derror_RSP_los(3,:,:)),1,7);
151 derror_spt_b = reshape(mean(derror_RSP_los(4,:,:)),1,7);
152
153 figure(4)

```

```

154 plot(distance_ground_truth(1:6),perror_spt_los(1:6), ...
155 'ro-.','Linewidth',1.5)
156 hold on
157 plot(distance_ground_truth(1:6),perror_spt_b(1:6), ...
158 'go--','Linewidth',1.5)
159 plot(distance_ground_truth,perror_tt_los,'b*-','Linewidth',1.5)
160 plot(distance_ground_truth,perror_tt_b,'b*--','Linewidth',1.5)
161 xlabel('True Distance (m)')
162 ylabel('Estimation Error (%)')
163 set(gca, 'fontsize', 14);
164 set(gca, 'XMinorTick', 'on');
165 set(gca, 'XGrid', 'on');
166 set(gca, 'YMinorTick', 'on');
167 set(gca, 'YGrid', 'on');
168 set(gca, 'LineWidth', .5);
169 matlab2tikz('errorlos.tex');
170
171 figure(5)
172 plot(distance_ground_truth,derror_spt_los,'ro-.','Linewidth',1.5)
173 hold on
174 plot(distance_ground_truth,derror_spt_b,'go--','Linewidth',1.5)
175 plot(distance_ground_truth,derror_tt_los,'b*-','Linewidth',1.5)
176 plot(distance_ground_truth,derror_tt_b,'b*--','Linewidth',1.5)
177 xlabel('True Distance (m)')
178 ylabel('Estimation Error (m)')
179 set(gca, 'fontsize', 14);
180 set(gca, 'XMinorTick', 'on');
181 set(gca, 'XGrid', 'on');
182 set(gca, 'YMinorTick', 'on');
183 set(gca, 'YGrid', 'on');
184 set(gca, 'LineWidth', .5);
185 matlab2tikz('errorlos.tex');
186 %% Plot the CDF of the measured distance error

```

```

187 cdfperror_tt_los=100.*reshape(perror_RSP_los(1, :, :), 1, 7*ii);
188 cdfperror_tt_b=100.*reshape(perror_RSP_los(2, :, :), 1, 7*ii);
189 cdfperror_spt_los=100.*reshape(perror_RSP_los(3, :, 1:7), 1, 7*ii);
190 cdfperror_spt_b=100.*reshape(perror_RSP_los(4, :, 1:7), 1, 7*ii);
191 cdfderror_tt_los=reshape(derror_RSP_los(1, :, :), 1, 7*ii);
192 cdfderror_tt_b=reshape(derror_RSP_los(2, :, :), 1, 7*ii);
193 cdfderror_spt_los=reshape(derror_RSP_los(3, :, 1:7), 1, 7*ii);
194 cdfderror_spt_b=reshape(derror_RSP_los(4, :, 1:7), 1, 7*ii);
195
196 figure(6);
197 cdfplot(cdfperror_spt_los)
198 hold on
199 cdfplot(cdfperror_spt_b)
200 cdfplot(cdfperror_tt_los)
201 cdfplot(cdfperror_tt_b)
202 xlabel('Estimation Error (%)')
203 set(gca, 'fontsize', 14);
204 set(gca, 'XMinorTick', 'on');
205 set(gca, 'XGrid', 'on');
206 set(gca, 'YMinorTick', 'on');
207 set(gca, 'YGrid', 'on');
208 set(gca, 'LineWidth', .5);
209 lgd = legend('SpT-Los', 'SpT-NLoS', 'TT-Los', 'TT-NLoS');
210 lgd.Location = 'southeast';
211 lgd.Color='none';
212 lgd.FontSize=12;
213 lgd.Box='off';
214 matlab2tikz('cdfpw20.tex');
215
216 figure(7);
217 cdfplot(cdfderror_spt_los)
218 hold on
219 cdfplot(cdfderror_spt_b)

```

```

220 cdfplot(cdfderror_tt_los)
221 cdfplot(cdfderror_tt_b)
222 xlabel('Estimation Error (m)')
223 set(gca, 'fontsize', 14);
224 set(gca, 'XMinorTick', 'on');
225 set(gca, 'XGrid', 'on');
226 set(gca, 'YMinorTick', 'on');
227 set(gca, 'YGrid', 'on');
228 set(gca, 'LineWidth', .5);
229 lgd = legend('SpT-Los', 'SpT-NLoS', 'TT-Los', 'TT-NLoS');
230 lgd.Location = 'southeast';
231 lgd.Color='none';
232 lgd.FontSize=12;
233 lgd.Box='off';
234 matlab2tikz('cdfw20.tex');

```

### C.3 MATLAB Code Example for Chapter 7

