COMPARISON OF ZIGBEE REPLAY ATTACKS USING A UNIVERSAL SOFTWARE RADIO PERIPHERAL AND USB RADIO

THESIS

Scott D. Dalrymple, Captain, USAF

AFIT-ENG-14-M-23

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

DISTRIBUTION STATEMENT A:
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the United States Government.

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

AFIT-ENG-14-M-23

COMPARISON OF ZIGBEE REPLAY ATTACKS USING A UNIVERSAL SOFTWARE RADIO PERIPHERAL AND USB RADIO

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Master of Science in Computer Engineering

Scott D. Dalrymple, B.S.Cp.E.

Captain, USAF

March 2014

DISTRIBUTION STATEMENT A:
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AFIT-ENG-14-M-23

COMPARISON OF ZIGBEE REPLAY ATTACKS USING A UNIVERSAL SOFTWARE RADIO PERIPHERAL AND USB RADIO

Scott D. Dalrymple, B.S.Cp.E.
Captain, USAF

Approved:

//signed//	10 Mar 2014
Barry E. Mullins, PhD (Chairman)	Date
//signed//	10 Mar 2014
Maj Jonathan W. Butts, PhD (Member)	Date
//signed//	10 Mar 2014
Timothy H. Lacey, PhD (Member)	Date

Abstract

Low-Rate Wireless Personal Area Networks are a prevalent solution for communication among embedded devices. ZigBee is a leading network protocol stack based on the low-rate IEEE 802.15.4 standard that operates smart utility meters, residential and commercial building automation, and heath care networks. Such networks are essential, but low-rate, low-cost hardware is challenging to protect because end devices have tight limitations on hardware cost, memory use, and power consumption. KillerBee is a python-based framework for attacking ZigBee and other 802.15.4 networks that makes traffic eavesdropping, packet replay, and denial of service attacks straightforward to conduct. Recent works investigate software-defined radios as an even more versatile attack platform. Software defined radios can operate with greater flexibility and at greater transmit power than traditional network hardware. Software-defined radios also enable novel physical-layer attacks including reflexive jamming and synchronization header manipulation that are not possible with traditional hardware.

This research implements a replay attack against a ZigBee device using a software defined radio. Replay attacks consist of an attacker recording legitimate traffic on a network and then replaying that traffic at will to cause malicious effects. Replay attacks can be very disruptive to operational systems, from turning valves in industrial controls systems to disarming door locks. Specifically, how software-defined radios can extend the effective attack range far beyond what is possible with hardware currently utilized by KillerBee is investigated.

A software defined radio is tested with both directed and omnidirectional antennas and the effective attack range is compared to that of a USB radio. Tests are conducted both line-of-sight outdoors and through interior walls. The replay attack is implemented with

beacon request frames. Legitimate beacon request frames are prerecorded with the software defined radio, and at a later time, replayed against a target device. Results demonstrate that, in addition to being a more versatile attack platform, software-defined radios extend the effective wireless attack range beyond that of fixed KillerBee hardware.

Acknowledgments

I would like to thank my advisor, Dr. Barry Mullins for his support and guidance throughout this thesis. I would also like to thank Capt Ben Ramsey for his support in getting me started with ZigBee.

Thank you to my wife for all her support and late night dinners in the student lounge.

Scott D. Dalrymple

Table of Contents

Page

Page

List of Figures

Figure Page

List of Tables

Table Page

Table Page

List of Symbols

Symbol	Definition
P	power (dbm)
$RSSI$	received signal strength indication

List of Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
APL	application
APS	application support sublayer
CBC-MAC	cipher block chaining message authentication code
CCM	counter with cipher block chaining message authentication code (CBC-MAC)
CPU	central processing unit
CUT	component under test
db	decibel
dbm	decibel referenced to one milliwatt
FFD	full-fuction device
IPv6	Internet protocol version six
JTAG	Joint Test Action Group
LED	light emitting diode
LR-WPAN	low-rate wireless personal area network
MAC	medium access control
MIC	Message Integrity Code
NWK	network
PAN	personal area network
PHY	physical layer
RAM	random access memory
RF	radio frequency
RF4CE	Radio Frequency for Consumer Electronics

Acronym	Definition
RFD	reduced-function device
RSSI	received signal strength indication
RZUSBSTICK	Atmel RZ Raven universal serial bus (USB) stick
SDR	software defined radio
SUT	system under test
TC	Trust Center
UHD	USRP Hardware Driver
USB	universal serial bus
USRP	universal software radio peripheral
ZDO	ZigBee Device Object

COMPARISON OF ZIGBEE REPLAY ATTACKS USING A
UNIVERSAL SOFTWARE RADIO PERIPHERAL AND USB RADIO

I. Introduction

1.1 Motivation

As the world becomes increasingly interconnected, low power communication solutions are necessary for embedded devices. One such solution is the ZigBee protocol. ZigBee is commonly used in home automation, health care networks, and the smart energy grid. However, with demands for low power consumption being paramount, security concerns are often secondary. Some developer guides discourage the use of security. A recent study shows several in-use ZigBee networks operate in an insecure state [RMSB13]. software defined radio (SDR) is a field of study of increasing interest; it allows for one set of hardware to switch between multiple implementations. This could allow for a single platform to test the attack surface of multiple protocols.

1.2 Research Goals

The goal of this research is to determine the viability of using a SDR, specifically National Instrument's $1,700 USRP, as a tool for exploring and attacking ZigBee and other 802.15.4 networks [ER14]. By looking at replay attacks, this research intends to demonstrate range improvements of SDR over 802.15.4 USB radios. This research investigates the feasibility of the USRP as a tool for exploring and attacking ZigBee and other 802.15.4 networks. Performance is evaluated by comparing success rates and power. The Atmel Atmel RZ Raven USB stick (RZUSBSTICK), a $40 802.15.4 USB radio, is

chosen because it is the recommended hardware for use with the KillerBee attack suite [CWL10]. Due to superior transmission power, the USRP is expected to achieve a higher success rate at greater distances than the RZUSBSTICK.

1.3 Thesis Layout

This chapter introduced the motivation and goals of this thesis. Chapter 2 gives background on ZigBee, USRP, and GNU Radio as well as related work in ZigBee security and ZigBee using GNU Radio. Chapter 3 details the experiment conducted during this thesis. Chapter 4 discusses and analyzes the results of the experiments detailed in Chapter 3. Chapter 5 presents conclusions and guidance for future work.

II. Background

This chapter discusses the ZigBee protocol and the threats against it. Section 2.1 details the ZigBee protocol and how it works. Section 2.2 discusses current attacks against ZigBee. Section 2.3 discusses SDR and attempts to implement ZigBee on the USRP.

2.1 ZigBee

2.1.1 ZigBee Functionality.

ZigBee is a wireless protocol based on IEEE standard 802.15.4. The standard is intended for the creation of low-rate wireless personal area networks (LR-WPANs) for devices that require low complexity, cost, power consumption, and connectivity (e.g., embedded devices) [80211]. The ZigBee protocol itself is maintained by a non-profit association of businesses, universities, and government agencies known as the ZigBee Alliance [Zig13].

2.1.1.1 Radio Frequency Bands.

IEEE standard 802.15.4 defines several sets of radio frequency bands to communicate. The main frequency range used is 2400-2483.5 MHz; however, 868-868.6 MHZ and 902-928 MHz are also defined in the 802.15.4 standard. In China, 314-316 MHz, 430-434 MHz, and 779-787 MHz ranges are allowed while, in Japan, the 950-956 MHz band is defined for use in 802.15.4 networks [80211].

As shown in Figure 2.1, networks using the 802.15.4 standard operate over 27 possible channels. The 868 MHz frequency band only contains channel 0. The 902 MHz band contains 10 channels, numbered 1 to 10. The 2400 MHz frequency band contains 16 channels, numbered 11 through 26 [80211]. ZigBee specifically operates in the 2400 MHz band, using channels 11 through 26. This is due to a lack of speed in the sub 1 GHz bands [Gis08].

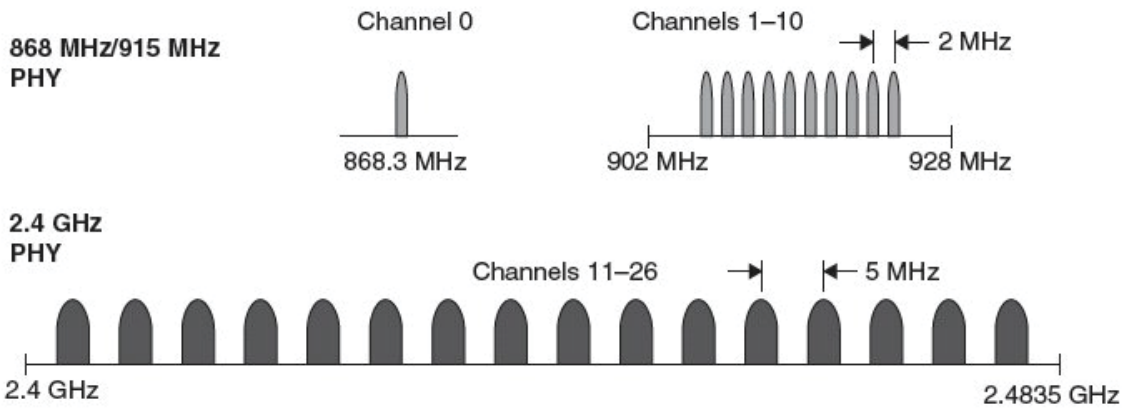


Figure 2.1: The 802.15.4 Frequency Bands [LLC14]

2.1.2 Current Uses.

The ZigBee Alliance offers three different specifications: ZigBee, ZigBee IP, and ZigBee Radio Frequency for Consumer Electronics (RF4CE). The core ZigBee specification is further split into two feature sets, ZigBee and ZigBee PRO. The main difference between the two is the number of devices a network can include. Also, ZigBee PRO includes some optimizations over ZigBee such as improved battery-free support and traffic load capacity. ZigBee PRO is the more popular feature set due to increased functionality [Zig13]. The ZigBee IP specification is an open standard Internet protocol version six (IPv6) based mesh networking solution. It is designed to support the ZigBee Smart Energy standard, and is intended to provide seamless Internet connectivity to low-power devices.

The ZigBee RF4CE specification is designed to be simpler than the core ZigBee standard; it is used in simple two-way device connections that do not need a full mesh network, thus requiring less resources and reducing implementation costs [Zig13].

The ZigBee Alliance also offers ten standards, each for a specific use of ZigBee. They include ZigBee Building Automation, Remote Control, Smart Energy, Smart Energy

Profile 2, Health Care, Home Automation, Input Device, Light Link, Retail Services, Telecom Services, and Network Devices. ZigBee devices can be used in applications ranging from light emitting diode (LED) and light control to communication between health care devices and the Smart Energy Grid [Zig13].

2.1.3 Topologies.

ZigBee devices are categorized into two different types: full-fuction devices (FFDs) and reduced-function devices (RFDs). The difference between an FFD and an RFD is that the FFD can act as a coordinator and communicate with any node within the network. RFDs can only communicate with a single FFD [Gis08]. A coordinator is a device that provides synchronization to other devices in the LR-WPAN. While a LR-WPAN can have multiple coordinators, there is a single personal area network (PAN) coordinator that controls the network. The PAN coordinator is responsible for network and security management, and each 802.15.4 network must have at least one PAN coordinator [80211].

ZigBee devices can be configured to communicate in either a star network or a peer-to-peer network. In a star network, peripheral devices can only communicate with the PAN coordinator. In a peer-to-peer network, FFDs can talk to any other FFDs within range, while RFDs can only talk to the FFD with which they are associated. Multiple peer-to-peer networks can be joined together to form mesh networks [80211].

2.1.4 ZigBee Stack.

As shown in Figure 2.2, ZigBee contains four layers in its stack. The 802.15.4 standard defines the physical layer (PHY) and medium access control (MAC) layers [80211]. The ZigBee Alliance, a collection of companies that implement the ZigBee stack, define the network (NWK) and application (APL) layers. Within the APL layer, the ZigBee Alliance further defines an application support sublayer (APS), a ZigBee Device Object (ZDO), and application objects.

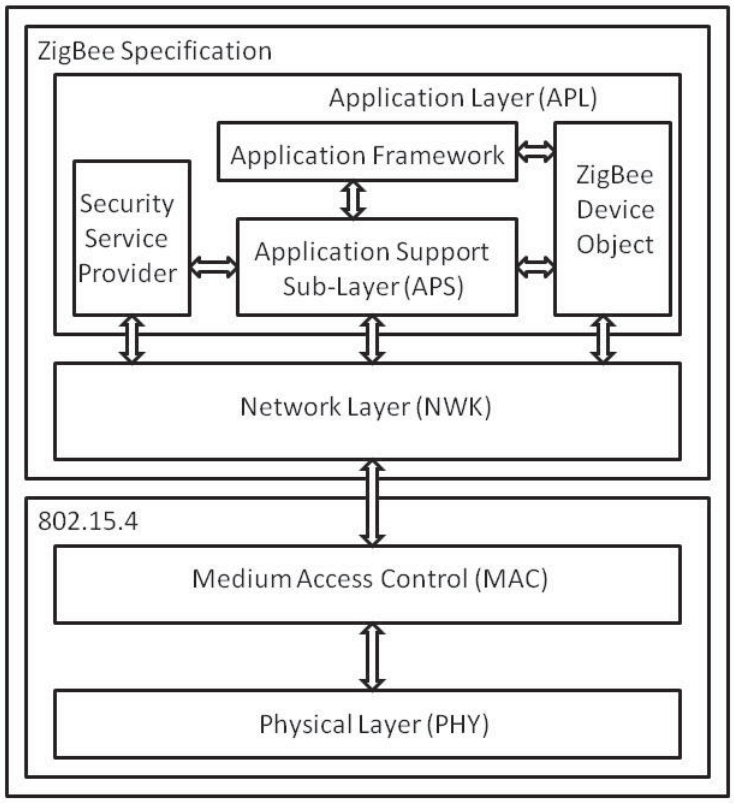


Figure 2.2: The ZigBee Stack. Adapted from [Gis08]

2.1.4.1 Physical (PHY).

The PHY layer consists of devices' radio frequency (RF) transceivers. The PHY layer provides services such as activation and deactivation of the radio transceiver, channel selection, clear channel assessment, and transmitting and receiving packets [80211].

2.1.4.2 Medium Access Control (MAC).

The MAC layer provides several features. They include beacon management, channel access, frame validation, acknowledged frame delivery, association, and disassociation [80211]. However, ZigBee does not use all of the services offered by the IEEE 802.15.4 standard. For example, it does not use guaranteed time slots. This allows

ZigBee to be more flexible and less resource intensive depending on each vendor's implementation [Gis08].

2.1.4.3 Network (NWK).

The NWK layer is the lowest layer defined solely by the ZigBee protocol. Networks are formed by ZigBee Coordinators at the NWK layer. For a ZigBee Coordinator to form a network, it first must determine if there are other networks in range. This is accomplished with a beacon request frame. Any ZigBee nodes within range must reply with a beacon frame. The ZigBee Coordinator can then decide whether it wants to join an existing network, or create a new one. The parameters of the network it wants to create includes the channel(s), PAN ID, and security level. The beacon request frame also ensures that a new network will not be set up with a conflicting PAN ID [Gis08].

2.1.4.4 Application Layer (APL).

The APL is split into four parts: the application support sublayer (APS), a ZigBee Device Object (ZDO), application objects, and security services. The APS acts as an interface between device applications and ZigBee. The APS is the layer that offers end-to-end acknowledgment of data. The APS allows one ZigBee device to bind to another. This is what denotes a connection [Gis08]. The APL also includes the security services inherent in ZigBee as discussed in Section 2.1.5 [Gis08].

The ZDO is the part of the APL that keeps track of the state of the ZigBee device. It also interacts with the NWK layer. It decides when to form, join, or leave a network. It acts as an application interface between the NWK layer and the APL [Gis08].

2.1.5 ZigBee Security.

2.1.5.1 Security Modes.

The ZigBee PRO feature set has two security modes, high security and standard security; whereas the ZigBee feature set only has standard security mode. The difference

between the two security modes involves key management and distribution. Standard security is designed for use in residential situations. Standard security allows in-band unsecured key transport [YNN08]. That is, in standard security mode network keys are allowed to traverse the network during rekeying [VHnA+13]. In high security mode, a list of all keys in use on the network is maintained and keys are not allowed to traverse the network unencrypted [YNN08].

2.1.5.2 Trust Center.

The main concept of ZigBee security revolves around the Trust Center (TC). The TC is an application that all devices in the network trust. It is set up by the PAN coordinator and, by default, runs on the PAN coordinator. In standard security mode, the TC controls the network key and network admittance policies. In high security mode, the TC must in addition maintain a list of all devices in the network and all relevant keys [YNN08].

2.1.5.3 Keys.

ZigBee defines three keys: Link Key, Network Key, and Master Key. A Link Key is shared between two devices that want to communicate. A Network Key is shared by all devices on a network and is used in broadcast communications. A Master Key is shared by a device and the TC for key establishment and rekeying purposes. A Master Key is also sometimes called a Transport Key [YNN08] [DT10].

2.1.5.4 Security Levels.

ZigBee uses Advanced Encryption Standard (AES) to optionally secure communications with a security mechanism known as counter with CBC-MAC (CCM). The 802.15.4 standard defines eight security levels that are used in ZigBee. Yang lists the various security levels as shown in Table 2.1. Each security level has varying levels of data confidentiality and data authenticity. The first four offer no confidentiality, while the others offer 128 bit AES encryption. Six levels offer a Message Integrity Code (MIC) of

varying length to ensure message integrity. The first security level offers no security whatsoever [Yan09].

Table 2.1: Security Levels Available to the MAC, NWK, and APS Layers [Yan09]

Security Level Identifier	Security Level Sub-field	Security Suite	Security Attributes	Data Encryption	Frame Integrity (length M of MIC, in Number of Octets)
0x00	000	None	None	OFF	NO (M=0)
0x01	001	AES-CBC-MAC-32	MIC-32	OFF	YES (M=4)
0x02	010	AES-CBC-MAC-64	MIC-64	OFF	YES (M=8)
0x03	011	AES-CBC-MAC-128	MIC-128	OFF	YES (M=16)
0x04	100	AES-CTR	ENC	ON	NO (M=0)
0x05	101	AES-CCM-32	ENC-MIC-32	ON	YES (M=4)
0x06	110	AES-CCM-64	ENC-MIC-64	ON	YES (M=8)
0x07	111	AES-CCM-128	ENC-MIC-128	ON	YES (M=16)

2.2 Current Attacks

Several attacks are currently possible against ZigBee networks. Some examples are sniffing, physical attacks, replay attacks, and denial-of-service attacks. This section discusses the theory behind these attacks and some of the software and hardware tools available to accomplish these attacks.

2.2.1 Theory.

2.2.1.1 Sniffing.

A sniffing attack is the collection of information from a network. Given correct hardware and software, sniffing packets from a ZigBee network is fairly straightforward. Some ZigBee networks do not use encryption [RMSB13]. In these networks, communications are easily sniffed by anyone with the proper equipment.

When a ZigBee network uses the standard security level, it is possible for the network key to be sent over the air in plaintext, which can be easily intercepted through sniffing. This can be prevented by preinstalling the network key on ZigBee devices or using high security [VHnA$^+$13].

2.2.1.2 Replay Attacks.

A replay attack consists of an attacker recording legitimate traffic on a network and replaying it at a later time to cause malicious effects. In ZigBee networks that do not use encryption, replay attacks are straightforward [CWL10]. Replay attacks can be circumvented in ZigBee through implementation of a freshness counter. Every packet transmitted is assigned a freshness number and the counter is incremented. Packets are only accepted if their freshness number is greater than the freshness counter. In practice, the freshness counter can cause problems because it must be manually reset by the administrator of the ZigBee network [VHnA+13].

2.2.1.3 Physical Attacks.

Physical attacks involve locating and tampering with a device. If a ZigBee device is located, it can be subjected to a physical attack.

Goodspeed has shown that keys can be extracted from several ZigBee devices if physical access is achieved [Goo09]. First generation chip sets consist of a radio and microcontroller on separate chips. Using contact probes, keys can be sniffed off the bus between the two chips. Second generation devices contain both radio and microcontroller on a single chip. However, a vulnerability exists that allows an attacker to dump keys off of a ZigBee device by analyzing flash memory [Goo09].

ZigBee networks do not invalidate keys when a device is removed from a network, allowing keys stolen in this manner to be used against the network [DT10].

2.2.1.4 Denial-of-Service.

There are currently several methods of disrupting service on a ZigBee network. Some include maximization of the frame counter, reflexive jamming, acknowledgment spoofing, and selective jamming.

One possible denial-of-service attack against a ZigBee network is to set the frame counter to the maximum possible value. If the MIC is not verified, as is the case under some security configurations, the frame counter can be used to force ZigBee devices to ignore legitimate packets. Even if the contents of a packet are gibberish, the frame counter value will still be accepted. Packets received after the malicious packet with lower frame counter values will be ignored by the device. Since the frame counter is at a maximum, no packets will be accepted until the frame counter is reset [VHnA+13].

Reflexive jamming is when a malicious device sniffs a network for communications and then immediately switches into transmission mode. It then broadcasts noise to cause interference with packet reception [GBM+12].

Acknowledgment spoofing is when a device is tricked into thinking that a packet it sent was received when in fact it was not. This is achieved by jamming a desired packet. The attacker then sends an acknowledgment to the victim device to make it appear that the packet was received [GBM+12].

Selective jamming works by sniffing a network and waiting for a specific transmission and then transmitting noise or another packet to disrupt the transmission. Due to the current technology's speed constraints, this technique is mainly used against ZigBee networks to jam acknowledgment packets [GBM+12].

2.2.2 KillerBee.

One of the earliest tools created to manipulate and attack ZigBee networks is KillerBee. KillerBee is a free and open source tool written by Joshua Wright. Since KillerBee is written in Python, it is able to be used in both Linux, Windows, and OS X. Its goal is to simplify attack tasks and explore the attack surface of ZigBee networks and devices. KillerBee offers several tools including zbstumbler, zbdump, zbreplay, zbdsniff, and zbfind [CWL10].

Zbstumbler is a tool designed to identify nearby ZigBee networks. It works in a way similar to conventional WiFi discovery. Zbstumbler transmits beacon request frames and hops to a different channel every two seconds. ZigBee devices within range reply to the beacon requests with information about the network as required by the specification. Since beacon requests and beacon frames are integral to the operation of the ZigBee protocol, this type of discovery is impossible to stop [CWL10].

Zbdump is a packet sniffer designed to capture ZigBee traffic on a particular channel, specified with the -f flag. The contents are directed to a libpcap file designated by the -w flag or a Daintree SNA capture via the -W flag [CWL10].

Zbreplay is an implementation of a replay attack against a ZigBee network. It takes the contents of a libpcap file or Daintree SNA capture file and replays it on the ZigBee channel specified by the -f flag [CWL10].

Zbdsniff is a key sniffer. It parses a packet capture file for Key-Transport commands and displays the key if one is found [CWL10] .

Zbfind is a tool used to locate the physical location of ZigBee devices. It takes the power received from any packets received and outputs it to the user. The user can use this information to move closer to a device as the signal strength increases [CWL10].

Zbassocflood is a denial-of-service tool that implements an attack that attempts to associate to a PAN to cause a target device to crash [SR13]. This attack works by exhausting the number of devices with which the target device associates. Once a device is connected with too many other devices, it crashes.

2.2.2.1 KillerBee Hardware.

Although KillerBee can be used with any hardware that can interact with 802.15.4 networks, the primary development hardware is the RZUSBSTICK. It only interacts with ZigBee networks in the 2.4 GHz frequency band. The RZUSBSTICK also requires specialized firmware to be able to inject packets into a ZigBee network. This firmware is

distributed along with the KillerBee framework. However, in order to reprogram the RZUSBSTICK, another piece of hardware, an Atmel on-chip programmer, is required [CWL10].

KillerBee also offers support for the GoodFet, a device that uses the Joint Test Action Group (JTAG) protocol to interface with ZigBee chips. The GoodFet can be used to dump the memory of a ZigBee chip. The zbgoodfind tool can then be used to extract keys from the memory dump [CWL10].

2.2.3 Api-do.

Api-do is another set of tools intended for penetration testing of ZigBee networks that builds upon the KillerBee framework. Api-do contains tools for sniffing, frame injection, and jamming [GBM+12]. Specifically, the project website contains the OpenEar, Scapy dot15d4, and zbWarDrive tools along with the KillerBee framework [SMB12].

The OpenEar tool integrates multiple RZUSBSTICKs together to listen on all 16 ZigBee channels in the 2.4 GHz frequency band. This is done by using multiple program threads to run multiple instances of the KillerBee packet capture process. The zbWarDrive tool injects a beacon request frame to determine if ZigBee networks are in the vicinity based on beacon responses [GBM+12].

In order to effect responses in a ZigBee network, proper 802.15.4 frames must be constructed. To create 802.15.4 frames, Api-do implements dot15d4, a layer extension for Scapy, which is a powerful networking tool that allows a user to create packets manually. The extension allows for packets to be generated for ZigBee and transmitted by conventional hardware [GBM+12].

2.3 Software Defined Radio

Mitola notes that SDR can be defined as a radio that implements a specific range of capabilities through elements that are software-reconfigurable [Mit99]. Another definition

of SDR from the Software Defined Radio Forum is a ”Radio in which some or all of the physical layer functions are Software Defined” [For11]. SDR allows for common hardware to implement a family of radios or switch between implementations. It allows for radios to be reprogrammed on the fly to solve bug fixes and upgrades leading to a longer life cycle and reduced maintenance time and cost [For11].

2.3.1 GNU Radio.

GNU Radio is an open source software development toolkit for the implementation of USRPs. It offers signal processing blocks that are typically written in C++, while higher-level applications are written in Python. GNU Radio also includes GNU Radio Companion which acts as a graphical user interface to connect signal blocks together [Lan13].

2.3.2 Universal Software Radio Peripheral.

One of the SDRs supported by GNU Radio is the USRP [Lan13]. The USRP family is built by Ettus Research, a subsidiary of National Instruments. Ettus Research builds several SDR products including devices that are controlled by a computer and communicate via USB or Ethernet [ER14]. USRP Hardware Driver (UHD) is the software driver for GNU Radio that controls the USRP. It was implemented to be a standard driver for all USRPs, regardless of connection type [SEB12].

National Instruments offers a basic record and playback tool that uses LabVIEW, a product of the parent company. Known as “NI USRP Record and Playback - I16”, it allows a user to record and playback raw RF with a USRP [Ins12].

2.3.3 ZigBee on Software Defined Radio.

There are several research projects for implementing ZigBee in GNU Radio. The main project of implementing ZigBee on the USRP was written by Thomas Schmid. Schmid also did a study on the feasibility of the USRP in 802.15.4 networks. The study

concluded that the USRP is able to decode 92.8% of the messages compared to a ZigBee device [SSS07].

Dabčević used Schmid's code to implement a transmitter and receiver on the USRP and measure packet reception rates. Dabčević was able to maintain reception between two USRPs at up to 30 meters with blocked line of sight [Dab11].

Thandee used Schmid's code, updated the compatibility with UHD, and then implemented it on the USRP E100 to broadcast a message with arbitrary payload. The USRP E100 is the embedded version of the USRP [Tha12].

2.4 Summary

This chapter discussed the ZigBee Protocol. It then detailed some of the current attacks against the ZigBee Protocol. Finally, this chapter discussed SDR and attempts to implement ZigBee on a specific SDR, the USRP.

III. Methodology

3.1 Problem Definition

This research compares the performance of different categories of ZigBee attack tools by implementing a replay attack against a target at various distances.

3.1.1 Goals and Hypothesis.

The goal of this research is to compare the performance and range of a replay attack against a ZigBee network. Specifically, it compares an implementation of a replay attack conducted with a laptop and RZUSBSTICK and compares it to the probability of success and power ratings of the replay attack for the USRP at the same distances. The Atmel RZUSBSTICK is the recommended hardware for the KillerBee attack suite [CWL10]. The USRP is a relatively inexpensive SDR that should be capable of implementing the ZigBee protocol [Dab11].

Due to superior transmission power, the USRP is expected achieve a higher probability of success at greater distances than the RZUSBSTICK.

3.1.2 Approach.

The approach of this research is to implement a specific replay attack on a laptop with USB dongle and a USRP. The attack is conducted on a ZigBee device at varying distances.

3.2 System Boundaries

As shown in Figure 3.1, the system under test (SUT) is the ZigBee Replay Attack System. It includes a targeted ZigBee Device (victim), malicious user with the equipment to perform a replay attack (attacking device), and a sensor at the victim device to record outcomes. Other parts of the system include the wireless network and physical layout of the devices. The component under test (CUT) is the attacking device.

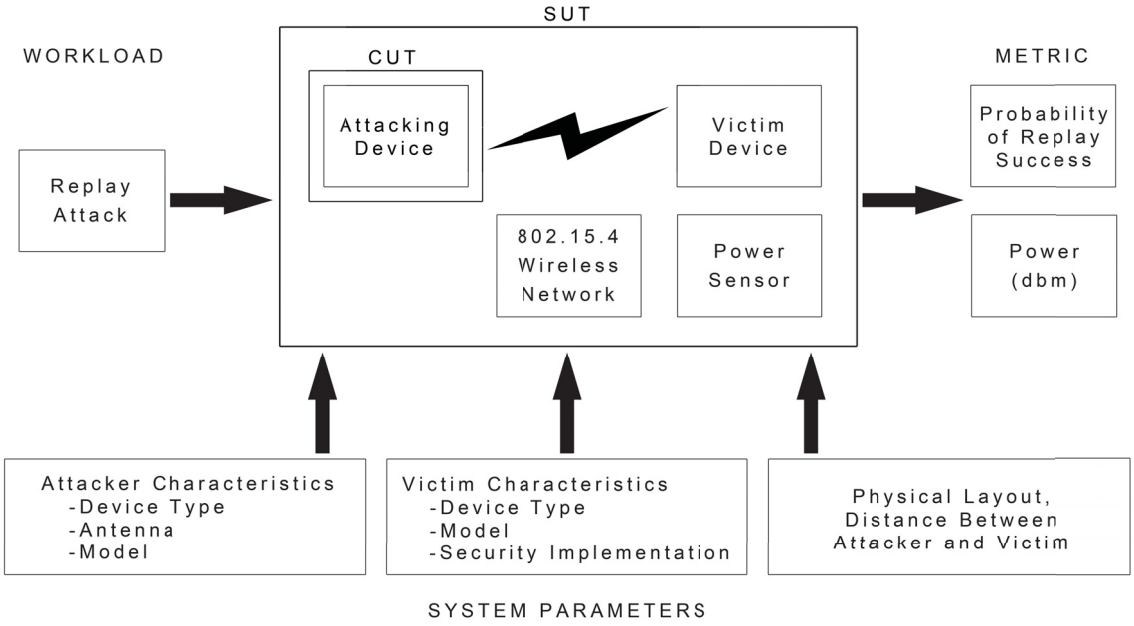


Figure 3.1: System Under Test

3.3 System Services

The service provided by the system is the execution of a replay attack against a chosen victim device. For the purpose of this test network, the attack consists of a beacon request frame sent from the attacking device. The victim should provide a corresponding beacon with information about the network. The system has two outcomes. The victim device either responds with a beacon or it does not. A success is defined as a beacon frame being returned to the attacker after it has been requested.

3.4 Workload

The workload of the system is the simulated replay attack. The attacking device transmits a beacon request frame. The victim then responds with a beacon frame. A sensor near the victim senses the power levels of both transmissions.

3.5 Performance Metrics

System performance is measured by the success or failure of the replay attack and the power level of the beacon request received at the victim. Each trial is a binomial test. Success is the attacker eliciting a beacon frame from the victim device. Failure is no response from the victim. The possibility of false positives and false negatives exists. A false positive is when a beacon is sent by the victim when directed by a device other than the attacking node. To minimize the likelihood of false positives, experiments are conducted at least 300 meters away from other ZigBee or 802.15.4 networks. A false negative is when a beacon frame is sent by the victim device when directed by the attacking device, but is not noticed by the sensor. Since the recording of the beacon request frame using the NI USRP Record and Playback - I16 tool is three seconds long and contains only one beacon request frame, the trials occur at least three seconds apart.

The overall performance of each configuration is measured by a probability of success. The probability of success is the number of successes in a given configuration divided by the total number of trials in said configuration. Performance is also evaluated based on the power received at the victim device. However, since the device used as the victim cannot directly report the power received, the power measured is the power reported by the sensor. The sensor returns a received signal strength indication (RSSI) value which can be converted to power in decibel referenced to one milliwatt (dbm) [RMW12].

$$P = 3 \times RSSI - 91 \tag{3.1}$$

3.6 System Parameters

Several parameters affect system performance.

- Brand and Model of Device Used - Several companies manufacture hardware based on the ZigBee standard. Variances between manufacturers and models introduce differences in range between devices.

- External Interference - External Interference can change the noise floor so that transmissions can fail if the signal strength is not enough. The experiments are conducted away from other ZigBee devices. Also, the attack is conducted on ZigBee channel 26 (2.48 GHz), which does not overlap with WiFi, although bleed over could still affect the experiment.

- Security Implementation/Posture - The implementation of security, or lack thereof, affects the probability of success of a replay attack. Devices that have replay protection and/or encryption enabled can be less susceptible to attack. All devices in this experiment operate without any encryption or integrity checks. However, since beacon frames cannot be disabled, the security implementation should not have a large effect.

- Signal Strength - The strength of the signal received by the target device dictates that device's ability to interpret the command received. This directly affects the probability of success for any given command.

  - Antenna Type and Orientation - The type of antenna used by both the transmitting and receiving device determines the strength of the signal sent or received. The orientation of an antenna affects how much power is sent in a given direction. This is especially true for directed antennae. Omnidirectional antennae can have null spots where little to no power reaches.

  - Distance Between Devices - The signal received by the victim device decreases by the square of the distance between devices.

  - Device Motion - Although many ZigBee devices are stationary, it is possible for a mobile platform to implement the ZigBee protocol. A ZigBee device in motion would have a variable distance from it to the next node. Therefore, signal strength would be variable. Mobile devices are not investigated in this thesis.
  - Physical Layout - The ability of the attacker to be in direct line of sight with the victim affects the strength of signal received by the victim.
  - Time of Day - The time day could affect the signal strength and thus the probability of success while outside. This is possibly due to changes in background radiation.

- Type of Device Used - The architecture on which a ZigBee stack is implemented will change system performance. The device type could be one of many types of standalone devices, a USB dongle, a SDR, or any device that can implement the ZigBee standard. The specific devices used in this thesis are discussed in Section 3.7.

3.7 Factors

The following factors are used in the scope of this thesis.

