The Effects of Cognitive Jamming on Wireless Sensor Networks used for Geolocation

THESIS

Michael A. Huffman, Captain, USAF

AFIT/GE/ENG/12-21

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GE/ENG/12-21

The Effects of Cognitive Jamming on Wireless Sensor Networks used for Geolocation

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 Electrical Engineering

Michael A. Huffman, B.S.E.E.

Captain, USAF

March 2012

AFIT/GE/ENG/12-21

The Effects of Cognitive Jamming on Wireless Sensor Networks used for Geolocation

Michael A. Huffman, B.S.E.E.
Captain, USAF

Approved:

Richard K. Martin	2 Mar 2012
Dr. Richard K. Martin (Chairman)	date
Michael A. Temple	2 Mar 2012
Dr. Michael A. Temple (Member)	date
Mark D. Silvius	2 Mar 2012
Maj. Mark D. Silvius, PhD (Member)	date

Abstract

The increased use of Wireless Sensor Networks (WSN) for geolocation has led to the increased reliance of this technology. Jamming, protecting and detecting jamming in a WSN are areas of study that have increased in interest because of this. To learn more about the effects of jamming, this research uses simulations and hardware to test the effects of jamming on a WSN. For this research the hardware jamming was tested using a Universal Software Radio Peripheral (USRP) version 2 to assess the effects of jamming on a cooperative network of Java Sun SPOTs. This research combined simulations and data collected from hardware experiments to see the effects of jamming on cooperative and non-cooperative geolocation.

Acknowledgements

First and foremost, I owe a large debt of gratitude to my wife for all of her support throughout this whole process. I would not have made it without her.

I also owe a lot of thanks to my advisor Dr. Martin. The advice and technical expertise gave me the support I needed to complete my thesis.

I would also like to thank my friends at AFIT. They assisted in both my education here at AFIT and made it bearable those long days in the winter term. Thank you everyone!

Michael A. Huffman

Table of Contents

Page

List of Figures

List of Tables

List of Abbreviations

Abbreviation		Page
RSS	Received Signal Strength	1
WSN	Wireless Sensor Network	1
SDR	Software Defined Radio	1
USRP	Universal Software Radio Peripheral	4
GCL	Geometry-Covering based Localization	7
WARP	Rice Wireless Open-Access Research Platform	8
BEE3	Berkeley Emulation Engine 3	8
KUAR	Kansas University Agile Radio	8
SFF-SDR	Small Form Factor Software Defined Radio	8
ITS	Intelligent Transport System	9
FPGA	Field Programmable Gate Array	9
ADCs	Analog to Digital Converters	9
DACs	Digital to Analog Converters	9
DSP	Digital Signal Processing	9
RF	Radio Frequency	10
GRC	GNU Radio Companion	10
WLAN	Wireless Local Area Network	12
E911	Enhanced 911	12
FCC	Federal Communications Commission	12
TOA	Time of Arrival	12
AOA	Angle Of Arrival	12
TDOA	Time Difference of Arrival	12
PSD	Power Spectral Density	14
SNR	Signal to Noise Ratio	14
MLE	Maximum Likelihood Estimation	15

Abbreviation		Page
WND	Wireless Network Discovery	15
ROC	Receiver Operating Characteristic	15
OTA	Over-the-Air	17
ISM	Industrial, Scientific and Medical	17
AWGN	Additive White Gaussian Noise	22
PDF	Probability Density Function	23
UDP	User Datagram Protocol	30
MIMO	Multiple Input Multiple Output	70

The Effects of Cognitive Jamming on Wireless Sensor Networks used for Geolocation

I. Introduction

This chapter provides a brief overview of relevant background material to this research, including the development of localization via Received Signal Strength (RSS), jamming of Wireless Sensor Networks (WSN) and Software Defined Radio (SDR). The motivation and research objectives for this work are also discussed.

1.1 Background

Localization or geolocation is used for various applications and can be used indoors and outdoors. For example, geolocation can be used to find mobile robots indoors [20] or to find a mobile user in a cellular environment [22]. A WSN can be used for geolocation to locate a transmitter. There are many applications for WSNs, some examples are:

- Cellphone network (voice, text and data)
- Animal monitoring (location tracking of animals)
- Machine monitoring (sensors on equipment in manufacturing)
- Vehicle monitoring (sensors monitoring functions of racecars)
- Medical monitoring (sensors on patients in hospitals)
- Wi-Fi 802.11 networks (internet, printing, storage, etc.)

A WSN can also be a set of inexpensive sensors used to collect RSS measurements. Java Sun SPOT sensors are used as a WSN in this research. Sun SPOT sensors can be programmed to perform various functions including transmitting and receiving. WSN are also prone to interference either intentional or unintentional.

Jamming can be unintentional interference or noise that can degrade the performance or disrupt a WSN. Jamming can also be in the form of an attack, which is intended to disrupt a WSN. Jamming is an effective form of attack since no special hardware is required and it is easy to monitor and broadcast in the same frequency band as the network which is being jammed. If jamming is implemented wisely, it can cause great harm to the network being jammed and can provide great benefits to the attacker with minimal cost [15]. With the increase of location based services (e.g. cell phones and Facebook Check In service) comes the increased dependence on this technology. The more we depend on this technology, the greater the adverse effects will be when it stops working. If the WSN is disrupted or jammed, this causes problems for the users. In addition to civilian uses of localization, the military has an increased need for geolocation. Geolocation can be used to locate enemy transmitters, soldiers or communication devices. The enemy can also use jammers to block or reduce the effect of a WSN used for geolocation. This can cause problems with the military's use of WSN for tracking enemy transmitters or soldiers.

The main focus of this research is assessing jamming impacts on sensor networks. There are a few effective ways to jam a WSN:

- Constant Jammer
- Deceptive Jammer
- Random Jammer
- Reactive Jammer

Each of these methods has their strengths and weaknesses, which will be discussed in more detail in Chapter II. For this research a Constant Jammer will be used. Constant Jamming is where the jammer is on continuously at a steady power level maintaining a single type of waveform.

There are two different types of WSNs that are discussed in this research, Cooperative Network and Non-cooperative Network. In a Cooperative Network, the

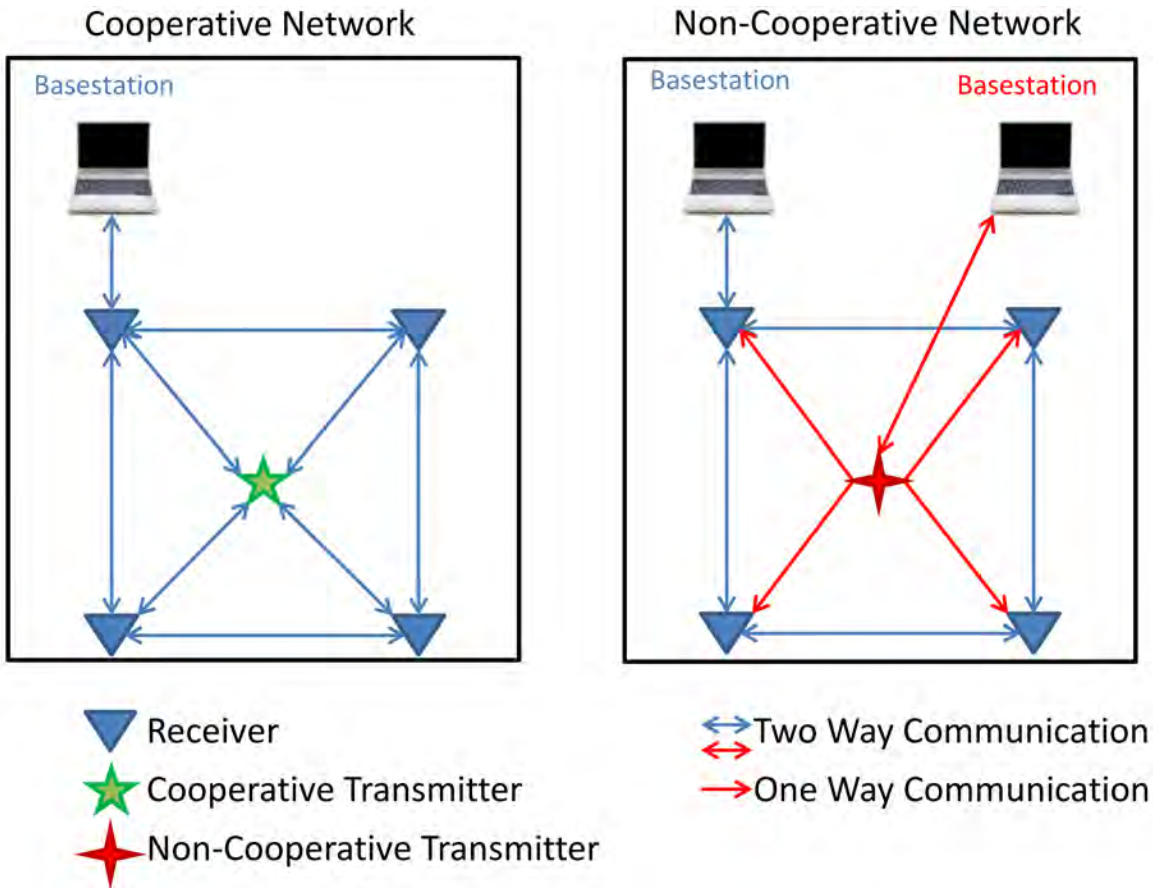


Figure 1.1: Diagram showing the difference betweet a Cooperative Network and Non-Cooperative Network [3].

receivers communicate with each other and communicate with the transmitter. The receivers know the transmitter's modulation scheme and are able to decode the signal. They are all part of the same network communicating with each other. In a Non-Cooperative Network the receivers still work together, but the transmitter is not part of the network. The transmitter's modulation scheme is generally unknown and it is not able to be decoded. The received power is measured by taking the power spectral density of the transmitter. Figure 1.1 shows the difference between Cooperative and Non-Cooperative Networks [3].

1.2 Research Objectives

The effects of jamming a WSN used for geolocation has not been studied in great detail. The main goal and objective of this research is to determine the effects of jamming on the Sun SPOT devices used as a WSN for geolocation. To accomplish this, the Universal Software Radio Peripheral (USRP) version 2, a type of SDR, is used as a jammer to disrupt the Sun Spot WSN. This is first simulated in MATLAB to get a baseline on what to expect from the Sun SPOT sensors. To determine the effect of jamming, the location estimate of the geolocation algorithm is compared in both non-jamming (clear air) and jamming environments. A baseline is established by collecting clear air data and performing the estimation algorithm. The same estimation algorithm is used for the jamming environment. This allows the data from the two environments to be compared. An existing algorithm from [16] is used for the geolocation estimates; the algorithm is not part of the new contributions.

1.3 Motivation

There are several motivating factors that propel this research. One factor is the increased use of WSNs in both the military and civilian sectors. Wireless networks are the future of communications and every year the number of WSNs have been increasing [4]. With the growth and reliance on WSNs, jamming and the effects of jamming WSNs is becoming a topic of interest.

Another motivating factor is that the military is increasing the use of WSNs on the battlefield. Similar to how the Global Positioning System (GPS) can be jammed, WSNs can also be jammed [32]. Since most WSNs operate at higher received power levels compared to GPS signals they are not as susceptible to jamming as GPS [11], [21], but they can still be effected by jamming. The effects of jamming WSNs have not been studied as much as GPS jamming, therefore it is crucial to understand the effects of jamming as this technology continues to grow. As WSNs grows into the military realm, lives may depend on the ability of WSNs operating as intended in both clear air and jamming environments.

1.4 Organization

Chapter II is the background information which discusses the literature review and key technical background research areas. This includes RSS techniques, SDR and jamming WSN. In Chapter III, the derivations for the geolocation solution, simulation and hardware set-up details are described. Chapter IV provides the results for the simulations hardware experiments and analyzes how the jammer effected the geolocation solution. Finally, Chapter V gives a summary of this research as well as the potential follow-on research areas.

II. Background Information

This chapter will discuss theory and experimental results related to this research. The review will address several main areas that are covered in this work. The areas of research are Jamming Sensor Networks, Software Defined Radio, Wireless Sensor Networks, Localization, Recieved Signal Strength Techniques, Detection and Estimation, and Wireless Network Discovery.