```

1 clc;clear all;close all;
2 start_id=[34939, 22580, 50820, 17540, 30870];
3 distance_ground_truth=linspace(20,100,5);
4 data_len=100;
5 name1='0807';
6 name2='ep200k200ms01.bin';
7 for nm=1:5
8 filename = sprintf('%s%d%s',name1,distance_ground_truth(nm),name2);
9 data_15m_qt01=read_complex_binary (filename, 10000000,start_id(nm));
10
11 %% Data Extraction
12 for i=1:750
13     data_15m_qt_0((i-1)*data_len+1:i*data_len)= ...

```

```

14     data_15m_qt01((i-1)*1955+101:(i-1)*1955+100+data_len);
15
16 end
17 angle_15m_qt_f=angle(data_15m_qt_0)/2/pi*360;
18 %% Data cleaning and range estimation
19 mean_angel_15m_qt=zeros(1,750);
20 for j=1:750
21     if max(angle_15m_qt_f((j-1)*data_len+1:j*data_len)) ...
22         -min(angle_15m_qt_f((j-1)*data_len+1:j*data_len)) >170
23         for k =1:data_len
24             if angle_15m_qt_f((j-1)*data_len+k) <90
25                 angle_15m_qt_f((j-1)*data_len+k)= ...
26                     angle_15m_qt_f((j-1)*data_len+k)+180;
27             end
28         end
29     end
30     mean_angel_15m_qt(j)= ...
31         mean(angle_15m_qt_f((j-1)*data_len+1:j*data_len));
32 end
33 for j=1:750
34     mean_mag_15m_qt(j)=-10*log10(50)+ ...
35         20*log10(mean(abs(data_15m_qt_0((j-1)*data_len+1:j*data_len))));
36     mag_f(j,nm)=-10*log10(50)+ ...
37         20*log10(mean(abs(data_15m_qt_0((j-1)*data_len+1:j*data_len))));
38 end
39 diff_angel_15m_qt=zeros(1,749);
40 distance_25m_qt=zeros(1,749);
41 for m = 1:749
42     diff_angel_15m_qt(m)=mean_angel_15m_qt(m+1)-mean_angel_15m_qt(m);
43     if diff_angel_15m_qt(m) ≤ -50
44         diff_angel_15m_qt(m)=diff_angel_15m_qt(m)+180;
45     end
46 end

```



```

47 distance_uncal(nm)=5*mean(diff_angel_15m_qt(1:749))/720*300;
48 RSS_qt(nm) = mean(mean_mag_15m_qt);
49 angles=zeros(1,750);
50 angles(1)=mean_angel_15m_qt(1);
51 t=0;
52 for i=1:749
53     angles(i)=mod(mean_angel_15m_qt(i)+180*t,360);
54     if mean_angel_15m_qt(i+1)-mean_angel_15m_qt(i)<-30
55         t=t+1;
56     end
57 end
58
59 %% Calculate the normalized and un-normalized delay profile
60 x=10.^(mean_mag_15m_qt(1:750)/10).* ...
61 cos(-2*mean_angel_15m_qt(1:750)/180*pi)+ ...
62 1i*10.^(mean_mag_15m_qt(1:750)/10).* ...
63 sin(-2*mean_angel_15m_qt(1:750)/180*pi);
64 d= 3e8/150e6/4*linspace(1, 750, 2048);
65 x0=zeros(1,2048-750);
66 xx=[x x0];
67 delay_profile=abs(ifft(xx));
68 normalized_pro=delay_profile/max(delay_profile);
69 x1=cos(-angles(1:750)/180*pi)+1i.*sin(-angles(1:750)/180*pi);
70 d= 3e8/150e6/2*linspace(0, 750, 2048);
71 x0=zeros(1,2048-750);
72 xx=[x1 x0];
73 delay_profile=abs(ifft(xx));
74 [max_p distance_fft_wo_rss(nm)]=max(delay_profile);
75 distance_fft_wo_rss(nm)=distance_fft_wo_rss(nm)*d(2);
76 normalized_pro_wo_rss(:,nm)=delay_profile/max(delay_profile);
77 x1=10.^(mean_mag_15m_qt(1:750)/10).*cos(-angles(1:750)/180*pi)+ ...
78 1i.*10.^(mean_mag_15m_qt(1:750)/10).*sin(-angles(1:750)/180*pi);
79 d= 3e8/150e6/2*linspace(0, 750, 2048);

```