- Antenna Type - The USB dongle has an internal antenna that cannot be changed. The SDR is attached to an external antenna, which is either an omni-directional and a directed antenna. This factor has three levels: internal, external, and directional antenna.
  - Antenna Orientation - The omnidirectional antenna is oriented in such a way that nulls spots, as shown in Figure 3.2, do not include the victim device. The directed antenna is oriented to point at the victim device. The antenna pattern

of the RZUSBSTICK is not known, so a pilot study is conducted. Two RZUSBSTICKs are positioned three meters apart in one of eight tested orientations as shown in Figure 3.3. Since the RZUSBSTICK is a USB dongle, it must be plugged into a laptop. Thus, orientations seven and eight have one or two laptop(s) between the RZUSBSTICKs. The results of the study are shown in Figure 3.4. The results indicate that the first orientation allows the most amount of power to be transmitted between the two RZUSBSTICKs. Therefore, the RZUSBSTICK is oriented to point at the victim device as in orientation 1 in Figure 3.3.

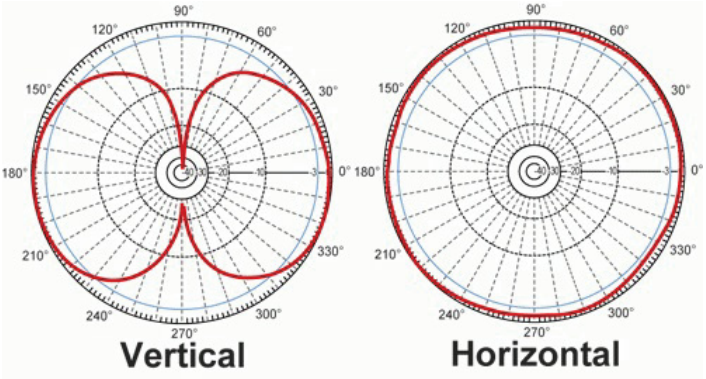
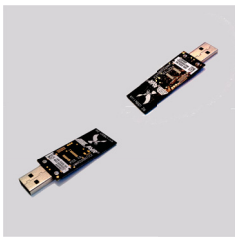


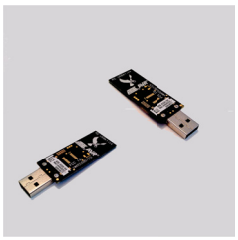
Figure 3.2: Antenna Pattern for Omnidirectional Antenna

[ver09]

- Physical Layout - The experiment is conducted in two parts: indoors and outdoors. While outdoors, the victim and attacker are always in direct line of sight. When in an indoor setting, the two nodes have two closets and between four and six walls blocking line of sight. The walls are consistent throughout the experiment. A map

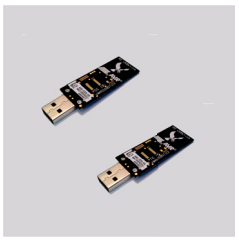


(a) Orientation 1: Co-Linear, both sticks pointing at each other.



(b) Orientation 2: Perpendicular, one stick is pointing at the other.

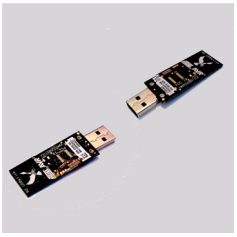
(c) Orientation 3: Perpendicular, one stick is pointing at the other, which is on its side.



(d) Orientation 4: Parallel, the sticks are parallel to each other.

(e) Orientation 5: Parallel, both sticks are on their sides.

(f) Orientation 6: Parallel, the sticks are parallel to each other with one on its side.



(g) Orientation 7: Co-Linear, the sticks are pointing away from each other with two laptops between them.

(h) Orientation 8: Perpendicular, one stick is pointing away from the other, which is perpendicular to it. There is one laptop between the sticks.

Figure 3.3: Orientations Tested during Pilot Study

of the victim locations are shown in Figure 3.5. This factor has two levels: indoors (no line of sight) and outdoors (line of sight).

- Distance Between Devices - Distance between the victim and attacking device vary during the experiment. Two sets of distances are used in this thesis. While the devices are in line of sight, measurements are taken in twenty meter increments between 20 and 100 meters. The advertised range of ZigBee is 100 meters, therefore the experiment is conducted in ten meter increments between 100 and 150 meters [Zig13]. Interesting areas are evaluated further at five meter increments. While the devices are not in line of sight, the distance varies linearly in five meter

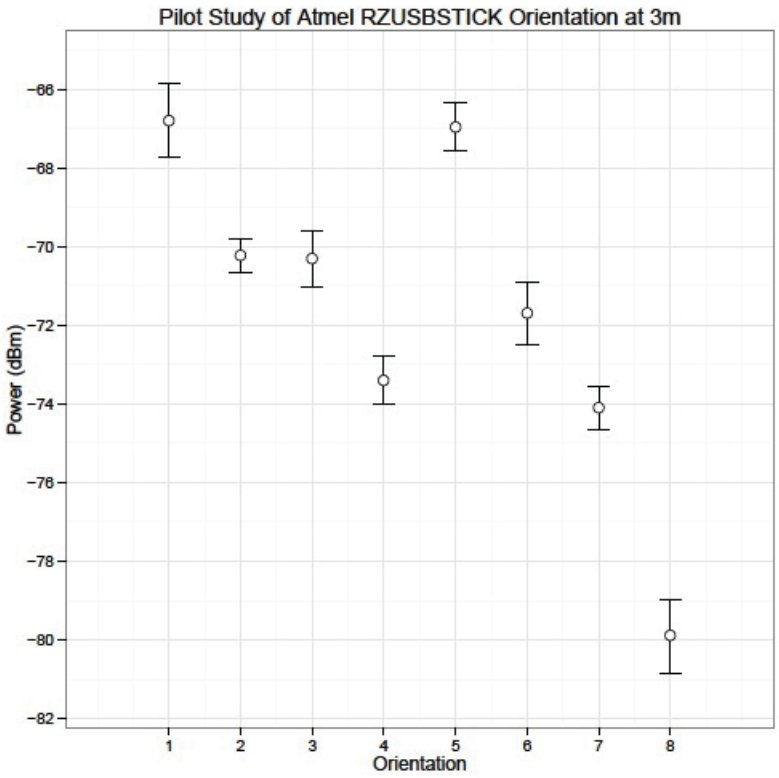


Figure 3.4: Results of the Atmel RZUSBSTICK Orientation Pilot Study

increments from 15 to 35 meters. This factor has ten levels while in line of sight: 20, 40, 60, 80, 100, 110, 120, 130, 140, and 150 meters. It has five levels while not in line of sight: 15, 20, 25, 30, and 35 meters.

- Time of Day - To determine that time of day is a factor, a pilot study was conducted. To determine the effect time of day has, the replay attack described in Section 3.8 was run in the afternoon and evening. The afternoon data set was collected between 1300 and 1405 hours. The evening data set was collected between 1910 and 1945 hours. The experiment was conducted in ten meter increments with thirty trials each. Additional samples are taken in 5 meter increments near locations where the reception is less than 25%. Since the afternoon data set has more locations with that

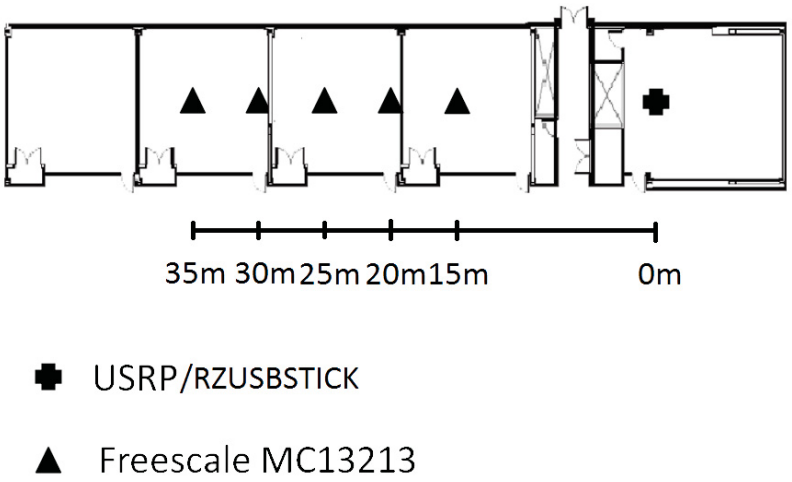


Figure 3.5: A Map of the Indoor Locations

criteria, the afternoon data set took a longer time to complete. Figure 3.6 shows the probability of success results of this pilot study. When run in the evening, the probability of success for the RZUSBSTICK is 100% until approximately 100 meters. The reception rate does not drop to 0% until approximately 130 meters. When run in the afternoon, the probability of success for the RZUSBSTICK is nearly 100% until approximately 60 meters. The reception rate does not drop to 0% until approximately 110 meters. Between 60 and 110 meters, the probability of success of the afternoon run varies significantly. Due to more samples being taken in the afternoon,

During the main experiment, in order to minimize the effect of the time of day of the experiment, two repetitions of the experiment are performed. The first starts at 20 meters and increases in distance. The second starts at 150 meters and decreases in distance. Both start around noon, local time, and finish between 1700 and 1900, local time. This is only for the line of sight experiment as the blocked line of sight

experiment is run indoors, and the time of day should not affect the experiment when indoors.

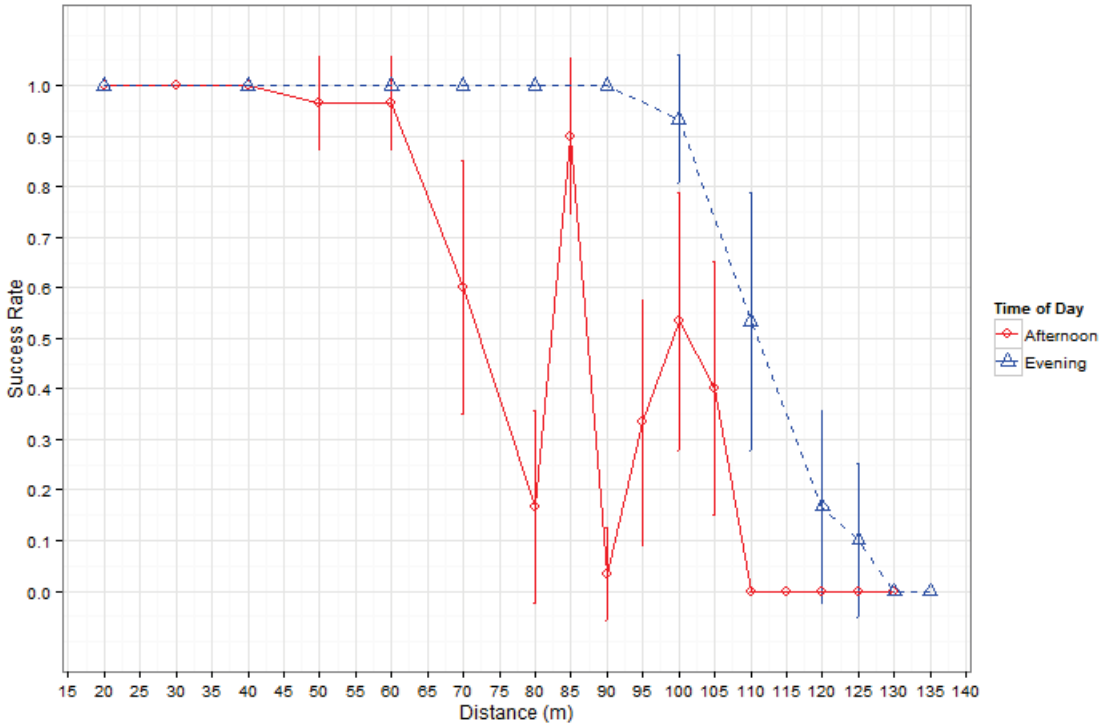


Figure 3.6: Probability of Success of the RZUSBSTICK while in Line of Sight of the Victim in the Afternoon and Evening

- Type of Device Used - Two separate device types are investigated: a RZUSBSTICK dongle attached to a laptop computer and a USRP SDR. This factor has two levels, but by its nature, they are incorporated into the antenna type factor. However, the USRP is also configured in one of two ways, as a raw RF repeater and with a ZigBee stack via GNU Radio.

  - Raw RF repeater - Using the NI USRP Record and Playback - I16 tool, the USRP records a beacon request frame as raw RF energy before the experiment. This beacon request frame is recorded during the power on sequence of a ZigBee device. The Record and Playback tool saves the raw energy as a binary file and includes noise from the RF band that the beacon request frame is recorded. During the experiment, the frame is replayed by the NI USRP Record and Playback - I16 tool as is.
  - GNU Radio - The USRP is configured with GNU Radio. The implementation is the similar as used by Thandee, but has been modified to transmit beacon request frames. A similar beacon request frame is captured during the power on sequence of a ZigBee device using KillerBee's zbdump tool and saved as a pcap file. This file is analyzed and the bits that are used are inserted into the code used by Thandee. The contents of the frame are (in hexadecimal): 03 08 37 FF FF FF FF 07 39 F2. The pcap file is then used by the RZUSBSTICK via KillerBee's zbreplay tool. The modified file from Thandee [Tha12], as well as the scripts using that file, are shown in Appendix B.

- USRP Transmission Gain Setting - The USRP is given three gain settings: a high, medium, and low setting. The medium and low setting are set to 15 decibel (db) and 3 db, respectively. The National Instruments software allows for gain settings of up to 30 db. GNU Radio recommends that the gain setting not be set higher than 20 db. The high setting is 30 db and 20 db for the raw RF repeater and GNU Radio configurations, respectively.

Table 3.1 summarizes the factors and their levels in this experiment. Table 3.2 summarizes those factors that are specific to the USRP.

Table 3.1: Summary of Factors and Levels

Factor	Levels
Antenna Type	Internal Omnidirectional Directed
Physical Layout	Outdoor Indoor
Device	RZUSBSTICK USRP
Distance Between Devices (Outdoor)	20 m 40 m 60 m 80 m 100 m 110 m 120 m 130 m 140 m 150 m
Distance Between Devices (Indoor)	15 m 20 m 25 m 30 m 35 m

Table 3.2: Summary of Factors and Levels Pertaining to the USRP

Factor	Levels
USRP Configuration	Raw RF Repeater GNU Radio
USRP Transmit Gain	3 db 15 db 30 db/20 db

3.8 Evaluation Technique

System evaluation is determined by experimentation. The experiment is conducted in two parts. In the first part, the USRP uses National Instrument's record and playback tool as a raw RF repeater. This experiment is conducted both indoors and outdoors. In the second part, the USRP is configured to use GNU Radio. This experiment is only conducted indoors.

Figure 3.7 shows the sequence of the experiment. First, the attacker sends a beacon request frame. Second, the victim device should respond with a beacon frame. Third, the sensing laptop should detect both and register a RSSI number for each.

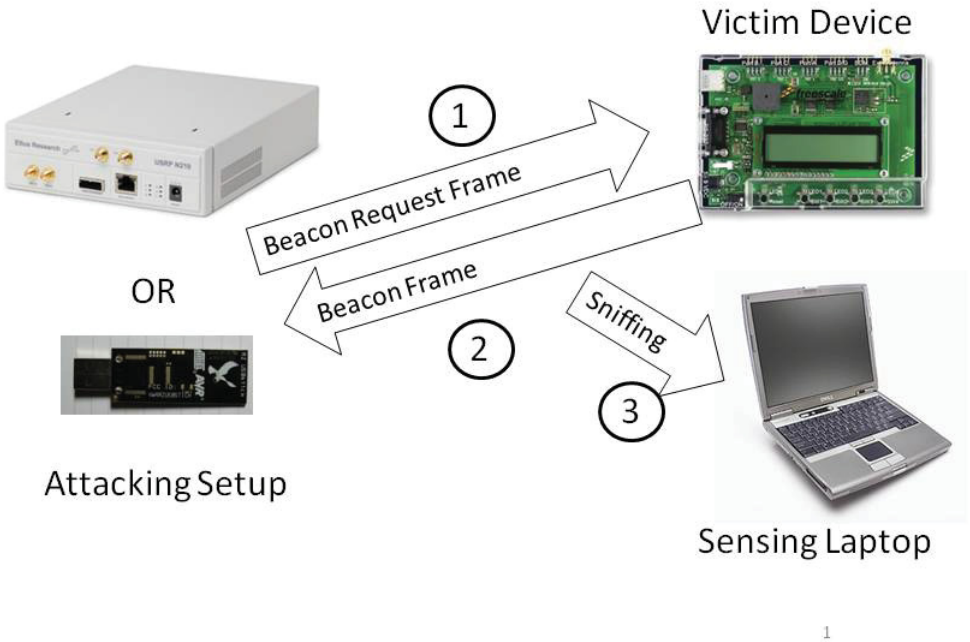


Figure 3.7: The Attack Sequence

3.8.1 Attacker.

Figure 3.8 shows the attacking setup. The KillerBee Laptop is a Dell Precision M4600 laptop with an Intel core i7-2620M central processing unit (CPU) and 8 gigabytes of random access memory (RAM) running Backtrack 5, revision 3 Linux operating system and the KillerBee attack suite. It is connected to the Atmel RZUSBSTICK. A second laptop, the USRP Laptop, is a Dell Precision M4500 with an Intel core i7-620M

CPU and 8 gigabytes of RAM. It runs 64-bit Windows 7 and is connected to the USRP via gigabit Ethernet. In this configuration, the USRP Laptop is running the NI USRP Record and Playback - I16 tool via LabVIEW Version 13.0 (32-bit). The USRP is a National Instruments NI USRP-2921 running firmware compatibility version 9 connected to omnidirectional and directed antennae.

During the GNU Radio portion of the experiment, the USRP Laptop is changed to an HP Envy 17 Laptop with an Intel i7-720Q CPU and 8 gigabytes of RAM running 32-bit Linux Mint 15 operating system. The USRP Laptop is configured with USRP Hardware Driver (UHD) version 003.004.005 as it is compatible with the firmware of the USRP, which was not updated to the latest version as it was unknown if an update would make the USRP incompatible with National Instrument's software tool. GNU Radio version 3.6.1 is used.

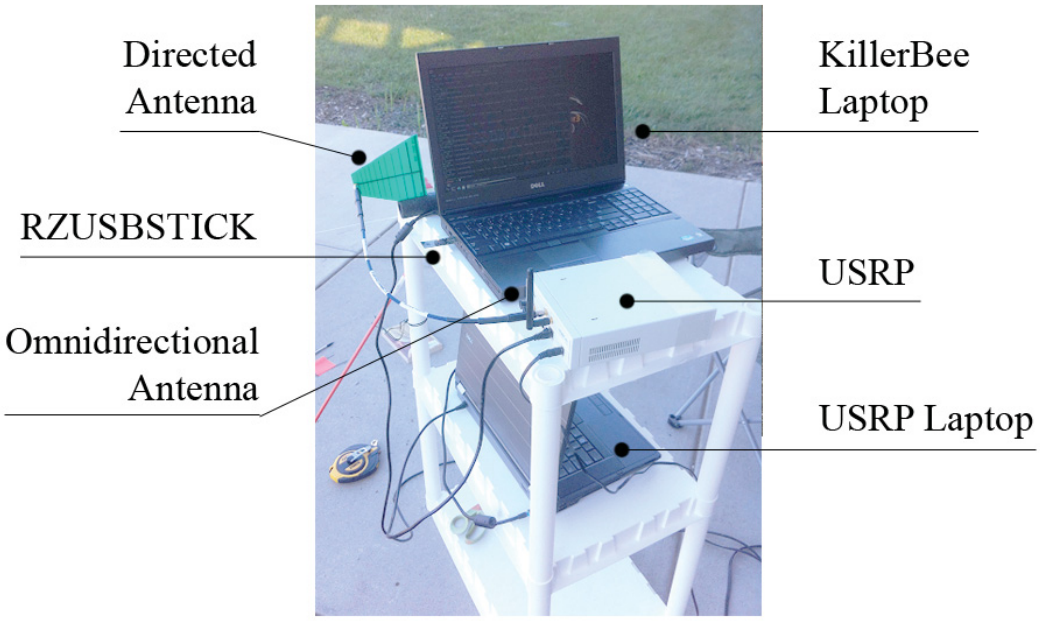


Figure 3.8: The Attacking Setup

3.8.2 Victim.

Figure 3.9 shows the victim setup. The victim devices is a Freescale MC13213 ZigBee device. The Sensing Laptop is a Dell Latitude D630 laptop with an Intel Core 2 Duo T7300 CPU and 2 gigabytes of RAM running Backtrack 5, revision 3 and KillerBee. It uses a second RZUSBSTICK as an antenna. This laptop, using the zbfind tool, records the RSSI signal strength of the replay attack near the victim as well as the beacon response from the Freescale MC13213. This instrument is not extremely precise as the RSSI signal strength is only reported as an integer. From (3.1), this means the sensor only has a resolution of 3 dbm. Also, 0 RSSI is mapped to -91 dbm, thus the sensor cannot detect 802.15.4 signals below that level. Data points that do not register a power level are discarded, as opposed to set to zero, as it is impossible to determine if the power level was extremely low or if there is another reason for the sensor to not receive the data.

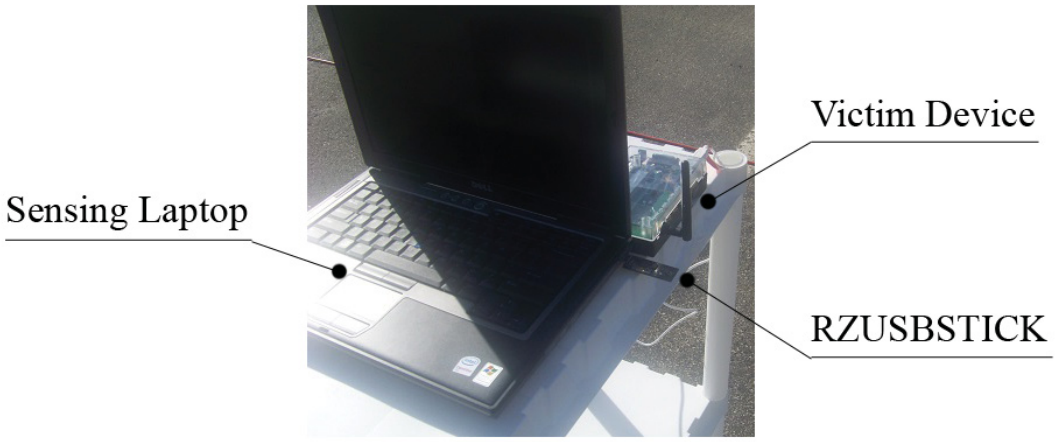


Figure 3.9: The Victim Setup

3.9 Experimental Design

Interaction between factors are determined by a full factorial experiment. From Table 3.1 and Table 3.2, there are six factors. However, antenna type and device are integrated together as the RZUSBSTICK can only use its internal antenna and the USRP uses the other two antenna types, the omnidirectional and directed antennae. Thus, there are seven attacking configurations: the RZUSBSTICK and the USRP with two antenna types and three different transmit gain settings. Also, the levels of the distance factor is different between the outdoor and indoor experiments, with 10 and 5 levels, respectively. Since the GNU Radio portion of the experiment is only conducted inside, there are twenty locations for the victim device. This leads to 140 configurations.

Each configuration is repeated multiple times. When the USRP acts as a raw RF repeater, each experimental configuration is repeated 30 times. Due to superior automation, when the USRP is configured with GNU Radio each experimental configuration is repeated 100 times. Since there are 140 configurations with 105 requiring 30 trials and 35 requiring trials, 6650 trials are conducted. Once the experiment is configured, each trial takes between three and six seconds. Each trial consists of an attacking ZigBee device sending a saved ZigBee packet over the LR-WPAN to the victim device. Set up consists of configuring the victim and attacking devices. Between each experiment the attack platform moves to a set distance from the stationary victim. A confidence level of 99 percent is used. Thirty repetitions of each experiment is enough to ensure a sufficiently small variance.

3.10 Methodology Summary

The ZigBee Replay Attack System is used to conduct an analysis of replay attacks. Several factors are varied including antenna type, distance between devices, physical layout, and configuration of the attacking device. A captured beacon request frame is sent

from the attacking device to the victim device in an effort to elicit a beacon frame. The success or failure of the attack is recorded. The power of the attack near the victim is also recorded.

IV. Results and Analysis

This chapter presents and discusses the experimental results. The data sets are split into those that maintain line of sight between the attacker and victim, those that do not, and those that configure the USRP to use GNU Radio, for which data is only taken indoors. Section 4.1 details the results of the line of sight portion of the experiment. Section 4.2 details the results of the blocked line of sight portion of the experiment. Section 4.3 details the results of the experiment when the USRP is configured to use GNU Radio. Tables summarizing the data collected in this experiment are found in Appendix C.

4.1 Line of Sight Scenario

This section details the part of the experiment where the attacker is in line of sight of the victim. It is further broken down by configuration of the attacker. Section 4.1.1 presents the performance of the RZUSBSTICK. Section 4.1.2 presents the data relating to the USRP when it uses an omnidirectional antenna and compares it with the performance of the RZUSBSTICK. Section 4.1.3 presents the performance of the USRP when it uses a directed antenna and compares it with the RZUSBSTICK.

4.1.1 RZUSBSTICK.

Figure 4.1 shows the probability of success of the RZUSBSTICK during the line of sight part of the experiment. In light of the reception of the RZUSBSTICK dropping between 60 and 80 meters, data is taken at 70 and 65 meters. Data is collected for the USRP at those data points for consistency as well. The probability of success graph can be can be subdivided into three zones, a full reception zone, a transition zone, and an out-of-range zone. A trend line with 99% confidence interval is added to the probability of success graph of Figure 4.1 of the approximate transition zone. This line runs from 40 to 110 meters. Most of the data is within the confidence interval of the trend line.

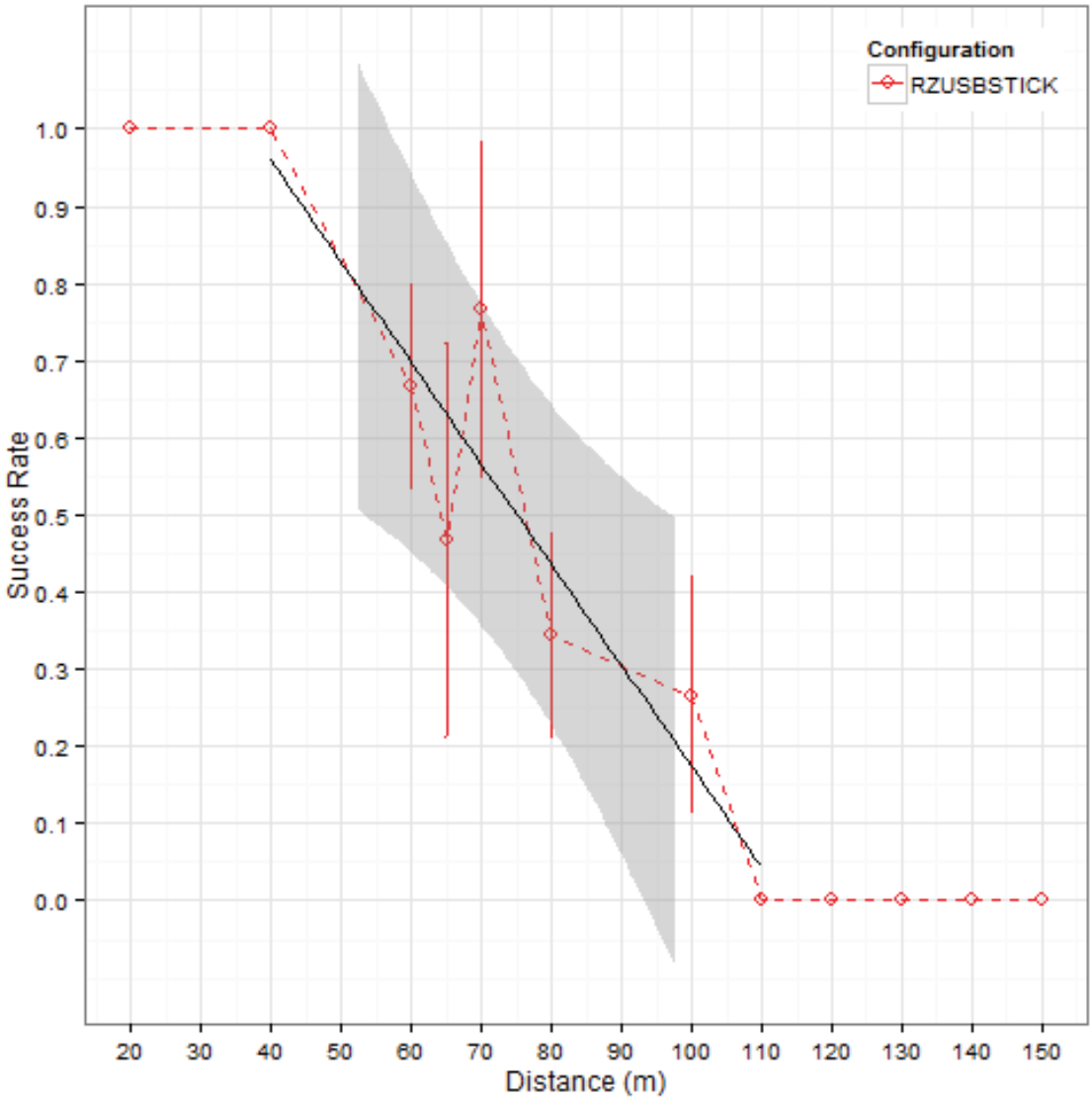


Figure 4.1: Probability of Success Versus Distance of the RZUSBSTICK

Figure 4.2 shows the power of the RZUSBSTICK during the line of sight part of the experiment, as reported by the sensor. The received power of the replay attack drops logarithmically until 65 meters before hitting the threshold of detection of the sensor at -91 dbm. A trend line is added from 20 to 70 meters to show the relationship. Beyond 120

meters, the sensor is unable to detect any of the attacks, so those data points have been omitted from the power versus distance graph.

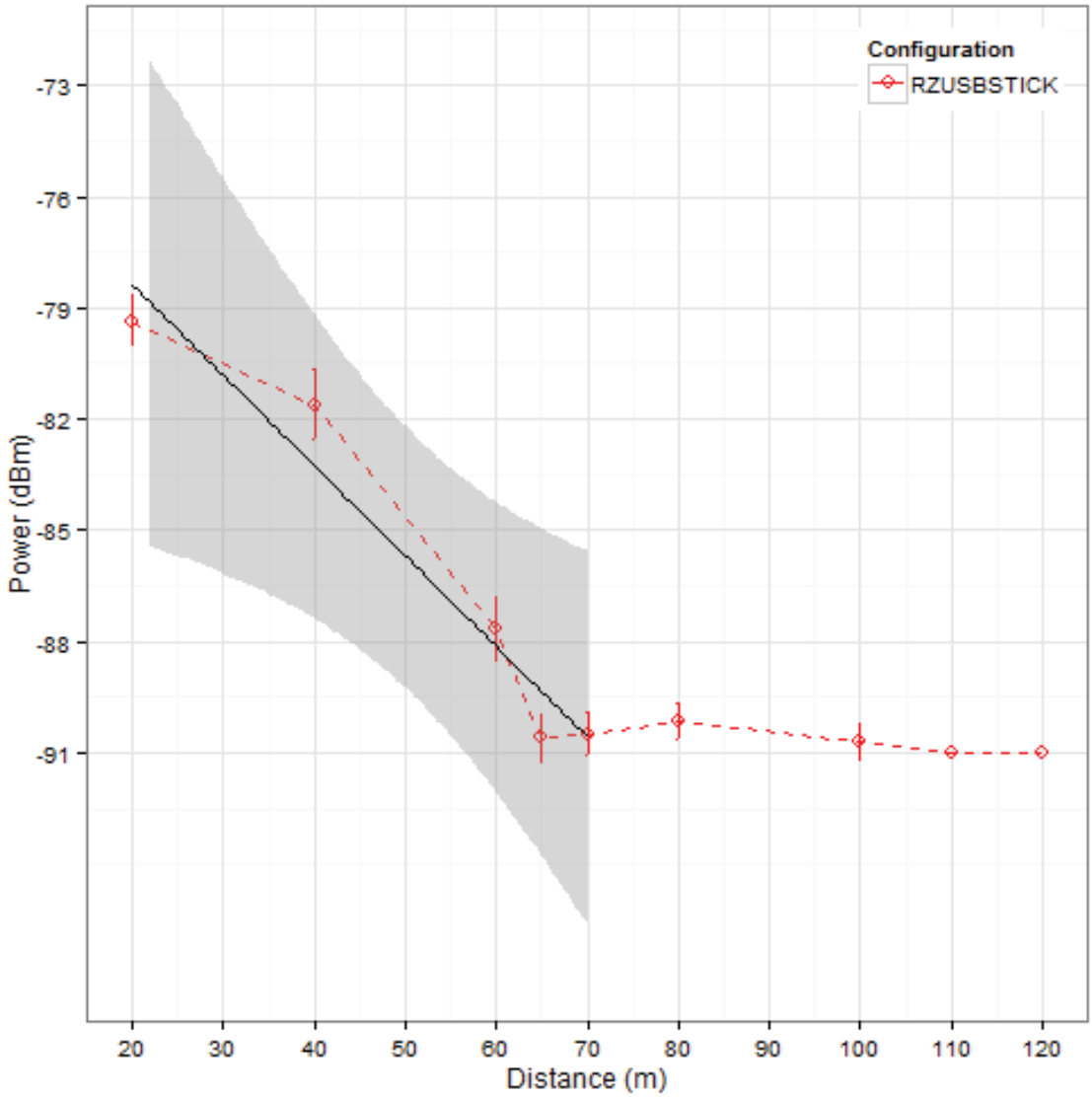


Figure 4.2: Power Versus Distance of the RZUSBSTICK

4.1.2 Omnidirectional Antenna.

Figure 4.3, Figure 4.4, and Figure 4.5 display the probability of success of the USRP with the omnidirectional antenna, using 30 db gain, 15 db gain, and 3 db gain, respectively. As with the RZUSBSTICK, each of the graphs can be subdivided into three zones, a full reception zone, a transition zone, and an out-of-range zone. A linear trend line of the transition zone has been inserted for each of the graphs, and a 99% confidence interval for the trend line is calculated and shaded on the graph. In Figure 4.4, the linear trend line runs from 80 to 150 meters. In Figure 4.5, the transition zone and corresponding trend line is from 65 to 110 meters. This trend line is not shown in Figure 4.3, as this experiment is limited to 150 meters and a transition zone did not appear in that range. In general, the data fits the linear trend lines. There are a few exceptions including the medium power at 120 meters. The probability of success when using the USRP with 30 db gain also unexpectedly decreases at 120 meters.