2.1 Jamming Sensor Networks

As mentioned in the introduction Jamming of Sensor Networks is one key area of related research. Sensor networks are widely used in many applications for data acquisition and data distribution [6]. Some examples include vehicle monitoring, animal monitoring, cellular phone and IEEE 802.11 networks. Wireless sensor networks are built upon a shared medium that makes it easy to interfere with or conduct jamming on the networks [31]. These attacks can be conducted many different ways; a few effective ways of jamming are described next.

2.1.1 Constant Jammer. The constant jammer continually emits a radio signal, and can be implemented using either a waveform generator that continuously sends a radio signal or a normal wireless device that continuously sends out random bits to the channel without following any MAC-layer etiquette [31]. Normally, the underlying MAC protocol allows legitimate nodes to send out packets only if the channel is idle. Thus, a constant jammer can effectively prevent legitimate traffic sources from getting hold of a channel and sending packets [31].

2.1.2 Deceptive Jammer. Instead of sending out random bits, the deceptive jammer constantly injects regular packets to the channel without any gap between subsequent packet transmissions. As a result, a normal communicator will be deceived into believing there is a legitimate packet and be duped to remain in the receive state. TinyOS is an open source software program used for WSN written in the nesC (similar to C language) programming language. For example, in TinyOS, if a preamble is

detected, a node remains in the receive mode, regardless of whether that node has a packet to send or not. Even if a node has packets to send, it cannot switch to the send state because a constant stream of incoming packets will be detected [31].

2.1.3 Random Jammer. Instead of continuously sending out a radio signal, a random jammer alternates between sleeping and jamming. Specifically, after jamming for a while, it turns off its radio and enters a "sleeping" mode. It will resume jamming after sleeping for some time. During its jamming phase, it can behave like either a constant jammer or a deceptive jammer. This jammer model tries to take energy conservation into consideration, which is especially important for those jammers that are battery powered [31]. Another advantage of a random jammer is that they are harder to detect since they randomly turn on and off for various amounts of time.

2.1.4 Reactive Jammer. The three models discussed above are active jammers in the sense that they try to block the channel irrespective of the traffic pattern on the channel. Active jammers are usually effective because they keep the channel busy all the time. An alternative approach to jamming wireless communication is to employ a reactive strategy. The reactive jammer stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel. A few advantages of a reactive jammer are that they are more energy efficient and they are harder to detect [31].

Of these types of jammers the constant jammer will be used in data collection for the experiments described in section III. The USRP2, a type of SDR, will be used to implement the jammer for the experiments.

2.1.5 Jamming Research. There are a few areas of research going on in the area of jamming sensor networks. Some of the work focuses on the detection and localization of jamming. The rest of the work mainly focuses on attack and defense strategies. In [26], a Geometry-Covering based Localization (GCL) algorithm, which utilizes the knowledge of computing geometry, especially the convex hull is proposed.

Simulation results showed that GCL is able to achieve higher accuracy than Centroid Localization in most cases. It was also noted that in general, when the density of nodes is higher, the localization error is smaller. In [2], jamming and sensing are two related functions in physical-layer based denial of service attacks against an encrypted wireless ad hoc network. The authors presented initial results in designing such a layered attacker for the Transport/Network layer. They showed that jamming can have significant gains of well over 100 when the packet type and timing of the network are known. It was shown that highly predictable timing in the wireless network can be exploited for easy attacks.

Optimal jamming attacks and network defense strategies are another key area of research. In [15], the authors studied controllable jamming attacks in wireless sensor networks, which are easy to launch and difficult to detect and difficult to locate. It was determined when there is a lack of knowledge of the attacker by the network and the attacker has a lack of knowledge of the network, the attacker and the network respond optimally to the worst-case strategy of the other. In [5], the authors discussed the problem of jamming a communication network under complete uncertainty. The authors derived upper and lower bounds for the optimal number of jamming devices required when they are located at the vertices of a uniform grid. They proved that their approach was more efficient than a solution provided by covering the square grid with circles of radius L. Even though their approach is more efficient, they still require a large number of jammers to accomplish their task.

2.2 Software Defined Radio

SDR is a flexible architecture, which can be configured to adapt various wireless standards, waveforms, frequency bands, bandwidths, and modes of operations [27]. There are various hardware platforms and software architectures that are used for defining the software radios. The USRP2, Rice Wireless Open-Access Research Platform (WARP), Berkeley Emulation Engine 3 (BEE3), Kansas University Agile Radio (KUAR), Small Form Factor Software Defined Radio (SFF-SDR) and Intelligent

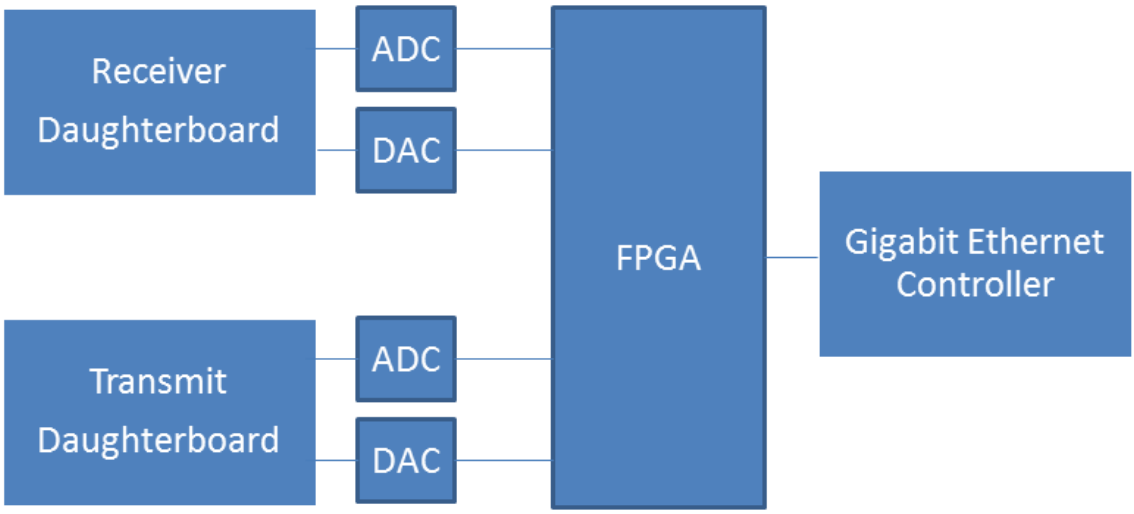


Figure 2.1: Block Diagram of the basic components of a USRP2 showing the possible daughterboards, FPGA, ADCs, DACs and Gigabit Ethernet Controller.

Transport System (ITS) are some platforms for SDR. In [27] these systems are explained in detail. For this thesis, the USRP2 will be explained in detail.

The Universal Software Radio Peripheral 2 (USRP2) is the creation of Matt Ettus (Ettus Research LLC) [7]. The USRP2 is a second generation of Universal Software Radio Peripheral. Its platform is made up of a Xilinx Spartan-III Field Programmable Gate Array (FPGA) and a general purpose AeMB processor [27]. The USRP2 is made of up a limited amount of components. Figure 2.1 shows a block diagram of the basic configuration of the USRP2. The USRP2 has removable daughter boards that can be swapped out depending on what frequency range the operator intends to operate in. This makes the USRP2 a very versatile software radio that can be configured to be virtually any type of wireless device. Some examples of the daughter boards are the DBSRX: 800 MHz to 2.4 GHz receiver, the RFX900: 750 to 1050 MHz transceiver and the WBX: 50 MHz to 2.2 GHz transceiver. The WBX daughterboard is shown in Figure 2.2.

On the USRP's main board there are Analog to Digital Converters (ADCs) and Digital to Analog Converters (DACs) along with a large FPGA. The FPGA is optimized for Digital Signal Processing (DSP) applications and allows for processing

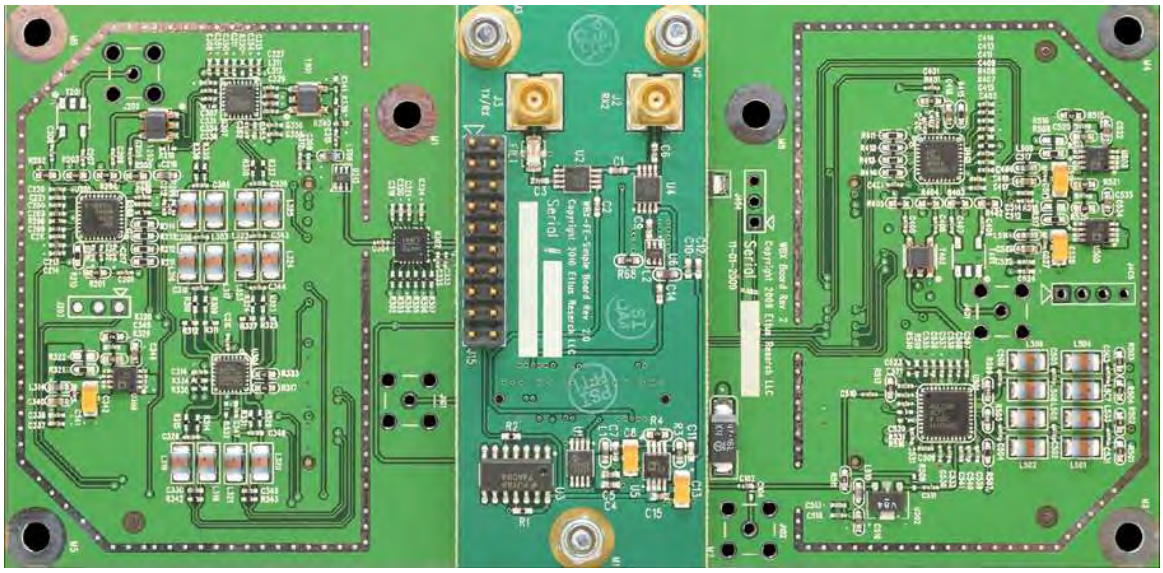


Figure 2.2: WBX Daughterboard [8].

complex waveforms at high sample rates [9]. A FPGA is like a small, massively parallel computer that a user can program to perform any task that is required [1].

GNU Radio is a free software development toolkit that provides the signal processing runtime and processing blocks to implement software radios using readily-available, low-cost external Radio Frequency (RF) hardware and commodity processors. It is widely used in hobbyist, academic and commercial environments to support wireless communications research as well as to implement real-world radio systems [7]. The radio applications are written in Python, while the critical signal processing components of the code are implemented in C++ using processor floating point extensions where available [27]. In GNU Radio Python there is a library of signal processing blocks which are used for the signal processing of the waveforms. There is also a program called GNU Radio Companion (GRC), which has a graphical user interface and is a tool for creating signal flow graphs and generating flow-graph source code [27].

GNU Radio is one of the ways to control a USRP2, LabView and Simulink can also be used to controll a USRP2. For this research Simulink will be used to control and program the USRP2. Only Simulink in MATLAB versions 2010b and 2011a

has the USRP2 blocks in the Communication blockset. Older versions of Simulink cannot be used with the USRP2. The common sources and blocks in Simulink can be connected to the USRP2 transmit or receive blocks and used to create numerous types of devices.

2.3 Wireless Sensor Networks

A WSN generally consists of a basestation (or "gateway") that can communicate with a number of wireless sensors via a radio link. Data is collected at the wireless sensor node, compressed, and transmitted to the gateway directly or, if required, uses other wireless sensor nodes to forward data to the gateway. The transmitted data are then presented to the system by the gateway connection [30]. The Java Sun SPOTs can be configured to be a WSN. The Sun SPOT unit is a small, wireless, battery powered experimental platform. It is programmed almost entirely in Java to allow programmers to easily create projects. Before the Sun SPOT unit was available it was a lot harder to program wireless sensors because of their special programming language. The Sun SPOT hardware platform includes a range of built-in sensors as well as the ability to easily interface to external devices [25].