```

80 x0=zeros(1,2048-750);
81 xx=[x1 x0];
82 delay_profile=abs(iff(x));
83 normalized_pro_w_rss(:,nm)=delay_profile/max(delay_profile);
84 [max_p distance_fft_w_rss(nm)]=max(delay_profile);
85 distance_fft_w_rss(nm)=distance_fft_w_rss(nm)*d(2);
86 end
87 %% Plot the results
88 figure(1)
89 for kk =1:5
90 plot(d(1:500),10*log10(normalized_pro_wo_rss(1:500,kk)))
91 ylabel('Normalized Amplitude')
92 xlabel('Distance(m) ')
93 xlim([0 180])
94 xticks([0 20 40 60 80 100 120 140 160 180])
95 ylim([-45 0])
96 yticks([-40 -30 -20 -10 0])
97 legend('tag at 20m','tag at 40m','tag at 60m', ...
98 'tag at 80m','tag at 100m','Location','southeast')
99 grid on
100 hold on
101 end
102 matlab2tikz('delay_profile_wo_rss_ep.tex');
103
104 figure(2)
105 for kk=1:5
106 plot(d(1:500),10*log10(normalized_pro_w_rss(1:500,kk)))
107 ylabel('Normalized Amplitude')
108 xlabel('Distance(m) ')
109 xlim([0 180])
110 xticks([0 20 40 60 80 100 120 140 160 180])
111 ylim([-45 0])
112 yticks([-40 -30 -20 -10 0])

```