Another anomaly is the reception of the USRP with 30 db transmit gain at close range. There are two possible explainations. First, it is possibly due to the data being used to attack the victim. When the beacon request frame was recorded, the recording also included any background noise during the recording. It is possible that 30 db transmit gain is so high as to make background noise indistinguishable from the actual data of the frame. Second, the beacon request frame could possibly be transmitted with enough power to saturate the victim.

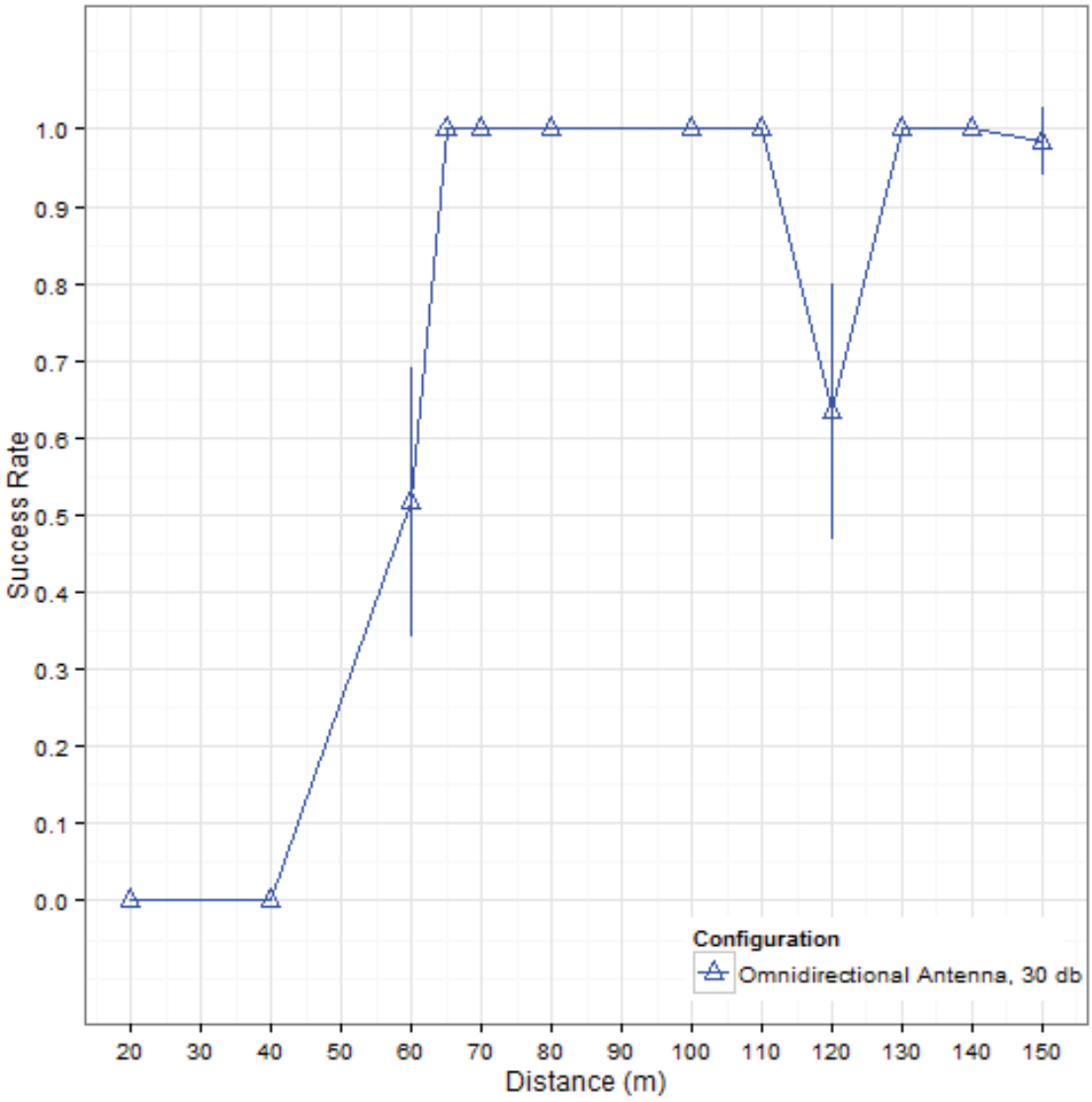


Figure 4.3: Probability of Success Versus Distance of the USRP with Omnidirectional Antenna and 30 db Gain

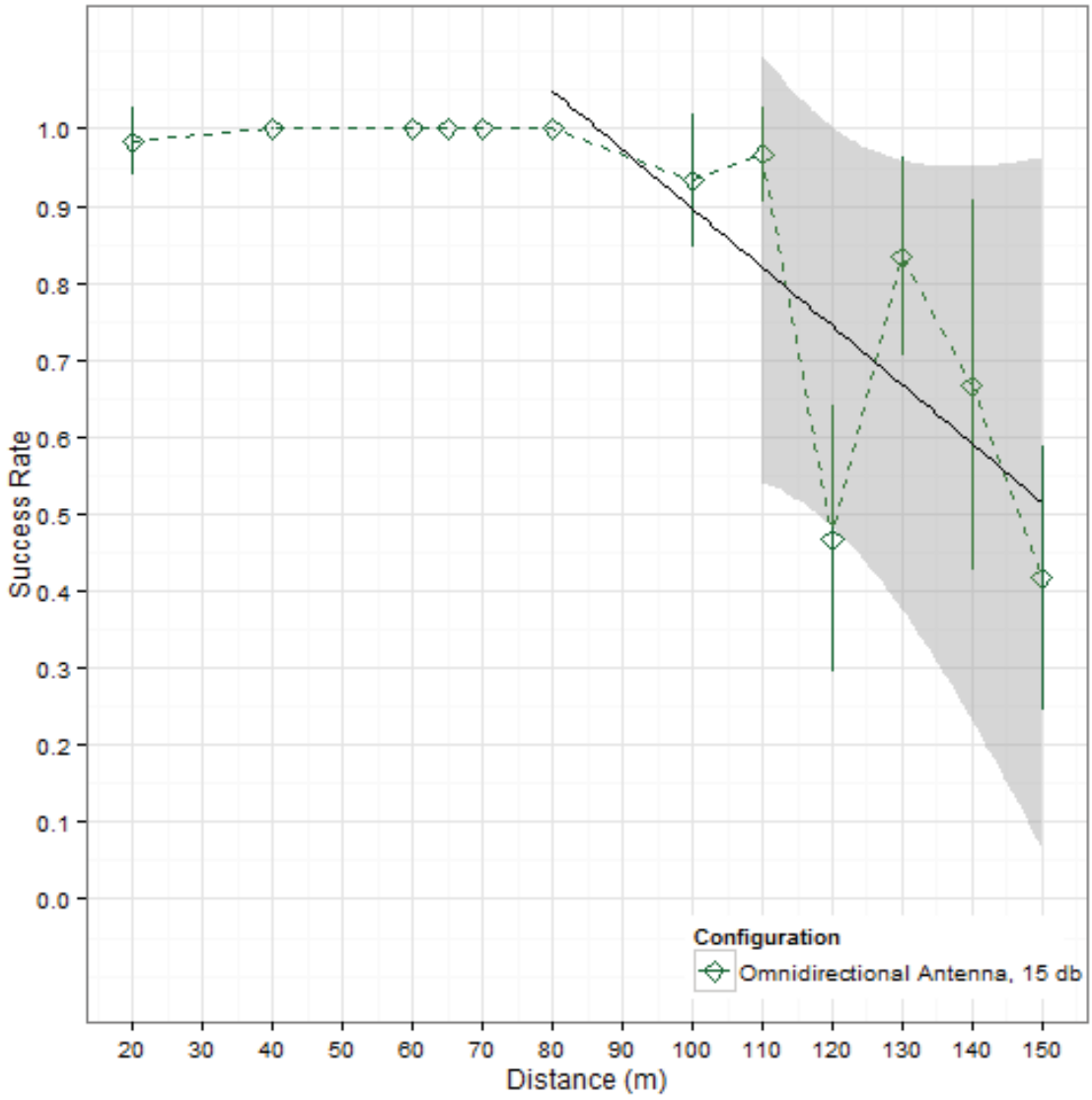


Figure 4.4: Probability of Success Versus Distance of the USRP with Omnidirectional Antenna and 15 db Gain

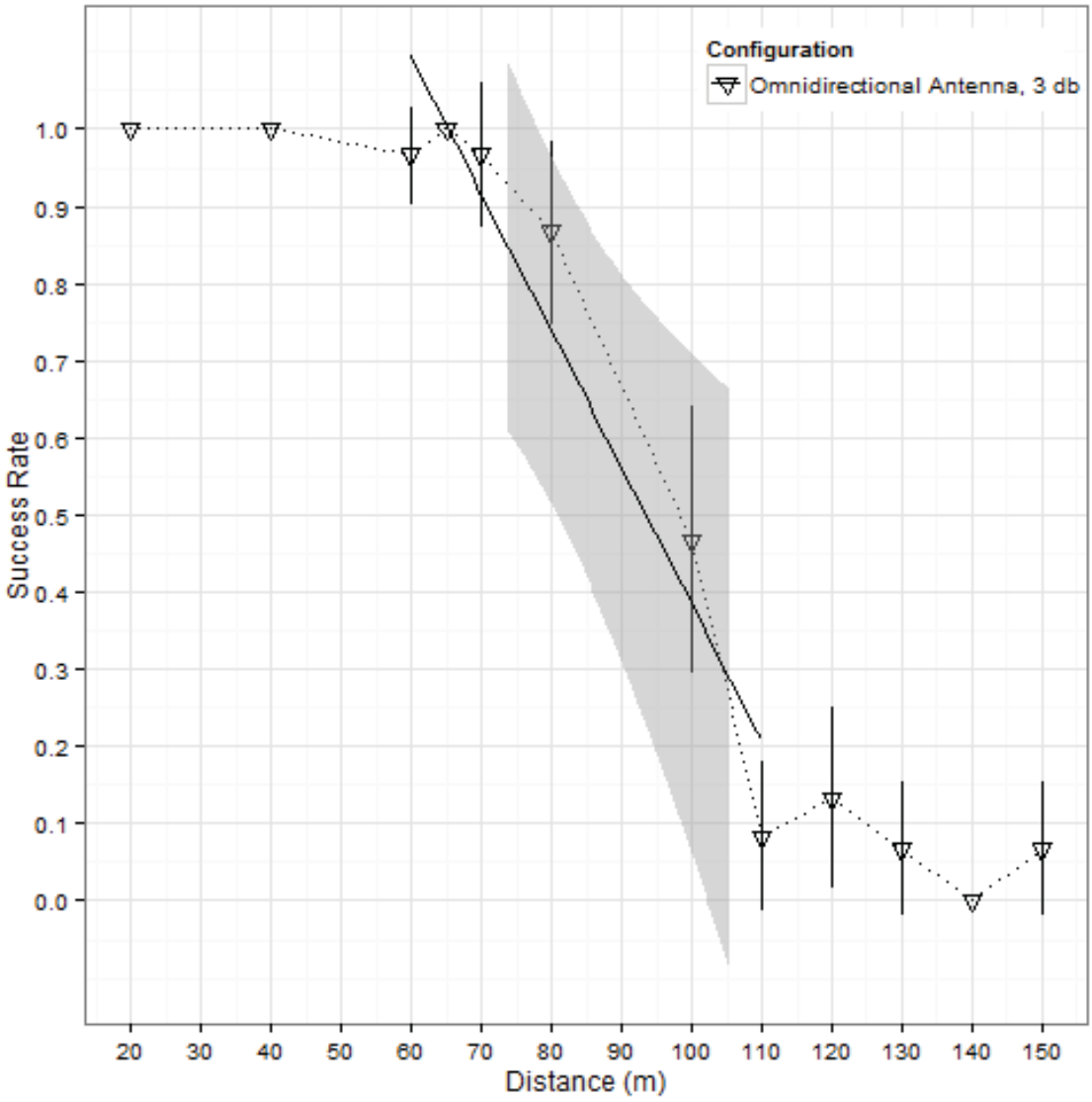


Figure 4.5: Probability of Success Versus Distance of the USRP with Omnidirectional Antenna and 3 db Gain

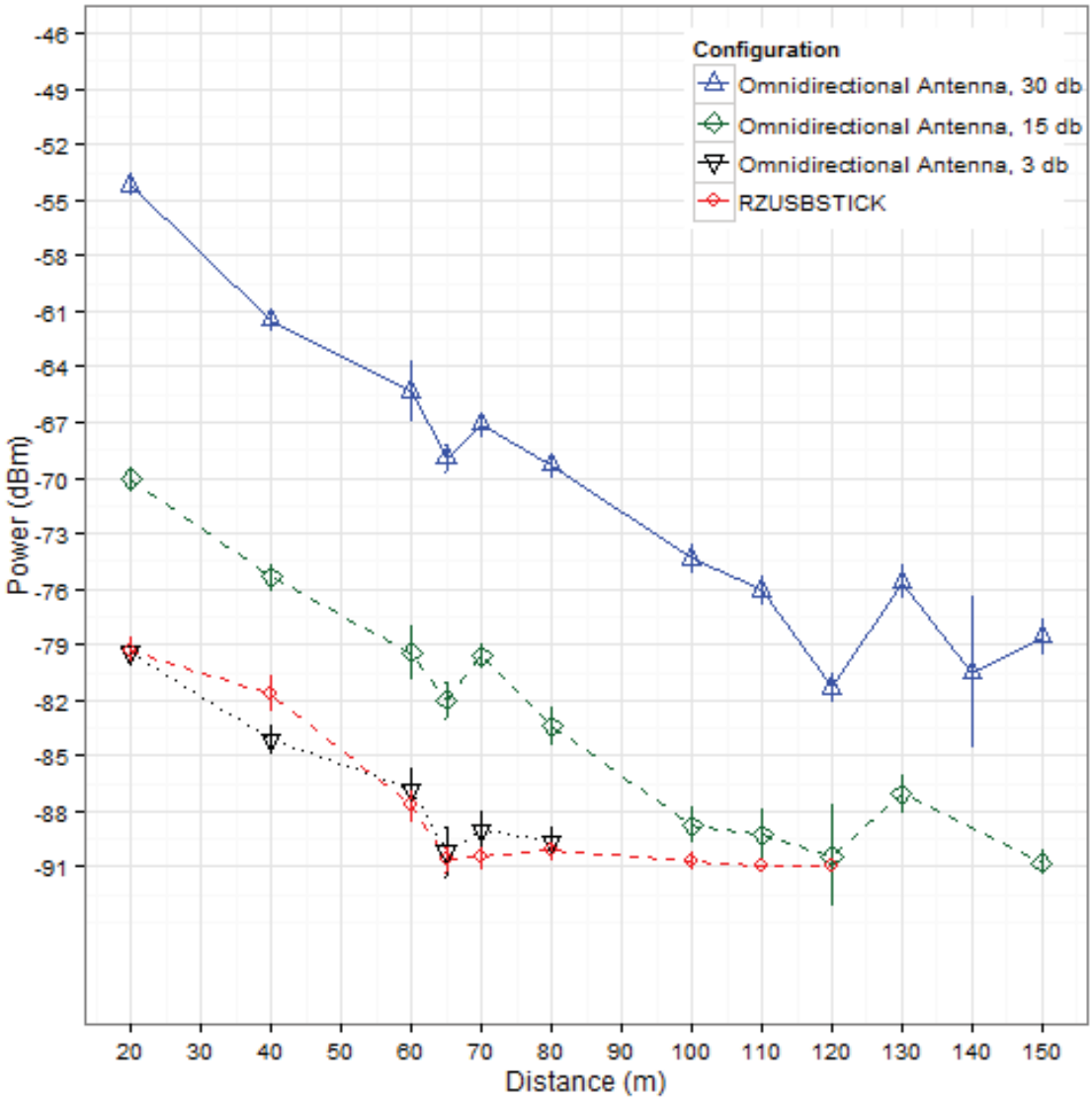


Figure 4.6: Power (dbm) of the RZUSBSTICK Compared to the USRP with Omnidirectional Antenna while in Line of Sight of the Victim

Figure 4.6 shows the power received by the sensor near the victim device in dbm for the RZUSBSTICK and the USRP using an omnidirectional antenna. Figure 4.7, Figure 4.8, and Figure 4.9 display the power received by the sensor in separate plots. Data points that were not measured due to reception reasons are omitted. Overall, each

decreases in a similar, logarithmic fashion. There is some anomalous behavior beyond 120 meters. There is also an dip in power at 65 meters, but it is still within the confidence interval of the logarithmic model.

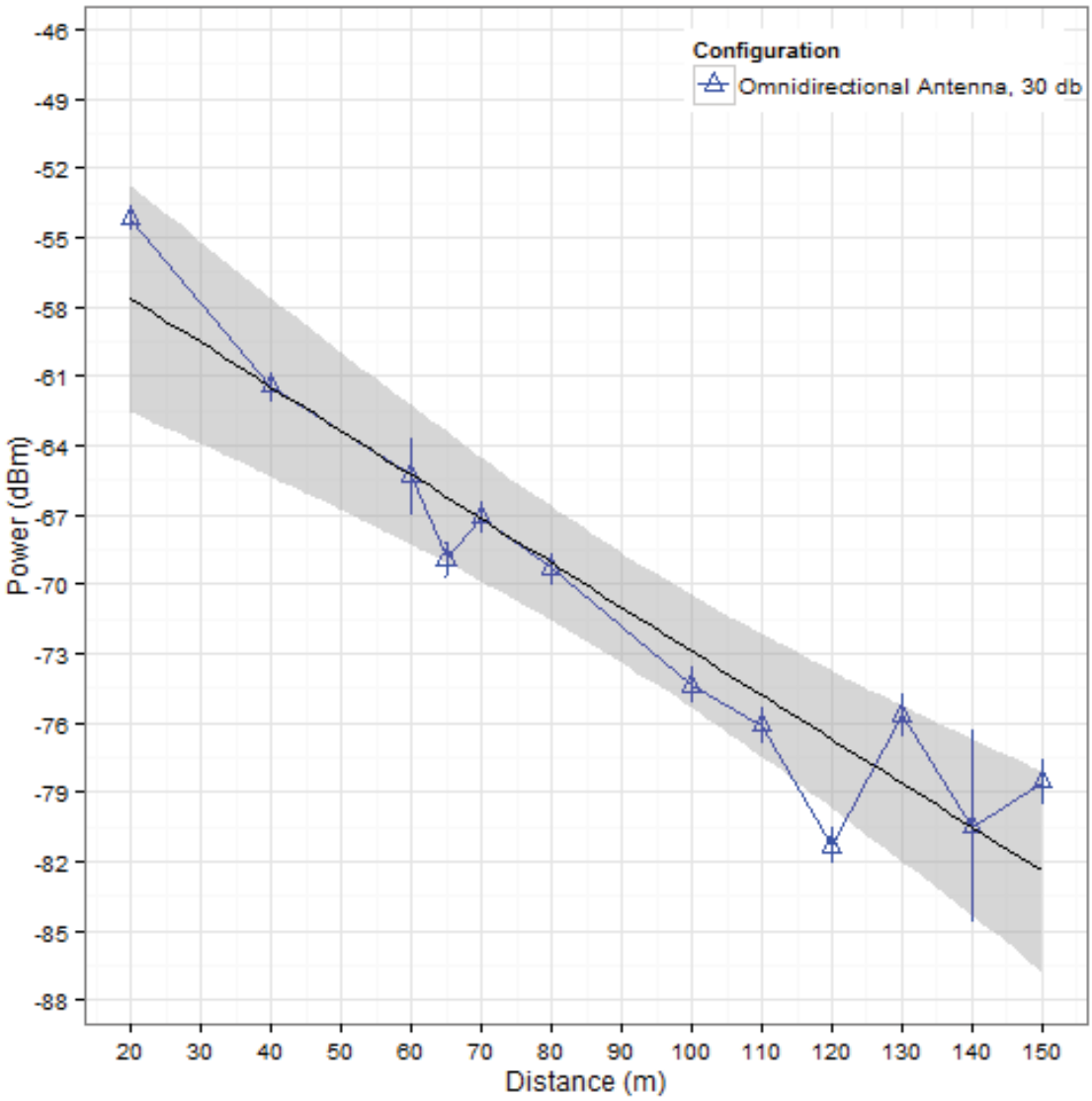


Figure 4.7: Power (dbm) Versus Distance of the USRP with Omnidirectional Antenna and 30 db Gain

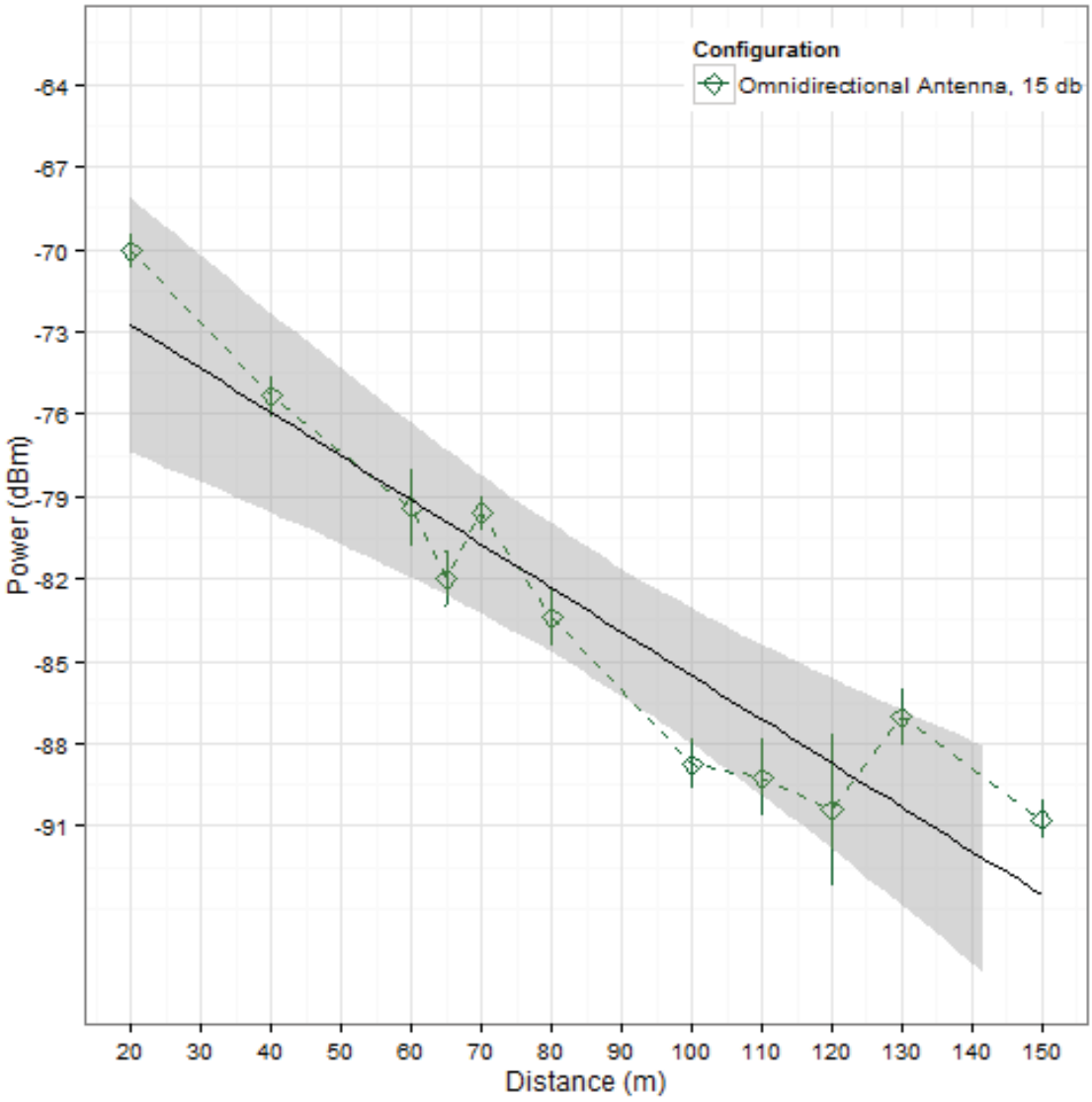


Figure 4.8: Power (dbm) Versus Distance of the USRP with Omnidirectional Antenna and 15 db Gain

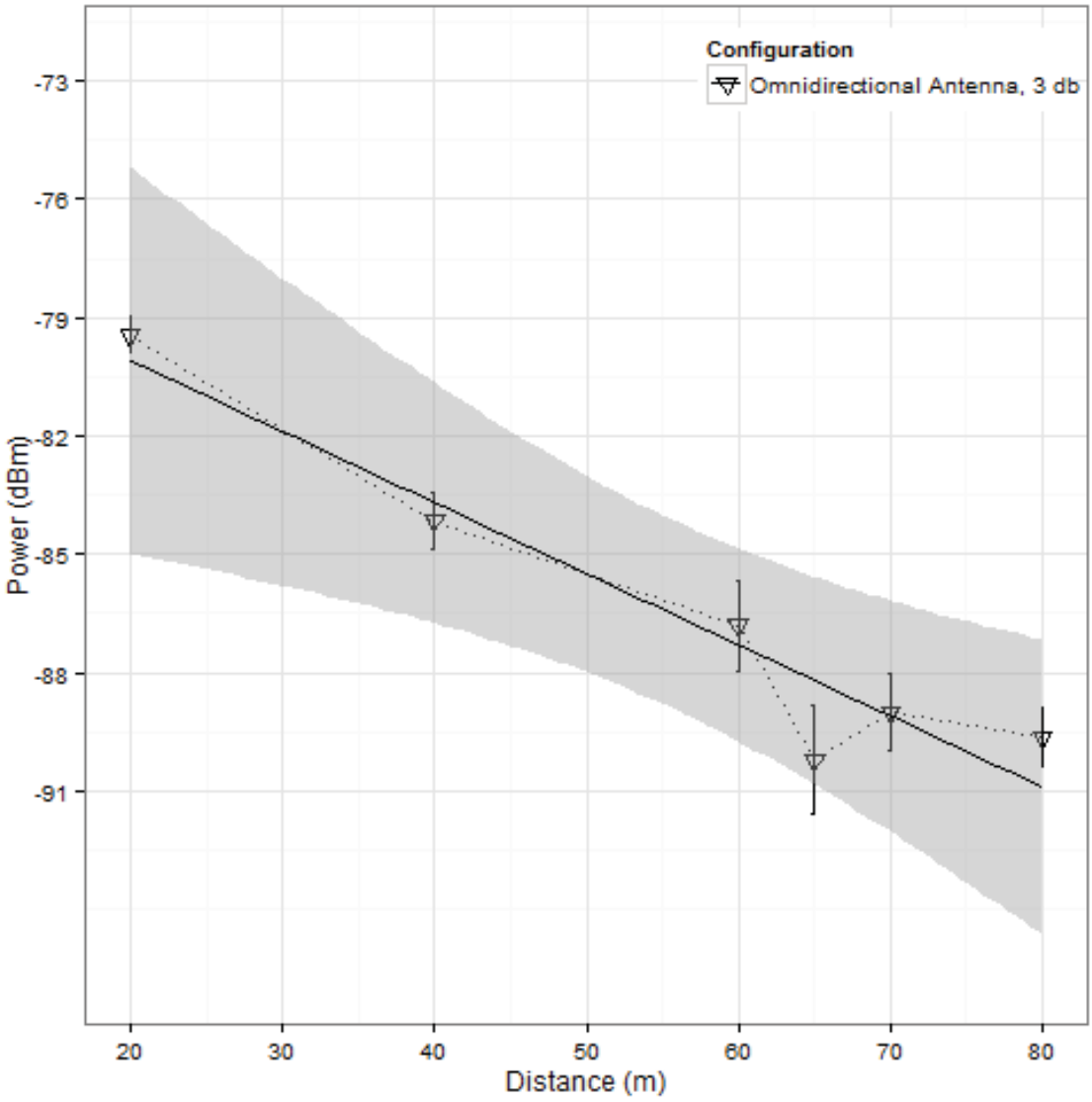


Figure 4.9: Power (dbm) Versus Distance of the USRP with Omnidirectional Antenna and 3 db Gain

4.1.3 Directed Antenna.

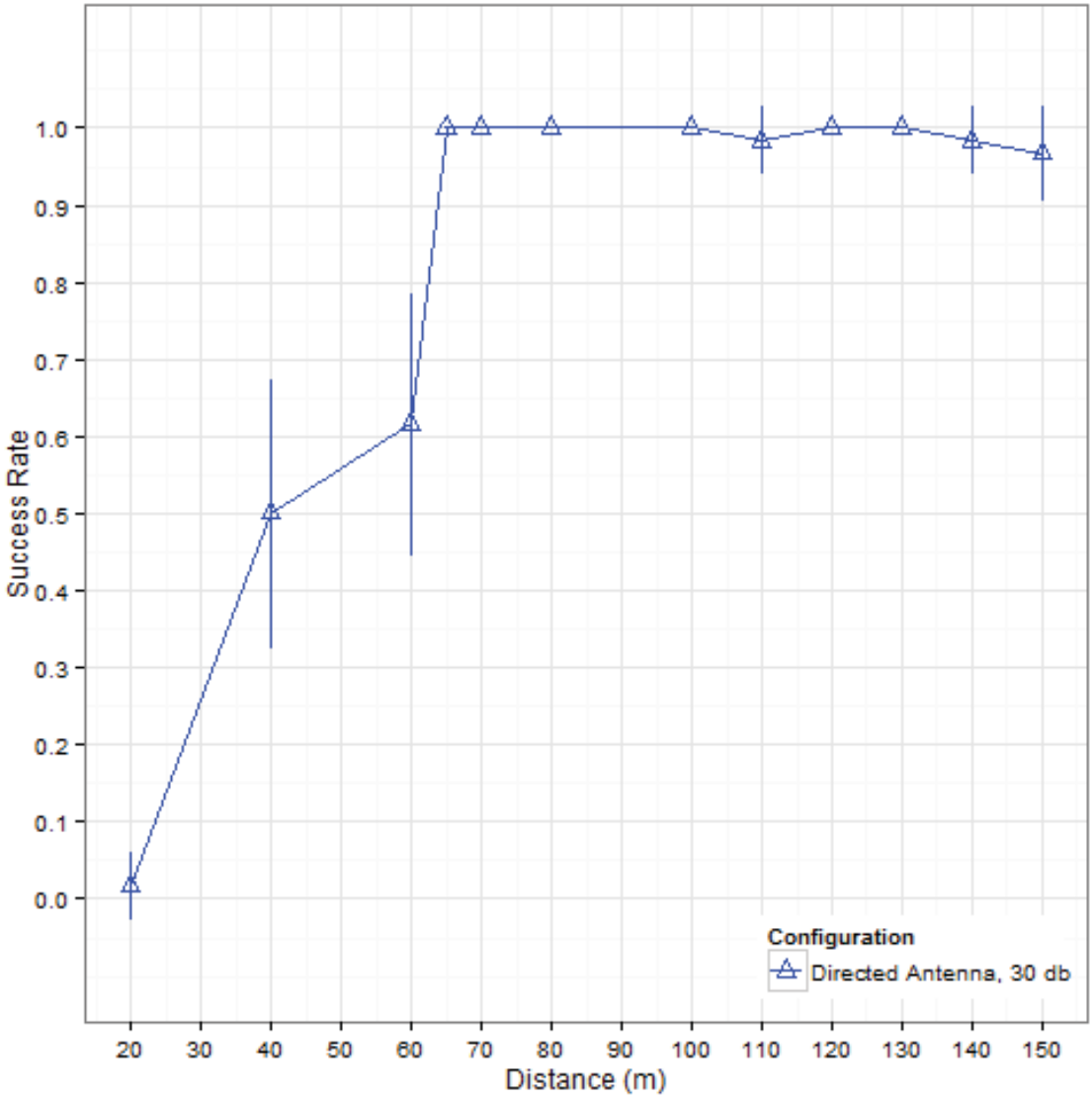


Figure 4.10: Probability of Success Versus Distance of the USRP with Directed Antenna and 30 db Gain

Figure 4.10, Figure 4.11, and Figure 4.12 display the probability of success of the USRP with the directed antenna. As with the omnidirectional antenna figures, each plot

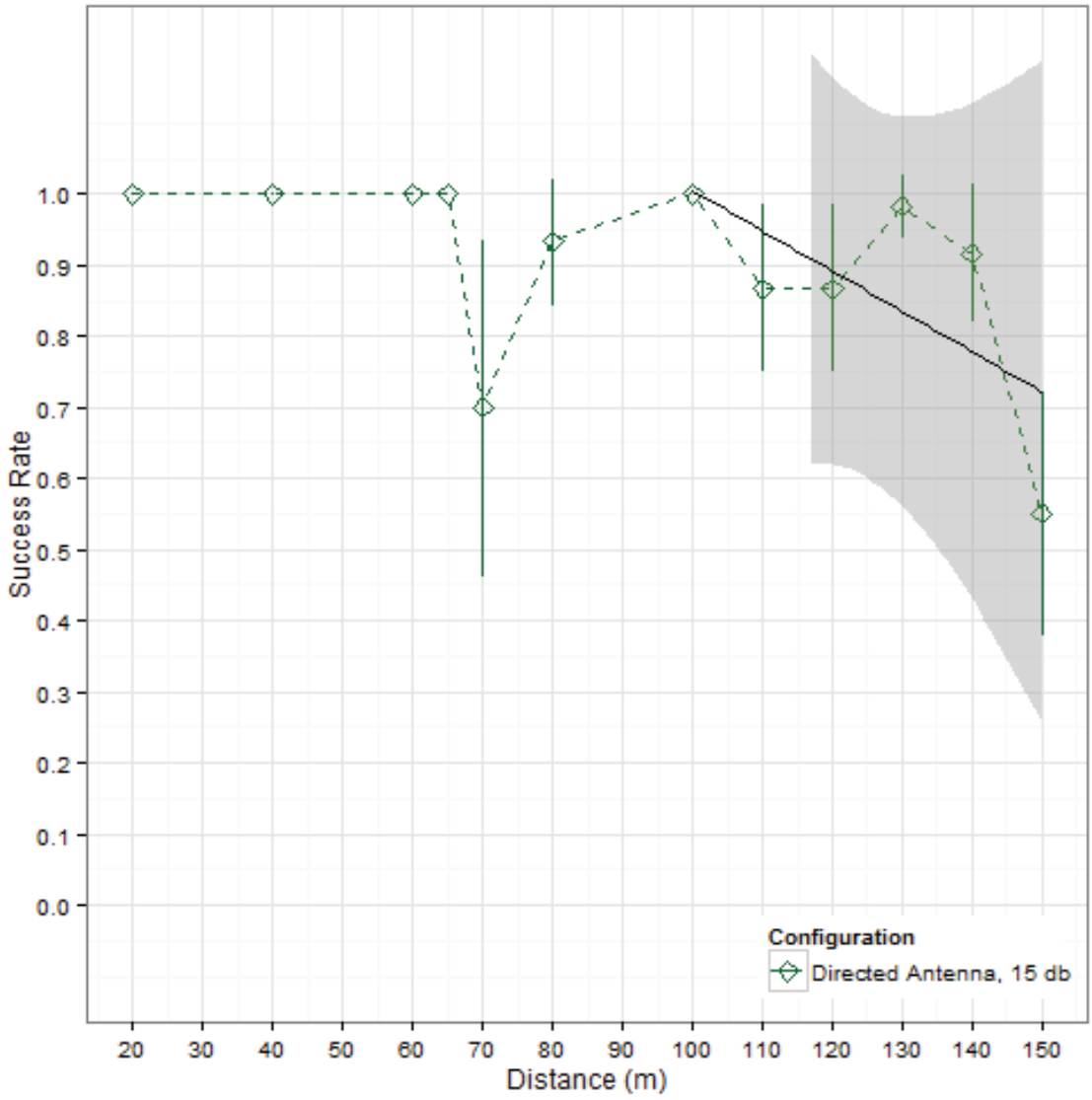


Figure 4.11: Probability of Success Versus Distance of the USRP with Directed Antenna and 15 db Gain

has three zones. Linear trend lines and shaded 99% confidence intervals are added to the transition zone of each. The attack with 30 db gain stays in the reception zone from 20 meters through 150 meters. The linear trend line of the transition zone of the USRP with 15 db gain is determined as 100 meters until the end of the experiment at 150 meters. The