For this research, the Sun SPOTs are configured to have one transmitter and a various number of receivers. The network of Sun SPOT receivers reports the RSS of the Sun SPOT transmitter to the Sun SPOT basestation. The computer connected to the Sun SPOT basestation records the data from all the Sun SPOTs which are configured as receivers. The collected data are then used to determine the location of the transmitter. This is one method used for localization also known as geolocation. In the next section localization methods will be described.

2.4 Localization

Localization in a WSN is used for many different applications. One example of localization is the location of mobile robots indoors [20]. RSS is converted to power in dBm, which is used to map a grid of locations using the indoor Wireless

Local Area Network (WLAN) system. Once the building is mapped with reference data, the RSS can be compared to the reference data and an estimated position of the mobile robot can be calculated. This technique is called RSS fingerprinting. Localization is also used in cell phones for Enhanced 911 (E911). The U.S. Federal Communications Commission (FCC) requires that the precise location of all E911 callers be automatically determined [23]. By using Time of Arrival (TOA), Angle Of Arrival (AOA), and Time Difference of Arrival (TDOA) algorithms, the location of the mobile phone can be estimated.

There are several different methods that have been developed and researched for localization. In [29], it is shown that there are four common methods used to determine the location of sensors. They are TOA, TDOA, AOA and RSS. Each of the methods uses a different aspect of the signal, and has advantages and disadvantages over the other methods. These methods will be discussed briefly.

2.4.1 Time of Arrival and Time Difference of Arrival. TOA and TDOA are very similar types of measurements. Both measurements measure the time at which a signal, either RF or acoustic, first arrives at a receiver [21]. Both methods do require a precise knowledge of time and need to be synchronized in order to have accurate results.

The measured TOA is the time of transmission plus a propagation-induced time delay [21]. TDOA uses a slightly different method to determine the distance. TDOA shares the arrival time with another transmitter or receiver, depending on the type of location or navigation, and the distance is based on the difference between the two arrival times. In general, TOA and TDOA systems are more complex compared to RSS systems and more expensive due to the fact that they require precise timing in order to achieve useable results. Another disadvantage is they are prone to multi-path interference. Multi-path is where the signal from the transmitter is received along with indirect signals reflected from surrounding objects. This can cause errors and reduce the accuracy of the estimated location.

2.4.2 Angle of Arrival. AOA uses a sensor array and employs array signal processing techniques at the sensor nodes to determine the direction of the arrival of the signal [21]. This information is often used along with TDOA and RSS to add additional information about the direction of the signal. AOA requires multiple antenna elements, which adds to the size and cost of a device used for AOA.

AOA is only able to determine the direction of the transmitter, not the distance to the transmitter. That is why AOA is commonly used along with either RSS or TDOA. This could be an issue if the cost and complexity of the system is a concern. Similar to TDOA, AOA is prone to multi-path interference.

2.4.3 Received Signal Strength. RSS uses the power of the signal measured at the receiver to estimate the distance to the transmitter. With multiple receivers, the location of a transmitter can be estimated. RSS relies on the fact that in free space the signal power decays proportional to d^{-2}, where d is the distance between the transmitter and receiver [21]. If the transmitted power is known or estimated, the distance to the transmitter from the receiver can be estimated. By increasing the number of receivers, the location accuracy estimate of the transmitter is increased. This method is used for this research. The main benefit of using RSS is that it is cost effective since the sensors are simple and do not require precise timing, complex antennas or processing.

There are some sources of error that affect the power measurements received. Multipath signals and shadowing are two major sources of error in the measured RSS. Multiple signals with different amplitudes and phases arrive at the receiver, and these signals add constructively or destructively as a function of the frequency, causing frequency-selective fading [21]. This effect can be reduced by using a spread-spectrum method (either direct-sequence or frequency hopping) which averages the received power over a range of frequencies.

With the device using a spread-spectrum technique to reduce these types of errors, there are still errors caused by shadowing. For example, the shadowing effect

caused by the attenuation of a signal due to obstructions (walls, buildings, trees, people, etc.). A signal must pass through or diffract around these obstructions on the path between the transmitter and receiver [21]. This error is usually modeled as a random variable.

2.5 Received Signal Strength Techniques

There are two main types of RSS localization techniques, cooperative and non-cooperative. In [21], cooperative localization, sensors work together in a peer-to-peer manner to make measurements and then form a map of the network. Various application requirements (such as scalability, energy efficiency, and accuracy) will influence the design of sensor localization systems. The Sun SPOT sensors used for this research work in a similar fashion and communicate to each other as a network. The Sun SPOT sensors are set-up as a network of receivers that communicate with each other and communicate with the Sun SPOT that is set-up as a transmitter. The Sun SPOT receivers know the modulation scheme and MAC address of the transmitter and only record the energy from the de-modulated Sun SPOT transmitter.

In non-cooperative RSS localization, the receivers record the raw power from a transmitter or multiple transmitters. The receivers do not communicate with the transmitter and are unable to de-modulate the transmitters signal. In non-cooperative systems, such as locating emitters in a hostile environment, the RSS may be determined by integrating the observed Power Spectral Density (PSD) [17]. However, the observed PSD is dominated by noise at low Signal to Noise Ratio (SNR) values. Thus, if the signal is low-power or far from a given receiver, the PSD may contain little information about the location of the emitter [18].

2.6 Detection and Estimation

Detection and Estimation is another key area of interest related to this research. All of the data collected by the sensors are relayed to a central node, the base station, where all the data are stored. This is where the processing of the data and the deci-

sions are made by using detection and estimation. Maximum Likelihood Estimation (MLE) is used to estimate the location of the transmitter. MLE is asymptotically unbiased and efficient for large data sets [13]. In [16], the position is estimated along with the transmitter's orientation, beam width, and transmit power, as well as the environment's path loss exponent, using received signal strength measurements. The derivations for how this estimator is used are included in Chapter III. The MLE of θ, a parameter of vector $\underline{P}$ which is the received power vector, is found by:

$$\underline{\hat{\theta}}_{\mathrm{ML}} = \arg\max_{\underline{\theta}} \mathcal{L} \tag{2.1}$$

$$\mathcal{L} = \ln p(\underline{P} \mid \underline{\theta}) \tag{2.2}$$

After the MLE is used to find the estimated position $\underline{\theta}$, the estimated position will be compared with estimates that have jamming and estimates that do not have jamming. The amount the estimates are off is the effect caused by jamming.

2.7 Wireless Network Discovery

Wireless Network Discovery (WND), refers to modeling all layers of a non-cooperative wireless network by finding the frequency of a device, locating the device, determining communication patterns, transmit power of the device, etc. In, [10] observations of physical layer data are used for decisions and calculations, and are based on just the measurements collected by the sensors. Although this information is packaged and distributed on the network layer, only the physical measurements are considered. This protocol is used to detect faulty nodes operating in the sensor network. In [10], the author used WND for the localization of transmitters and detection of sensors affecting the localization. To accomplish this, a model for faulty sensors and two methods of detection are developed. Detection rates are analyzed with Receiver Operating Characteristic (ROC) curves, and the trade-off of detection versus localization error is discussed. Classification between faulty sensors is also considered to determine an appropriate response to potential network attacks.

III. Methodology

This chapter details the methodology used to develop and test the algorithms used for geolocation and jamming. The setup of the simulations of the sensor network for cooperative and non-cooperative geolocation are explained. Following the simulation section the hardware configuration and layout for the system will also be shown. The various jammer configurations, antennas and power levels are discussed.

3.1 System Overview and Description

The system consists of four major components: the sensor network deployed by the user can be either a cooperative or non-cooperative network, the basestation used for collecting and processing data, the transmitter that is being tracked and the jammer that is disrupting the sensor network. Figure 3.1 shows the four main components of the system. This system is used to test and determine the effects of jamming on a WSN used for geolocation. All of these components are needed to understand how jamming effects a WSN, specifically the Sun SPOT sensors. In order to understand the effects of jamming, each component of the system will be described.

3.1.1 Sensor Network. The first component is a sensor network. As mentioned earlier there are two types of sensor networks, a cooperative and non-cooperative sensor network. The non-cooperative sensor network is simulated in MATLAB along with the cooperative sensor network. In hardware testing only the cooperative sensor network is used. This network is a group of Sun SPOTs that are able to estimate the RSS of a transmitted signal. The Sun SPOTs have knowledge of the frequency that the transmitter is operating at. The Sun SPOTs also communicate with each other and can send information from unit to unit back to the basestation. The Sun SPOTs are stationary and their locations are known and stored at the basestation. This knowledge is collected either from a GPS unit that was positioned at each unit location or from measuring the Sun SPOT network by hand. This is known as a priori knowledge of the unit locations. This will also be simulated in MATLAB.

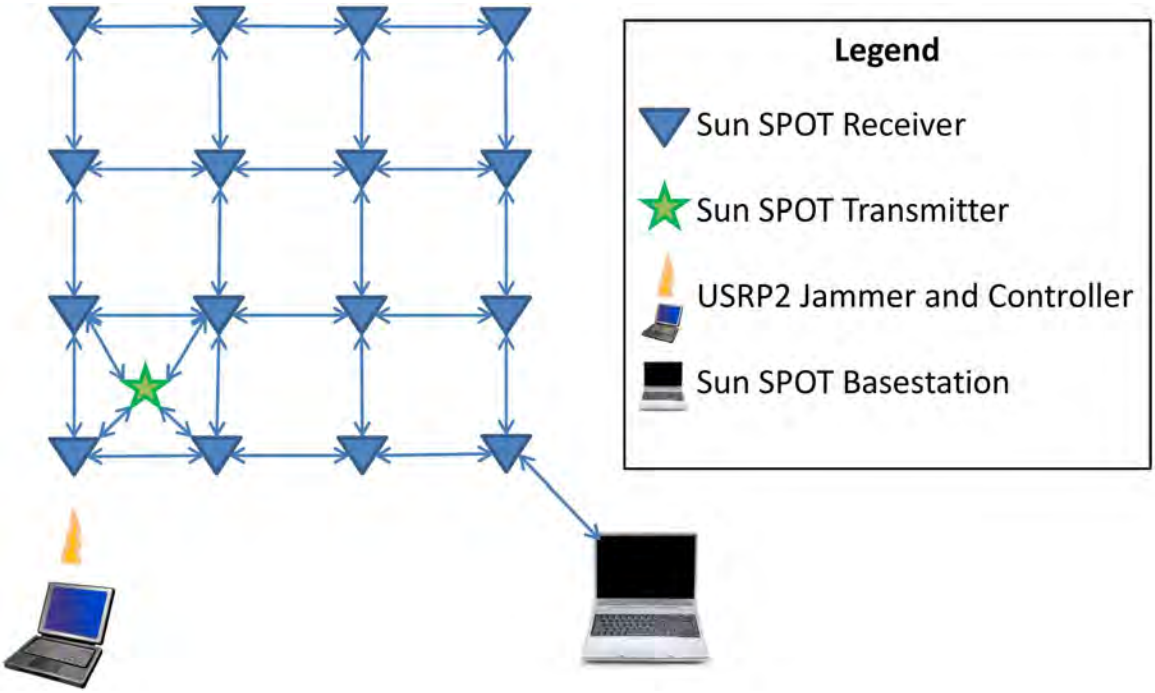


Figure 3.1: System overview showing the four main components: Sun SPOT sensor network as receivers and transmitter, the USRP2 jammer and the basestation for collecting the data from the Sun SPOT sensor network.

The Sun SPOTs do Over-the-Air (OTA) communication between each Sun SPOT. This allows the Sun SPOTs to form a cooperative network since the Sun SPOTs that are set-up as receivers communicate with the Sun SPOT set-up as a transmitter. This allows the Sun SPOTs to ignore interference in the 2.4 GHz Industrial, Scientific and Medical (ISM) band and this makes it harder to add interference to the network. To have a cooperative network, you would need to know the IEEE extended MAC address of each Sun SPOT. The IEEE extended MAC address is a 64-bit address, expressed as four sets of four-digit hexadecimal numbers: nnnn.nnnn.nnnn.nnnn. The first eight digits are always 0014.4F01. The last eight digits are device dependent and printed on a sticker visible through the translucent plastic on the radio antenna fin. A typical sticker would show something like 0000.77AE, implying an IEEE address for that SPOT of 0014.4F01.0000.77AE [24].