```

113 legend('tag at 20m','tag at 40m','tag at 60m', ...
114 'tag at 80m','tag at 100m','Location','southeast')
115 grid on
116 hold on
117 end
118 matlab2tikz('delay_profile_w_rss_ep.tex');
119
120 figure(3)
121 for kk =1:5
122 plot(mag_f)
123 hold on
124 legend('tag at 20m','tag at 40m','tag at 60m','tag at 80m', ...
125 'tag at 100m','Location','southeast')
126 ylabel('RSS (dBm)')
127 xlabel('Frequency Channel')
128 end
129 matlab2tikz('rss_ep.tex');
130 figure(4)
131 plot(distance_ground_truth,abs(distance_uncal- ...
132 distance_ground_truth-distance_uncal(1)+20),'d--')
133 hold on
134 plot(distance_ground_truth,abs(distance_fft_wo_rss- ...
135 distance_ground_truth-distance_fft_wo_rss(1)+20),'o-')
136 plot(distance_ground_truth,abs(distance_fft_w_rss- ...
137 distance_ground_truth-distance_fft_w_rss(1)+20),'*-.')
138 legend('RSP','FFT RSP','FFT Combined')
139 ylabel('Estimation Error (m)')
140 matlab2tikz('error_ep.tex');
141 xlabel('True Distance(m)')

```

## REFERENCES

- [1] F. Amato, C. W. Peterson, B. P. Degnan, and G. D. Durgin, "Tunneling RFID tags for long-range and low-power microwave applications," *IEEE Journal of Radio Frequency Identification*, vol. 2, no. 2, pp. 93–103, Jun. 2018.
- [2] M. Alhassoun, M. A. Varner, and G. D. Durgin, "Design and evaluation of a multi-modulation retrodirective RFID tag," in *2018 IEEE International Conference on RFID (RFID)*, 2018, pp. 1–8.
- [3] F. Amato, H. M. Torun, and G. D. Durgin, "RFID backscattering in long-range scenarios," *IEEE Transactions on Wireless Communications*, vol. 17, no. 4, pp. 2718–2725, Apr. 2018.
- [4] R. Zekavat and R. Buehrer, "Handbook of position location: Theory, practice, and advances," 2019.
- [5] Guolin Sun, Jie Chen, Wei Guo, and K. J. R. Liu, "Signal processing techniques in network-aided positioning: A survey of state-of-the-art positioning designs," *IEEE Signal Processing Magazine*, vol. 22, no. 4, pp. 12–23, 2005.
- [6] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of wireless indoor positioning techniques and systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 37, no. 6, pp. 1067–1080, 2007.
- [7] D. M. Dobkin, *The RF in RFID: UHF RFID in practice*. Newnes, 2012.
- [8] W. Liu, K. Huang, X. Zhou, and S. Durrani, "Next generation backscatter communication: Systems, techniques, and applications," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–11, 2019.
- [9] P. V. Nikitin, R. Martinez, S. Ramamurthy, H. Leland, G. Spiess, and K. V. S. Rao, "Phase based spatial identification of UHF RFID tags," in *2010 IEEE International Conference on RFID (IEEE RFID 2010)*, Apr. 2010, pp. 102–109.
- [10] M. Akbar, D. Taylor, and G. Durgin, "Hybrid inertial microwave reflectometry for mm-scale tracking in RFID systems," *IEEE Trans. Wireless Comm.*, vol. 14, no. 12, pp. 6805–6814, Dec. 2015.
- [11] M. B. Akbar, "Hybrid inertial microwave reflectometry for mm-scale tracking in RFID systems," Ph.D. dissertation, Georgia Institute of Technology, Atlanta, 2016.

- [12] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2347–2376, Oct. 2015.
- [13] R. Lodato and G. Marrocco, "Close integration of a UHF-RFID transponder into a limb prosthesis for tracking and sensing," *IEEE Sensors Journal*, vol. 16, no. 6, pp. 1806–1813, Mar. 2016.
- [14] S. Mirshahi, A. Akbari, and S. Uysal, "Implementation of structural health monitoring based on RFID and WSN," in *2015 IEEE 28th Canadian Conference on Electrical and Computer Engineering (CCECE)*, May 2015, pp. 1318–1323.
- [15] M. B. Akbar, C. Qi, M. Alhassoun, and G. D. Durgin, "Orientation sensing using backscattered phase from multi-antenna tag at 5.8 GHz," in *2016 IEEE International Conference on RFID (RFID)*, May 2016, pp. 1–8.
- [16] F. Amato, C. W. Peterson, M. B. Akbar, and G. D. Durgin, "Long range and low powered RFID tags with tunnel diode," in *2015 IEEE International Conference on RFID Technology and Applications (RFID-TA)*, Sep. 2015, pp. 182–187.
- [17] J. Griffin and G. Durgin, "Complete link budgets for backscatter-radio and RFID systems," *Antennas and Propag. Magazine, IEEE*, vol. 51, no. 2, pp. 11–25, Apr. 2009.
- [18] F. Amato, "Achieving hundreds-meter ranges in low powered RFID systems with quantum tunneling tags," Ph.D. dissertation, Georgia Institute of Technology, Atlanta, 2017.
- [19] C. Qi, F. Amato, M. Alhassoun, and G. D. Durgin, "Breaking the range limit of RFID localization: Phase-based positioning with tunneling tags," in *2019 IEEE International Conference on RFID (RFID)*, Apr. 2019, pp. 1–8.