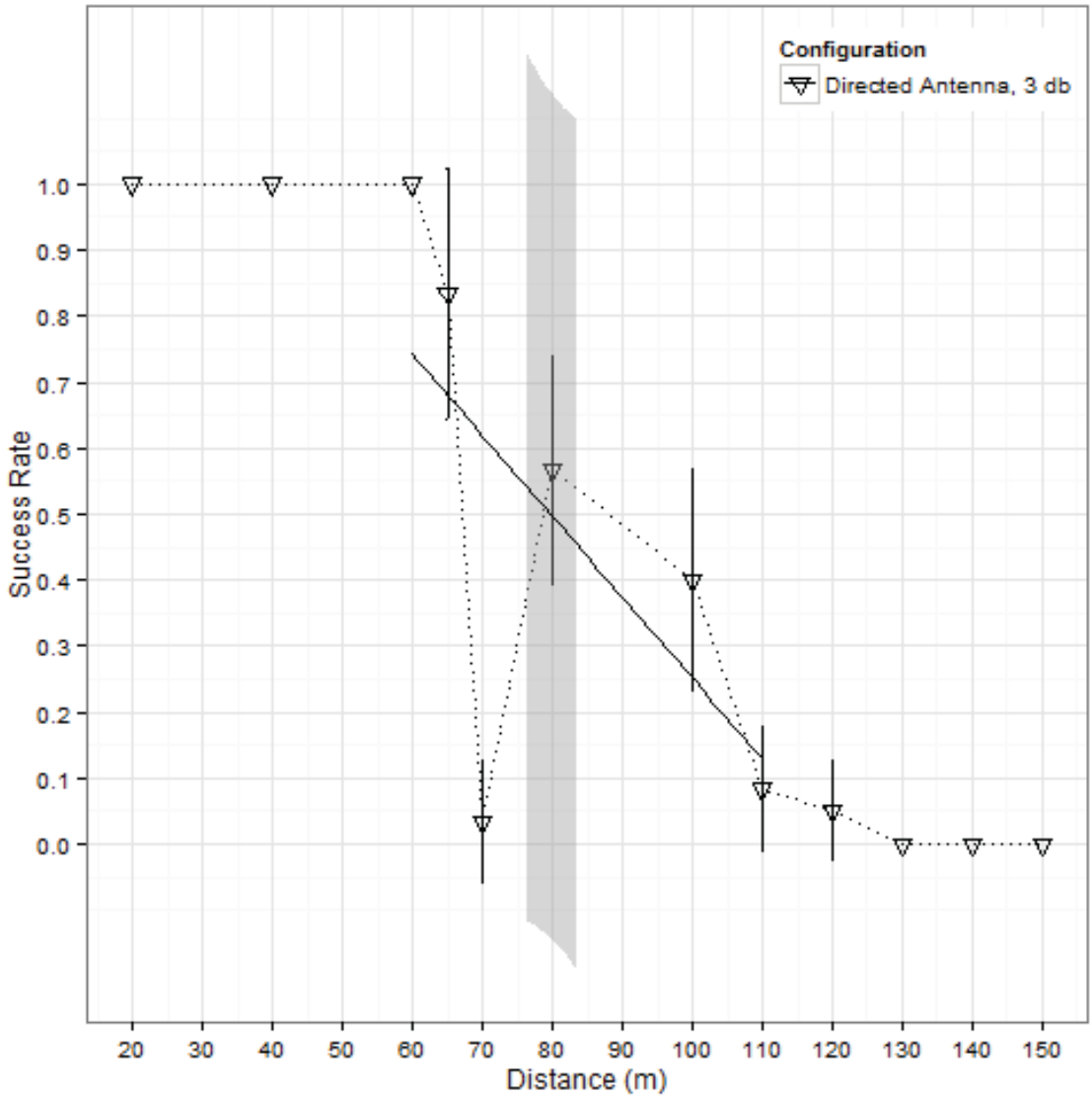


Figure 4.12: Probability of Success Versus Distance of the USRP with Directed Antenna and 3 db Gain

linear trend line of the transition zone of the USRP with 3 db gain is determined to be between 65 meters and 110 meters. The 30 db gain plot has similar low reception near the attacker as the omnidirectional antenna. This is probably due to the same reasons for the omnidirectional antenna's failure at close range. Both the low and medium power

receptions have drops in reception at 70 meters before rising to levels more in line with the logarithmic trend line. The cause is unknown, but as those measurements occurred at close to the same time of day, an external source of interference is possible.

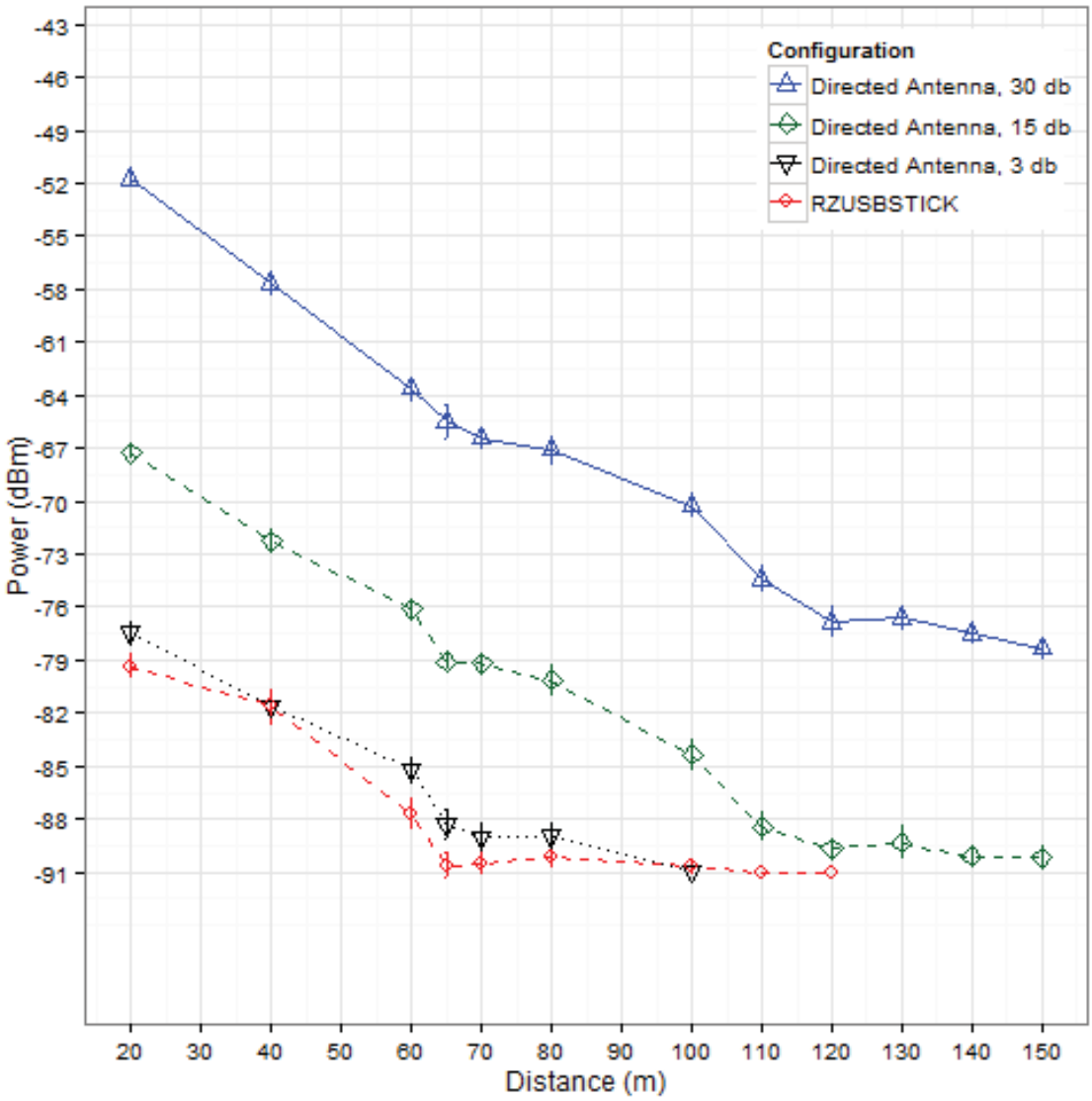


Figure 4.13: Power (dbm) of the RZUSBSTICK Compared to the USRP with Directed Antenna while in Line of Sight of the Victim

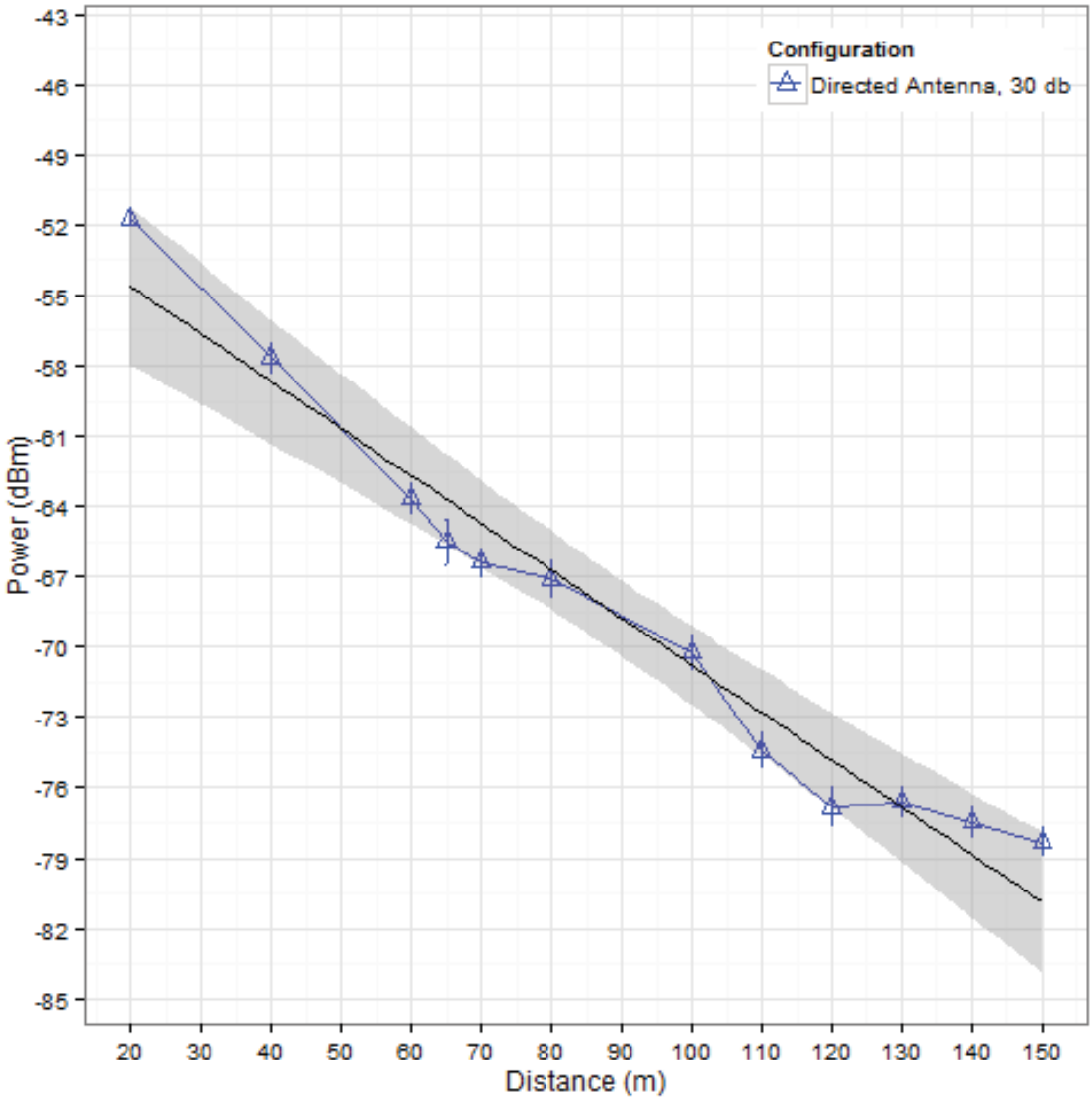


Figure 4.14: Power (dbm) Versus Distance of the USRP with Directed Antenna and 30 db Gain

Figure 4.13 shows the power received by the sensor near the victim device in dbm for the RZUSBSTICK and the USRP using a directed antenna. Figure 4.14, Figure 4.15, and Figure 4.16 display the power received by the sensor in separate plots. Again, data points that were not measured due to reception reasons are omitted. Overall, each decreases in a

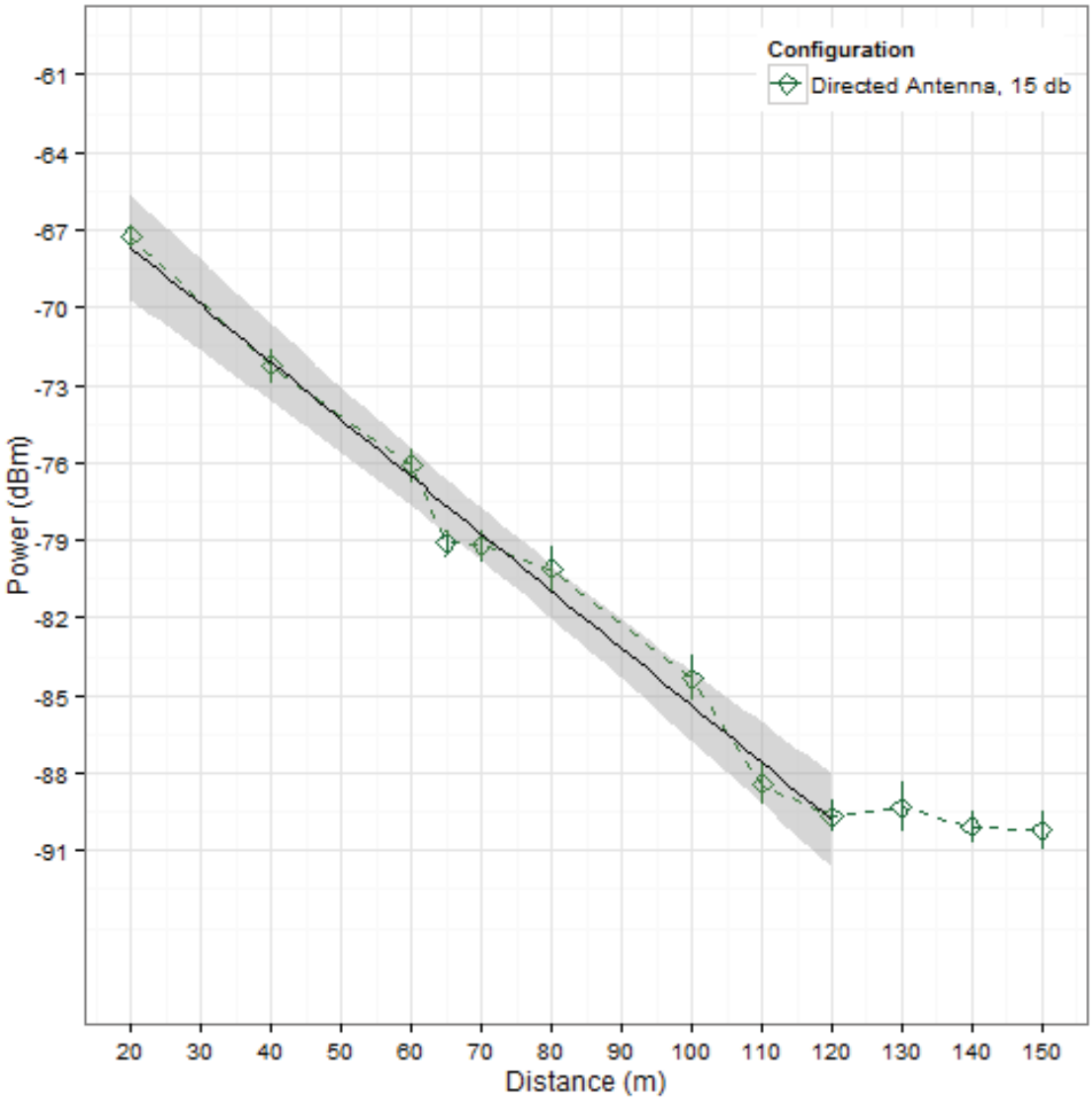


Figure 4.15: Power (dbm) Versus Distance of the USRP with Directed Antenna and 15 db Gain

similar fashion. Each appears logarithmic while the power level is above the power threshold of the sensor. The USRP with directed antenna clearly delivers more power than the RZUSBSTICK when the transmit gain is 15 or 30 db.

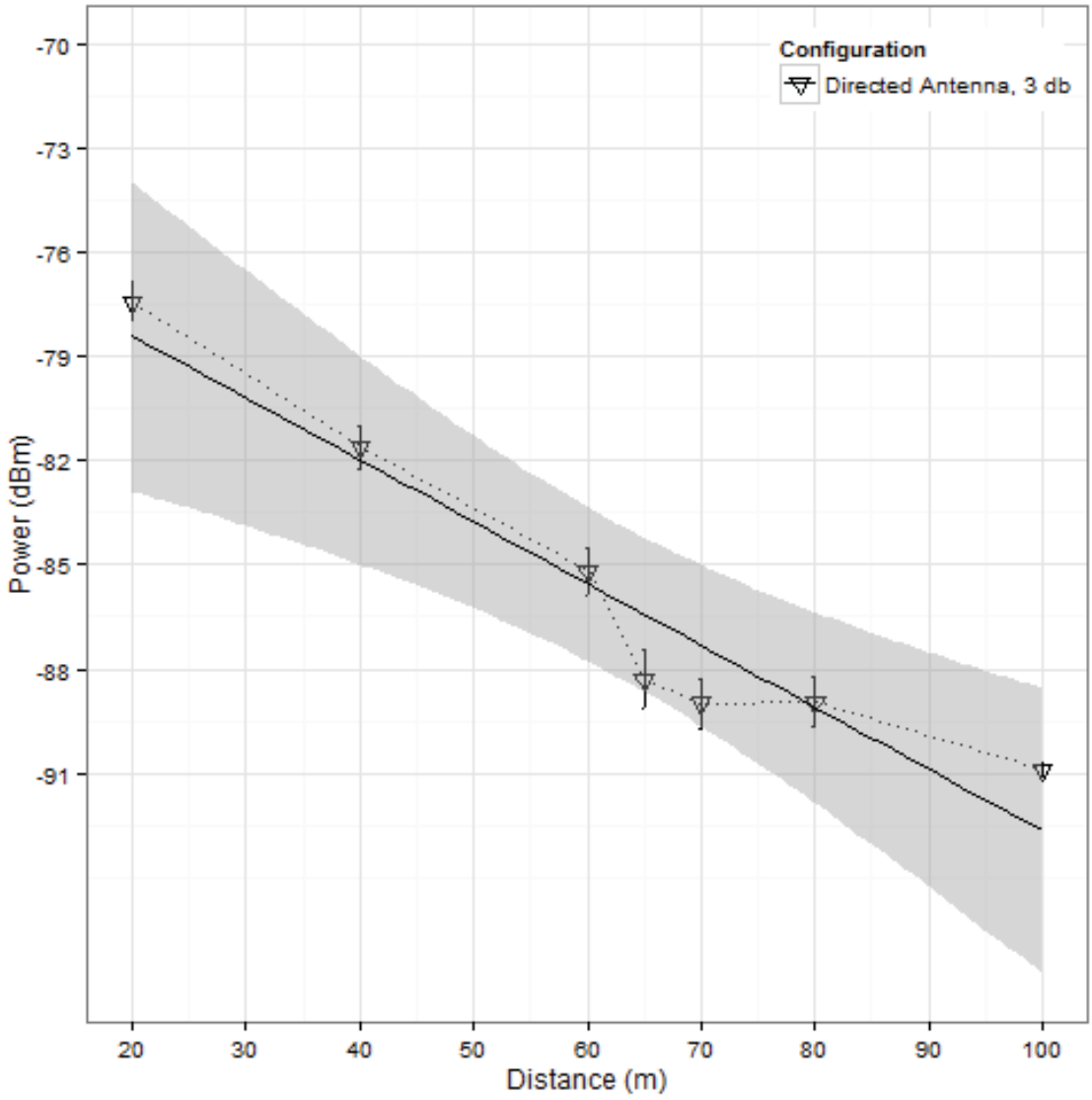


Figure 4.16: Power (dbm) Versus Distance of the USRP with Directed Antenna and 3 db Gain

4.2 Indoor Scenario

This section details the indoor part of the experiment where the line of sight between the attacker and victim is blocked. It is further broken down by configuration of the USRP. Section 4.2.1 presents the performance of the RZUSBSTICK. Section 4.2.2 presents the data relating to the USRP when it uses an omnidirectional antenna and compares it with the RZUSBSTICK. Section 4.2.3 presents the performance of the USRP when it uses a directed antenna and compares it with the RZUSBSTICK.

4.2.1 RZUSBSTICK.

Figure 4.17 shows the success rate of the RZUSBSTICK during the indoor part of the experiment, indicating that the probability of success of the RZUSBSTICK does not have the characteristic three zone structure. Instead, the probability of success drops cleanly from 100% reception to 0% reception between 20 and 25 meters. There is no transition zone.

Figure 4.18 shows the power received by the sensor is at the detection threshold. Since the victim is still responding to the beacon request frame, while the sensor reports an RSSI number at the threshold, the replay attack requires less power to succeed against the victim than the sensor is able to detect. Beyond 25 meters, neither the victim nor the sensor can detect the RZUSBSTICK.

4.2.2 Omnidirectional Antenna.

Figure 4.19 shows the probability of success versus distance of the replay attack for the RZUSBSTICK and the USRP using an omnidirectional antenna. While using a transmit gain of 3 db, the USRP offers 67% reception at 15 meters before dropping to 0% reception at 20 meters and beyond. With 15 db gain, the USRP has near 100% reception from 15 to 25 meters. It then enters the characteristic transition zone between 25 and 30

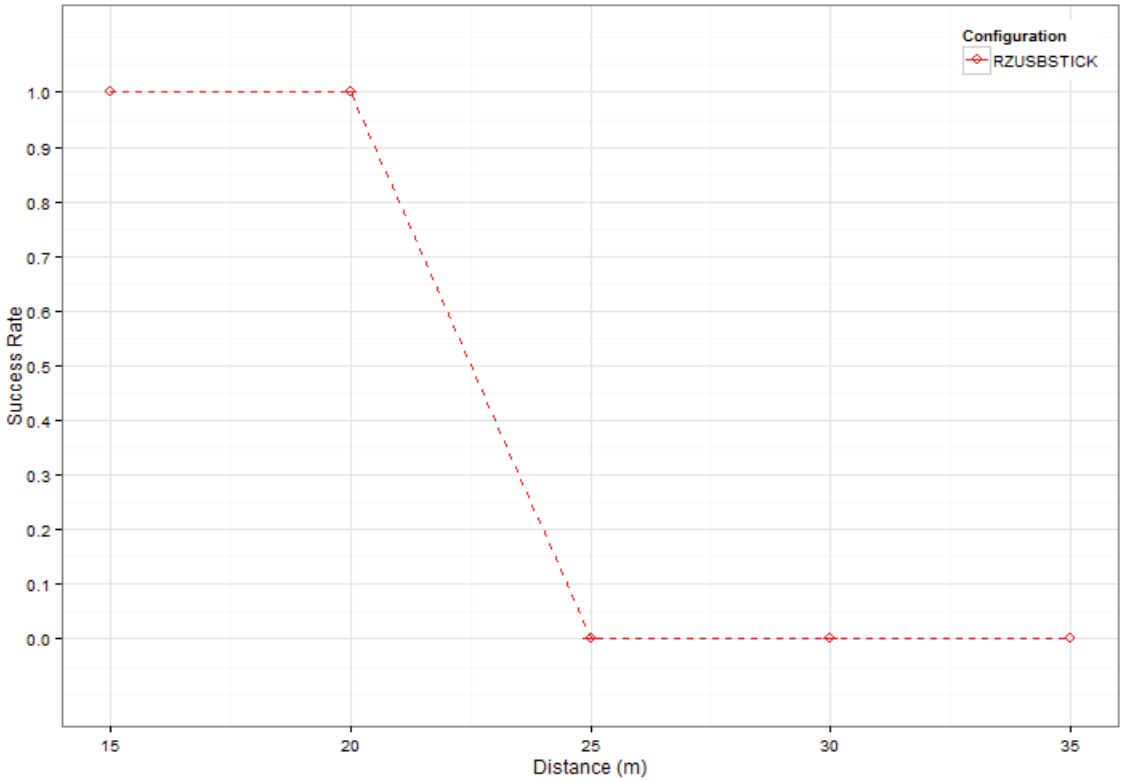


Figure 4.17: Probability of Success Versus Distance of the RZUSBSTICK

meters. With a transmit gain of 30 db, the USRP maintains 100% reception throughout this section of the experiment despite line of sight being blocked.

Figure 4.20 displays the power versus distance of the RZUSBSTICK and USRP for the indoor, blocked line of sight portion of the experiment. Figure 4.21 and Figure 4.23 display the power received by the sensor in separate plots. There is only a single mean for the low power data set, so the graph is omitted. Figure 4.21 shows that the 30 db power data set drops logarithmically until 30 meters where the power received falls unexpectedly. Figure 4.22 shows the data set with a logarithmic trend line that has omitted the 30 meter measurement. The power reading at 30 meters is clearly anomalous, but it is unclear what caused the power to drop. An additional wall is between the 25 and 30 meter

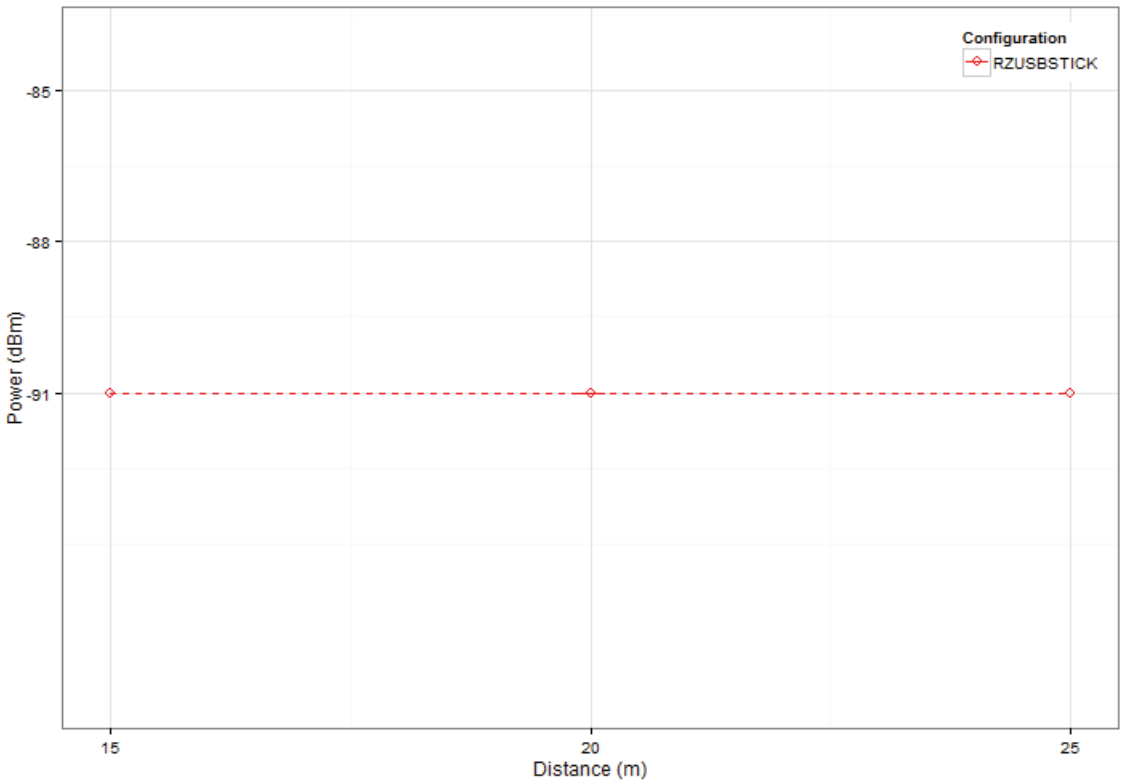


Figure 4.18: Power Versus Distance of the RZUSBSTICK

measurements, but that does not explain why the power at 35 meters is greater than the power at 30 meters. The 30 meter measurement is best explained as an outlier. Figure 4.23 displays the power of the USRP with 15 db transmit gain. The power drops logarithmically from 15 to 30 meters. The 35 meter measurement is at the detection threshold of the sensor.