The other type of network is a non-cooperative network. In a non-cooperative network, the receivers do not communicate with the transmitter. The transmitter

is a non-cooperative device that is not controlled by the user or the sensor network. The receivers will record the raw power of the transmitter in a set frequency band to detect the RSS of a non-cooperative transmitter. If there is interference in addition to the transmitter, this will affect the estimation of a non-cooperative network. From the author's experience, this type of network is affected more by jamming. The sensor network estimates the power of the transmitter along with the jammer reducing the accuracy of the estimation. This network is simulated in MATLAB.

3.1.2 Basestation. The basestation is an important part of the system. All data from the Sun SPOT sensor network is reported back and collected here. The data can be passed onto MATLAB for real time processing of the solution or stored for later processing. MATLAB uses the algorithms discussed in the next section for the estimation of the transmitter location.

3.1.3 Transmitter. The transmitter is another important part of the system. In the cooperative network, the Sun SPOT transmitter's frequency and MAC address are known. This allows the Sun SPOT network to ignore other interference in the 2.4 GHz band. In the real world, there are many unknown aspects to the device and channel that will affect how accurately the sensor network will be able to locate the transmitter. Some of the factors are the antenna polarization, the original transmission power, and various channel and environmental factors [10]. In [16], techniques are shown to estimate these factors without prior knowledge of them. For this research, these factors are considered known either from estimation or prior knowledge.

3.1.4 Jammer. The key aspect of the system for this research effort is the jammer. The USRP2, a type of SDR, is used as a jammer for this research. The USRP2 is controlled by Simulink and can be configured to be a constant or random jammer. In simulation, for the cooperative network, the jammer is simulated by removing sensors in a designated target area. This is similar to how the hardware jammer works since the hardware jammer increases the noise floor so that the receivers

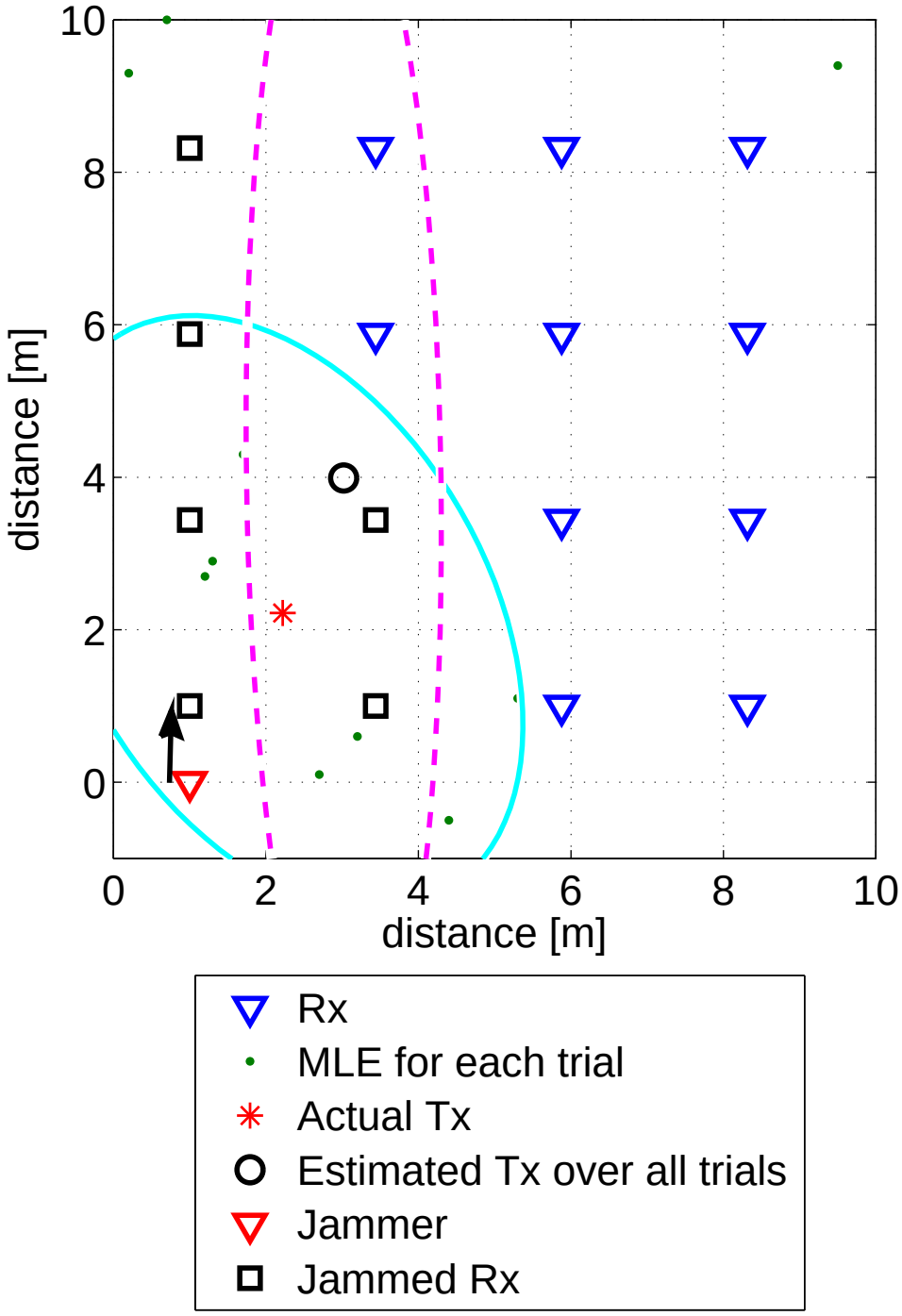


Figure 3.2: A four by four grid example of a cooperative sensor network containing 16 sensors with the CRLB in cyan and the Covariance in magenta of the estimate for the 10 trials simulated.

can't communicate with the transmitter; this effectively removes the receiver from the network. For the non-cooperative network the jammer is simulated by adding another device that acts similar to another transmitter. The system is implemented in MATLAB and an example of the sensor network is shown in Figure 3.2. Figure 3.2 shows the effects of jamming a cooperative sensor network and the error that the jammer introduces to the estimate. This can be seen with the estimated position being farther away than the actual position of the transmitter. Only 10 independent trials at each transmitter location were conducted to get similar results to the hardware trials that were conducted. Only a limited number of independent hardware trials were able to be accomplished for this research.

3.2 RSS Model for Simulation and Hardware

Table 3.1 is a collection of variables used in this research.

3.2.1 RF Signal Propagation. The derivation begins with the model for signal power. In free space, a RF signal will decay with respect to the distance squared. In previous research [16] the model for received power in dB can be shown to be:

$$m_s(d_s) = P_0 - \eta 10 \log_{10}\left(\frac{d_s}{d_0}\right) \tag{3.1}$$

where η is the path loss exponent and P_0 is the reference received power at a known reference distance d_0, typically 1m. This data has been collected for this research and Figure 3.3 shows the data for Sun SPOT 7B20 from Equation (3.1). The effect of noise in this log-normal model is assumed to be Gaussian with a standard deviation of σ. The noise in this model is error due to log-normal fading, not interference from jamming or other sources. The distance between the sensor and transmitter in this model is defined by a two dimensional distance. The distance is defined by $d_s = \left\|\underline{\phi_s} - \underline{\theta}\right\|$, where $[x_0, y_0] = \underline{\theta}$ is the location of the transmitter and $[x_s, y_s] = \underline{\phi_s}$ is the location of the s^{th} sensor. Next, the received power is described by the locations of the sensors and transmitters, $m_s(\underline{\phi_s}, \hat{\underline{\theta}})$ if the transmitter location is estimated or

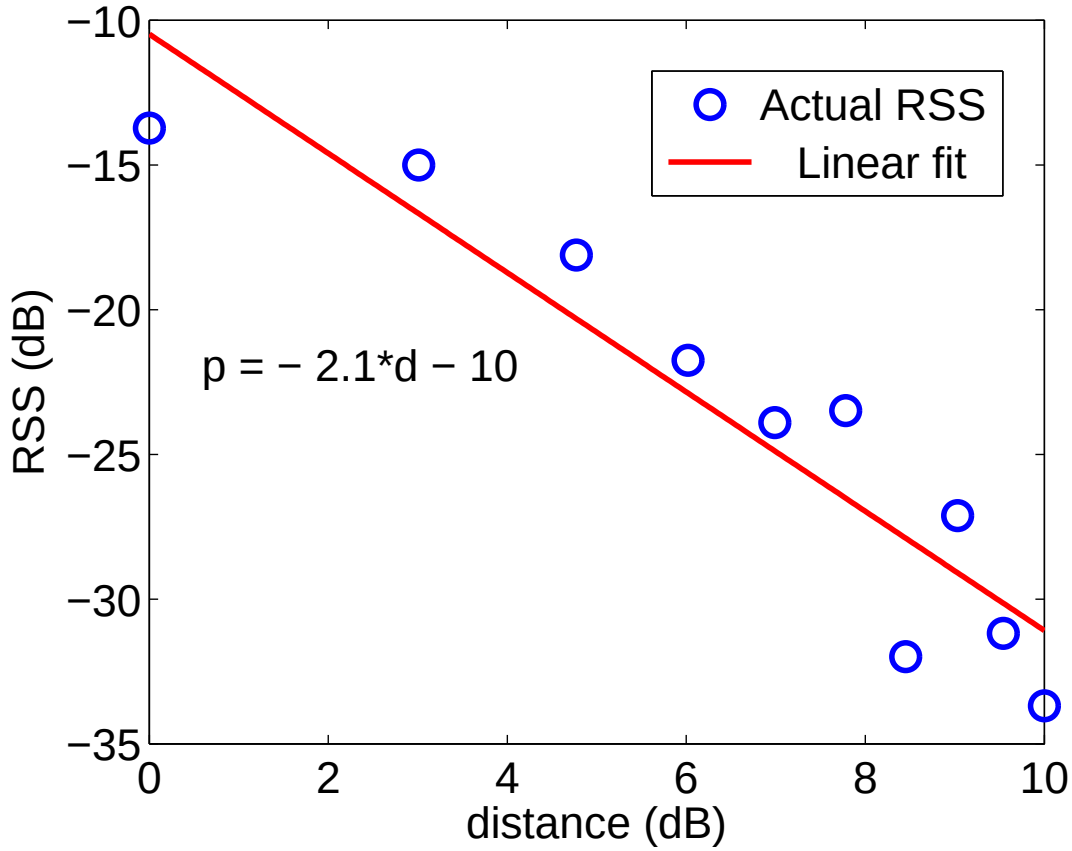


Figure 3.3: RSS vs. distance for Sun SPOT 7B20 showing Equation (3.1) with the data from this Sun SPOT, where $P_0 = -10$ and $\eta = 2.1$.

$m_s(\underline{\phi_s}, \underline{\theta})$ for derivations where the transmitter location is known. Using this model, the $S \times 1$ received power vector, $\underline{P}$, has a distribution of

$$\underline{P} = \underline{m}(\underline{\phi}, \underline{\theta}) + \underline{n} \tag{3.2}$$

$$\underline{n} \sim \mathcal{N}(\underline{0}, \sigma^2 I_s) \tag{3.3}$$

with I_s being defined as an $S \times S$ identity matrix, where S is defined as the number of sensors in the wireless network.