- [20] C. Zhou and J. D. Griffin, "Phased-based composite ranging for backscatter RF tags: System analysis and measurements," *IEEE Transactions on Antennas and Propagation*, vol. 66, no. 8, pp. 4202–4212, Aug. 2018.
- [21] G. M. Djuknic and R. E. Richton, "Geolocation and assisted GPS," *Computer*, vol. 34, no. 2, pp. 123–125, Feb. 2001.
- [22] A. Motroni, A. Buffi, and P. Nepa, "A survey on indoor vehicle localization through RFID technology," *IEEE Access*, vol. 9, pp. 17 921–17 942, 2021.
- [23] S. Park and S. Hashimoto, "An intelligent localization algorithm using read time of RFID system," *Advanced Engineering Informatics*, vol. 24, no. 4, pp. 490–497, 2010, Construction Informatics.

- [24] D. Boontrai, T. Jingwangsa, and P. Cherntanomwong, "Indoor localization technique using passive RFID tags," in *2009 9th International Symposium on Communications and Information Technology*, Sep. 2009, pp. 922–926.
- [25] X. Yinggang, K. JiaoLi, W. ZhiLiang, and Z. Shanshan, "Indoor location technology and its applications base on improved LANDMARC algorithm," in *2011 Chinese Control and Decision Conference (CCDC)*, May 2011, pp. 2453–2458.
- [26] M. Bouet and G. Pujolle, "L-VIRT: Range-free 3-D localization of RFID tags based on topological constraints," *Computer Communications*, vol. 32, no. 13, pp. 1485–1494, 2009.
- [27] L. M. Ni, Yunhao Liu, Yiu Cho Lau, and A. P. Patil, "LANDMARC: Indoor location sensing using active RFID," in *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, 2003. (PerCom 2003).*, 2003, pp. 407–415.
- [28] H. Jiang, C. Peng, and J. Sun, "Deep belief network for fingerprinting-based RFID indoor localization," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 2019, pp. 1–5.
- [29] R. Psiuk, A. Müller, T. Dräger, I. Ibrahim, H. Brauer, H. Töpfer, and A. Heuberger, "Simultaneous 2D localization of multiple coils in an LF magnetic field using orthogonal codes," in *2017 IEEE SENSORS*, Oct. 2017, pp. 1–3.
- [30] K. Chawla, C. McFarland, G. Robins, and C. Shope, "Real-time RFID localization using RSS," in *2013 International Conference on Localization and GNSS (ICL-GNSS)*, Jun. 2013, pp. 1–6.
- [31] D. A. Savochkin, "Simple approach for passive RFID-based trilateration without offline training stage," in *2014 IEEE RFID Technology and Applications Conference (RFID-TA)*, Sep. 2014, pp. 159–164.
- [32] Y. Ma, C. Tian, and Y. Jiang, "A multitag cooperative localization algorithm based on weighted multidimensional scaling for passive uhf rfid," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6548–6555, 2019.
- [33] Y. Zhao, Y. Liu, and L. M. Ni, "VIRE: Active RFID-based localization using virtual reference elimination," in *2007 International Conference on Parallel Processing (ICPP 2007)*, Sep. 2007, pp. 56–56.
- [34] I. Cnaan-On, S. J. Thomas, J. L. Krolik, and M. S. Reynolds, "Multichannel backscatter communication and ranging for distributed sensing with an FMCW radar," *IEEE Transactions on Microwave Theory and Techniques*, vol. 63, no. 7, pp. 2375–2383, 2015.

- [35] A. Motroni, P. Nepa, A. Buffi, and B. Tellini, "A phase-based method for mobile node localization through uhf-rfid passive tags," in *2019 IEEE International Conference on RFID Technology and Applications (RFID-TA)*, 2019, pp. 470–475.
- [36] S. Azzouzi, M. Cremer, U. Dettmar, R. Kronberger, and T. Knie, "New measurement results for the localization of UHF RFID transponders using an angle of arrival (AoA) approach," in *2011 IEEE International Conference on RFID*, Apr. 2011, pp. 91–97.
- [37] M. Cremer, U. Dettmar, C. Hudasch, R. Kronberger, R. Lerche, and A. Pervez, "Localization of passive UHF RFID tags using the AoA transmitter beamforming technique," *IEEE Sensors Journal*, vol. 16, no. 6, pp. 1762–1771, Mar. 2016.
- [38] C. Duan, X. Rao, L. Yang, and Y. Liu, "Fusing RFID and computer vision for fine-grained object tracking," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, May 2017, pp. 1–9.
- [39] Z. Wang, M. Xu, N. Ye, R. Wang, and H. Huang, "RF-MVO: Simultaneous 3D object localization and camera trajectory recovery using RFID devices and a 2D monocular camera," in *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, Jul. 2018, pp. 534–544.
- [40] M. Hasani, J. Talvitie, L. Sydänheimo, E. Lohan, and L. Ukkonen, "Hybrid WLAN-RFID indoor localization solution utilizing textile tag," *IEEE Antennas and Wireless Propagation Letters*, vol. 14, pp. 1358–1361, 2015.
- [41] N. Y. Keong, K. S. Chieh, M. F. Burhan, N. Balasubramaniam, and N. M. Din, "RFID and ZigBee integrated environment for indoor localization," in *2014 4th International Conference on Engineering Technology and Technopreneuship (ICE2T)*, Aug. 2014, pp. 213–217.