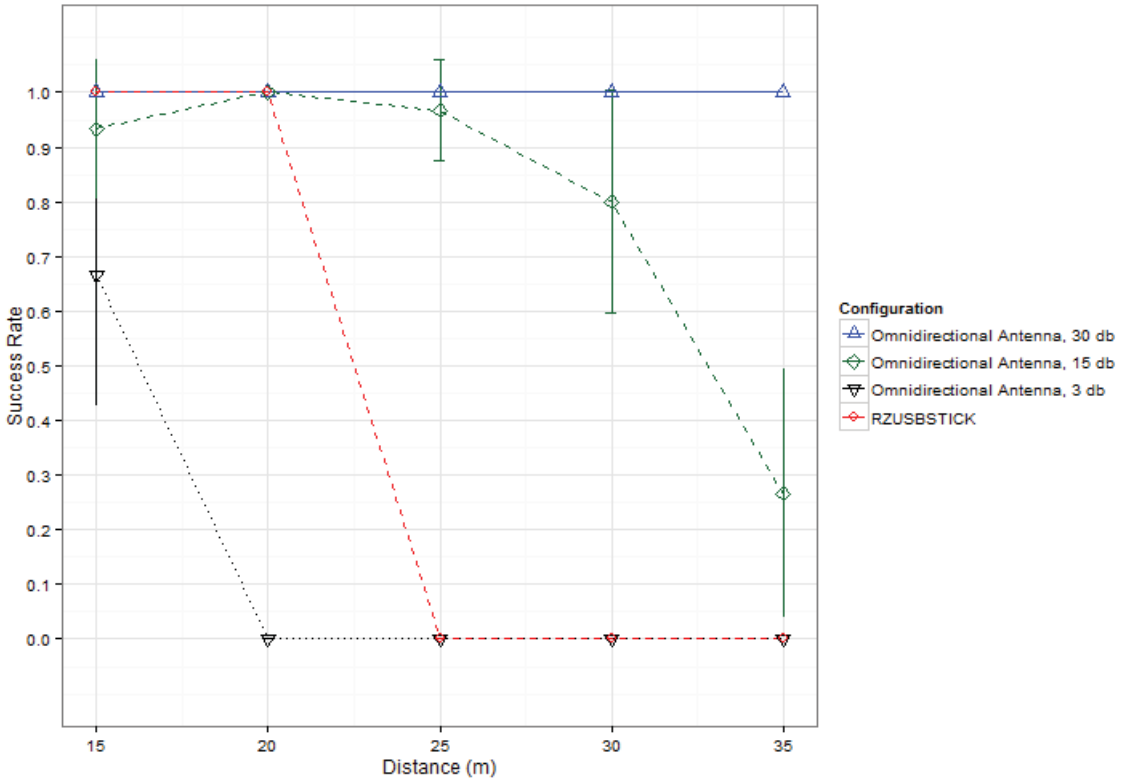


Figure 4.19: Probability of Success of the RZUSBSTICK Compared to the USRP with Omnidirectional Antenna while not in Line of Sight of the Victim

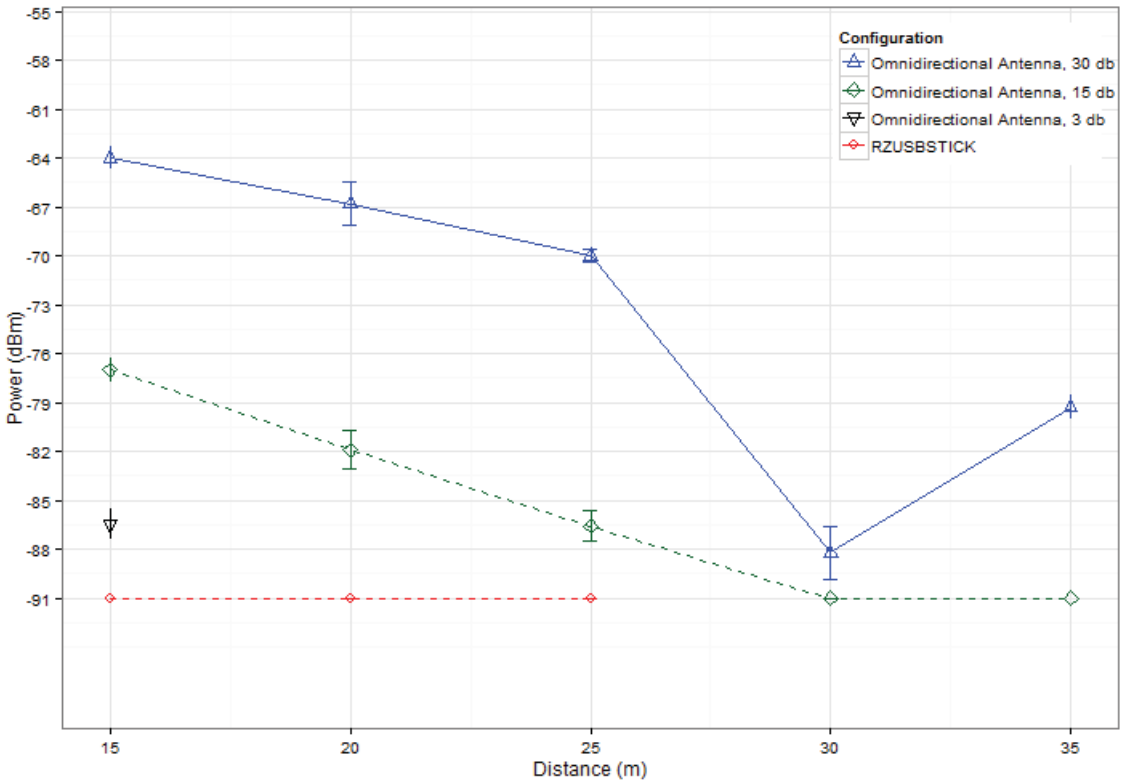


Figure 4.20: Power (dbm) of the RZUSBSTICK Compared to the USRP with Omnidirectional Antenna while not in Line of Sight of the Victim

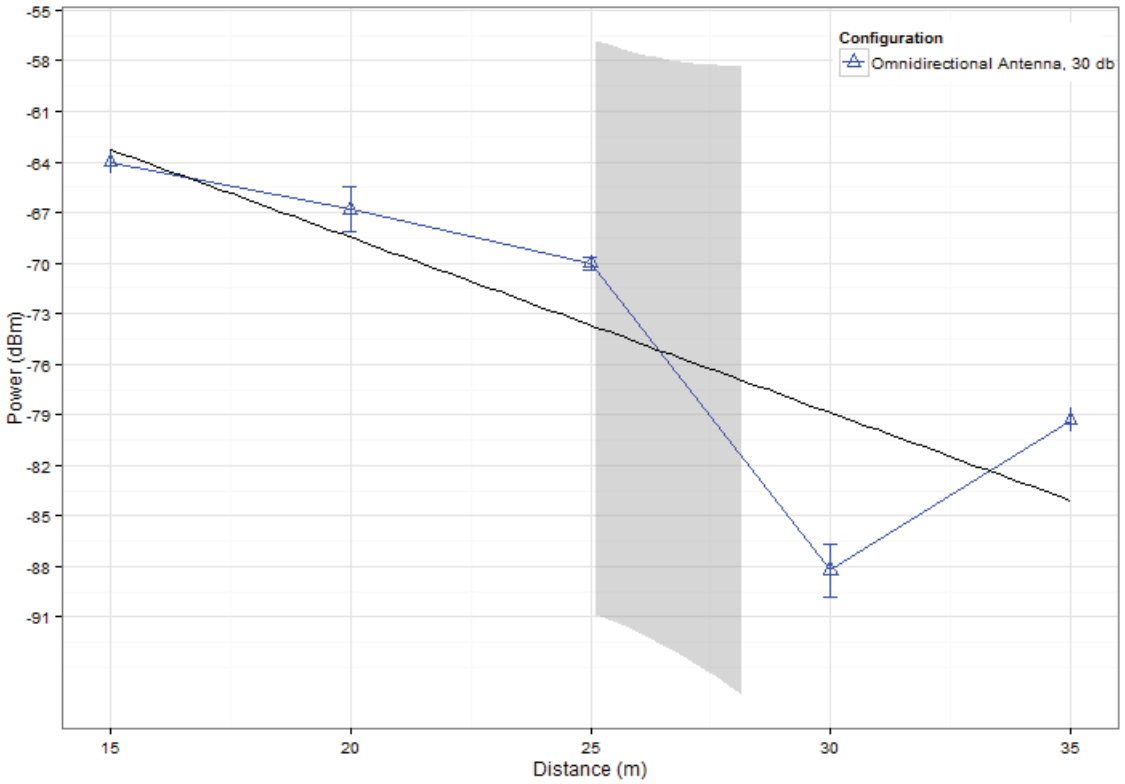


Figure 4.21: Power (dbm) Versus Distance of the USRP with Omnidirectional Antenna and 30 db Gain

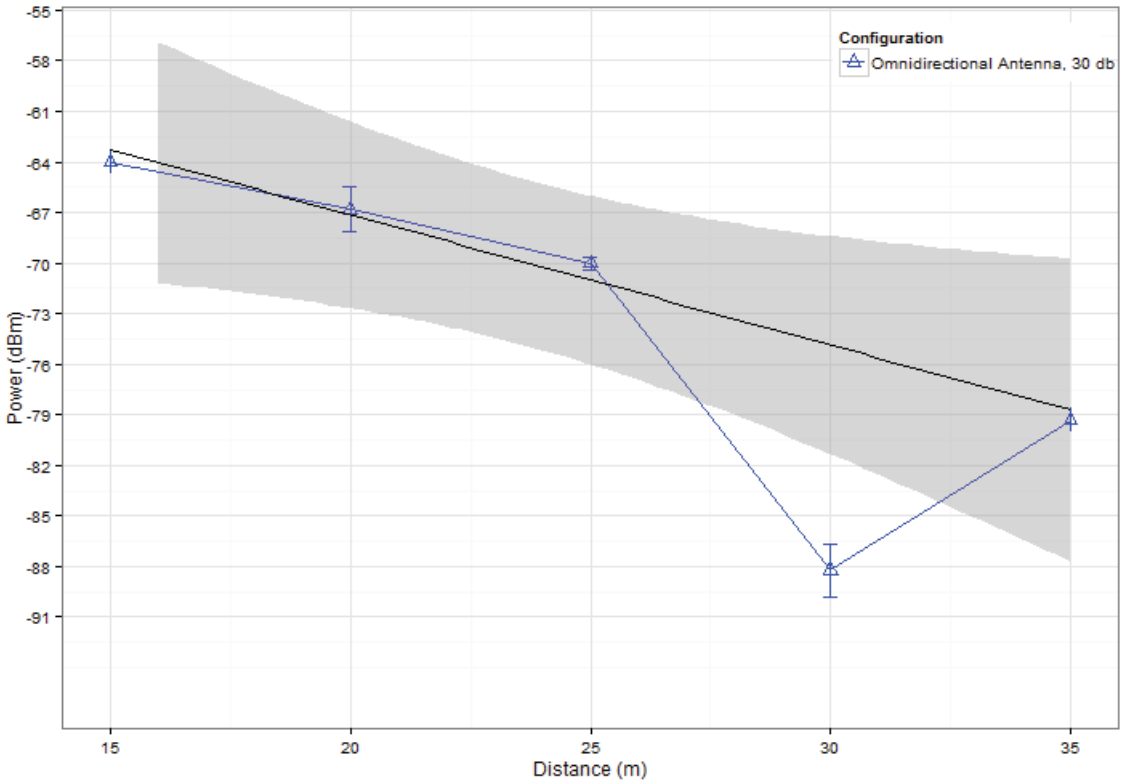


Figure 4.22: Power (dbm) Versus Distance of the USRP with Omnidirectional Antenna and 30 db Gain With More Appropriate Trend Line

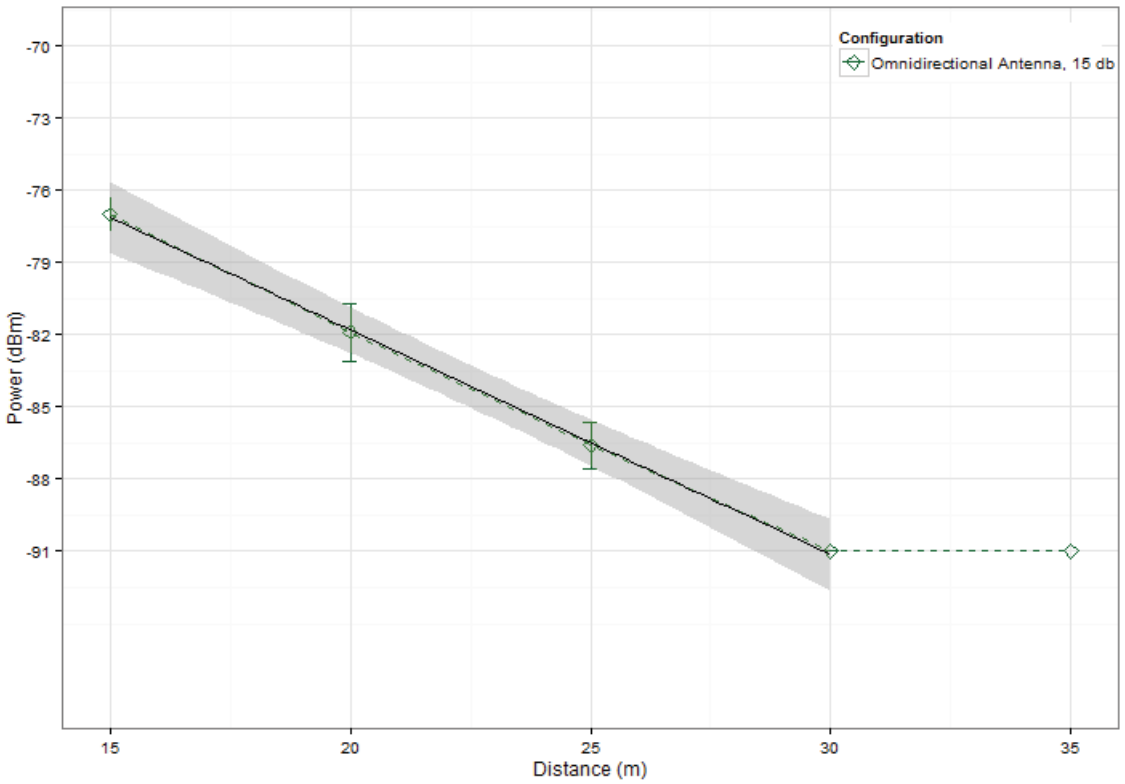


Figure 4.23: Power (dbm) Versus Distance of the USRP with Omnidirectional Antenna and 15 db Gain

4.2.3 Directed Antenna.

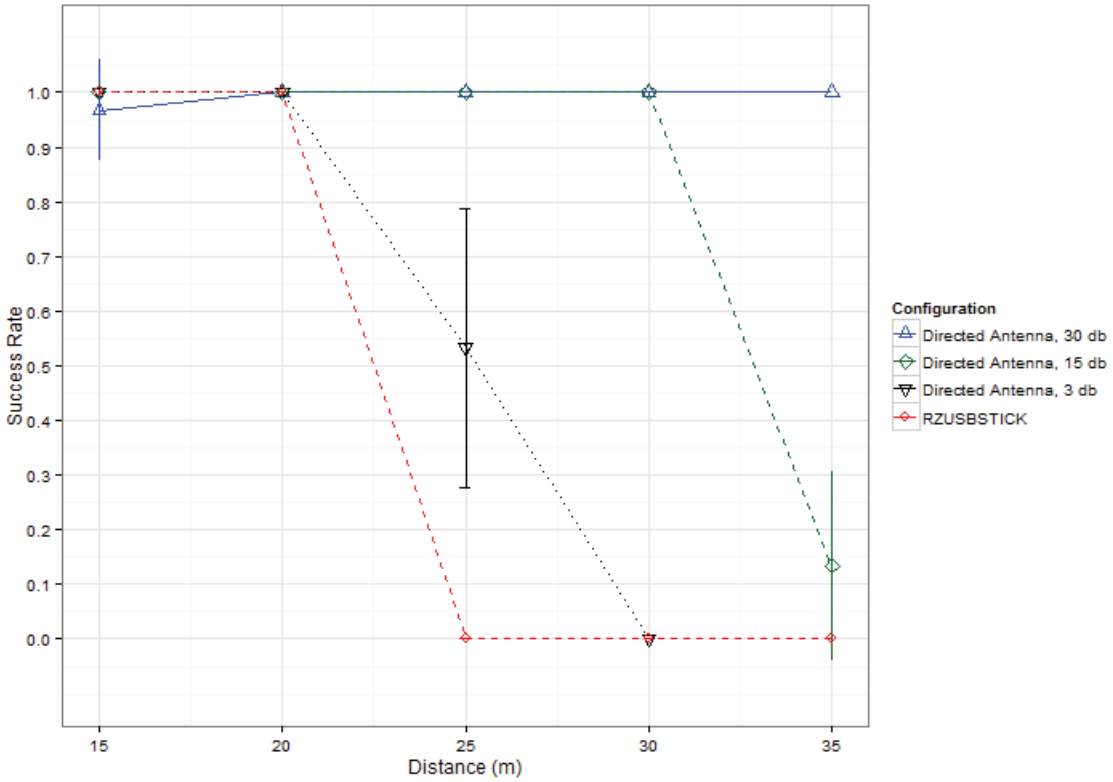


Figure 4.24: Probability of Success of the RZUSBSTICK Compared to the USRP with Directed Antenna while not in Line of Sight of the Victim

Figure 4.24 shows the probability of success versus distance of the replay attack for the RZUSBSTICK and the USRP using a directed antenna. Each transmit gain setting on the USRP offers superior reception to the RZUSBSTICK. The USRP transmitting at 3 db is able to execute the attack successfully at 15 and 20 meters. At 25 meters, the probability of success is approximately 50%. At further distances, there is 0% reception. While using a transmit gain of 15 db, the USRP maintains reception through 30 meters. The USRP with 30 db transmit gain is nearly 100% successful across all distances.

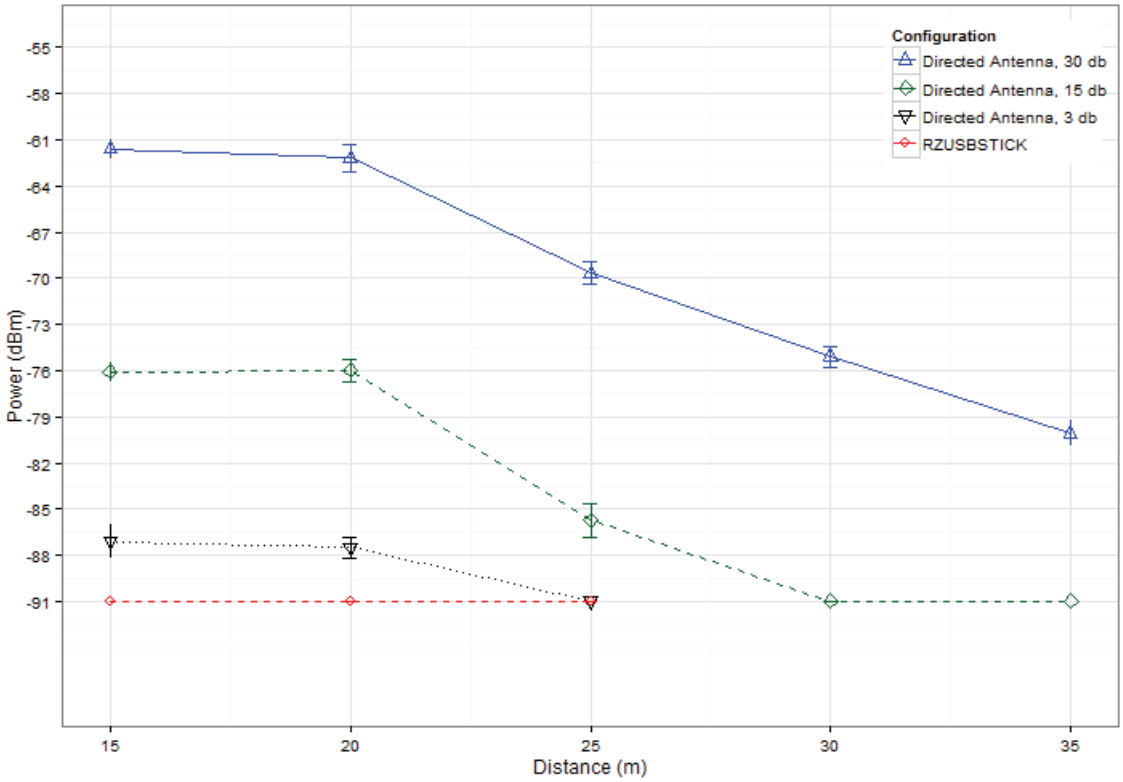


Figure 4.25: Power (dbm) of the RZUSBSTICK Compared to the USRP with Directed Antenna while in Line of Sight of the Victim

Figure 4.25 displays the power versus distance of the RZUSBSTICK and USRP with directed antenna for the blocked line of sight portion of the experiment. Figure 4.26, Figure 4.27, and Figure 4.28 display the power received by the sensor in separate plots. The power received by the sensor near the victim appears to decay logarithmically with distance for each gain setting of the USRP with directed antenna. This is interesting as there are no large drops in power received when an additional wall is placed between the attacker and victim. An additional wall is added between the 15 and 20 meter measurements and again between the 25 and 30 meter measurements. Also, the power received at 15 meters is similar to the power received at 20 meters. A larger drop would

normally be expected. From the trend line, the power received at 15 and 20 meters does not appear to be too far from the logarithmic model.

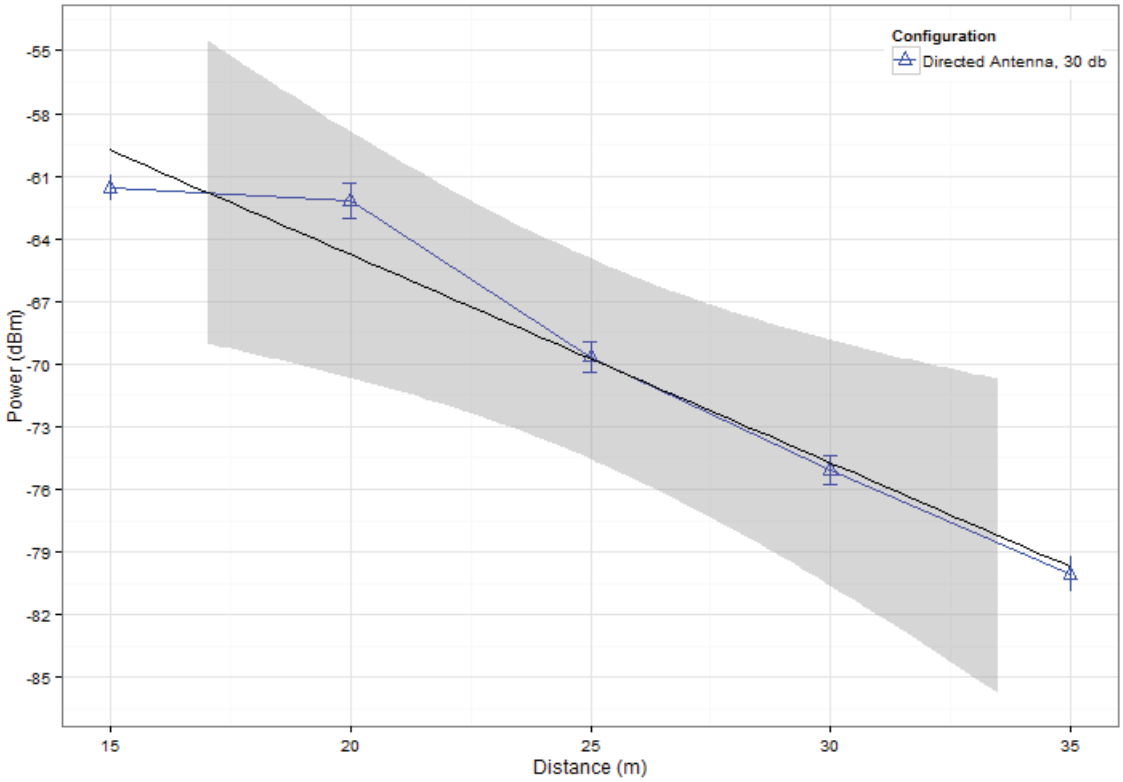


Figure 4.26: Power (dbm) Versus Distance of the USRP with Directed Antenna and 30 db Gain

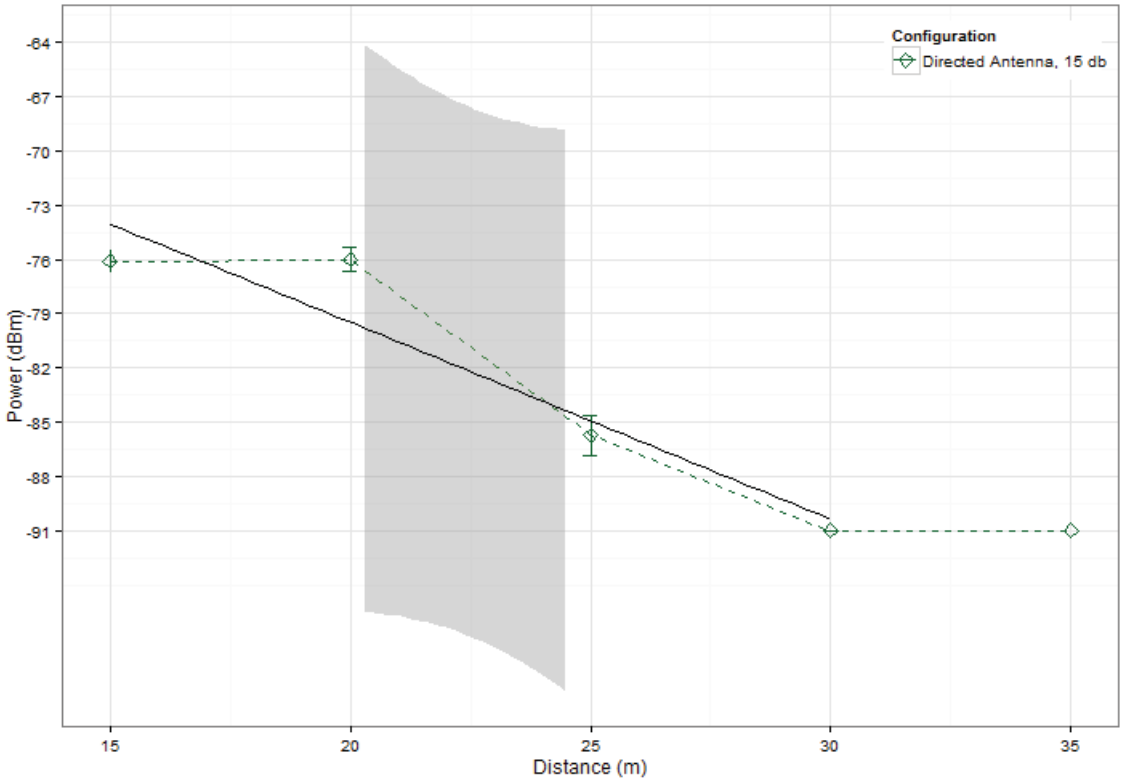


Figure 4.27: Power (dbm) Versus Distance of the USRP with Directed Antenna and 15 db Gain

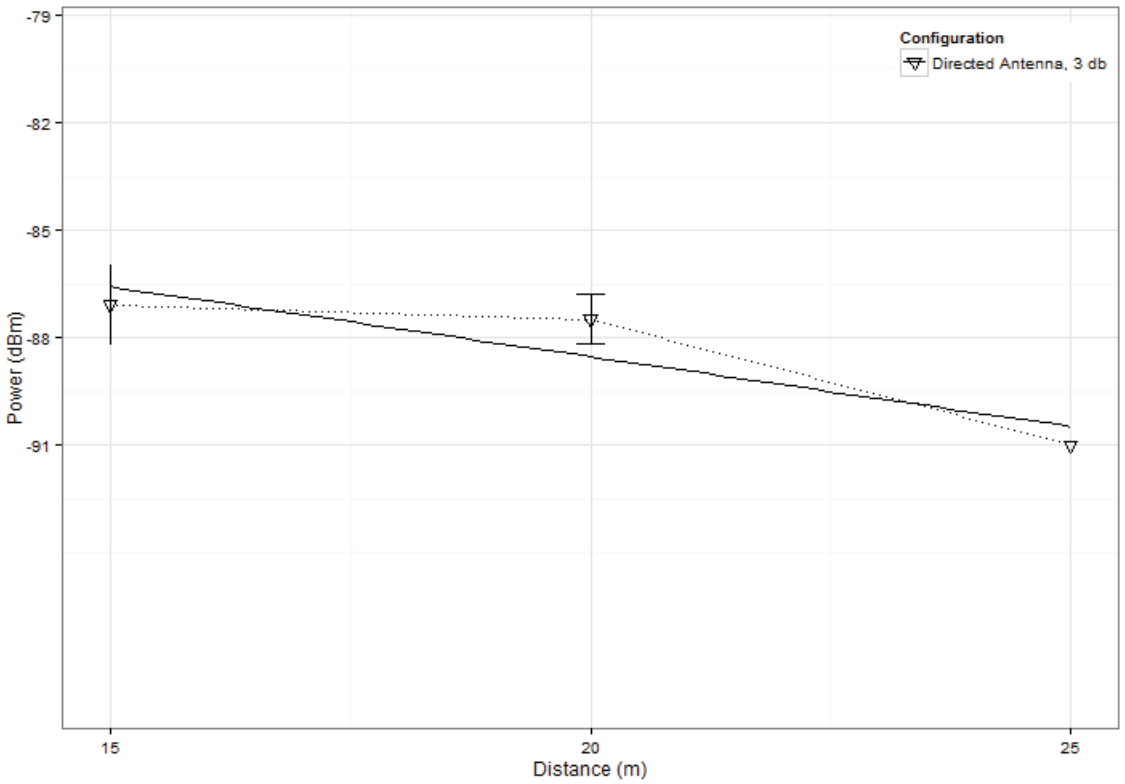


Figure 4.28: Power (dbm) Versus Distance of the USRP with Directed Antenna and 3 db Gain

4.3 GNU Radio Scenario

This section details the part of the experiment where the USRP is configured to use GNU Radio and ZigBee stack. In this portion of the experiment, line of sight between the attacker and victim is blocked. This section is further broken down by antenna used by the USRP. Section 4.3.1 presents the performance of the RZUSBSTICK. Section 4.3.2 presents the data relating to the USRP when it uses an omnidirectional antenna and compares it with the RZUSBSTICK. Section 4.3.3 presents the performance of the USRP when it uses a directed antenna and compares it with the RZUSBSTICK. The RZUSBSTICK does not use GNU Radio, but measurements are still taken to compare with the USRP.

4.3.1 RZUSBSTICK.

Figure 4.29 shows the success rate of the RZUSBSTICK during the GNU Radio part of the experiment. Since the number of trials is increased from 30 to 100 for this portion of the experiment, the attack with RZUSBSTICK is redone with the new number of trials. The RZUSBSTICK has similar results to the blocked line of sight experiment, as expected; except for a difference in reception at 20 meters. The exact cause of this deviation is unknown, but speculation is that the arrangement of furniture or items in closets could have changed between the experiments and affected the results. In this case, it has 100% reception at 15 meters and tapers off at 20 and 25 meters. Figure 4.30 shows the power of the RZUSBSTICK during the GNU Radio part of the experiment. The power never exceeds -91 dbm.

4.3.2 Omnidirectional Antenna.

Figure 4.31 shows the probability of success versus distance of the USRP using GNU Radio and an omnidirectional antenna and RZUSBSTICK. The USRP using GNU Radio demonstrates a poor success rate in executing the replay attack. When using a transmit

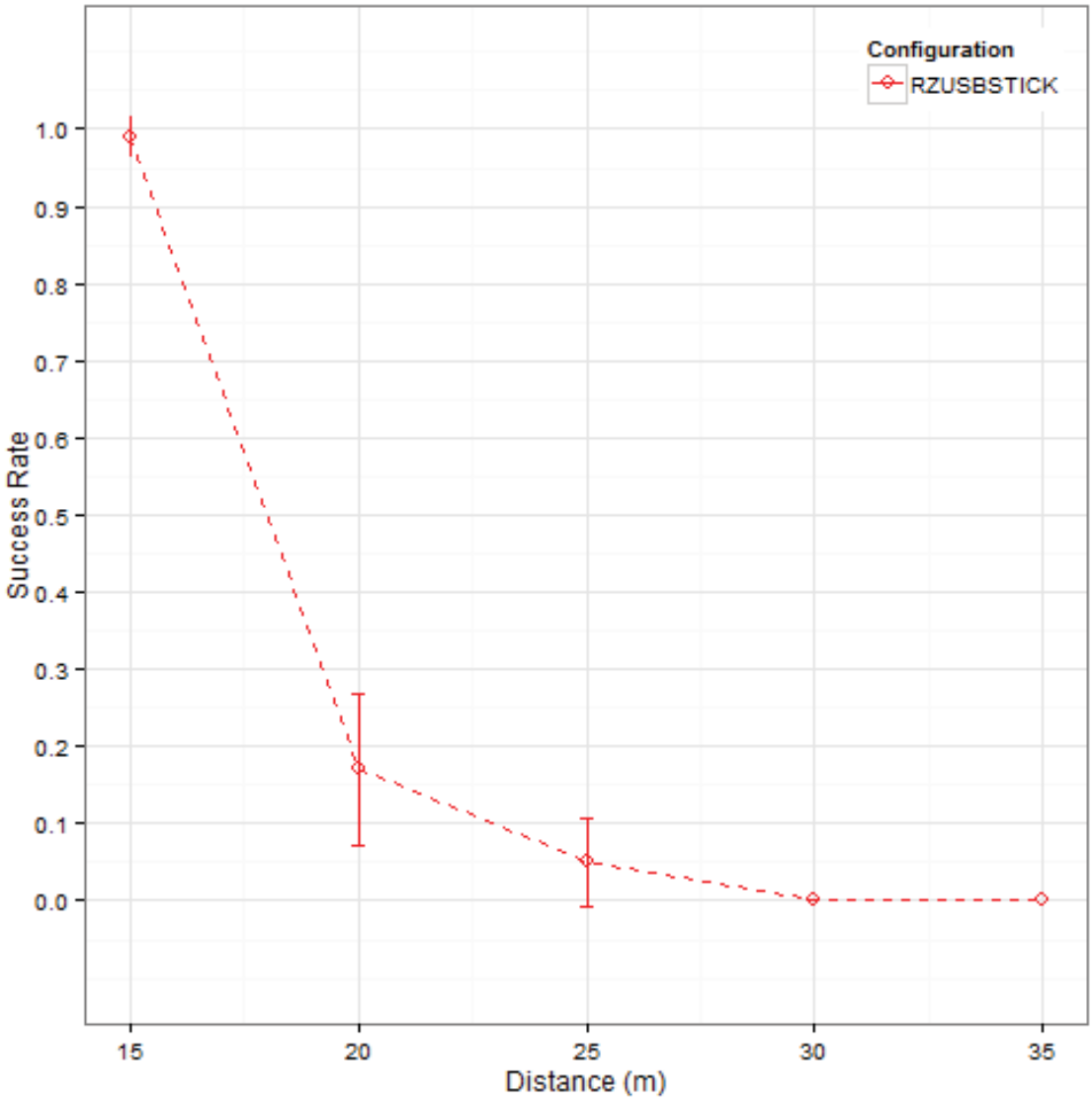


Figure 4.29: Probability of Success Versus Distance of the RZUSBSTICK

gain of 3 db, the USRP is able to achieve a success rate of 71% at 15 meters and 0% at 20 meters and above. From the indoor scenario, the USRP is expected to successfully complete the replay attack with transmit gains of 15 and 20 db, but the USRP is never able to achieve a greater mean success rate than 25% with 15 or 20 db transmit gain. However, the sensor was still able to sense ZigBee packets and register power levels for them.