3.2.2 Data Creation and Variation. For the hardware testing, these data are collected and used in the estimation algorithm. To simulate the various scenarios,

Table 3.1: Table of variables used in this research

Variable	**Definition**	**Dimensionality**	**Units**
S	Number of sensors	Scalar	Unitless
K	# of independent trials	Scalar	Unitless
$\underline{\theta}$	Location of transmitter	1×2	meters
$\underline{\hat{\theta}}$	Estimated location of transmitter	1×2	meters
$\underline{\hat{\theta}}_{ML}$	ML estimate of location of transmitter	1×2	meters
$\underline{\phi_s}$	Location of s^{th} sensor	1×2	meters
$\underline{n}$	Additive White Gaussian Noise (AWGN)	$S \times 1$	dBm
n_{sim}	AWGN generated by MATLAB	Scalar	dBm
P_s	Power received at s^{th} sensor including AWGN	Scalar	dBm
Γ_0	Power transmitted	Scalar	mW
P_0	Logarithmic transmitted power	Scalar	dBm
$\widehat{P_0}$	Estimated transmitted power from collected RSS	Scalar	dBm
P_{0j}	Logarithmic transmitted power of Jammer	Scalar	dBm
d_0	Reference distance	Scalar	meters
d_s	Euclidean distance between emitter and s^{th} sensor	Scalar	meters
$m_s(\phi, \theta)$	Received power at s^{th} sensor without noise present	Scalar	dBm
$\underline{m}$	Received power vector of all sensors without noise present	$S \times 1$	dBm
$\underline{P}$	Received power vector of all sensors with AWGN	$S \times 1$	dBm
I_S, I_T	Identity matrix	$S \times S$, $T \times T$	Unitless
$\widehat{\eta}$	Estimated η from collected RSS	Scalar	dBm

synthetic RSS values are needed. To create the RSS values, data are generated using the models for the power and noise similar to what was used in [10]. To create the RSS values, the location of the transmitter is used. The location of the transmitter is only used to create the RSS values, not for the estimation algorithm. Using Equation (3.1), $m_s(d_s)$ the ideal RSS value is calculated. Noise is then added to the ideal RSS value with the modeled noise, n_{sim}.

$$P_s = m_s(d_s) + n_{sim,s} \tag{3.4}$$

where n_{sim} is AWGN generated by MATLAB. Following the method described in [10], the noise is zero mean with unit variance, but is multiplied by the simulated variance, σ. Data are created for each independent trial of the simulation. By changing the standard deviation of the simulation, this varies the output of the simulation.

3.2.3 Transmitter Localization. Using the system model and distribution described above, a MLE can be made of the transmitter location $\underline{\theta}$. First, the Probability Density Function (PDF) is defined for the power of all the sensor observations by

$$p(\underline{P} \mid \underline{\theta}) = \prod_{s=1}^{S} \frac{1}{\sqrt{2\pi}\sigma} \exp \frac{-(P_s - m(\underline{\phi_s}, \underline{\theta}))^2}{2\sigma^2} \tag{3.5}$$

To find the MLE of $\underline{\theta}$, Equation (3.5) needs to be simplified. To simplify Equation (3.5), the log-likelihood function, $\mathcal{L}$, needs to be maximized. $\mathcal{L}$ is found by taking the logarithm of the joint distribution and finding the value $\underline{\theta}$ that maximizes the likelihood function [13].

$$\mathcal{L} = \ln[p(\underline{P} \mid \underline{\theta})] = \ln \left[\prod_{s=1}^{S} \frac{1}{\sqrt{2\pi}\sigma} \exp \frac{-(P_s - m(\underline{\phi_s}, \underline{\theta}))^2}{2\sigma^2} \right] \tag{3.6}$$

$$\mathcal{L} = S \cdot \ln \left(\frac{1}{\sqrt{2\pi}\sigma} \right) - \frac{1}{2\sigma^2} \sum_{s=1}^{S} (P_s - m(\underline{\phi_s}, \underline{\theta}))^2 \tag{3.7}$$

$$\widehat{\underline{\theta}}_{ML} = \arg \max_{\underline{\theta}} \mathcal{L} \tag{3.8}$$

The first term of Equation (3.7) is a constant and does not affect $\underline{\theta}$. Next, to find the values of $\underline{\theta}$ that maximize $\mathcal{L}$, the gradient with respect to $\underline{\theta}$ is found and set equal to $\underline{0}$.

$$\nabla_{\theta}\mathcal{L} = \underline{0} = \nabla_{\theta}\left(S \cdot \ln\left(\frac{1}{\sqrt{2\pi}\sigma}\right) - \frac{S}{2\sigma^2}\left\|\underline{P} - \underline{m}(\underline{\phi}, \underline{\theta})\right\|^2\right) \tag{3.9}$$

Solving Equation (3.9) gives the MLE of the position of the transmitter, $\widehat{\underline{\theta}}_{ML}$. This is very difficult to solve analytically because there is no closed form solution. In order to find the MLE, a numerical approach must be used. The MLE can be found by combining and reducing Equations (3.7) and (3.8). The first term of Equation (3.7) can be removed since it is a constant and will only affect the maximum value, not the location of the maximum value.

$$\widehat{\underline{\theta}}_{ML} = \arg\min_{\underline{\theta}} \left\|\underline{P} - \underline{m}(\underline{\phi}, \underline{\theta})\right\|^2 \tag{3.10}$$

with $\underline{\theta}$ being the possible transmitter location. Equation (3.10) is solved numerically in MATLAB using a search grid algorithm.

3.2.4 Location Estimation in Simulation. As mentioned previously, solving analytically for the location is difficult. To find the MLE of the position for the transmitter, a search grid is used in MATLAB. The search grid is defined to be 10 x 10 meters with 0.1 meter increments. The transmitter can be located at any location in the search grid. To find the location each index of the matrix in MATLAB is simulated as 0.1 meters to simulate the accuracy of the hardware set-up. At each index the simulated RSS and P_s are used to calculate cost, C. The values are stored in a matrix which is used to search for the minimum value which is $\widehat{\underline{\theta}}_{ML}$ as defined by Equation (3.10).

$$C = \left\|\underline{P} - \underline{m}(\underline{\phi}, \underline{\theta})\right\|^2 \tag{3.11}$$

Once the algorithm is completed and the matrix is full, a search for the minimum value is conducted and the location is put into a vector $\widehat{\underline{\theta}}_{ML}$.

3.2.5 Jammer in Simulation. The jammer can be placed anywhere in the search grid similar to how the transmitter can be placed anywhere in the search grid. The effects of the jammer in the cooperative network simulations remove sensors from the network within a certain distance from the jammer's location. The jammer can be either a directional or omni-directional antenna while the simulation is the cooperative network. This is done by choosing the area of the receiver network that will be affected by the jammer. Once the area is chosen, the sensors are removed from the simulation. In the non-cooperative network simulations, the jammer acts like another transmitter with a higher variable power that can be set independently from the transmitter. In the case for the non-cooperative network, the jammer is omni-directional.

3.2.6 Estimating for the Hardware Data Processing. The data that is collected from the Sun SPOT sensors are processed in MATLAB using the algorithm described in this section. For the simulation the path loss η and the reference received power P_0 are set in MATLAB. For the data collection from the Sun SPOT sensors, η and P_0 are unknown and must be estimated using the collected RSS data. Using one of the estimation algorithms from [16] and [19] this is accomplished.

The Sun SPOT network is a cooperative network, following the algorithm for the standard RSS, η and P_0 appear linearly in the RSS [19]. Unlike the position estimate $\underline{\theta}$, η and P_0 can be solved for analytically. Taking the gradient of $\mathcal{L}$ with respect to η and P_0 results in two equations that can be simplified into equation (3.12). From [16] and [19] the MLE for η and P_0 is

$$\begin{bmatrix} \widehat{P_0} \\ \widehat{\eta} \end{bmatrix} = \begin{bmatrix} 1 & -\left\langle \overline{d}_s(\widetilde{x}_0, \widetilde{y}_0) \right\rangle \\ \left\langle \overline{d}_s(\widetilde{x}_0, \widetilde{y}_0) \right\rangle & -\left\langle \overline{d}_s^2(\widetilde{x}_0, \widetilde{y}_0) \right\rangle \end{bmatrix}^{-1} \begin{bmatrix} \langle p_s \rangle \\ \langle p_s \overline{d}_s \rangle \end{bmatrix} \tag{3.12}$$

$$\overline{d}_s \triangleq 10 \log_{10} \left(\frac{d_s}{d_0} \right) \tag{3.13}$$

where $\overline{d}_s$ is defined from the second half of Equation (3.1) and $\langle\cdot\rangle$ denotes an average over s. By performing the inverse and multiplying out the terms the estimates for P_0 and η are

$$\widehat{P_0} = \frac{\left\langle \overline{d}_s^2(\widetilde{x}_0, \widetilde{y}_0) \right\rangle - \left\langle \overline{d}_s(\widetilde{x}_0, \widetilde{y}_0) \right\rangle \left\langle p_s \overline{d}_s(\widetilde{x}_0, \widetilde{y}_0) \right\rangle}{\left\langle \overline{d}_s^2(\widetilde{x}_0, \widetilde{y}_0) \right\rangle - \left\langle \overline{d}_s(\widetilde{x}_0, \widetilde{y}_0) \right\rangle^2} \tag{3.14}$$

$$\widehat{\eta} = \frac{\left\langle \overline{d}_s(\widetilde{x}_0, \widetilde{y}_0) \right\rangle \langle p_s \rangle - \left\langle p_s \overline{d}_s(\widetilde{x}_0, \widetilde{y}_0) \right\rangle}{\left\langle \overline{d}_s^2(\widetilde{x}_0, \widetilde{y}_0) \right\rangle - \left\langle \overline{d}_s(\widetilde{x}_0, \widetilde{y}_0) \right\rangle^2} \tag{3.15}$$

These two Equations (3.14) and (3.15) are used for the estimates for $\widehat{P_0}$ and $\widehat{\eta}$ from the RSS values collected during hardware testing. During each grid point in the search $\widetilde{x}_0$ and $\widetilde{y}_0$ are assumed to be constant and used to solve Equations (3.14) and (3.15) for $\widehat{P_0}$ and $\widehat{\eta}$. The ML is evaluated using the parameters just solved for from Equations (3.14) and (3.15). This process is repeated until all the grid points have been used. $\widetilde{x}_0$ and $\widetilde{y}_0$ are chosen from the grid that minimize Equation (3.10) and the corresponding $\widehat{P_0}$ and $\widehat{\eta}$ are retained.

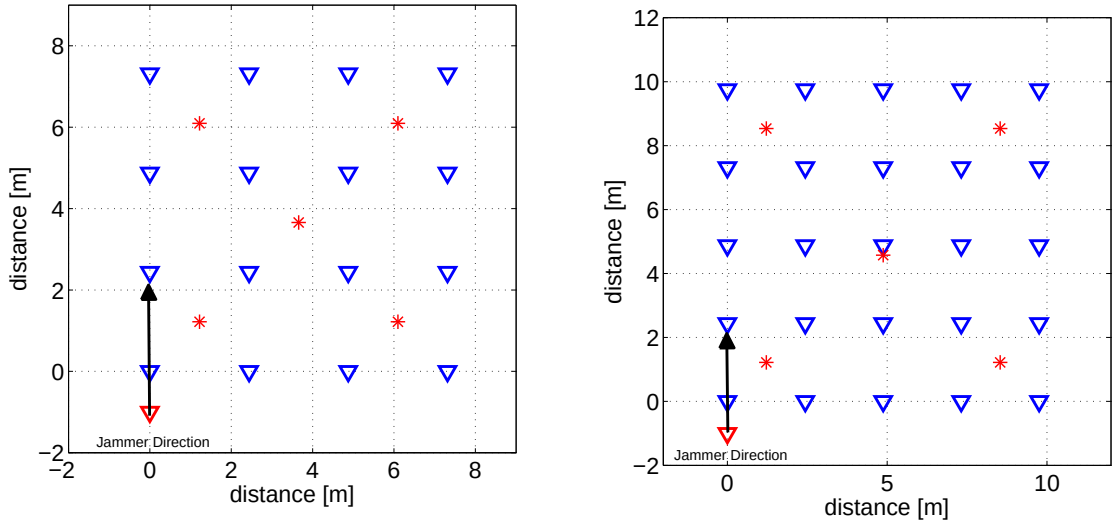
3.3 Hardware Set-up

As stated in the system overview, there are four main components to the system:

- Cooperative or non-cooperative sensor network
- Basestation used for collecting and processing data
- Transmitter
- Jammer

The next four sub-sections describe the layout of the sensor network and the hardware configuration for all parts of the system.