- [42] J. Chai, C. Wu, C. Zhao, H.-L. Chi, X. Wang, B. W.-K. Ling, and K. L. Teo, "Reference tag supported RFID tracking using robust support vector regression and kalman filter," *Advanced Engineering Informatics*, vol. 32, pp. 1–10, 2017.
- [43] Q. Yang, D. G. Taylor, and G. D. Durgin, "Kalman filter based localization and tracking estimation for HIMR RFID systems," in *2018 IEEE International Conference on RFID (RFID)*, Apr. 2018, pp. 1–5.
- [44] X. Zhuang, X. Yu, D. Zhou, Z. Zhao, W. Zhang, L. Li, and Z. Liu, "A novel 3D position measurement and structure prediction method for RFID tag group based on deep belief network," *Measurement*, vol. 136, pp. 25–35, 2019.
- [45] G. Koo, "Signal constellation of a retrodirective array phase modulator," M.S. thesis, Georgia Institute of Technology, Elect. and Comp. Eng., Atlanta, GA, 2011.

- [46] J. Cespedes, F. Giuppi, A. Collado, and A. Georgiadis, "A retro-directive UHF RFID tag on paper substrate," in *2012 IEEE International Conference on RFID-Technologies and Applications (RFID-TA)*, Nov. 2012, pp. 263–266.
- [47] M. M. Islam, K. Rasilainen, S. K. Karki, and V. Viikari, "Designing a passive retrodirective wireless sensor," *IEEE Antennas and Wireless Propagation Letters*, vol. 16, pp. 1739–1742, 2017.
- [48] L. C. Van Atta, "Electromagnetic reflector," 2 908 002, Oct. 1959.
- [49] A. Povalac and J. Sebesta, "Phase difference of arrival distance estimation for rfid tags in frequency domain," in *2011 IEEE International Conference on RFID-Technologies and Applications*, 2011, pp. 188–193.
- [50] C. Qi, Q. Frederick, K. Davis, D. Lindsay, J. Cox, S. Parke, J. D. Griffin, and G. D. Durgin, "A 5.8 GHz energy harvesting tag for sensing applications in space," in *2018 6th IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE)*, Dec. 2018, pp. 218–223.
- [51] *Near space launch*, <https://nearspacelaunch.com/>, Accessed Aug. 15, 2018.
- [52] I. Mayordomo, R. Berenguer, A. Garcia-Alonso, I. Fernandez, and Í. Gutierrez, "Design and implementation of a long-range RFID reader for passive transponders," *IEEE Transactions on Microwave Theory and Techniques*, vol. 57, no. 5, pp. 1283–1290, May 2009.
- [53] I. Kwon, Y. Eo, H. Bang, K. Choi, S. Jeon, S. Jung, D. Lee, and H. Lee, "A single-chip CMOS transceiver for UHF mobile RFID reader," *IEEE Journal of Solid-State Circuits*, vol. 43, no. 3, pp. 729–738, Mar. 2008.
- [54] G. Durgin, C. Valenta, M. Akbar, M. Morys, B. Marshall, and Y. Lu, "Modulation and sensitivity limits for backscatter receivers," in *Proc. IEEE RFID Int. Conf.*, Apr. 2013, pp. 124–130.
- [55] F. Yang, X.-X. Zhang, X. Ye, and Y. Rahmat-Samii, "Wide-band E-shaped patch antennas for wireless communications," *IEEE Transactions on Antennas and Propagation*, vol. 49, no. 7, pp. 1094–1100, Jul. 2001.
- [56] C. Qi, P. Hillyard, A. Al-Husseiny, N. Patwari, and G. D. Durgin, "On-wall, wide bandwidth E-shaped patch antenna for improved whole-home radio tomography," *IEEE Journal of Radio Frequency Identification*, vol. 1, no. 1, pp. 22–31, Mar. 2017.



- [57] R. R. Ramirez and F. D. Flaviis, “A mutual coupling study of linear and circular polarized microstrip antennas for diversity wireless systems,” *IEEE Transactions on Antennas and Propagation*, vol. 51, no. 2, pp. 238–248, Feb. 2003.
- [58] A. Boaventura, J. Santos, A. Oliveira, and N. B. Carvalho, “Perfect isolation: Dealing with self-jamming in passive RFID systems,” *IEEE Microwave Magazine*, vol. 17, no. 11, pp. 20–39, Nov. 2016.
- [59] K. Lin, Y. E. Wang, C. Pao, and Y. Shih, “Aka-band FMCW radar front-end with adaptive leakage cancellation,” *IEEE Transactions on Microwave Theory and Techniques*, vol. 54, no. 12, pp. 4041–4048, Dec. 2006.
- [60] C. Y. Chiu, C. H. Cheng, R. D. Murch, and C. R. Rowell, “Reduction of mutual coupling between closely-packed antenna elements,” *IEEE Transactions on Antennas and Propagation*, vol. 55, no. 6, pp. 1732–1738, Jun. 2007.
- [61] U.S. National Archives and Records Administration, *Code of Federal Regulations*. Title 47, Chapter 1, Sub-Chapter A, Part 15: Radio Frequency Devices, 2018.
- [62] R. Corless, “Part 15 compliant frequency hopping backscatter communication at 5.8 GHz,” M.S. thesis, Georgia Institute of Technology, Atlanta, GA, 2018.
- [63] A. P. Sample, D. J. Yeager, P. S. Powledge, A. V. Mamishev, and J. R. Smith, “Design of an RFID-based battery-free programmable sensing platform,” *IEEE Transactions on Instrumentation and Measurement*, vol. 57, no. 11, pp. 2608–2615, Nov. 2008.