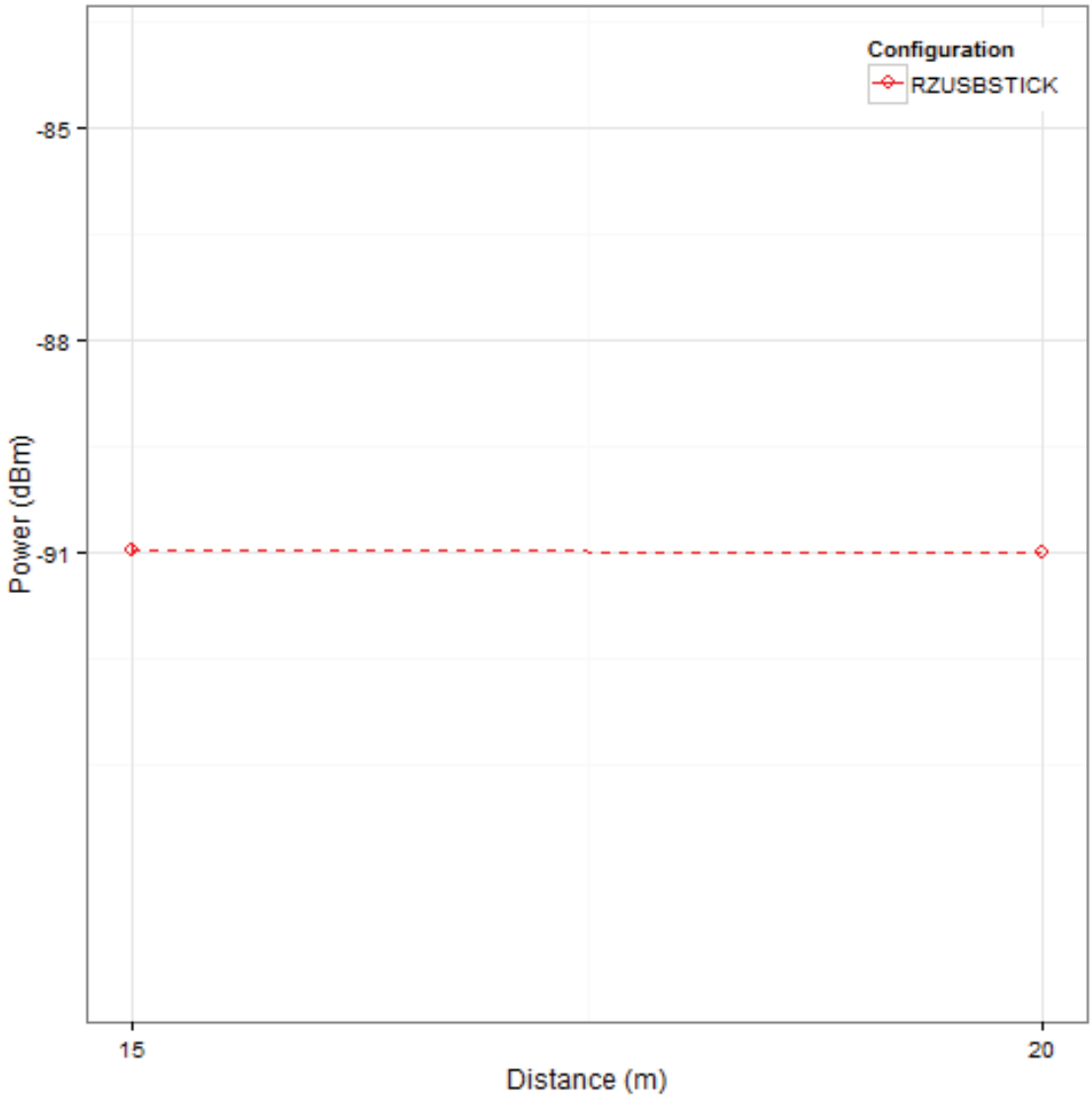


Figure 4.30: Power Versus Distance of the RZUSBSTICK

Figure 4.32 shows the probability that the sensor is able to detect a ZigBee packet versus distance of the USRP with omnidirectional antenna. That is, Figure 4.32 shows how often the sensor is able to measure the power near the victim and expresses it as a probability. The RZUSBSTICK has similar reception on both the victim and sensor. The reception is higher for the sensor at 20 meters. Reception is also similar for the USRP

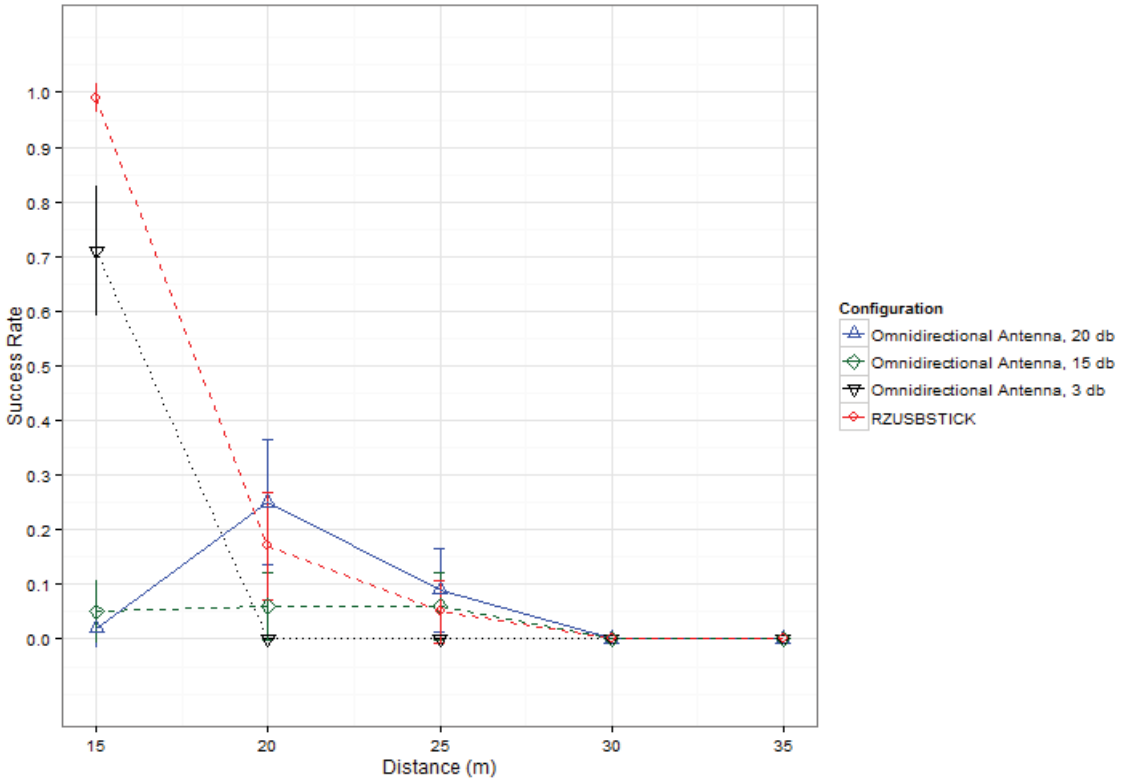


Figure 4.31: Probability of Success of the RZUSBSTICK Compared to the USRP with Omnidirectional Antenna and GNU Radio while not in Line of Sight of the Victim

with a transmit gain of 3 db. However, the results are very different for transmit gains of 15 and 20 db. In this plot, there is a drop in reception at 25 meters. The cause is unknown. Also, the reception rate is significantly higher against the sensor than against the victim. The exact cause is unknown. However, the sensor and victim are different devices. It is possible that this implementation of the ZigBee stack on GNU Radio is not entirely compatible with the Freescale victim.

Figure 4.33 displays the power versus distance of the RZUSBSTICK and USRP for the blocked line of sight portion of the experiment. Figure 4.34 and Figure 4.35 display the power received by the sensor in separate plots. The low power data set consists of two

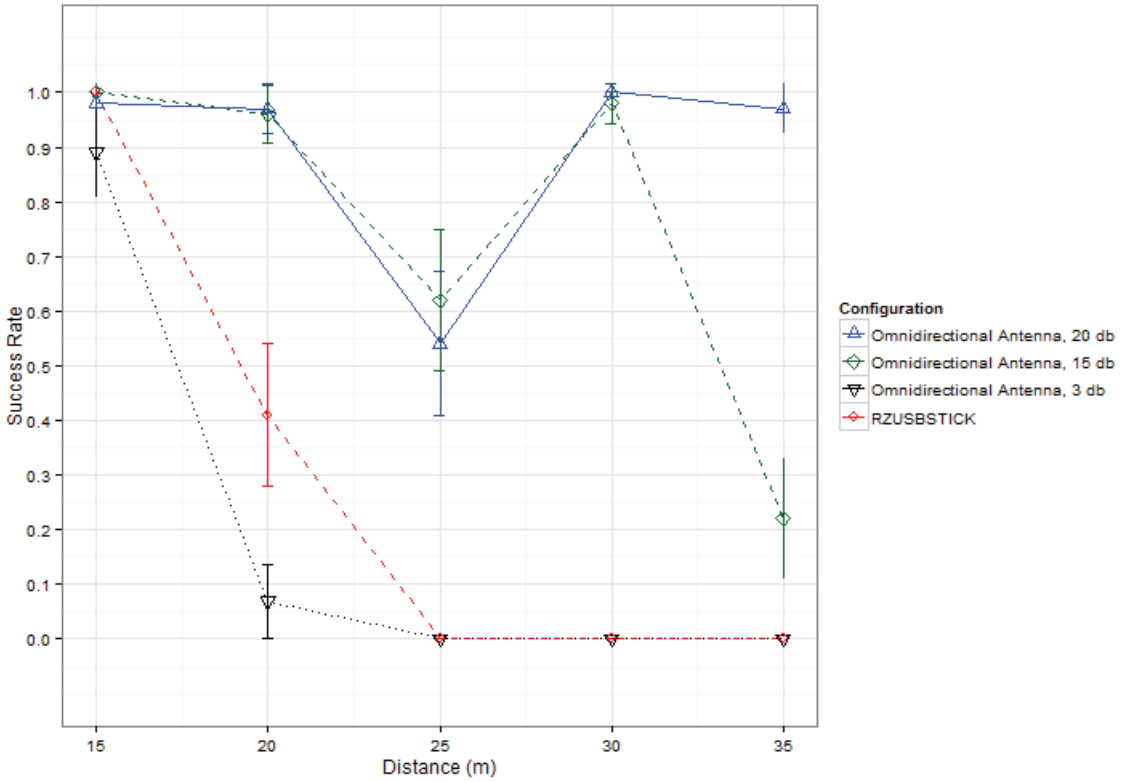


Figure 4.32: Probability of Success against the sensor of the RZUSBSTICK Compared to the USRP with Omnidirectional Antenna and GNU Radio while not in Line of Sight of the Sensor

means, so the graph is omitted. Linear trend lines with 99% confidence intervals are added to the high and medium power graphs. Both the medium and high power data sets drop logarithmically during this part of the experiment.

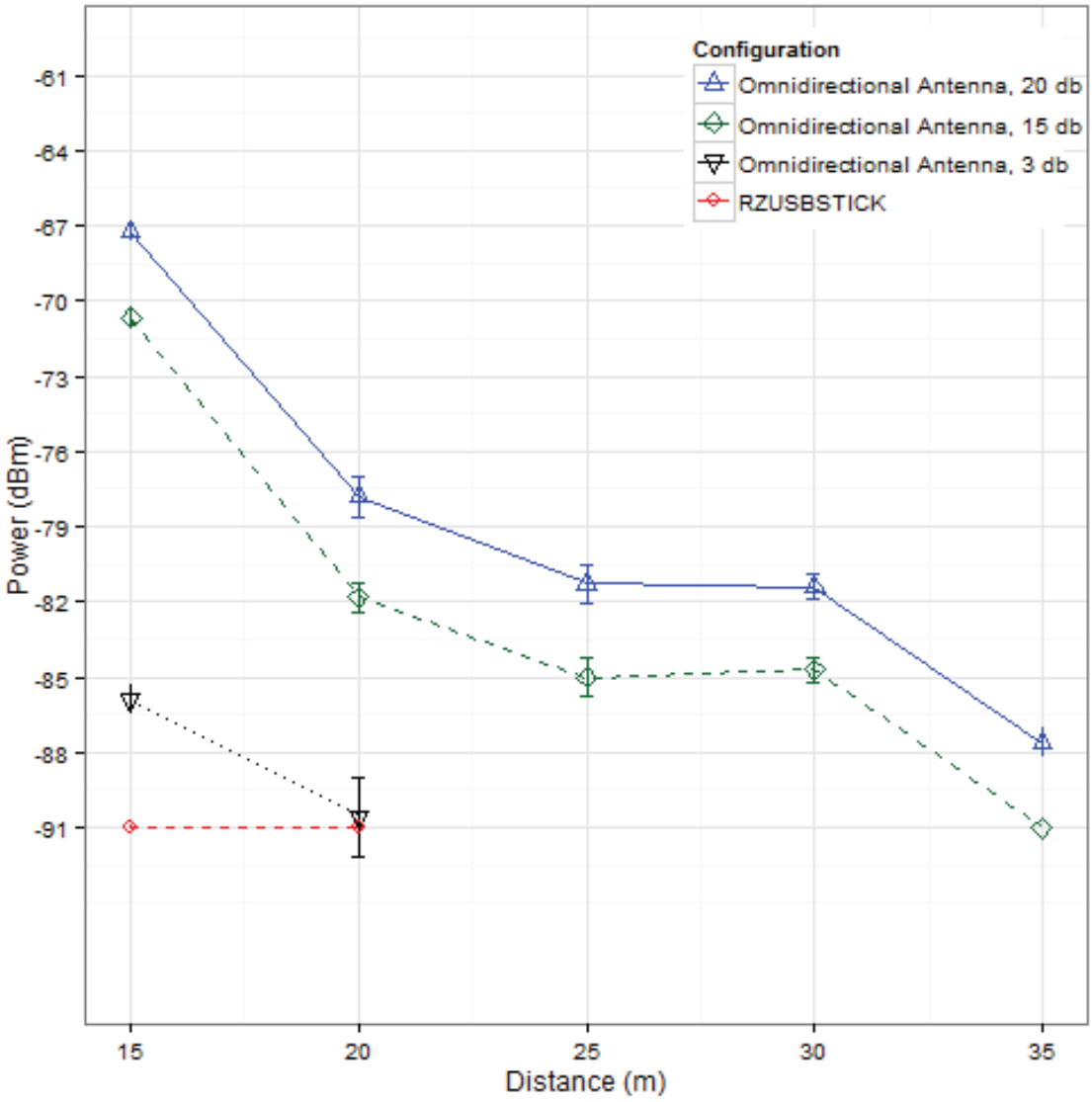


Figure 4.33: Power (dbm) of the RZUSBSTICK Compared to the USRP with Omnidirectional Antenna and GNU Radio while not in Line of Sight of the Victim

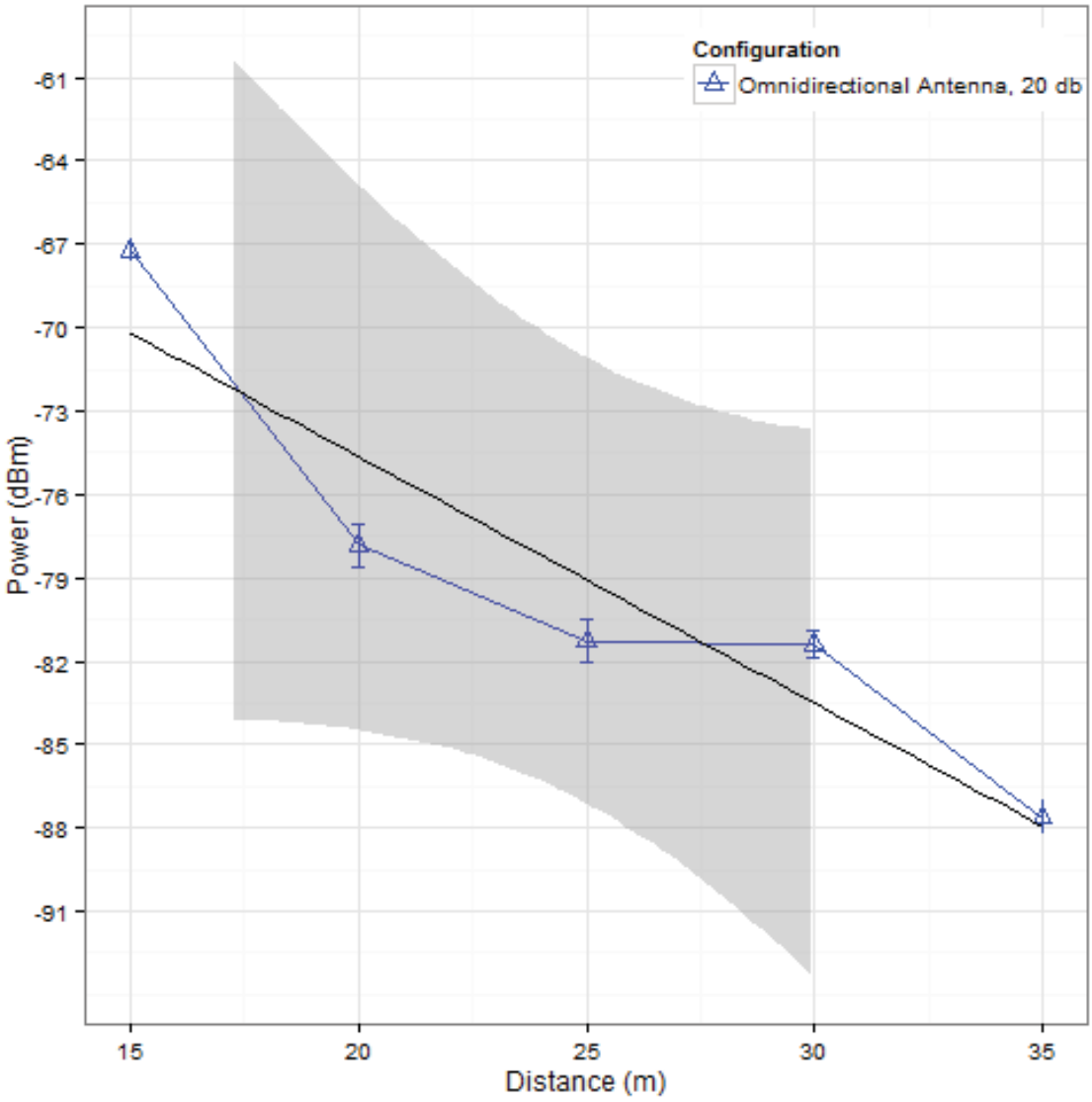


Figure 4.34: Power Versus Distance of the USRP with Omnidirectional Antenna and 20 db Gain

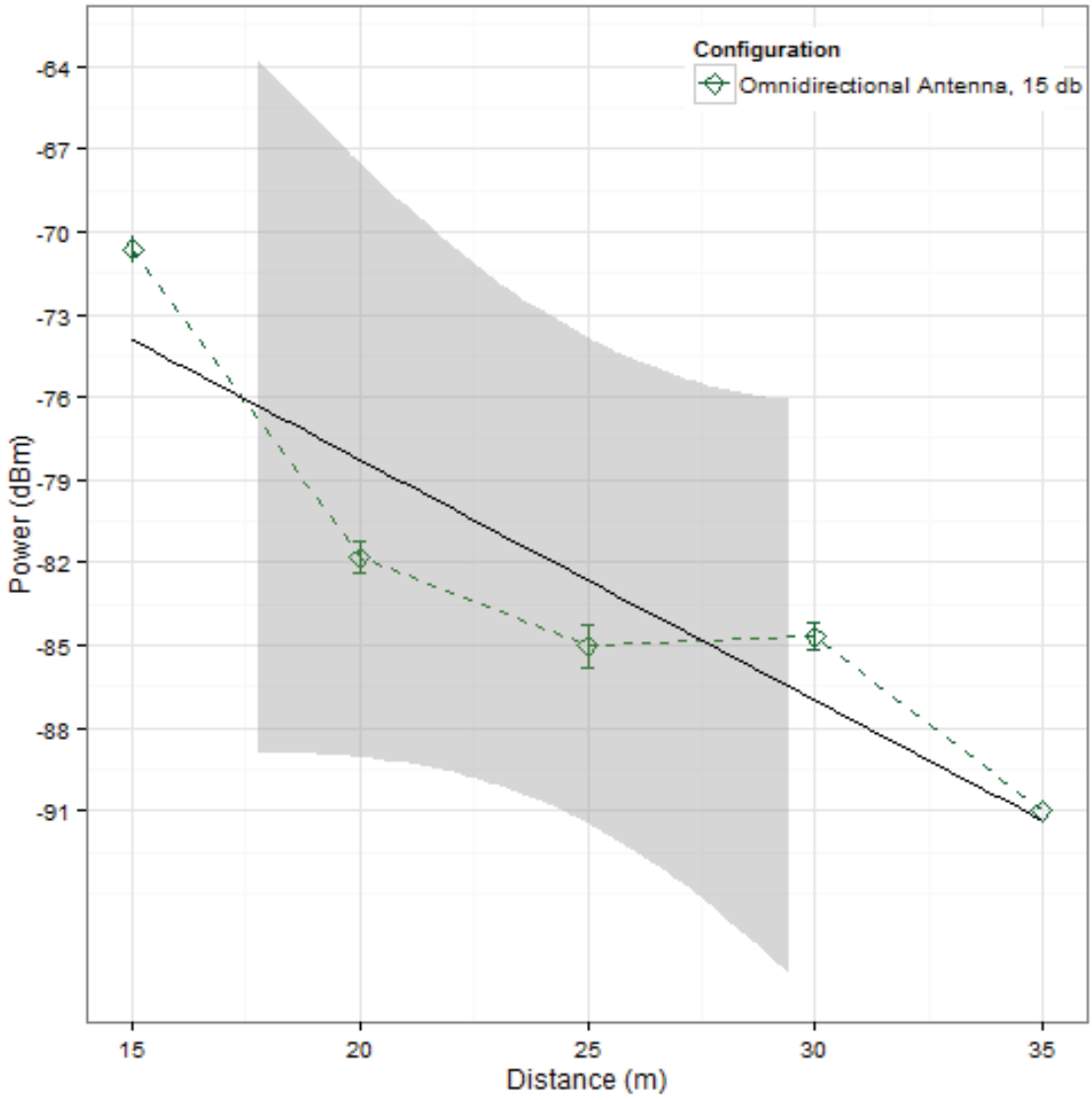


Figure 4.35: Power (dbm) Versus Distance of the USRP with Omnidirectional Antenna and 15 db Gain

4.3.3 Directed Antenna.

Figure 4.36 shows the probability of success versus distance of the USRP using GNU Radio and a directed antenna and RZUSBSTICK. From the indoor scenario, the success rate of the USRP with 15 and 20 db transmit gain is expected to be nearly 100%. The USRP using GNU Radio and a directed antenna demonstrates poor success rates when executing the replay attack. It does offer slightly better reception than that achieved by the omnidirectional antenna. The USRP with 20 db transmit gain is able to achieve a maximum success rate of 77% at 20 meters. However, the sensor is still able to sense ZigBee packets from the USRP and RZUSBSTICK and register power levels for them.

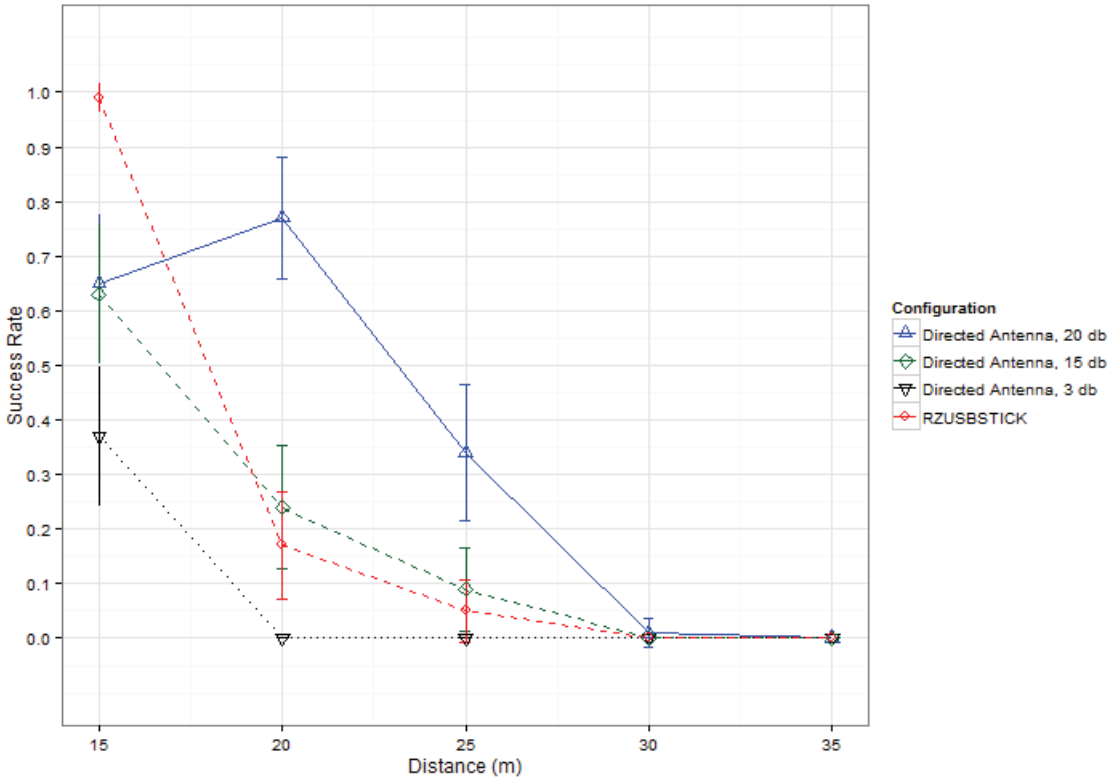


Figure 4.36: Probability of Success of the RZUSBSTICK Compared to the USRP with Directed Antenna and GNU Radio while not in Line of Sight of the Victim

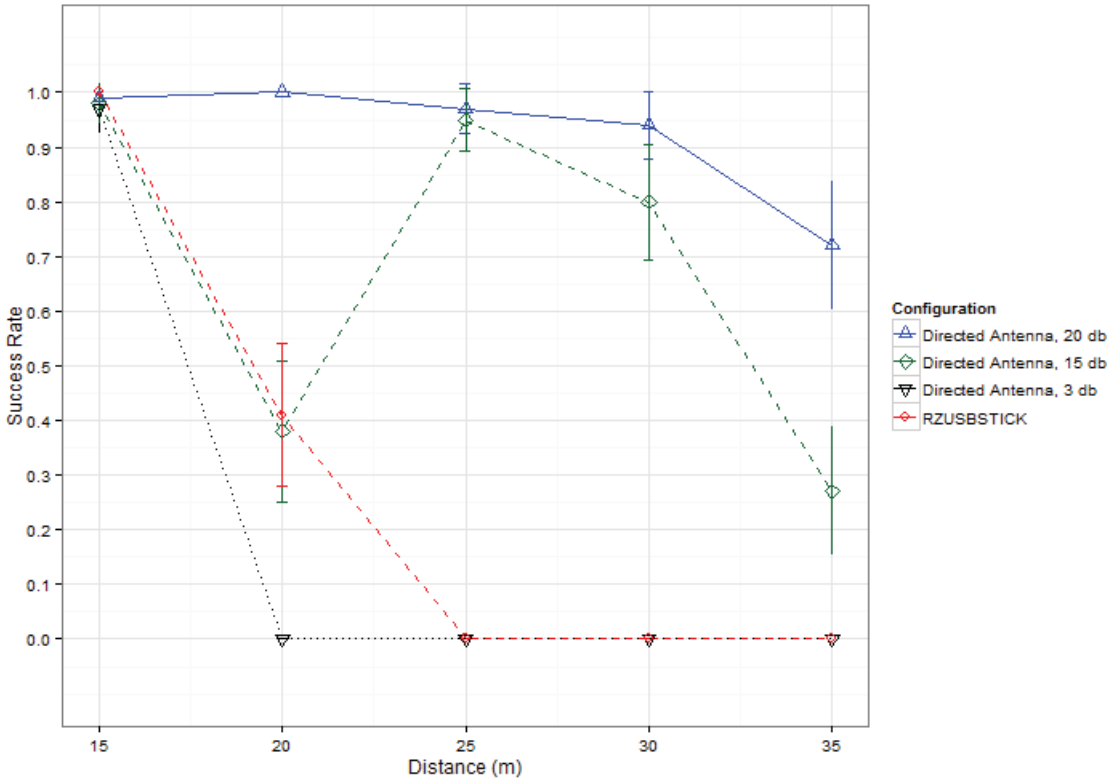


Figure 4.37: Probability of Success of the sensor for the RZUSBSTICK Compared to the USRP with Directed Antenna and GNU Radio while not in Line of Sight of the Victim

Figure 4.37 graphs the probability that the sensor was able to detect the replay attack from the RZUSBSTICK and USRP with directed antenna. The sensor is much better at detecting the replay attack from the USRP than the Freescale victim; the sensor detects 897 of the 1500 attacks whereas the victim only responds to 310. The sensor is able to detect the attack from the USRP with directed antenna and 3 transmit gain at 15 meters. It is undetectable from 20 meters on. The sensor can detect beacon request frames sent by the USRP with medium power at 15 and 20 meters. Reception begins to taper off at 30 meters and is detectable 27% of the time at 35 meters. The sensor is able to detect the USRP with high power with a high success rate up to 30 meters. At 35 meters reception begins to taper.

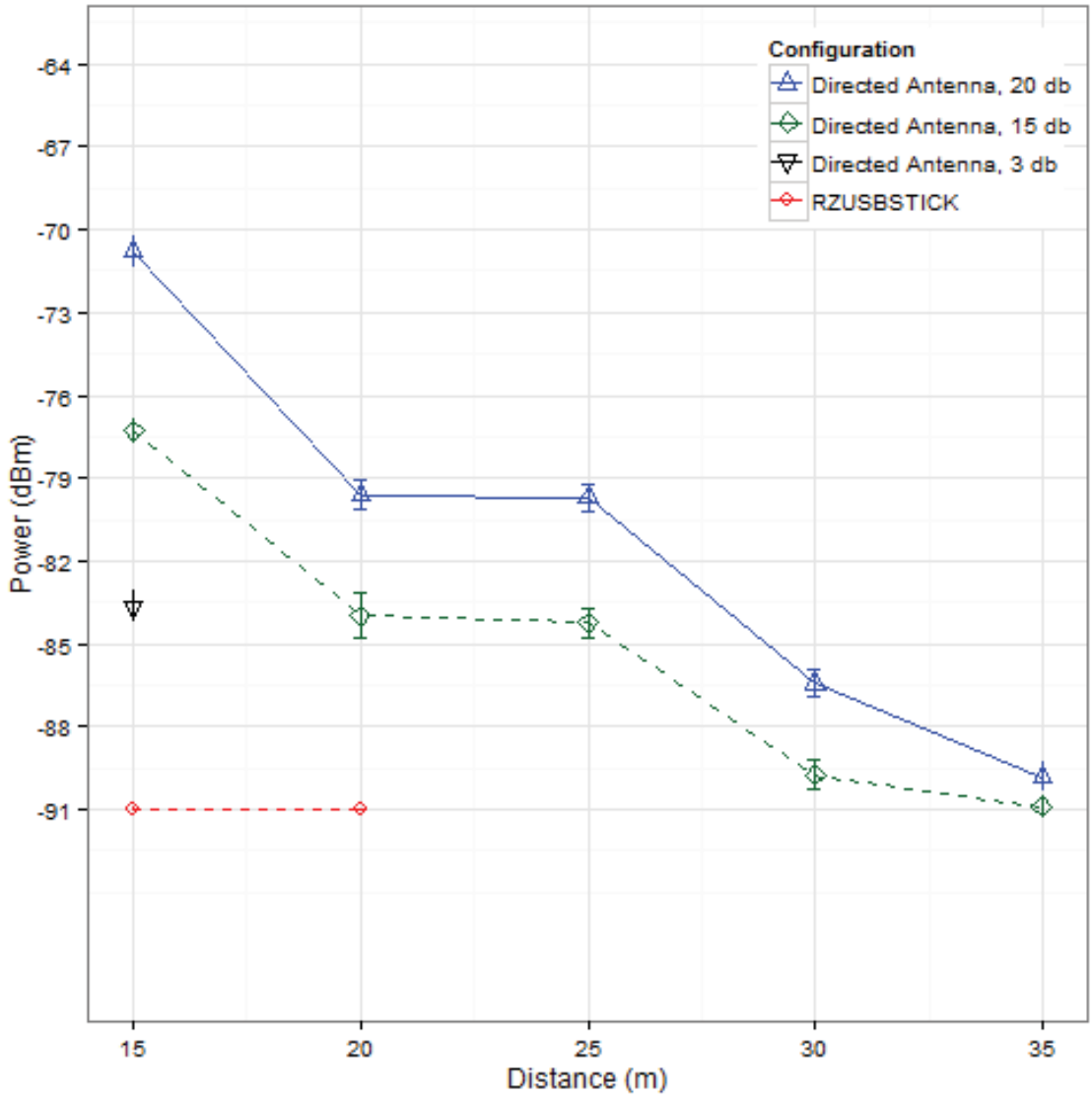


Figure 4.38: Power (dbm) of the RZUSBSTICK Compared to the USRP with Directed Antenna and GNU Radio while in Line of Sight of the Victim

Figure 4.38 displays the power versus distance of the RZUSBSTICK and USRP for the blocked line of sight portion of the experiment. Figure 4.39 and Figure 4.40, display the power received by the sensor in separate plots. The low power data set consists of a single mean, so the graph is omitted. Linear trend lines with 99% confidence intervals are

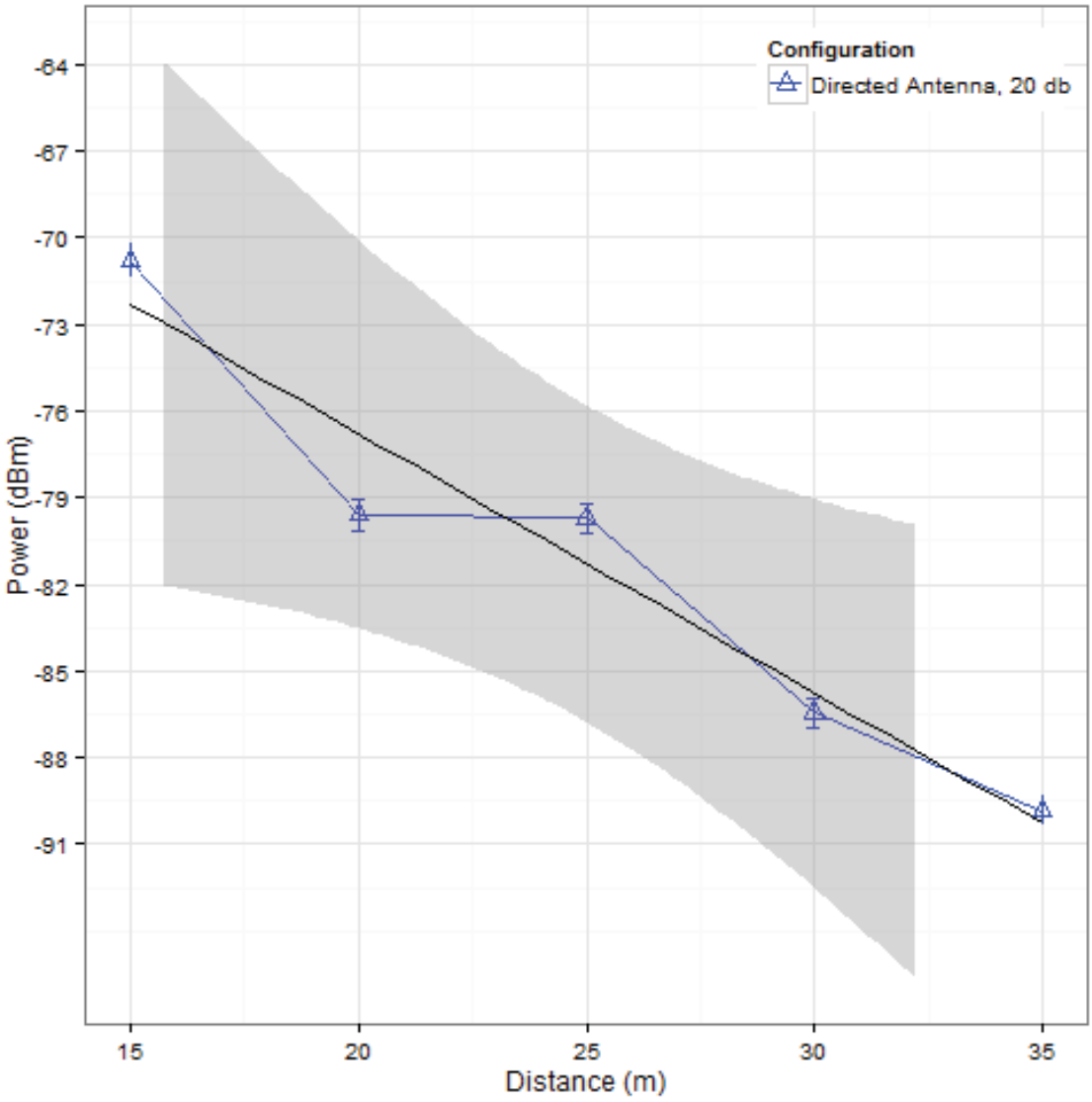


Figure 4.39: Power (dbm) Versus Distance of the USRP with Directed Antenna and 30 db Gain

added to the high and medium power graphs. Both the medium and high power data sets drop logarithmically during this part of the experiment. Both data sets are consistent with a logarithmic model.