3.3.1 Sun SPOT Sensor Network. The Sun SPOT units are configured in a grid pattern allowing for the best possible coverage over a certain area. There are two grid patterns used in this research; a four by four grid and a five by five grid



(a) (b)

Figure 3.4: (a) The first set-up is a four by four grid of Sun SPOT sensors containing 16 receivers designated by the symbol ∇. The transmitter can be located at the five locations shown with the symbol ∗. The jammer is designated by the symbol ∇. (b) The second set-up is a five by five grid of Sun SPOT sensors containing 25 receivers designated by the symbol ∇. The transmitter can be located at the five locations shown with the symbol ∗. The jammer is designated by the symbol ∇.

each with approximately 2.44 m (8 ft.) spacing between each pair of receivers. In the real world the transmitter can be placed anywhere inside or outside the grid. For this research the transmitter will be kept inside the grid and to designated locations shown in Figure 3.4. The transmitter is moved from one location to the next and data are collected at each location. The Sun SPOT units are attached to plastic poles approximately 1 m off the ground as seen in Figure 3.5. The plastic poles allow the Sun SPOTs to easily be configured and allow the transmitter to be moved easily.

3.3.2 Basestation and Transmitter. All data from the sensor network is reported back to a Sun SPOT unit configured as a basestation, plugged into the USB

(a) (b)

Figure 3.5: (a) Sun SPOT sensor on the plastic pole used for data collection. (b) Sun SPOT sensors on the plastic poles set-up in a grid for data collection.

port of a laptop. This entire set-up is called the basestation. The data from the Sun SPOT receivers are collected with this basestation sensor and recorded on the laptop using NetBeans. NetBeans is an open-source software program that is used for developing desktop, mobile and web applications with Java and other programming languages. Data can be passed on to MATLAB for real time processing of the position solution or stored for later processing.

The transmitter is also a Sun SPOT unit configured as a transmitter. The software program in NetBeans dictates what Sun SPOT will be a transmitter and the rest of the Sun SPOTs will be receivers. This allows the Sun SPOTs to know what the MAC address of the transmitter is and ignore any other device in the 2.4 GHz range. This is the key aspect of the cooperative network. In order to see the effects of jamming in a cooperative network, the receivers will have to be blocked from reading the RSS of the transmitter. This is done by having the jammer transmit

Figure 3.6: RFX2400 Daughterboard [8].

at a higher power in the same frequency band as the transmitter in order to disrupt communications with the receiver.

3.3.3 USRP2 as a Jammer. As mentioned earlier, the USRP2 is a SDR. A SDR can be programmed to become almost any type of transmitter or receiver. The USRP2 used for this research has the RFX2400 Daughterboard installed in it. The RFX2400 has a frequency range from 2.3 to 2.9 GHz and a typical transmit power of 50 mW. The RFX2400 has a band-pass filter around the 2400 to 2483 MHz ISM band on the TXRX port The other port on the RFX2400 board, the RX2 port, is unfiltered allowing for coverage of the entire frequency range without attenuation [8]. The TXRX port is the only transmitter port on the RFX2400 board. TXRX port can also be set up to receive signals, while the RX2 port can only be set up to receive signals. Figure shows the RFX2400 daughterboard.

The USRP2 is used as a noise jammer for this research. The USRP2 is controlled with Simulink version 7.7 from MATLAB 2011a. Simulink has two blocks that work with the USRP2; the USRP2 Transmitter and USRP2 Receiver block. The USRP2 Transmitter block enables communication with a USRP2 board on the same Ethernet

Figure 3.7: Front view of a USRP2.

subnetwork. This block accepts a column vector input signal from Simulink and transmits signal and control data to a USRP2 board using User Datagram Protocol (UDP) packets. Although the USRP2 Transmitter block sends data to a USRP2 board, the block acts as a Simulink sink [28]. This allows the user to create numerous types of signals and waveforms and send them to the USRP2. For this research, Gaussian noise is added to a complex sine wave and sent to the USRP2. The center frequency, gain and interpolation can be set under the USRP2 Transmitter block properties. This allows for easy change in-between test scenarios.

The USRP2 Receiver block, similar to the USRP2 Transmitter block, also enables communication with a USRP2. This block receives signal and control data from a USRP2 board using UDP packets. Although the USRP2 Receiver block receives data from a USRP2 board, the block acts as a Simulink source that outputs a column vector signal of fixed length [28]. The center frequency, gain and decimation can be set under the USRP2 Receiver block properties.

For this research to control the power of the jammer, the amplitude of the complex sine wave is adjusted. To adjust the amplitude of the sine wave, the number required is entered in the amplitude box in the sine wave block parameters. The amount of Gaussian noise can also be adjusted by changing the mean value and variance values in the block parameter for the Gaussian Noise Generator. Figure 3.8 shows a block diagram of how the USRP2 is configured and all the components

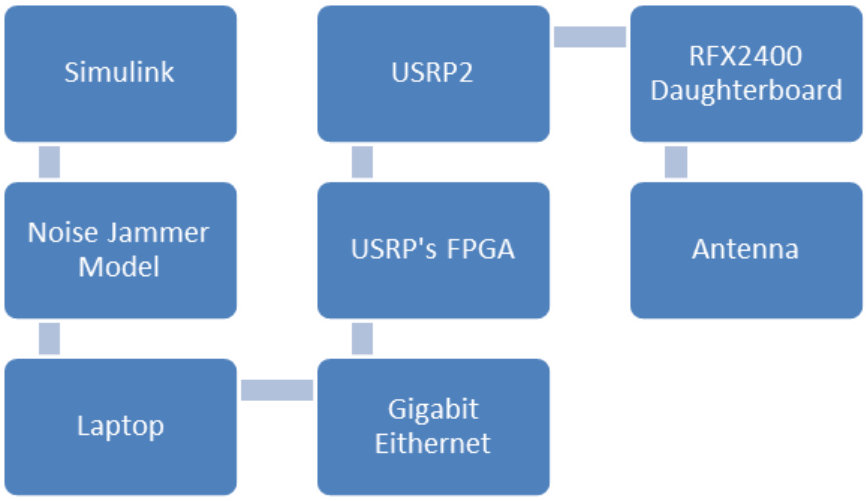


Figure 3.8: Block diagram showing the hardware configuration for the USRP2 jammer.

required to operate as a jammer. Figure 3.9 shows the Simulink block diagram of the components and how they interact to create the noise jammer.

There are three different types of antennas used for this research.

- 3 dBi gain omni-directional antenna
- Log Periodic Printed Circuit Board Antenna 900 - 2600 MHz by Kent Electronics
- Hawking HiGain 90° Directional Corner Antenna with 15dBi of gain

These antennas are used to test the ability of the jammer with various amounts of directionality and gain. In each scenario, the antenna is set up along the edge of the sensor network. The directional antennas are set up in the same configuration to test the effects of the antennas. Figure 3.10 shows the antennas, Figure 3.11 shows the gain vs. frequency for the log periodic antenna, Figure 3.12 shows the antenna pattern of the Hawking HiGain Directional Corner Antenna and Figure 3.13 shows the different configurations for the antenna layout of the test.

The directional antenna is used to focus the energy from the jammer and knock out only certain portions of the sensor network. This gives the user more control over the area of the sensor network that will be jammed. The directional antenna is

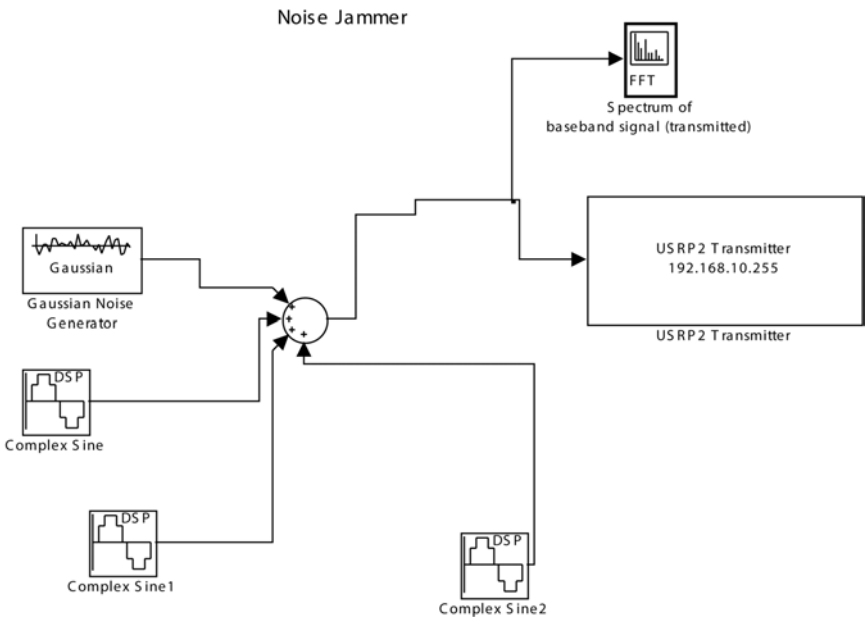
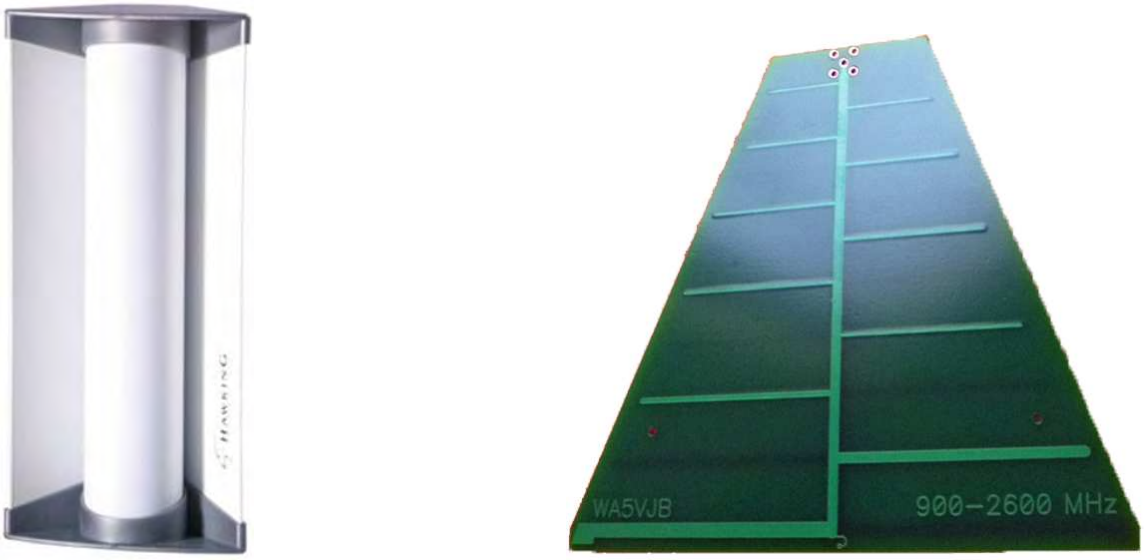


Figure 3.9: Simulink diagram showing the configuration for the USRP2 noise jammer.



(a) (b)

Figure 3.10: (a) Hawking HiGain Directional Corner Antenna, 2.4 - 2.4835 GHz. (b) Kent Electronics, WA5VJB, 900 - 2600 MHz log periodic antenna.

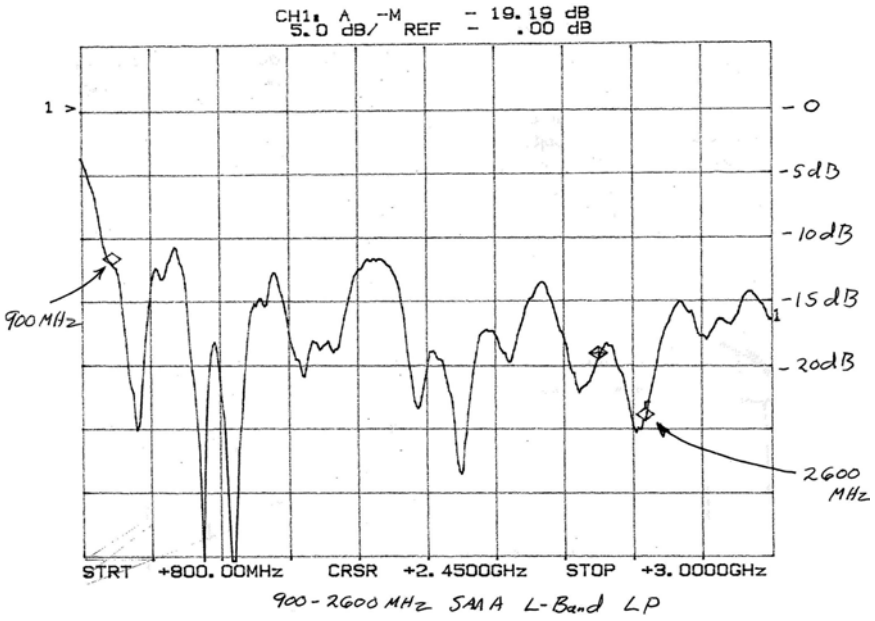


Figure 3.11: The gain of the log periodic antenna vs. frequency [14].