- [64] D. D. Donno, L. Catarinucci, and L. Tarricone, “An UHF RFID energy-harvesting system enhanced by a DC-DC charge pump in silicon-on-insulator technology,” *IEEE Microwave and Wireless Components Letters*, vol. 23, no. 6, pp. 315–317, Jun. 2013.
- [65] C. R. Valenta and G. D. Durgin, “Harvesting wireless power: Survey of energy-harvester conversion efficiency in far-field, wireless power transfer systems,” *IEEE Microwave Magazine*, vol. 15, no. 4, pp. 108–120, Jun. 2014.
- [66] C. H. P. Lorenz, S. Hemour, and K. Wu, “Physical mechanism and theoretical foundation of ambient RF power harvesting using zero-bias diodes,” *IEEE Transactions on Microwave Theory and Techniques*, vol. 64, no. 7, pp. 2146–2158, Jul. 2016.
- [67] C. Wang, N. Shinohara, and T. Mitani, “Study on 5.8-GHz single-stage charge pump rectifier for internal wireless system of satellite,” *IEEE Transactions on Microwave Theory and Techniques*, vol. 65, no. 4, pp. 1058–1065, Apr. 2017.
- [68] G. Durgin, *Space-Time Wireless Channels*. Upper Saddle River, NJ: Pearson, 2003.

- [69] J. Högbom, “Aperture synthesis with a non-regular distribution of interferometer baselines,” *Astronomy and Astrophysics Supplement Series*, vol. 15, p. 417, 1974.
- [70] T. C. .- Liu, D. I. Kim, and R. G. Vaughan, “A high-resolution, multi-template deconvolution algorithm for time-domain UWB channel characterization,” in *2007 Canadian Conference on Electrical and Computer Engineering*, Apr. 2007, pp. 1183–1186.
- [71] R. G. Vaughan and N. L. Scott, “Super-resolution of pulsed multipath channels for delay spread characterization,” *IEEE Transactions on Communications*, vol. 47, no. 3, pp. 343–347, 1999.
- [72] C. Qi, J. D. Griffin, and G. D. Durgin, “Low-power and compact microwave RFID reader for sensing applications in space,” in *2018 IEEE International Conference on RFID Technology Application (RFID-TA)*, Sep. 2018, pp. 1–6.
- [73] C. Qi, R. W. Corless, J. D. Griffin, and G. D. Durgin, “Low-power and compact frequency hopping RFID reader at 5.8 GHz for sensing applications in space,” *IEEE Journal of Radio Frequency Identification*, vol. 3, no. 3, pp. 133–142, Sep. 2019.
- [74] M. C. Budge and M. P. Burt, “Range correlation effects on phase and amplitude noise,” in *Proceedings of Southeastcon '93*, 1993, pp. 5–9.
- [75] J.-H. Bae, J.-C. Kim, B.-W. Jeon, J.-W. Jung, J.-S. Park, B.-J. Jang, H.-R. Oh, Y.-J. Moon, and Y.-R. Seong, “Analysis of phase noise requirements on local oscillator for rfid system considering range correlation,” in *2007 European Radar Conference*, 2007, pp. 385–388.
- [76] P. Hillyard, C. Qi, A. Al-Husseiny, G. D. Durgin, and N. Patwari, “Focusing through walls: An E-shaped patch antenna improves whole-home radio tomography,” in *2017 IEEE Int. Conf. on RFID (RFID)*, May 2017, pp. 174–181.
- [77] J. Li, Z. Zeng, J. Sun, and F. Liu, “Through-wall detection of human being’s movement by UWB radar,” *IEEE Geoscience and Remote Sensing Letters*, vol. 9, no. 6, pp. 1079–1083, Nov. 2012.
- [78] J. Wilson and N. Patwari, “See-through walls: Motion tracking using variance-based radio tomography networks,” *IEEE Trans. Mobile Comput.*, vol. 10, no. 5, pp. 612–621, May 2011.
- [79] J. Peabody Jr, G. L. Charvat, J. Goodwin, and M. Tobias, “Through-wall imaging radar,” Massachusetts Institute of Technology-Lincoln Laboratory Lexington United States, Tech. Rep., 2012.

- [80] M. G. Amin and F. Ahmad, “Chapter 17 - through-the-wall radar imaging: Theory and applications,” in *Academic Press Library in Signal Processing: Volume 2*, ser. Academic Press Library in Signal Processing, N. D. Sidiropoulos, F. Gini, R. Chellappa, and S. Theodoridis, Eds., vol. 2, Elsevier, 2014, pp. 857–909.
- [81] Y. Ma, L. Zhou, K. Liu, and J. Wang, “Iterative phase reconstruction and weighted localization algorithm for indoor RFID-based localization in NLOS environment,” *IEEE Sensors J.*, vol. 14, no. 2, pp. 597–611, Feb. 2014.
- [82] S. Zhang, C. Yang, D. Jiang, X. Kui, S. Guo, A. Y. Zomaya, and J. Wang, “Nothing blocks me: Precise and real-time LOS/NLOS path recognition in RFID systems,” *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5814–5824, Jun. 2019.
- [83] M. A. Koledoye, T. Facchinetti, and L. Almeida, “Mitigating effects of NLOS propagation in MDS-based localization with anchors,” in *2018 IEEE Int. Conf. on Autonomous Robot Systems and Competitions (ICARSC)*, Apr. 2018, pp. 148–153.
- [84] M. A. Koledoye, T. Facchinetti, and L. Almeida, “Improved MDS-based localization with non-line-of-sight RF links,” *Journal of Intelligent & Robotic Systems*, Apr. 2019.