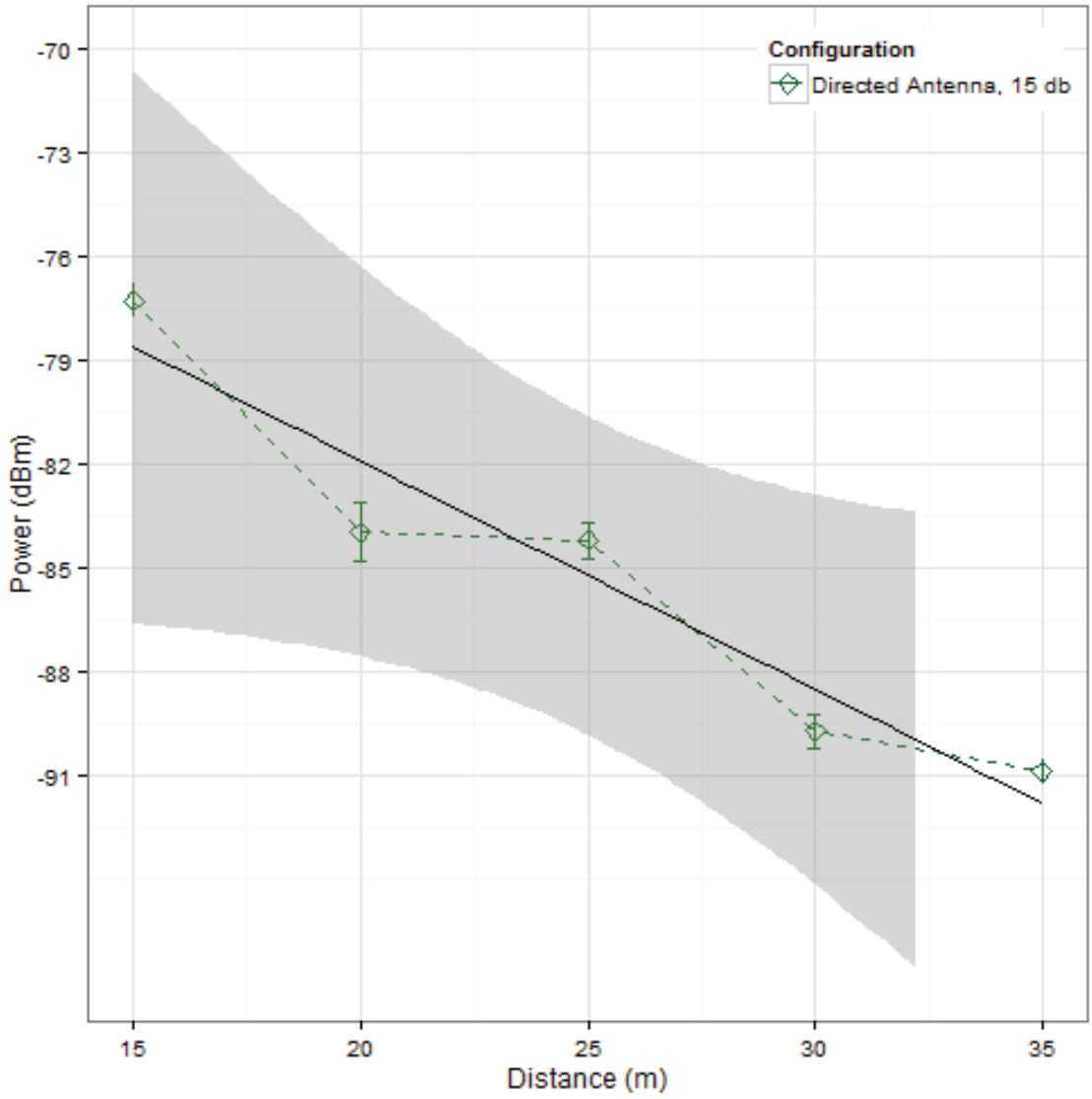


Figure 4.40: Power (dbm) Versus Distance of the USRP with Directed Antenna and 15 db Gain

4.4 Summary

Overall, the data shows that the USRP, when using the National Instruments NI USRP Record and Playback - I16 tool, is able to conduct a successful replay attack at greater distances than the RZUSBSTICK. When outdoors, in line of sight, the USRP is

able to conduct replay attacks at 150 meters whereas the RZUSBSTICK has a range of 100 meters. When indoors, the USRP achieves a range of 35 meters, as opposed to the RZUSBSTICK which has a range of 20 meters. However, when the USRP is configured to use GNU Radio, the reliability of the attack drops. The USRP is still able to be detected at ranges of up to 35 meters by the RZUSBSTICK sniffer, but not at a 100% reception rate.

V. Conclusion

This chapter presents the conclusions drawn from this research. Section 5.1 discusses how the results of the experiment relate to the goals for this research. Section 5.2 discusses the impact of this research. Section 5.3 presents recommendations for future work.

5.1 Research Conclusions

The goal of this research is to determine the viability of the USRP as a tool for exploring and attacking ZigBee and 802.15.4 networks. Specifically, the goal is to determine if the USRP can achieve an attack range greater than that of a conventional ZigBee USB dongle radio — the Atmel RZ Raven USB stick (RZUSBSTICK).

The results indicate a fairly large difference in range between the USRP and RZUSBSTICK. When in line of sight, the RZUSBSTICK is observed to have a range of up to 110 meters. The range of the USRP with omnidirectional antenna and 30 db transmit gain is over 150 meters, the maximum distance tested in this research. However, at high power, the USRP is unable to successfully complete the attack. If the transmit gain is lowered to 15 or 3 db, the close range attacks can be achieved.

In order to make the attack more efficient, GNU Radio is used to implement a ZigBee stack on the USRP. From the line of sight and blocked line of sight experiments, the USRP is physically capable of carrying out effective replay attacks. However, when the USRP implements a ZigBee stack on GNU Radio, it is not reliable enough to affect all ZigBee devices.

5.2 Impact of Research

This research investigates the feasibility of the USRP as a tool for exploring and attacking ZigBee and other 802.15.4 networks. Also, this research has shown that an

attacker can easily exploit a ZigBee network using no security at over 150 meters in line of sight and over 35 meters with a blocked line of sight. A similar attack could be used to disarm ZigBee residential doorlocks. An attacker could sniff a packet that is sent to unlock a ZigBee door lock and then replay it at a later date to gain access to the residence. Many other attacks are possible including those mentioned in Chapter 2. This underscores the need to secure ZigBee networks, including residential and commercial.

5.3 Future Work

The implementation of GNU Radio used in this thesis is unable to reliably perform a replay attack against ZigBee devices. The exact reason requires further research. The issue could be in the version of GNU Radio, the version of USRP firmware used, or the implementation of ZigBee in GNU Radio. The most up-to-date version of the UHD software, USRP firmware, and GNU Radio should be used. Other SDR platforms and implementations should be investigated to find effective and cost-efficient platforms to explore 802.15.4 networks. As KillerBee is a Python-based program, an integration of the KillerBee framework into GNU Radio is a logical step.

5.4 Summary

This research focused on a comparison of range in the USRP and RZUSBSTICK during replay attacks against ZigBee devices. Overall, the USRP is able to achieve better range than the RZUSBSTICK, but improvements in usability and reliability are required. However, cost is a factor that must be taken into account. At this time, the USRP used in this research costs $1,700, whereas the RZUSBSTICK costs approximately $40 [ER14] [CWL10]. Depending on the desired flexibilty of the system, the RZUSBSTICK is a more cost-effective method of manipulating ZigBee networks.

Appendix A: GNURadio Installation Directions

This appendix contains directions on the installation of a ZigBee stack for the USRP2 using GNU Radio on a Linux operating system.

A.1 Prerequisites

The programs require Subversion and Git to obtain their respective sources.

```
sudo apt-get install subversion git
```

GNU Radio has a long list of requirements. For Ubuntu Linux, the exact requirements can be found at http://gnuradio.org/redmine/projects/gnuradio/wiki/UbuntuInstall . For the version used in this thesis, Raring Ringtail, the following command will install all prerequisites: [Lan13]

```
sudo apt-get -y install git-core autoconf automake  libtool g++ python-dev swig \
pkg-config libfftw3-dev libboost1.53-all-dev libcppunit-dev libgsl0-dev \
libusb-dev sdcc libsdl1.2-dev python-wxgtk2.8 python-numpy \
python-cheetah python-lxml doxygen python-qt4 python-qwt5-qt4 libxi-dev \
libqt4-opengl-dev libqwt5-qt4-dev libfontconfig1-dev libxrender-dev qt4-default
```

A.2 UHD

In order to use the USRP with GNURadio, its controlling software must first be installed. This software is referred to as UHD. The version used in this thesis is version 003.004.005. The following code will install that version. For other versions, replace the checkout number with the appropriate version code.

```
git clone git://ettus.sourcerepo.com/ettus/uhd.git
cd uhd
git checkout 22103c8
```

```
cd host
mkdir build
cd build
cmake ../
make
make test
sudo make install
sudo ldconfig
```

A.3 GNU Radio

```
git clone http://gnuradio.org/git/gnuradio.git
cd gnuradio
git checkout 0d47f1353a90a54cdb84e40a847191976ca3b401
mkdir build
cd build
cmake ../
make
make test
sudo make install
sudo ldconfig
```

Everything from /usr/local/include/gruel/swig might need to be copied or linked into /usr/local/include/gnuradio/swig before the next part is executed.

A.4 UCLA Physical

```
svn co https://www.cgran.org/cgran/projects/ucla_zigbee_phy/trunk ucla_zigbee_phy
cd ucla_zigbee_phy
./bootstrap && ./configure && make
make check
sudo make install
```

A.5 Utah Update

```
git clone git://wiesel.ece.utah.edu/gr-ieee802-15-4.git
cd gr-ieee802-15-4
./bootstrap && ./configure && make
make check
sudo make install
```

There are some problems with the code. In ieee802_15_4_pkt.py,

```
import Numeric
```

should be commented out and replaced with

```
import numpy
```

In ieee802_15_4.py, add the line

```
from gnuradio import digital
```

and change

```
self.clock_recovery = gr.clock_recovery_mm_ff(omega, gain_omega, mu, gain_mu,
                                                omega_relative_limit)
```

to

```
self.clock_recovery = digital.clock_recovery_mm_ff(omega, gain_omega, mu, gain_mu,
                                                omega_relative_limit)
```

Appendix B: Replay Attack Scripts and Python Source Files

This appendix contains the scripts used to conduct the replay attacks in this research as well as the modified Python source code used in GNU Radio to transmit a beacon request frame.

B.1 KillerBee Replay Attack Script

This script contains the KillerBee replay attack script as used in the GNU Radio part of the experiment. It conducts 100 replay attacks using the zbreplay program from the KillerBee framework. It replays the contents of the file beacon.pcap, a single beacon request frame, once every five seconds as zbreplay has an automatic 1 second delay. For the line of sight and blocked line of sight portions of the experiment, the 100 would need to be changed to 30 in order to lower the number of repetitions.

```
#! /bin/bash


for i in {1..100}
do
   echo "Run $i"
   zbreplay -f 26 -r beacon.pcap
   sleep 4
done
```

B.2 GNU Radio Replay Attack Script

This script contains the GNU Radio replay attack script as used in the GNU Radio part of the experiment. It conducts 100 replay attacks of beacon request frames as specified by the -b flag. It sends a single beacon request frame approximately every five seconds as it takes around three seconds to run the Python script. This script uses 3 db

transmit gain as specified by the -g flag, but that is changed to 15 and 20 for the medium and high transmit gain tests, respectively.

```
#! /bin/bash


for i in {1..100}
do
   echo "Run $i"
   python usrp2_txtest.py -x 1 -X 1 -b -g 3
   sleep 2
done
```

B.3 GNU Radio Beacon Request Python File

This Python script was converted to create the -b flag which sends a beacon request frame instead of the string ”Hello World”. Modifications to the code are underlined.

```
#!/ usr / bin / env python
#
# Transmitter of IEEE 802.15.4 RADIO Packets .
#
# Modified by : Thomas Schmid , Sanna Leidelof
#
# March 2012 Modified by: Rithirong Thandee
# December 2013 Modified by: Scott Dalrymple
from gnuradio import gr, eng_notation
from gnuradio import uhd
from gnuradio import ucla
from gnuradio.ucla_blks import ieee802_15_4_pkt
from gnuradio.eng_option import eng_option

from optparse import OptionParser

import math, struct, time

class transmit_path(gr.top_block):
```

```
    def __init__(self,options):
        gr.top_block.__init__(self)
        self.normal_gain = 8000
        self._spb = 2
        self.u = uhd.usrp_sink( device_addr ="", io_type=uhd.io_type.COMPLEX_FLOAT32,num_channels=1)
        self.u.set_samp_rate(options.sample_rate)
        self.u.set_center_freq(options.cordic_freq)
        self.u.set_gain(options.gain)

        # transmitter
    self.packet_transmitter=ieee802_15_4_pkt.ieee802_15_4_mod_pkts(self, spb=self._spb, msgq_limit=2)
        self.gain = gr.multiply_const_cc(self.normal_gain)
        self.connect(self.packet_transmitter, self.gain, self.u)
    def set_gain(self, gain):
        self.gain = gain
        self.subdev.set_gain(gain)
    def send_pkt(self, options, payload ='', eof = False):
        if options.beacon:
            payload=struct.pack("B",0x07)
            return self.packet_transmitter.send_pkt(0x37, struct.pack("HH",0xFFFF,0xFFFF),payload,eof)
        else:
            return self.packet_transmitter.send_pkt(0xe5,
                                                    struct.pack ("HHHHHHHHH",
                                                    #PAN ID
                                                    0x5678,
                                                    #addresss1
                                                    0x5A70,
                                                    0x4063,
                                                    0xA200,
                                                   0x0013,
                                                    #address2
                                                    0x5A22,
                                                    0x4063,
                                                    0xA200,
                                                    0x0013),
                                                    payload,
                                                    eof)
def main():
    parser = OptionParser ( option_class = eng_option )
```

```
    parser.add_option ("-A", "--antenna", type="string", default=None,
    help="Select Antenna where appropriate (J1 or J0)")
    parser.add_option ("-c", "--cordic-freq", type ="eng_float", default=2480000000,
    help ="set Tx cordic frequency to FREQ ", metavar =" FREQ ")
    parser.add_option ("-r", "--data-rate", type ="eng_float", default=4000000)
    parser.add_option ("-g", "--gain", type="eng_float", default=15,
    help="set Rx PGA gain in dB 0,20")
    parser.add_option ("-s", "--sample_rate", type ="eng_float", default =4000000)
    parser.add_option ("-x", "--num_msg", type="int", default=1000)
    parser.add_option ("-X", "--spacing", type="eng_float", default=0.001)
    parser.add_option ("-b", "--beacon", action="store_true", dest="beacon", default=False,
    help="send a beacon request frame instead")

    (options, args) = parser.parse_args()

    print options
    print args

    tb = transmit_path( options )
    tb.start()

    for i in range ( options.num_msg ):
        print "send message %d:" %(i)
        if options.beacon:
            tb.send_pkt(options)
            print "Sending a Beacon Request"
        else:
            print "Hello World = 48:65:6c:6c:6f:20:57:6f:72:6c:64"
            tb.send_pkt(options, payload = struct.pack ('11B',0x48, 0x65, 0x6c, 0x6c, 0x6f,
            0x20, 0x57, 0x6f, 0x72, 0x6c, 0x64))
        time.sleep(options.spacing)
    tb.stop()
if __name__ == '__main__':
# insert this in your test code ...
    import os
    print 'Blocked waiting for GDB attach (pid = %d)' % (os.getpid(),)
    #raw_input('Press Enter to continue: ')
    main()
```

Appendix C: Summary Data Tables

C.1 Line of Sight Scenario

C.1.1 RZUSBSTICK.

Table C.1 summarizes the data for the line of sight portion of the experiment when using the RZUSBSTICK.

Table C.1: Summary of Line of Sight Experiment using the RZUSBSTICK

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
20 m	60	60	100%	60	3.8833	-79.3500
40 m	60	60	100%	60	3.1333	-81.6000
60 m	90	60	66.6667%	80	1.1125	-87.6625
65 m	30	14	46.6667%	30	0.1333	-90.6000
70 m	30	23	76.6667%	30	0.1667	-90.5000
80 m	90	31	34.4444%	60	0.2833	-90.1500
100 m	60	16	26.6667%	29	0.1034	-90.6897
110 m	60	0	0%	11	0	-91
120 m	60	0	0%	2	0	-91
130 m	60	0	0%	0	NA	NA
140 m	30	0	0%	0	NA	NA
150 m	30	0	0%	0	NA	NA

Table C.2 shows the statistics for the probability of success of the replay attack when using the RZUSBSTICK. Table C.3 shows the statistics of the power of the replay attack when using the RZUSBSTICK as measured by the sensor near the victim.

C.1.2 Omnidirectional Antenna.

Table C.4 summarizes the data for the line of sight experiment when using the USRP with omnidirectional antenna and 30 db transmit gain. Table C.5 summarizes the data for the line of sight experiment when using the USRP with omnidirectional antenna and 15 db transmit gain. Table C.6 summarizes the data for the line of sight experiment when using the USRP with omnidirectional antenna and 3 db transmit gain.

Table C.2: Probability of Success Statistics during the Line of Sight Experiment using the RZUSBSTICK

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
20 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
40 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
60 m	90	0.6667	0.4740	0.0500	(0.5351, 0.7982)
65 m	30	0.4667	0.5074	0.0926	(0.2113, 0.7220)
70 m	30	0.7667	0.4302	0.0785	(0.5502, 0.9832)
80 m	90	0.3444	0.4778	0.0504	(0.2119, 0.4770)
100 m	60	0.2667	0.4459	0.0576	(0.1134, 0.4199)
110 m	60	0.0000	0.0000	0.0000	(0.0000, 0.0000)
120 m	60	0.0000	0.0000	0.0000	(0.0000, 0.0000)
130 m	60	0.0000	0.0000	0.0000	(0.0000, 0.0000)
140 m	30	0.0000	0.0000	0.0000	(0.0000, 0.0000)
150 m	30	0.0000	0.0000	0.0000	(0.0000, 0.0000)

Table C.3: Power Statistics during the Line of Sight Experiment using the RZUSBSTICK

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
20 m	60	-79.3500	1.9985	0.2580	(-80.0368, -78.6632)
40 m	60	-81.6000	2.7321	0.3527	(-82.5388, -80.6612)
60 m	80	-87.6625	2.8237	0.3157	(-88.4958, -86.8292)
65 m	30	-90.6000	1.3025	0.2378	(-91.2555, -89.9445)
70 m	30	-90.5000	1.1371	0.2076	(-91.0723, -89.9277)
80 m	60	-90.1500	1.3633	0.1760	(-90.6185, -89.6815)
100 m	29	-90.6897	0.9298	0.1727	(-91.1668, -90.2126)
110 m	11	-91.0000	0.0000	0.0000	(-91.0000, -91.0000)
120 m	2	-91.0000	0.0000	0.0000	(-91.0000, -91.0000)
130 m	0	NA	NA	NA	(NA, NA)
140 m	0	NA	NA	NA	(NA, NA)
150 m	0	NA	NA	NA	(NA, NA)

Table C.4: Summary of Line of Sight Experiment using the USRP with Omnidirectional Antenna and 30 db Transmit Gain

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
20 m	60	0	0%	60	12.2667	-54.2
40 m	60	0	0%	60	9.85	-61.45
60 m	60	31	51.67%	60	8.5667	-65.3
65 m	30	30	100%	30	7.3667	-68.9
70 m	30	30	100%	30	7.9667	-67.1
80 m	60	60	100%	60	7.2333	-69.3
100 m	60	60	100%	59	5.5423	-74.373
110 m	60	60	100%	35	4.9713	-76.086
120 m	60	38	63.33%	22	3.2273	-81.318
130 m	60	60	100%	54	5.111	-75.667
140 m	30	30	100%	6	3.5	-80.5
150 m	60	59	98.33%	34	4.147	-78.559

Table C.5: Summary of Line of Sight Experiment using USRP with Omnidirectional Antenna and 15 db Transmit Gain

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
20 m	60	59	98.333%	60	6.9833	-70.05
40 m	60	60	100%	60	5.2167	-75.35
60 m	90	90	100%	60	3.8667	-79.4
65 m	30	30	100%	30	3	-82
70 m	30	30	100%	30	3.8	-79.6
80 m	90	90	100%	60	2.533	-83.4
100 m	60	56	93.333%	52	0.75	-88.75
110 m	60	57	96.667%	12	0.5833	-89.25
120 m	60	28	46.667%	5	0.2	-90.4
130 m	60	50	83.333%	22	1.3183	-87.045
140 m	30	20	66.667%	0	NA	NA
150 m	60	25	41.667%	13	0.077	-90.769

Table C.6: Summary of Line of Sight Experiment using USRP with Omnidirectional Antenna and 3 db Transmit Gain

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
20 m	60	60	100%	60	3.85	-79.45
40 m	60	60	100%	60	2.2833	-84.15
60 m	90	87	96.667%	43	1.3953	-86.814
65 m	30	30	100%	15	0.2667	-90.2
70 m	30	29	96.667%	30	0.6667	-89.0
80 m	90	78	86.667%	35	0.457	-89.629
100 m	60	28	46.667%	0	NA	NA
110 m	60	5	8.333%	0	NA	NA
120 m	60	8	13.333%	0	NA	NA
130 m	60	4	6.667%	0	NA	NA
140 m	30	0	0%	0	NA	NA
150 m	60	4	6.667%	0	NA	NA

Table C.7 displays the probability of success statistics for the USRP with omnidirectional antenna with 30 db transmit gain. Table C.8 shows the probability of success statistics for the USRP with omnidirectional antenna with 15 db transmit gain. Table C.9 details the probability of success statistics for the USRP with omnidirectional antenna with 3 db transmit gain.

Table C.10 shows the statistics of the power of the replay attack when using the USRP with omnidirectional antenna and 30 db transmit gain as measured by the sensor near the victim. Table C.11 shows the statistics of the power of the replay attack when

Table C.7: Probability of Success Statistics during the Line of Sight Experiment using the USRP with Omnidirectional Antenna and 30 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
20 m	60	0.0000	0.0000	0.0000	(0.0000, 0.0000)
40 m	60	0.0000	0.0000	0.0000	(0.0000, 0.0000)
60 m	60	0.5167	0.5039	0.0651	(0.3435, 0.6898)
65 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
70 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
80 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
100 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
110 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
120 m	60	0.6333	0.4860	0.0627	(0.4663, 0.8003)
130 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
140 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
150 m	60	0.9833	0.1291	0.0167	(0.9390, 1.0277)

Table C.8: Probability of Success Statistics during the Line of Sight Experiment using the USRP with Omnidirectional Antenna and 15 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
20 m	60	0.9833	0.1291	0.0167	(0.9390, 1.0277)
40 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
60 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
65 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
70 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
80 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
100 m	60	0.9333	0.2515	0.0325	(0.8469, 1.0198)
110 m	60	0.9667	0.1810	0.0234	(0.9045, 1.0289)
120 m	60	0.4667	0.5031	0.0649	(0.2938, 0.6395)
130 m	60	0.8333	0.3758	0.0485	(0.7042, 0.9625)
140 m	30	0.6667	0.4795	0.0875	(0.4254, 0.9080)
150 m	60	0.4167	0.4972	0.0642	(0.2458, 0.5875)

using the USRP with omnidirectional antenna and 15 db transmit gain as measured by the sensor near the victim. Table C.12 shows the statistics of the power of the replay attack when using the USRP with omnidirectional antenna and 3 db transmit gain as measured by the sensor near the victim.

C.1.3 Directed Antenna.

Table C.13 summarizes the data for the line of sight experiment when using the USRP with directed antenna and 30 db transmit gain. Table C.14 summarizes the data for

Table C.9: Probability of Success Statistics during the Line of Sight Experiment using the USRP with Omnidirectional Antenna and 3 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
20 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
40 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
60 m	60	0.9667	0.1810	0.0234	(0.9045, 1.0289)
65 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
70 m	30	0.9667	0.1826	0.0333	(0.8748, 1.0585)
80 m	60	0.8667	0.3428	0.0443	(0.7489, 0.9845)
100 m	60	0.4667	0.5031	0.0649	(0.2938, 0.6395)
110 m	60	0.0833	0.2787	0.0360	(-0.0124, 0.1791)
120 m	60	0.1333	0.3428	0.0443	(0.0155, 0.2511)
130 m	60	0.0667	0.2515	0.0325	(-0.0198, 0.1531)
140 m	30	0.0000	0.0000	0.0000	(0.0000, 0.0000)
150 m	60	0.0667	0.2515	0.0325	(-0.0198, 0.1531)

Table C.10: Power Statistics during the Line of Sight Experiment using the USRP with Omnidirectional Antenna and 30 db Transmit Gain

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
20 m	60	-54.2000	1.5492	0.2000	(-54.7324, -53.6676)
40 m	60	-61.4500	1.7313	0.2235	(-62.0449, -60.8551)
60 m	60	-65.3000	4.7311	0.6108	(-66.9257, -63.6743)
65 m	30	-68.9000	1.4704	0.2685	(-69.6400, -68.1600)
70 m	30	-67.1000	1.2415	0.2267	(-67.7248, -66.4752)
80 m	60	-69.3000	1.8622	0.2404	(-69.9399, -68.6601)
100 m	59	-74.3729	2.2507	0.2930	(-75.1533, -73.5925)
110 m	35	-76.0857	1.7042	0.2881	(-76.8716, -75.2998)
120 m	22	-81.3182	1.2868	0.2743	(-82.0950, -80.5414)
130 m	54	-75.6667	2.5179	0.3426	(-76.5821, -74.7512)
140 m	6	-80.5000	2.5100	1.0247	(-84.6317, -76.3683)
150 m	34	-78.5588	2.1061	0.3612	(-79.5461, -77.5716)

the line of sight experiment when using the USRP with directed antenna and 15 db transmit gain. Table C.15 summarizes the data for the line of sight experiment when using the USRP with directed antenna and 3 db transmit gain.

Table C.16 displays the probability of success statistics for the USRP with directed antenna with 30 db transmit gain. Table C.17 shows the probability of success statistics for the USRP with directed antenna with 15 db transmit gain. Table C.18 details the

Table C.11: Power Statistics during the Line of Sight Experiment using the USRP with Omnidirectional Antenna and 15 db Transmit Gain

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
20 m	60	-70.0500	1.7891	0.2310	(-70.6648, -69.4352)
40 m	60	-75.3500	2.0734	0.2677	(-76.0625, -74.6375)
60 m	60	-79.4000	4.0388	0.5214	(-80.7879, -78.0121)
65 m	30	-82.0000	1.9298	0.3523	(-82.9712, -81.0288)
70 m	30	-79.6000	1.2205	0.2228	(-80.2142, -78.9858)
80 m	60	-83.4000	2.8416	0.3668	(-84.3765, -82.4235)
100 m	52	-88.7500	2.5117	0.3483	(-89.6820, -87.8180)
110 m	12	-89.2500	1.5448	0.4459	(-90.6350, -87.8650)
120 m	5	-90.4000	1.3416	0.6000	(-93.1625, -87.6375)
130 m	22	-87.0455	1.7037	0.3632	(-88.0739, -86.0170)
140 m	0	NA	NA	NA	(NA, NA)
150 m	13	-90.7692	0.8321	0.2308	(-91.4741, -90.0643)

Table C.12: Power Statistics during the Line of Sight Experiment using the USRP with Omnidirectional Antenna and 3 db Transmit Gain

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
20 m	60	-79.4500	1.4430	0.1863	(-79.9459, -78.9541)
40 m	60	-84.1500	2.1457	0.2770	(-84.8873, -83.4127)
60 m	43	-86.8140	2.7882	0.4252	(-87.9612, -85.6667)
65 m	15	-90.2000	1.7809	0.4598	(-91.5688, -88.8312)
70 m	30	-89.0000	1.9827	0.3620	(-89.9978, -88.0022)
80 m	35	-89.6286	1.6818	0.2843	(-90.4042, -88.8529)
100 m	0	NA	NA	NA	(NA, NA)
110 m	0	NA	NA	NA	(NA, NA)
120 m	0	NA	NA	NA	(NA, NA)
130 m	0	NA	NA	NA	(NA, NA)
140 m	0	NA	NA	NA	(NA, NA)
150 m	0	NA	NA	NA	(NA, NA)

probability of success statistics for the USRP with directed antenna with 3 db transmit gain.

Table C.19 displays the power statistics for the USRP with directed antenna with 30 db transmit gain. Table C.20 shows the power statistics for the USRP with directed antenna with 15 db transmit gain. Table C.21 details the power statistics for the USRP with directed antenna with 3 db transmit gain.

Table C.13: Summary of Line of Sight Experiment using USRP with Directed Antenna and 30 db Transmit Gain

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
20 m	60	1	1.667%	60	13.0833	-51.75
40 m	60	30	50%	60	11.1167	-57.65
60 m	60	37	61.667%	60	9.1167	-63.65
65 m	30	30	100%	30	8.5	-65.5
70 m	30	30	100%	30	8.2	-66.4
80 m	60	60	100%	60	7.9667	-67.1
100 m	60	60	100%	60	6.9167	-70.25
110 m	60	59	98.333%	60	5.5167	-74.45
120 m	60	60	100%	59	4.712	-76.864
130 m	60	60	100%	54	4.7963	-76.611
140 m	60	59	98.333%	58	4.5	-77.5
150 m	60	58	96.667%	55	4.2183	-78.345

Table C.14: Summary of Line of Sight Experiment using USRP with Directed Antenna and 15 db Transmit Gain

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
20 m	60	60	100%	60	7.9167	-67.25
40 m	60	60	100%	60	6.25	-72.25
60 m	60	60	100%	60	4.9667	-76.1
65 m	30	30	100%	30	3.9667	-79.1
70 m	30	23	70%	30	3.9333	-79.2
80 m	60	56	93.333%	60	3.6333	-80.1
100 m	60	60	100%	60	2.2167	-84.35
110 m	60	52	86.667%	57	0.8597	-88.421
120 m	60	52	86.667%	54	0.4443	-89.667
130 m	60	59	98.333%	43	0.558	-89.326
140 m	60	55	91.667%	40	0.3	-90.1
150 m	60	33	55%	26	0.2693	-90.192

Table C.15: Summary of Line of Sight Experiment using USRP with Directed Antenna and 3 db Transmit Gain

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
20 m	60	60	100%	60	4.5167	-77.45
40 m	60	60	100%	60	3.1333	-81.6
60 m	60	60	100%	60	1.9333	-85.2
65 m	30	25	83.333%	30	0.9	-88.3
70 m	30	1	3.333%	30	0.6667	-89
80 m	60	34	56.667%	56	0.6787	-88.964
100 m	60	24	40%	40	0.025	-90.925
110 m	60	5	8.333%	0	NA	NA
120 m	60	3	5%	0	NA	NA
130 m	60	0	0%	0	NA	NA
140 m	60	0	0%	0	NA	NA
150 m	60	0	0%	0	NA	NA

Table C.16: Probability of Success Statistics during the Line of Sight Experiment using the USRP with Directed Antenna and 30 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
20 m	60	0.0167	0.1291	0.0167	(-0.0277, 0.0610)
40 m	60	0.5000	0.5042	0.0651	(0.3267, 0.6733)
60 m	60	0.6167	0.4903	0.0633	(0.4482, 0.7851)
65 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
70 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
80 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
100 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
110 m	60	0.9833	0.1291	0.0167	(0.9390, 1.0277)
120 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
130 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
140 m	60	0.9833	0.1291	0.0167	(0.9390, 1.0277)
150 m	60	0.9667	0.1810	0.0234	(0.9045, 1.0289)

Table C.17: Probability of Success Statistics during the Line of Sight Experiment using the USRP with Directed Antenna and 15 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
20 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
40 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
60 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
65 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
70 m	30	0.7000	0.4661	0.0851	(0.4654, 0.9346)
80 m	60	0.9333	0.2515	0.0325	(0.8469, 1.0198)
100 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
110 m	60	0.8667	0.3428	0.0443	(0.7489, 0.9845)
120 m	60	0.8667	0.3428	0.0443	(0.7489, 0.9845)
130 m	60	0.9833	0.1291	0.0167	(0.9390, 1.0277)
140 m	60	0.9167	0.2787	0.0360	(0.8209, 1.0124)
150 m	60	0.5500	0.5017	0.0648	(0.3776, 0.7224)

Table C.18: Probability of Success Statistics during the Line of Sight Experiment using the USRP with Directed Antenna and 3 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
20 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
40 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
60 m	60	1.0000	0.0000	0.0000	(1.0000, 1.0000)
65 m	30	0.8333	0.3790	0.0692	(0.6426, 1.0241)
70 m	30	0.0333	0.1826	0.0333	(-0.0585, 0.1252)
80 m	60	0.5667	0.4997	0.0645	(0.3949, 0.7384)
100 m	60	0.4000	0.4940	0.0638	(0.2302, 0.5698)
110 m	60	0.0833	0.2787	0.0360	(-0.0124, 0.1791)
120 m	60	0.0500	0.2198	0.0284	(-0.0255, 0.1255)
130 m	60	0.0000	0.0000	0.0000	(0.0000, 0.0000)
140 m	60	0.0000	0.0000	0.0000	(0.0000, 0.0000)
150 m	60	0.0000	0.0000	0.0000	(0.0000, 0.0000)

Table C.19: Power Statistics during the Line of Sight Experiment using the USRP with Directed Antenna and 30 db Transmit Gain

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
20 m	60	-51.7500	1.0021	0.1294	(-52.0944, -51.4056)
40 m	60	-57.6500	1.9207	0.2480	(-58.3100, -56.9900)
60 m	60	-63.6500	1.8395	0.2375	(-64.2821, -63.0179)
65 m	30	-65.5000	1.8892	0.3449	(-66.4507, -64.5493)
70 m	30	-66.4000	1.2205	0.2228	(-67.0142, -65.7858)
80 m	60	-67.1000	2.2751	0.2937	(-67.8818, -66.3182)
100 m	60	-70.2500	2.1599	0.2788	(-70.9922, -69.5078)
110 m	60	-74.4500	2.2431	0.2896	(-75.2208, -73.6792)
120 m	59	-76.8644	2.4945	0.3248	(-77.7293, -75.9995)
130 m	54	-76.6111	1.8775	0.2555	(-77.2938, -75.9285)
140 m	58	-77.5000	1.8848	0.2475	(-78.1595, -76.8405)
150 m	55	-78.3455	1.7020	0.2295	(-78.9582, -77.7327)

Table C.20: Power Statistics during the Line of Sight Experiment using the USRP with Directed Antenna and 15 db Transmit Gain

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
20 m	60	-67.2500	1.0021	0.1294	(-67.5944, -66.9056)
40 m	60	-72.2500	1.8832	0.2431	(-72.8971, -71.6029)
60 m	60	-76.1000	1.7438	0.2251	(-76.6992, -75.5008)
65 m	30	-79.1000	0.9595	0.1752	(-79.5829, -78.6171)
70 m	30	-79.2000	1.0954	0.2000	(-79.7513, -78.6487)
80 m	60	-80.1000	2.3412	0.3023	(-80.9045, -79.2955)
100 m	60	-84.3500	2.5961	0.3352	(-85.2421, -83.4579)
110 m	57	-88.4211	2.2987	0.3045	(-89.2329, -87.6092)
120 m	54	-89.6667	1.6136	0.2196	(-90.2534, -89.0800)
130 m	43	-89.3256	2.2962	0.3502	(-90.2703, -88.3808)
140 m	40	-90.1000	1.3923	0.2201	(-90.6961, -89.5039)
150 m	26	-90.1923	1.3570	0.2661	(-90.9341, -89.4505)

Table C.21: Power Statistics during the Line of Sight Experiment using the USRP with Directed Antenna and 3 db Transmit Gain

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
20 m	60	-77.4500	1.7017	0.2197	(-78.0348, -76.8652)
40 m	60	-81.6000	1.7870	0.2307	(-82.2141, -80.9859)
60 m	60	-85.2000	2.0568	0.2655	(-85.9068, -84.4932)
65 m	30	-88.3000	1.6432	0.3000	(-89.1269, -87.4731)
70 m	30	-89.0000	1.4384	0.2626	(-89.7239, -88.2761)
80 m	56	-88.9643	1.9906	0.2660	(-89.6740, -88.2545)
100 m	40	-90.9250	0.4743	0.0750	(-91.1281, -90.7219)

C.2 Blocked Line of Sight Scenario

C.2.1 RZUSBSTICK.