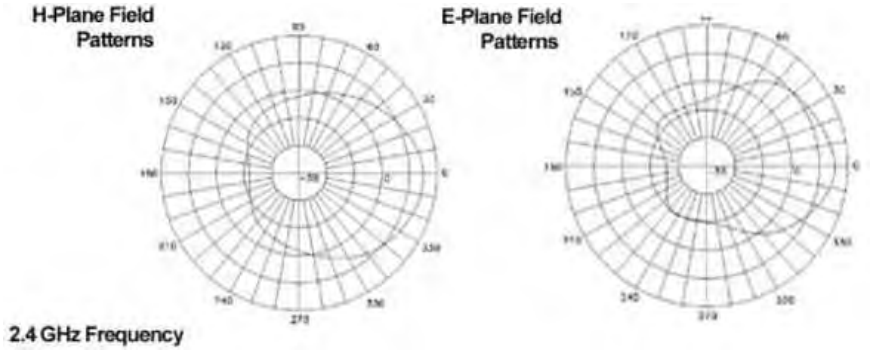
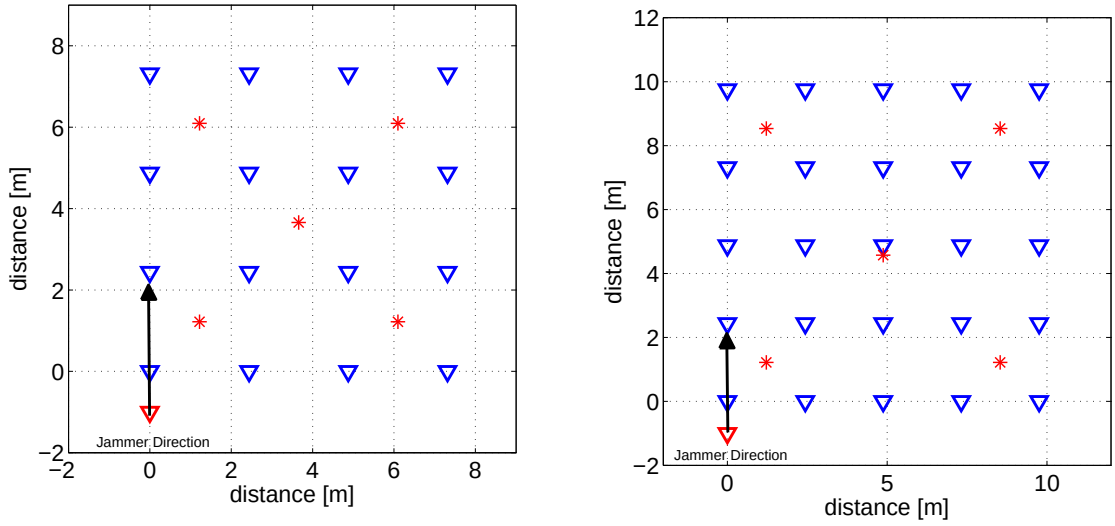


Figure 3.12: The gain pattern of the Hawking HiGain Directional Corner Antenna [12].



(a) (b)

Figure 3.13: (a) Jammer in a four by four network of Sun SPOT sensors (b) Jammer in a five by five network of Sun SPOT sensors.

also designed specifically for the 2.4GHz ISM band which should allow the jammer to operate more efficiently than the other antennas used in this research. Using a Wi-Spy spectrum analyzer, a view of the RF environment before jamming is shown in Figure 3.14 and a view of the RF environment with the jammer on using the HiGain antenna is shown in Figure 3.15. To get a sense of what the jammer is jamming, Figure 3.16 shows what the RF spectrum of the Sun SPOTs look like.

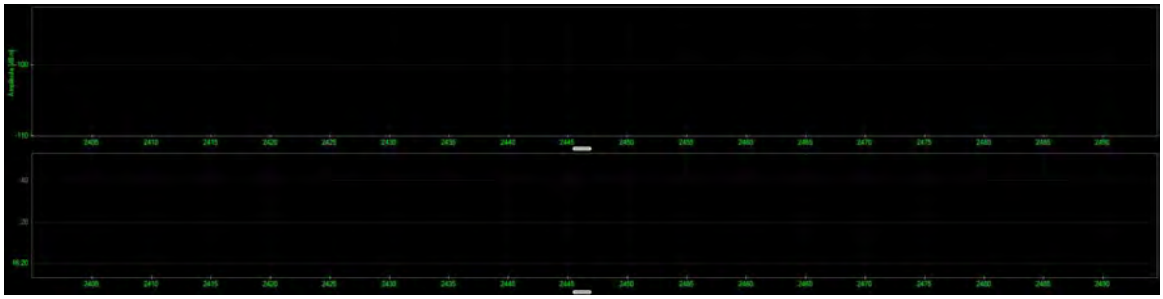


Figure 3.14: The RF environment outside with nothing on.

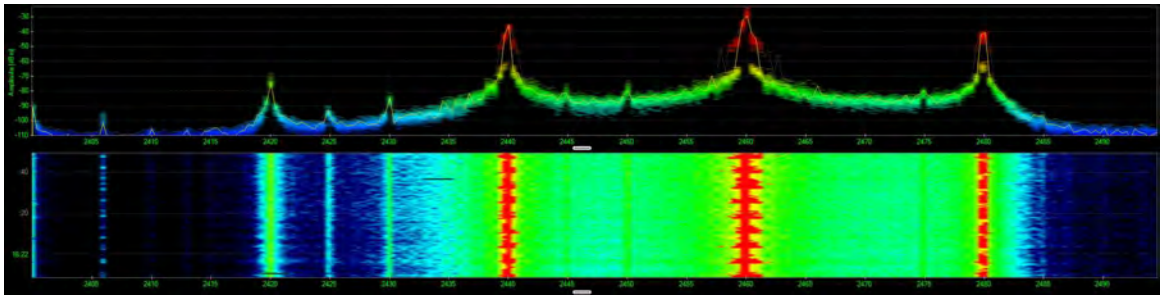


Figure 3.15: The RF environment outside with the jammer using the Hawking HiGain 90° Directional Corner Antenna.

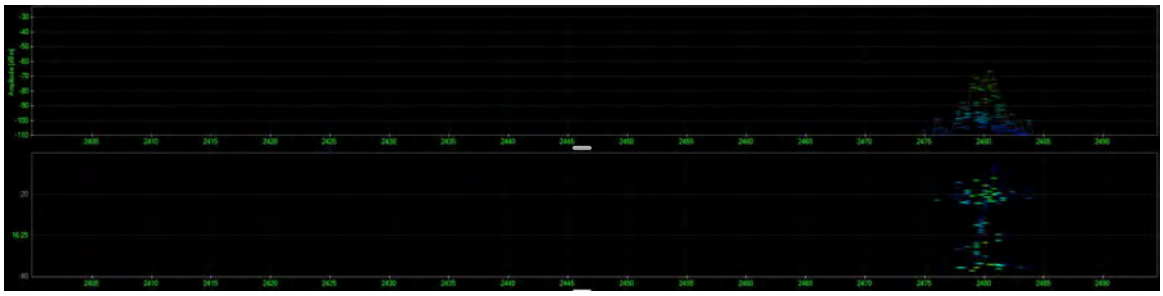


Figure 3.16: The RF environment outside with 16 Sun SPOT sensors on. The SUN SPOTs spectrum is centered around 2.48 GHz.

IV. Results and Analysis

This chapter details results from the simulations and hardware testing described in Chapter 3. Section 4.1 describes the simulation and hardware parameters used for this research. Section 4.2 illustrates the results for geolocation when used in a non-jamming environment. Section 4.3 discusses the simulation results for jamming the cooperative and non-cooperative sensor networks. Section 4.4 discusses the hardware results for jamming the cooperative and non-cooperative sensor networks. Section 4.5 discusses the results of the comparison between non-jamming, jamming, simulation and hardware. Section 4.6 discusses the results of jamming the basestation used to collect the data from the Sun SPOTs.

4.1 Simulation and Hardware Parameters

Table 4.1 shows the parameters used for the various test and simulations. Figure 4.1 gives an overview of the five possible transmitter locations that are used in this research. These locations will be referred to when discussing transmitter locations in this chapter.

4.2 Non-Jamming Geolocation Results

This section covers the performance of the geolocation algorithm in simulation and hardware collection in non-jamming environments. The purpose of this section is to give a baseline to compare the results of the jamming simulations and test against. The non-jamming tests give an idea of how the Sun SPOT sensors behave in a normal outside environment. First the results of the simulations are shown in Figures 4.2 and 4.3.

The results from hardware testing with the Sun SPOT sensors are displayed next. For hardware testing, data from the Sun SPOT sensors were collected and stored on the basestation laptop. For each transmitter location 400 to 1000 data points were used to average the RSS data collected. Figure 4.4 shows transmitter location one in the four by four network of Sun SPOT receivers. As discussed in Chapter III, η and

Table 4.1: Table of parameters used in this research

Figure	**# of Sensors (S)**	**# of Independent trials (K)**	P_0 [dBm]	P_{0j} [dBm]
4.1	16	N/A	N/A	N/A
4.2	16	10	-7	N/A
4.3	25	10	-7	N/A
4.4	16	1	-5.3	N/A
4.5	16	1	-16.3 to 5	N/A
4.6	16	10	-7	3
4.7	16	10	-7	3
4.8	16	10	-7	3
4.9	16	10	-7	3
4.10	16	10	-7	-4
4.11	16	10	-7	-4
4.12	25	1	-14.8	5
4.13	25	1	-14.8 to 6.2	5
4.14	16	1	-6.2	5
4.15	16	3	-6.2 to 5.4	5
4.16	16	1	-16.5	5
4.17	16	1	-16.5 to 2.8	5
4.18	16	2	-24.4 to 4.9	5
4.19	16	3	-6.2 to 5.4	5
4.20	16	2	-24.4 to 4.9	5
4.21	25	1	-14.8 to 6.2	5