- [85] C. Qi, F. Amato, M. Alhassoun, and G. D. Durgin, “A phase-based ranging method for long-range RFID positioning with quantum tunneling tags,” *IEEE Journal of Radio Frequency Identification*, pp. 1–1, 2020.
- [86] C. Qi, F. Amato, B. Kihei, and G. D. Durgin, “Fine-scale through-wall positioning using tunneling RFID tags,” in *2020 IEEE International Conference on RFID (RFID)*, 2020, pp. 1–7.
- [87] A. Varshney, A. Soleiman, and T. Voigt, “Tunnelscatter: Low power communication for sensor tags using tunnel diodes,” in *The 25th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom ’19, Los Cabos, Mexico: Association for Computing Machinery, 2019, ISBN: 9781450361699.
- [88] L. Esaki, “New phenomenon in narrow germanium p-n junctions,” *Phys. Rev.*, vol. 109, no. 2, pp. 603–604, Jan. 1958.
- [89] F. Farzami, S. Khaledian, B. Smida, and D. Erricolo, “Reconfigurable dual-band bidirectional reflection amplifier with applications in Van Atta array,” *IEEE Trans. Microw. Theory Tech.*, vol. 65, no. 11, pp. 4198–4207, Nov. 2017.
- [90] Ettus Research, *USRP N200 software defined radio (SDR)*, <https://www.ettus.com/all-products/un200-kit/>, (Accessed Feb. 02, 2021).

- [91] GNU Radio, *GNU radio the free & open source radio ecosystem*, <https://www.gnuradio.org/>, (Accessed Feb. 03, 2021).
- [92] G. Goertzel, “An algorithm for the evaluation of finite trigonometric series,” *The American Mathematical Monthly*, vol. 65, no. 1, pp. 34–35, 1958.
- [93] R. Beck, A. G. Dempster, and I. Kale, “Finite-precision goertzel filters used for signal tone detection,” *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 48, no. 7, pp. 691–700, 2001.
- [94] Q. Yang, D. G. Taylor, M. B. Akbar, and G. D. Durgin, “Analysis of kalman filter-based localization for HIMR RFID systems,” *IEEE Journal of Radio Frequency Identification*, vol. 3, no. 3, pp. 164–172, 2019.
- [95] W. Newhall, T. Rappaport, and D. Sweeney, *A spread spectrum sliding correlator system for propagation measurements*, Apr. 1996.
- [96] Z. Latinović, C. Geng, and H. Huang, “Channel measurements and performance of indoor time-of-arrival localization at 5GHz,” in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, IEEE, 2018, pp. 1–6.
- [97] R. J. Pirkl and G. D. Durgin, “Optimal sliding correlator channel sounder design,” *IEEE Transactions on Wireless Communications*, vol. 7, no. 9, pp. 3488–3497, 2008.
- [98] C. J. Durkin, R. J. Pirkl, A. J. Trzeciecki, and G. D. Durgin, “Broadband spatio-temporal channel sounder for the 2.4 GHz ISM band,” Georgia Institute of Technology, Tech. Rep., 2006.
- [99] C. R. Anderson, “Design and implementation of an ultrabroadband millimeter-wavelength vector sliding correlator channel sounder and in-building multipath measurements at 2.5 & 60 GHz,” Ph.D. dissertation, Virginia Tech, 2002.
- [100] C. Geng, X. Yuan, and H. Huang, “Exploiting channel correlations for NLoS ToA localization with multivariate gaussian mixture models,” *IEEE Wireless Communications Letters*, vol. 9, no. 1, pp. 70–73, 2020.
- [101] IXYS, *IXOLAR high efficiency solarBIT*. Accessed Oct. 18, 2020.
- [102] Texas Instrument, *Design files*, <https://www.ti.com/tool/LAUNCHXL-F28027>, Accessed Apr. 05, 2021.
- [103] Cheng Qi, *Positioning using tunneling tags*, <https://github.com/navelorange93/Positioning-Using-Tunneling-Tags>, (Accessed Apr. 28, 2021).

## VITA

Cheng Qi received the B.S. (2014) and M.S. (2015) degrees from Tianjin University and Georgia Institute of Technology. In 2015, he joined the Propagation Group at Georgia Tech as a graduate research assistant, where he pursues the Ph.D. degree.

His research focuses on antenna design, RFID system design, long-range backscatter communication, space solar power harvesting, and RFID localization technology. He has authored or co-authored more than 12 technical papers and presented his work in multiple international conferences. He received the best paper award for the article presented at the IEEE RFID Conference (2019) and the best student paper award for the paper presented at IEEE RFID-TA Conference (2018). He is a recipient of the William C. Brown Fellowship (2017), a winner of the People's Choice Award in NSF Innovation Corps program (2018) in San Francisco, and the winner of first place Ph.D. mentor in Opportunity Research Scholar (ORS) program at Georgia Tech (2018). He is also the winner of the Third Prize of the Bell Labs Prize (2020). He has served as a poster session chair and a technical program committee member for the IEEE RFID conference since 2018.