Table C.22 summarizes the data for the blocked line of sight portion of the experiment when using the RZUSBSTICK.

Table C.22: Summary of Blocked Line of Sight Experiment using the RZUSBSTICK

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
15 m	30	30	100%	30	0	-91
20 m	30	30	100%	11	0	-91
25 m	30	0	0%	30	0	-91
30 m	30	0	0%	0	NA	NA
35 m	30	0	0%	0	NA	NA

Table C.23 shows the statistics for the probability of success of the replay attack when using the RZUSBSTICK. Table C.24 shows the statistics of the power of the replay attack when using the RZUSBSTICK as measured by the sensor near the victim.

Table C.23: Probability of Success Statistics during the Blocked Line of Sight Experiment using the RZUSBSTICK

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
20 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
25 m	30	0.0000	0.0000	0.0000	(0.0000, 0.0000)
30 m	30	0.0000	0.0000	0.0000	(0.0000, 0.0000)
35 m	30	0.0000	0.0000	0.0000	(0.0000, 0.0000)

Table C.24: Power Statistics during the Blocked Line of Sight Experiment using the RZUSBSTICK

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
15 m	30	-91.0000	0.0000	0.0000	(-91.0000, -91.0000)
20 m	11	-91.0000	0.0000	0.0000	(-91.0000, -91.0000)
25 m	30	-91.0000	0.0000	0.0000	(-91.0000, -91.0000)
30 m	0	NA	NA	NA	(NA, NA)
35 m	0	NA	NA	NA	(NA, NA)

C.2.2 Omnidirectional Antenna.

Table C.25 summarizes the data for the blocked line of sight experiment when using the USRP with omnidirectional antenna and 30 db transmit gain. Table C.26 summarizes the data for the blocked line of sight experiment when using the USRP with omnidirectional antenna and 15 db transmit gain. Table C.27 summarizes the data for the blocked line of sight experiment when using the USRP with omnidirectional antenna and 3 db transmit gain.

Table C.25: Summary of Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 30 db Transmit Gain

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
15 m	30	30	100%	30	9	-64
20 m	30	30	100%	30	8.0667	-66.8
25 m	30	30	100%	30	7	-70
30 m	30	30	100%	25	0.92	-88.24
35 m	30	30	100%	29	3.8966	-79.3103

Table C.26: Summary of Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 15 db Transmit Gain

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
15 m	30	28	93.33%	30	4.6667	-77
20 m	30	30	100%	30	3.0333	-81.9
25 m	30	29	96.67%	30	1.4667	-86.6
30 m	30	24	80%	23	0	-91
35 m	30	8	26.67%	23	0	-91

Table C.27: Summary of Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 3 db Transmit Gain

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
15 m	30	20	66.67%	30	1.5	-86.5
20 m	30	0	0%	0	NA	NA
25 m	30	0	0%	0	NA	NA
30 m	30	0	0%	0	NA	NA
35 m	30	0	0%	0	NA	NA

Table C.28 displays the probability of success statistics for the USRP with omnidirectional antenna with 30 db transmit gain. Table C.29 shows the probability of success statistics for the USRP with omnidirectional antenna with 15 db transmit gain. Table C.30 details the probability of success statistics for the USRP with omnidirectional antenna with 3 db transmit gain.

Table C.28: Probability of Success Statistics during the Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 30 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
20 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
25 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
30 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
35 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)

Table C.29: Probability of Success Statistics during the Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 15 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	30	0.9333	0.2537	0.0463	(0.8057, 1.0610)
20 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
25 m	30	0.9667	0.1826	0.0333	(0.8748, 1.0585)
30 m	30	0.8000	0.4068	0.0743	(0.5953, 1.0047)
35 m	30	0.2667	0.4498	0.0821	(0.0403, 0.4930)

Table C.30: Probability of Success Statistics during the Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 3 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	30	0.6667	0.4795	0.0875	(0.4254, 0.9080)
20 m	30	0.0000	0.0000	0.0000	(0.0000, 0.0000)
25 m	30	0.0000	0.0000	0.0000	(0.0000, 0.0000)
30 m	30	0.0000	0.0000	0.0000	(0.0000, 0.0000)
35 m	30	0.0000	0.0000	0.0000	(0.0000, 0.0000)

Table C.31 shows the statistics of the power of the replay attack when using the USRP with omnidirectional antenna and 30 db transmit gain as measured by the sensor

near the victim. Table C.32 shows the statistics of the power of the replay attack when using the USRP with omnidirectional antenna and 15 db transmit gain as measured by the sensor near the victim. Table C.33 shows the statistics of the power of the replay attack when using the USRP with omnidirectional antenna and 3 db transmit gain as measured by the sensor near the victim.

Table C.31: Power Statistics during the Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 30 db Transmit Gain

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
15 m	30	-64.0000	1.3646	0.2491	(-64.6867, -63.3133)
20 m	30	-66.8000	2.6050	0.4756	(-68.1110, -65.4890)
25 m	30	-70.0000	0.7878	0.1438	(-70.3965, -69.6035)
30 m	25	-88.2400	2.8618	0.5724	(-89.8409, -86.6391)
35 m	29	-79.3103	1.4664	0.2723	(-80.0628, -78.5579)

Table C.32: Power Statistics during the Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 15 db Transmit Gain

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
15 m	30	-77.0000	1.4384	0.2626	(-77.7239, -76.2761)
20 m	30	-81.9000	2.4262	0.4430	(-83.1209, -80.6791)
25 m	30	-86.6000	1.8864	0.3444	(-87.5493, -85.6507)
30 m	23	-91.0000	0.0000	0.0000	(-91.0000, -91.0000)
35 m	23	-91.0000	0.0000	0.0000	(-91.0000, -91.0000)

Table C.33: Power Statistics during the Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 3 db Transmit Gain

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
15 m	30	-86.5000	1.8892	0.3449	(-87.4507, -85.5493)
20 m	0	NA	NA	NA	(NA, NA)
25 m	0	NA	NA	NA	(NA, NA)
30 m	0	NA	NA	NA	(NA, NA)
35 m	0	NA	NA	NA	(NA, NA)

C.2.3 Directed Antenna.

Table C.34 summarizes the data for the blocked line of sight experiment when using the USRP with directed antenna and 30 db transmit gain. Table C.35 summarizes the data for the blocked line of sight experiment when using the USRP with directed antenna and 15 db transmit gain. Table C.36 summarizes the data for the blocked line of sight experiment when using the USRP with directed antenna and 3 db transmit gain.

Table C.34: Summary of Blocked Line of Sight Experiment using the USRP with Directed Antenna and 30 db Transmit Gain

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
15 m	30	29	96.67%	30	9.8	-61.6
20 m	30	30	100%	30	9.6	-62.2
25 m	30	30	100%	30	7.1	-69.7
30 m	30	30	100%	30	5.3	-75.1
35 m	30	30	100%	30	3.6333	-80.1

Table C.35: Summary of Blocked Line of Sight Experiment using the USRP with Directed Antenna and 15 db Transmit Gain

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
15 m	30	30	100%	30	4.9667	-76.1
20 m	30	30	100%	30	5	-76
25 m	30	30	100%	30	1.7667	-85.7
30 m	30	30	100%	23	0	-91
35 m	30	4	13.33%	23	0	-91

Table C.36: Summary of Blocked Line of Sight Experiment using the USRP with Directed Antenna and 3 db Transmit Gain

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
15 m	30	30	100%	30	1.3	-87.1
20 m	30	30	100%	30	1.1667	-87.5
25 m	30	16	53.33%	23	0	-91
30 m	30	0	0%	0	NA	NA
35 m	30	0	0%	0	NA	NA

Table C.37 displays the probability of success statistics for the USRP with directed antenna with 30 db transmit gain. Table C.38 shows the probability of success statistics for the USRP with directed antenna with 15 db transmit gain. Table C.39 details the probability of success statistics for the USRP with directed antenna with 3 db transmit gain.

Table C.37: Probability of Success Statistics during the Blocked Line of Sight Experiment using the USRP with Directed Antenna and 30 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	30	0.9667	0.1826	0.0333	(0.8748, 1.0585)
20 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
25 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
30 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
35 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)

Table C.38: Probability of Success Statistics during the Blocked Line of Sight Experiment using the USRP with Directed Antenna and 15 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
20 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
25 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
30 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
35 m	30	0.1333	0.3457	0.0631	(-0.0407, 0.3073)

Table C.39: Probability of Success Statistics during the Blocked Line of Sight Experiment using the USRP with Directed Antenna and 3 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
20 m	30	1.0000	0.0000	0.0000	(1.0000, 1.0000)
25 m	30	0.5333	0.5074	0.0926	(0.2780, 0.7887)
30 m	30	0.0000	0.0000	0.0000	(0.0000, 0.0000)
35 m	30	0.0000	0.0000	0.0000	(0.0000, 0.0000)

Table C.40 displays the power statistics for the USRP with directed antenna with 30 db transmit gain. Table C.41 shows the power statistics for the USRP with directed

antenna with 15 db transmit gain. Table C.42 details the power statistics for the USRP with directed antenna with 3 db transmit gain.

Table C.40: Power Statistics during the Blocked Line of Sight Experiment using theUSRP with Directed Antenna and 30 db Transmit Gain

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
15 m	30	-61.6000	1.2205	0.2228	(-62.2142, -60.9858)
20 m	30	-62.2000	1.6897	0.3085	(-63.0503, -61.3497)
25 m	30	-69.7000	1.4420	0.2633	(-70.4257, -68.9743)
30 m	30	-75.1000	1.3983	0.2553	(-75.8037, -74.3963)
35 m	30	-80.1000	1.6682	0.3046	(-80.9395, -79.2605)

Table C.41: Power Statistics during the Blocked Line of Sight Experiment using the USRP with Directed Antenna and 15 db Transmit Gain

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
15 m	30	-76.1000	1.2415	0.2267	(-76.7248, -75.4752)
20 m	30	-76.0000	1.3646	0.2491	(-76.6867, -75.3133)
25 m	30	-85.7000	2.1838	0.3987	(-86.7990, -84.6010)
30 m	24	-91.0000	0.0000	0.0000	(-91.0000, -91.0000)
35 m	25	-91.0000	0.0000	0.0000	(-91.0000, -91.0000)

Table C.42: Power Statistics during the Blocked Line of Sight Experiment using the USRP with Directed Antenna and 3 db Transmit Gain

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
15 m	30	-87.1000	2.2491	0.4106	(-88.2319 -85.9681)
20 m	30	-87.5000	1.3834	0.2526	(-88.1962 -86.8038)
25 m	23	-91.0000	0.0000	0.0000	(-91.0000 -91.0000)
30 m	0	NA	NA	NA	(NA, NA)
35 m	0	NA	NA	NA	(NA, NA)

C.3 GNU Radio Scenario

C.3.1 RZUSBSTICK.

Table C.43 summarizes the data for the GNU Radio portion of the experiment when using the RZUSBSTICK.

Table C.43: Summary of GNU Radio Blocked Line of Sight Experiment using the RZUSBSTICK

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
15 m	100	99	99%	100	0.01	-90.97
20 m	100	17	17%	41	0	-91
25 m	100	5	5%	0	NA	NA
30 m	100	0	0%	0	NA	NA
35 m	100	0	0%	0	NA	NA

Table C.44 shows the statistics for the probability of success of the replay attack when using the RZUSBSTICK. Table C.45 shows the statistics of the power of the replay attack when using the RZUSBSTICK as measured by the sensor near the victim. Table C.46 shows the statistics for the probability of the sensor detecting the replay attack from the RZUSBSTICK.

Table C.44: Probability of Success Statistics during the GNU Radio Blocked Line of Sight Experiment using the RZUSBSTICK

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	100	0.9900	0.1000	0.0100	(0.9637, 1.0163)
20 m	100	0.1700	0.3775	0.0378	(0.0708, 0.2692)
25 m	100	0.0500	0.2190	0.0219	(-0.0075, 0.1075)
30 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)
35 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)

Table C.45: Power Statistics during the GNU Radio Blocked Line of Sight Experiment using the RZUSBSTICK

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
15 m	100	-90.9700	0.3000	0.0300	(-91.0488, -90.8912)
20 m	41	-91.0000	0.0000	0.0000	(-91.0000, -91.0000)
25 m	0	NA	NA	NA	(NA, NA)
30 m	0	NA	NA	NA	(NA, NA)
35 m	0	NA	NA	NA	(NA, NA)

Table C.46: Probability of Success of the Sensor Statistics during the GNU Radio Blocked Line of Sight Experiment using the RZUSBSTICK

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	100	1.0000	0.0000	0.0000	(1.0000, 1.0000)
20 m	100	0.4100	0.4943	0.0494	(0.2802, 0.5398)
25 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)
30 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)
35 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)

C.3.2 Omnidirectional Antenna.

Table C.47 summarizes the data for the GNU Radio blocked line of sight experiment when using the USRP with omnidirectional antenna and 20 db transmit gain. Table C.48 summarizes the data for the GNU Radio blocked line of sight experiment when using the USRP with omnidirectional antenna and 15 db transmit gain. Table C.49 summarizes the data for the GNU Radio blocked line of sight experiment when using the USRP with omnidirectional antenna and 3 db transmit gain.

Table C.47: Summary of GNU Radio Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 20 db Transmit Gain

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
15 m	100	2	2%	98	7.9184	-67.2449
20 m	100	25	25%	97	4.3918	-77.8247
25 m	100	9	9%	54	3.2407	-81.2778
30 m	100	0	0%	100	3.2	-81.4
35 m	100	0	0%	97	1.1237	-87.6289

Table C.48: Summary of GNU Radio Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 15 db Transmit Gain

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
15 m	100	5	5%	100	6.78	-70.66
20 m	100	6	6%	96	3.0625	-81.8125
25 m	100	6	6%	62	2	-85
30 m	100	0	0%	98	2.1021	-84.6939
35 m	100	0	0%	22	0	-91

Table C.49: Summary of GNU Radio Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 3 db Transmit Gain

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
15 m	100	71	71%	89	1.6966	-85.9101
20 m	100	0	0%	7	0.1429	-90.5714
25 m	100	0	0%	0	NA	NA
30 m	100	0	0%	0	NA	NA
35 m	100	0	0%	0	NA	NA

Table C.50 displays the probability of success statistics for the USRP with omnidirectional antenna with 20 db transmit gain. Table C.51 shows the probability of success statistics for the USRP with omnidirectional antenna with 15 db transmit gain. Table C.52 details the probability of success statistics for the USRP with omnidirectional antenna with 3 db transmit gain.

Table C.50: Probability of Success Statistics during the GNU Radio Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 20 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	100	0.0200	0.1407	0.0141	(-0.0170, 0.0570)
20 m	100	0.2500	0.4352	0.0435	(0.1357, 0.3643)
25 m	100	0.0900	0.2876	0.0288	(0.0145, 0.1655)
30 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)
35 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)

Table C.51: Probability of Success Statistics during the GNU Radio Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 15 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	100	0.0500	0.2190	0.0219	(-0.0075, 0.1075)
20 m	100	0.0600	0.2387	0.0239	(-0.0027, 0.1227)
25 m	100	0.0600	0.2387	0.0239	(-0.0027, 0.1227)
30 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)
35 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)

Table C.53 displays the probability of success of the sensor statistics for the USRP with omnidirectional antenna with 20 db transmit gain. Table C.54 shows the probability

Table C.52: Probability of Success Statistics during the GNU Radio Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 3 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	100	0.7100	0.4560	0.4560	(0.5902, 0.8298)
20 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)
25 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)
30 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)
35 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)

of success of the sensor statistics for the USRP with omnidirectional antenna with 15 db transmit gain. Table C.55 details the probability of success of the sensor statistics for the USRP with omnidirectional antenna with 3 db transmit gain.

Table C.53: Probability of Success of the Sensor Statistics during the GNU Radio Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 20 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	100	0.9800	0.1407	0.0141	(0.9430, 1.0170)
20 m	100	0.9700	0.1714	0.0171	(0.9250, 1.0150)
25 m	100	0.5400	0.5009	0.0501	(0.4084, 0.6716)
30 m	100	1.0000	0.0000	0.0000	(1.0000, 1.0000)
35 m	100	0.9700	0.1714	0.0171	(0.9250, 1.0150)

Table C.54: Probability of Success of the Sensor Statistics during the GNU Radio Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 15 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	100	1.0000	0.0000	0.0000	(1.0000, 1.0000)
20 m	100	0.9600	0.1969	0.0197	(0.9083, 1.0117)
25 m	100	0.6200	0.4878	0.0488	(0.4919, 0.7481)
30 m	100	0.9800	0.1407	0.0141	(0.9430, 1.0170)
35 m	100	0.2200	0.4163	0.0416	(0.1107, 0.3293)

Table C.56 shows the statistics of the received power of the replay attack when using the USRP with omnidirectional antenna and 20 db transmit gain as measured by the sensor near the victim. Table C.57 shows the statistics of the received power of the replay

Table C.55: Probability of Success of the Sensor Statistics during the GNU Radio Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 3 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	100	0.8900	0.3145	0.0314	(0.8074, 0.9726)
20 m	100	0.0700	0.2564	0.0256	(0.0027, 0.1373)
25 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)
30 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)
35 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)

attack when using the USRP with omnidirectional antenna and 15 db transmit gain as measured by the sensor near the victim. Table C.58 shows the statistics of the received power of the replay attack when using the USRP with omnidirectional antenna and 3 db transmit gain as measured by the sensor near the victim.

Table C.56: Power Statistics during the GNU Radio Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 20 db Transmit Gain

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
15 m	98	-67.2449	1.5929	0.1609	(-67.6677, -66.8221)
20 m	97	-77.8247	2.8904	0.2935	(-78.5960, -77.0535)
25 m	54	-81.2778	2.1755	0.2960	(-82.0688, -80.4868)
30 m	100	-81.4000	1.8091	0.1809	(-81.8751, -80.9249)
35 m	97	-87.6289	2.2189	0.2253	(-88.2209, -87.0368)

Table C.57: Power Statistics during the GNU Radio Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 15 db Transmit Gain

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
15 m	100	-70.6600	1.7362	0.1736	(-71.1160, -70.2040)
20 m	96	-81.8125	2.1241	0.2168	(-82.3824, -81.2426)
25 m	62	-85.0000	2.3047	0.2927	(-85.7782, -84.2218)
30 m	98	-84.6939	1.9018	0.1921	(-85.1986, -84.1891)
35 m	22	-91.0000	0.0000	0.0000	(-91.0000, -91.0000)

Table C.58: Power Statistics during the GNU Radio Blocked Line of Sight Experiment using the USRP with Omnidirectional Antenna and 3 db Transmit Gain

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
15 m	89	-85.9101	2.1407	0.2269	(-86.5076, -85.3127)
20 m	7	-90.5714	1.1339	0.4286	(-92.1603, -88.9825)
25 m	0	NA	NA	NA	(NA, NA)
30 m	0	NA	NA	NA	(NA, NA)
35 m	0	NA	NA	NA	(NA, NA)

C.3.3 Directed Antenna.

Table C.59 summarizes the data for the GNU Radio blocked line of sight experiment when using the USRP with directed antenna and 20 db transmit gain. Table C.60 summarizes the data for the GNU Radio blocked line of sight experiment when using the USRP with directed antenna and 15 db transmit gain. Table C.61 summarizes the data for the GNU Radio blocked line of sight experiment when using the USRP with directed antenna and 3 db transmit gain.

Table C.59: Summary of GNU Radio Blocked Line of Sight Experiment using the USRP with Directed Antenna and 20 db Transmit Gain

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
15 m	100	65	65%	99	6.7373	-70.7879
20 m	100	77	77%	100	3.8	-79.6
25 m	100	34	34%	97	3.7629	-79.7113
30 m	100	1	1%	94	1.5213	-86.4362
35 m	100	0	0%	72	0.3889	-89.8333

Table C.60: Summary of GNU Radio Blocked Line of Sight Experiment using the USRP with Directed Antenna and 15 db Transmit Gain

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
15 m	100	63	63%	98	4.5714	-77.2857
20 m	100	24	24%	38	2.3421	-83.9737
25 m	100	9	9%	95	2.2632	-84.2105
30 m	100	0	0%	80	0.425	-89.725
35 m	100	0	0%	27	0.037	-90.8889

Table C.61: Summary of GNU Radio Blocked Line of Sight Experiment using the USRP with Directed Antenna and 3 db Transmit Gain

Distance	Number Of Trials	Number of Successes	Mean Probability of Success	Number of Power Samples	Mean RSSI	Mean Power (dbm)
15 m	100	37	37%	97	2.4536	-83.6392
20 m	100	0	0%	0	NA	NA
25 m	100	0	0%	0	NA	NA
30 m	100	0	0%	0	NA	NA
35 m	100	0	0%	0	NA	NA

Table C.62 displays the probability of success statistics for the USRP with directed antenna with 20 db transmit gain. Table C.63 shows the probability of success statistics for the USRP with directed antenna with 15 db transmit gain. Table C.64 details the probability of success statistics for the USRP with directed antenna with 3 db transmit gain.

Table C.62: Probability of Success Statistics during the GNU Radio Blocked Line of Sight Experiment using the USRP with Directed Antenna and 20 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	100	0.6500	0.4794	0.0479	(0.5241, 0.7759)
20 m	100	0.7700	0.4230	0.0423	(0.6589, 0.8811)
25 m	100	0.3400	0.4761	0.0476	(0.2150, 0.4650)
30 m	100	0.0100	0.1000	0.0100	(-0.0163, 0.0363)
35 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)

Table C.63: Probability of Success Statistics during the GNU Radio Blocked Line of Sight Experiment using the USRP with Directed Antenna and 15 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	100	0.6300	0.4852	0.0485	(0.5026, 0.7574)
20 m	100	0.2400	0.4292	0.0429	(0.1273, 0.3527)
25 m	100	0.0900	0.2876	0.0288	(0.0145, 0.1655)
30 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)
35 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)

Table C.65 displays the probability of success of the sensor statistics for the USRP with directed antenna with 20 db transmit gain. Table C.66 shows the probability of

Table C.64: Probability of Success Statistics during the GNU Radio Blocked Line of Sight Experiment using the USRP with Directed Antenna and 3 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	100	0.3700	0.4852	0.0485	(0.2426, 0.4974)
20 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)
25 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)
30 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)
35 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)

success of the sensor statistics for the USRP with directed antenna with 15 db transmit gain. Table C.67 details the probability of success of the sensor statistics for the USRP with directed antenna with 3 db transmit gain.

Table C.65: Probability of Success of the Sensor Statistics during the Blocked Line of Sight Experiment using the USRP with Directed Antenna and 20 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	100	0.9900	0.1000	0.0100	(0.9637, 1.0163)
20 m	100	1.0000	0.0000	0.0000	(1.0000, 1.0000)
25 m	100	0.9700	0.1714	0.0171	(0.9250, 1.0150)
30 m	100	0.9400	0.2387	0.0239	(0.8773, 1.0027)
35 m	100	0.7200	0.4513	0.0451	(0.6015, 0.8385)

Table C.66: Probability of Success of the Sensor Statistics during the GNU Radio Blocked Line of Sight Experiment using the USRP with Directed Antenna and 15 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	100	0.9800	0.1407	0.0141	(0.9430, 1.0170)
20 m	100	0.3800	0.4878	0.0488	(0.2519, 0.5081)
25 m	100	0.9500	0.2190	0.0219	(0.8925, 1.0075)
30 m	100	0.8000	0.4020	0.0402	(0.6944, 0.9056)
35 m	100	0.2700	0.4462	0.0446	(0.1528, 0.3872)

Table C.68 shows the statistics of the received power of the replay attack when using the USRP with directed antenna and 20 db transmit gain as measured by the sensor near the victim. Table C.69 shows the statistics of the received power of the replay attack when using the USRP with directed antenna and 15 db transmit gain as measured by the sensor

Table C.67: Probability of Success of the Sensor Statistics during the GNU Radio Blocked Line of Sight Experiment using the USRP with Directed Antenna and 3 db Transmit Gain

Distance	Number Of Trials	Mean Probability of Success	Standard Deviation	Standard Error	99% Confidence Interval
15 m	100	0.9700	0.1714	0.0171	(0.9250, 1.0150)
20 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)
25 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)
30 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)
35 m	100	0.0000	0.0000	0.0000	(0.0000, 0.0000)

near the victim. Table C.70 shows the statistics of the received power of the replay attack when using the USRP with directed antenna and 3 db transmit gain as measured by the sensor near the victim.

Table C.68: Power Statistics during the GNU Radio Blocked Line of Sight Experiment using the USRP with Directed Antenna and 20 db Transmit Gain

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
15 m	99	-70.7879	2.2098	0.2221	(-71.3713, -70.2045)
20 m	100	-79.6000	2.0449	0.2045	(-80.1371, -79.0629)
25 m	97	-79.7113	1.9736	0.2004	(-80.2380, -79.1847)
30 m	94	-86.4362	1.8524	0.1911	(-86.9386, -85.9337)
35 m	72	-89.8333	1.7116	0.2017	(-90.3672, -89.2994)

Table C.69: Power Statistics during the GNU Radio Blocked Line of Sight Experiment using the USRP with Directed Antenna and 15 db Transmit Gain

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
15 m	98	-77.2857	1.7761	0.1794	(-77.7571, -76.8143)
20 m	38	-83.9737	1.8814	0.3052	(-84.8025, -83.1449)
25 m	95	-84.2105	1.9673	0.2018	(-84.7412, -83.6799)
30 m	80	-89.7250	1.7061	0.1907	(-90.2285, -89.2215)
35 m	27	-90.8889	0.5774	0.1111	(-91.1976, -90.5801)

Table C.70: Power Statistics during the GNU Radio Blocked Line of Sight Experiment using the USRP with Directed Antenna and 3 db Transmit Gain

Distance	Number of Power Samples	Mean Power (dbm)	Standard Deviation	Standard Error	99% Confidence Interval
15 m	97	-83.6392	2.0320	0.2063	(-84.1814, -83.0970)
20 m	0	NA	NA	NA	(NA, NA)
25 m	0	NA	NA	NA	(NA, NA)
30 m	0	NA	NA	NA	(NA, NA)
35 m	0	NA	NA	NA	(NA, NA)

Bibliography

[80211] IEEE Standard for Local and Metropolitan Area Networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs). *IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006)*, pages 1–314, 2011.

[CWL10] Johnny Cache, Joshua Wright, and Vincent Liu. *Hacking Wireless Exposed*. McGraw Hill, 2010.

[Dab11] Krešimir Dabčević. Evaluation of Software Defined Radio Platform with Respect to Implementation of 802.15.4 ZigBee, 2011.

[DT10] Gianluca Dini and Marco Tiloca. Considerations on Security in ZigBee Networks. In *2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, pages 58–65, 2010.

[ER14] A National Instruments Company Ettus Research. Ettus Research - Home. http://www.ettus.com/, 2014. Accessed: 2014-02-27.

[For11] Wireless Innovation Forum. Introduction to SDR - Wireless Innovation Forum. http://www.wirelessinnovation.org/assets/documents/SoftwareDefinedRadio.pdf, 2011. Accessed: 2014-02-27.

[GBM+12] T. Goodspeed, S. Bratus, R. Melgares, R. Speers, and S. W. Smith. Api-do: Tools for Exploring the Wireless Attack Surface in Smart Meters. In *System Science (HICSS), 2012 45th Hawaii International Conference on*, pages 2133–2140, 2012. ID: 1.

[Gis08] Drew Gislason. *ZigBee Wireless Networking*. Elsevier, 2008.

[Goo09] Travis Goodspeed. Extracting Keys from Second Generation ZigBee Chips. In *Black Hat USA*, 2009.

[Ins12] National Instruments. Record and Playback Demo With NI USRP. http://www.ni.com/white-paper/13881/en/, 2012. Accessed: 2014-02-27.

[Lan13] Jean-Philippe Lang. WikiStart - GNU Radio - gnuradio.org. http://gnuradio.org/redmine/projects/gnuradio/wiki, 2013. Accessed: 2014-02-27.

[LLC14] Fosiao LLC. ZigBee and Wifi RF Channels — Fosiao LLC. http://fosiao.com/content/zigbee-and-wifi-rf-channels, 2014. Accessed: 2014-02-27.

[Mit99] J. Mitola. Technical Challenges in the Globalization of Software Radio. *Communications Magazine, IEEE*, 37(2):84–89, Feb 1999.

[RMSB13] Benjamin W. Ramsey, Barry E. Mullins, Ryan Speers, and Katherine A. Batterton. Watching for Weakness in Wild WPANs. In *2013 IEEE Military Communications Conference*, pages 1404–1409, 2013.

[RMW12] B.W. Ramsey, B.E. Mullins, and E.D. White. Improved tools for indoor ZigBee warwalking. In *Local Computer Networks Workshops (LCN Workshops), 2012 IEEE 37th Conference on*, pages 921–924, Oct 2012.

[SEB12] Balint Seeber, Matt Ettus, and Philip Balister. Overview - UHD - Ettus Research LLC. http://code.ettus.com/redmine/ettus/projects/uhd/, 2012. Accessed: 2014-02-27.

[SMB12] R. Speers, R. Melgares, and S. Bratus. Api-do: Tools for ZigBee and 802.15.4 Security Auditing. http://code.google.com/p/zigbee-security/, 2012. Accessed: 2014-02-27.

[SR13] Bjorn Stelte and Gabi Dreo Rodosek. Thwarting attacks on ZigBee - Removal of the KillerBee stinger. In *Network and Service Management (CNSM), 2013 9th International Conference on*, pages 219–226, Oct 2013.

[SSS07] Thomas Schmid, Oussama Sekkat, and Mani B. Srivastava. An Experimental Study of Network Performance Impact of Increased Latency in Software Defined Radios. In *Proceedings of the Second ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization*, WinTECH '07, pages 59–66, New York, NY, USA, 2007. ACM.

[Tha12] Rithirong Thandee. IEEE 802.15.4 Implementation on an Embedded Device, April 2012.

[ver09] USRP: Vert2450 - KnowledgeBase. http://kb.microembedded.com/vert2450, 2009. Accessed: 2014-02-27.

[VHnA+13] Niko Vidgren, Keijo Haataja, José Luis Pati no Andres, Juan José Ramírez-Sanchis, and Pekka Toivanen. Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned. In *System Sciences (HICSS), 2032 46th Hawaii International Conference on*, pages 5132–5138, 2013.

[Yan09] Bin Yang. Study on Security of Wireless Sensor Network Based on ZigBee Standard. In *Computational Intelligence and Security, 2009. CIS '09. International Conference on*, volume 2, pages 426–430, 2009. ID: 1.

[YNN08] Ender Yüksel, Hanne Riis Nielson, and Flemming Nielson. ZigBee-2007 Security Essentials. In *Proceedings of the 13th Nordic Workshop on Secure IT Systems : NordSec 2008*, pages 65–82, Denmark, 2008. DTU Informatics, Building 321. Presented at: The 13th Nordic Workshop on Secure IT Systems : NordSec 2008 : Kongens Lyngby, Denmark, 2008.

[Zig13] ZigBee Alliance. ZigBee Alliance Home. http://www.zigbee.org/, 2013. Accessed: 2014-02-27.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704–0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
27–03–2014	Master's Thesis	Oct 2013–Mar 2014

4. TITLE AND SUBTITLE

Comparison of ZigBee Replay Attacks Using a Universal Software Radio Peripheral and USB Radio

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Dalrymple, Scott D., Captain, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB, OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENG-14-M-23

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Nick Carr
DHS ICS-CERT
245 Murray Lane SW
Bldg 410, Mail Stop 635
Washington, DC 20528
(208) 526-0900

10. SPONSOR/MONITOR'S ACRONYM(S)

DHS ICS-CERT

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A:
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

13. SUPPLEMENTARY NOTES

This work is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT

Low-Rate Wireless Personal Area Networks are a prevalent solution for communication among embedded devices. ZigBee is a leading network protocol stack based on the low-rate IEEE 802.15.4 standard that operates smart utility meters, residential and commercial building automation, and heath care networks. Such networks are essential, but low-rate, low-cost hardware is challenging to protect because end devices have tight limitations on hardware cost, memory use, and power consumption. KillerBee is a python-based framework for attacking ZigBee and other 802.15.4 networks that makes traffic eavesdropping, packet replay, and denial of service attacks straightforward to conduct. Recent works investigate software-defined radios as an even more versatile attack platform. Software defined radios can operate with greater flexibility and at greater transmit power than traditional network hardware. Software-defined radios also enable novel physical-layer attacks including reflexive jamming and synchronization header manipulation that are not possible with traditional hardware.

This research implements a replay attack against a ZigBee device using a software defined radio. Replay attacks consist of an attacker recording legitimate traffic on a network and then replaying that traffic at will to cause malicious effects. Replay attacks can be very disruptive to operational systems, from turning valves in industrial controls systems to disarming door locks. Specifically, how software-defined radios can extend the effective attack range far beyond what is possible with hardware currently utilized by KillerBee is investigated.

A software defined radio is tested with both directed and omnidirectional antennas and the effective attack range is compared to that of a USB radio. Tests are conducted both line-of-sight outdoors and through interior walls. The replay attack is implemented with beacon request frames. Legitimate beacon request frames are prerecorded with the software defined radio, and at a later time, replayed against a target device. Results demonstrate that, in addition to being a more versatile attack platform, software-defined radios can be effective in close-range proof of concept of fixed KillerBee hardware.

15. SUBJECT TERMS

ZigBee, software defined radio, KillerBee, USRP

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Barry E. Mullins (ENG)
U	U	U	UU	138	19b. TELEPHONE NUMBER *(include area code)* (937) 255-3636 x7979 Barry.Mullins@afit.edu