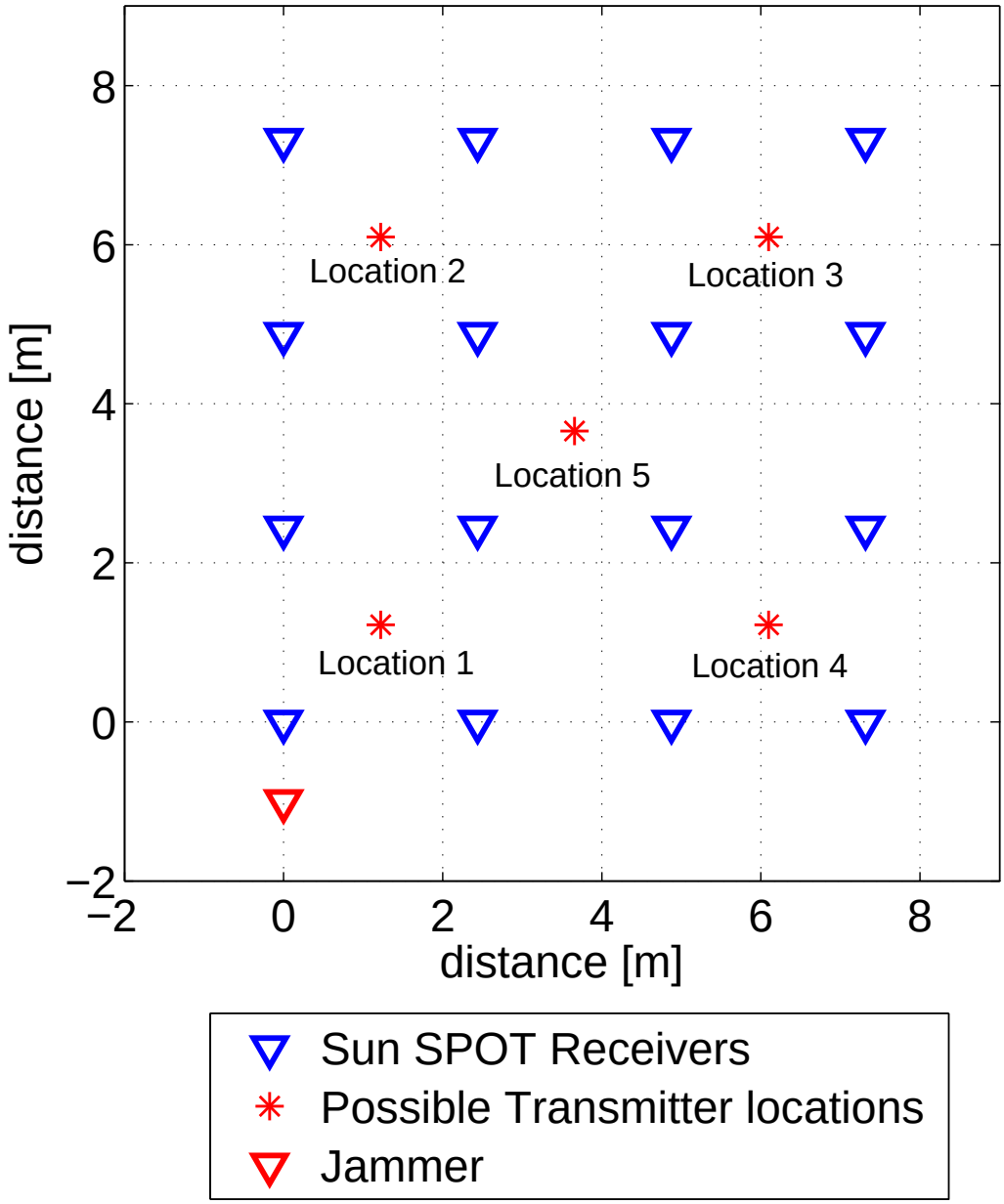


Figure 4.1: Showing the five possible transmitter locations in the receiver network used for simulation and hardware testing.

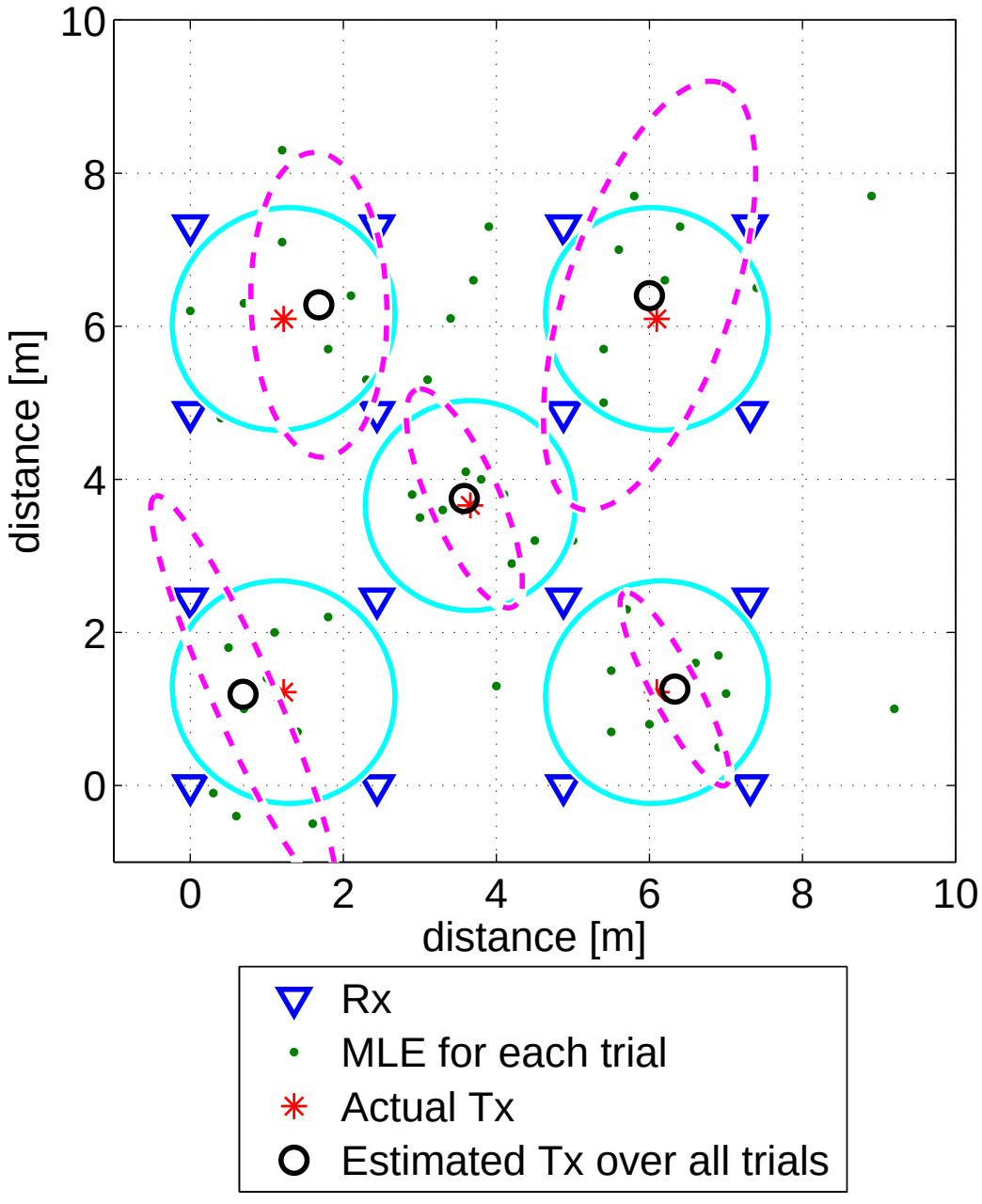


Figure 4.2: Non-jamming results simulated in a four by four grid of sensors. Showing five possible transmitter locations and five different simulations with the CRLB in cyan solid line and the Covariance in magenta dashed line of the estimate for the 10 trials simulated, with $\eta = 2$ and $\sigma_{noise} = 6$.

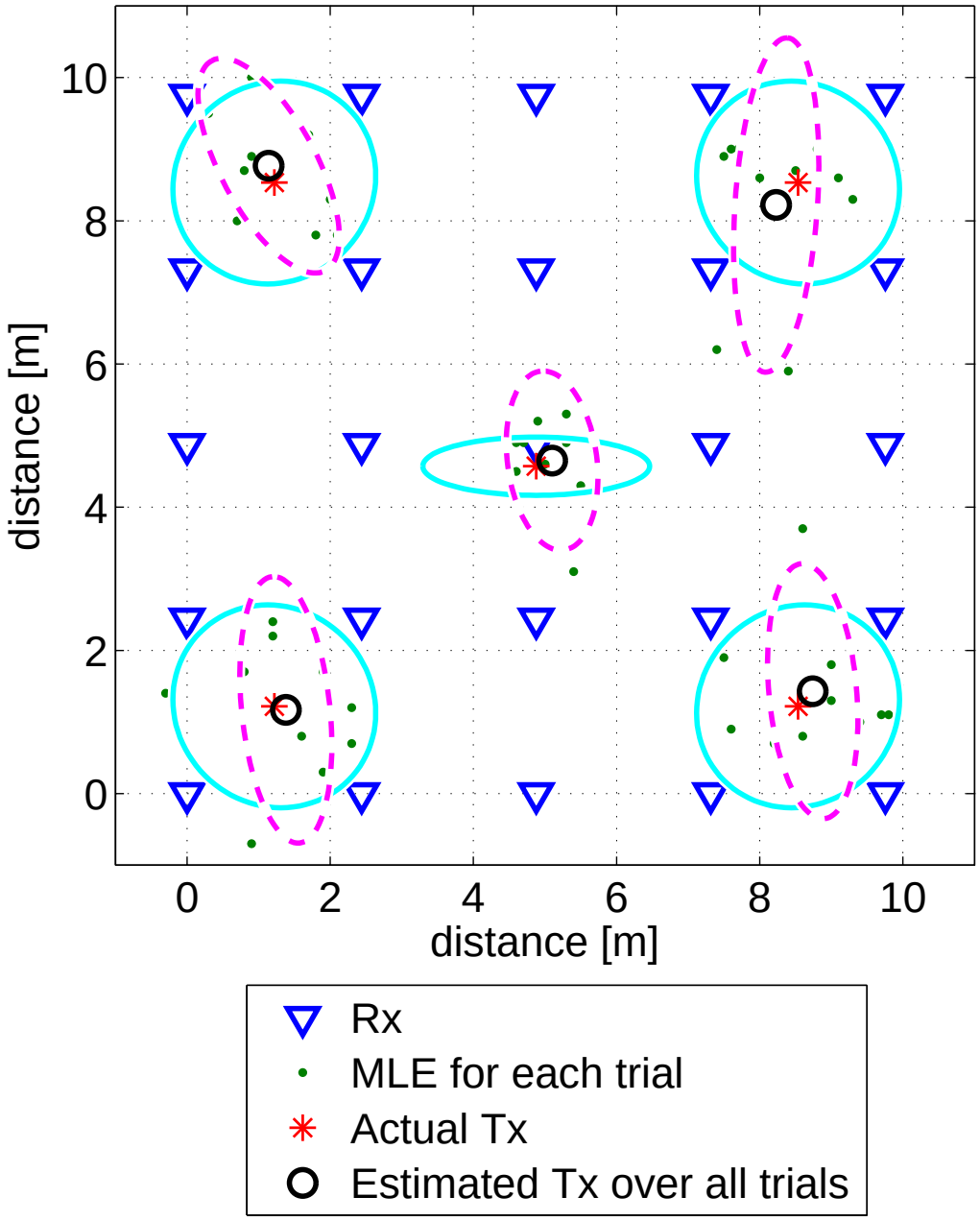


Figure 4.3: Non-jamming results simulated in a five by five grid of sensors. Showing five possible transmitter locations and five different simulations with the CRLB in cyan solid line and the Covariance in magenta dashed line of the estimate for the 10 trials simulated, with $\eta = 2$ and $\sigma_{noise} = 6$.

P_0 are estimated from the collected RSS values. To get statically accurate results, the non-jamming scenario was conducted K multiple times and averaged over each independent trial. The contours in Figure 4.4 are of C from Equation (3.11). The contours are shown to graphically represent the values calculated in the search grid to see the minimum value representing the estimated location of the transmitter. Figure 4.5 shows the individual trials and estimated location over the total number of trials for each of the five transmitter locations. The figures show that the hardware results are very similar to the simulation results. This validates the simulation and shows that the geolocation algorithm is working properly. This is important to know before the jamming results can be compared with the non-jamming results.

4.3 Jamming Sensor Networks in Simulation

This section will cover the performance of the geolocation algorithm in simulation against jamming environments. The purpose of this section is to give simulation data to compare with the hardware jamming test. As described earlier there are two types of sensor networks that were simulated; a cooperative sensor network and a non-cooperative sensor network. The affects of jamming each type of sensor network are slightly different. The data in this section shows the results of jamming on both types of networks.

The cooperative network is shown is Figure 4.6 and shows a simulated directional jammer. The jammer is pointed up the row of sensors on the left of the sensor network to simulate the effects of the directional hardware jammer. Figure 4.7 shows all five transmitter locations each with 10 trials. As the figure shows, the two locations that were in the path of the jammer have the worst estimates for the transmitter's location. In a cooperative network when the sensors are jammed, they do not report back to the basestation. The results of this simulation indicate that when the sensors around the transmitter are jammed, the estimation performance is reduced.

This can also be seen when an omni-directional antenna is simulated in MATLAB. The results shown in Figures 4.8 and 4.9 are similar to the results from the

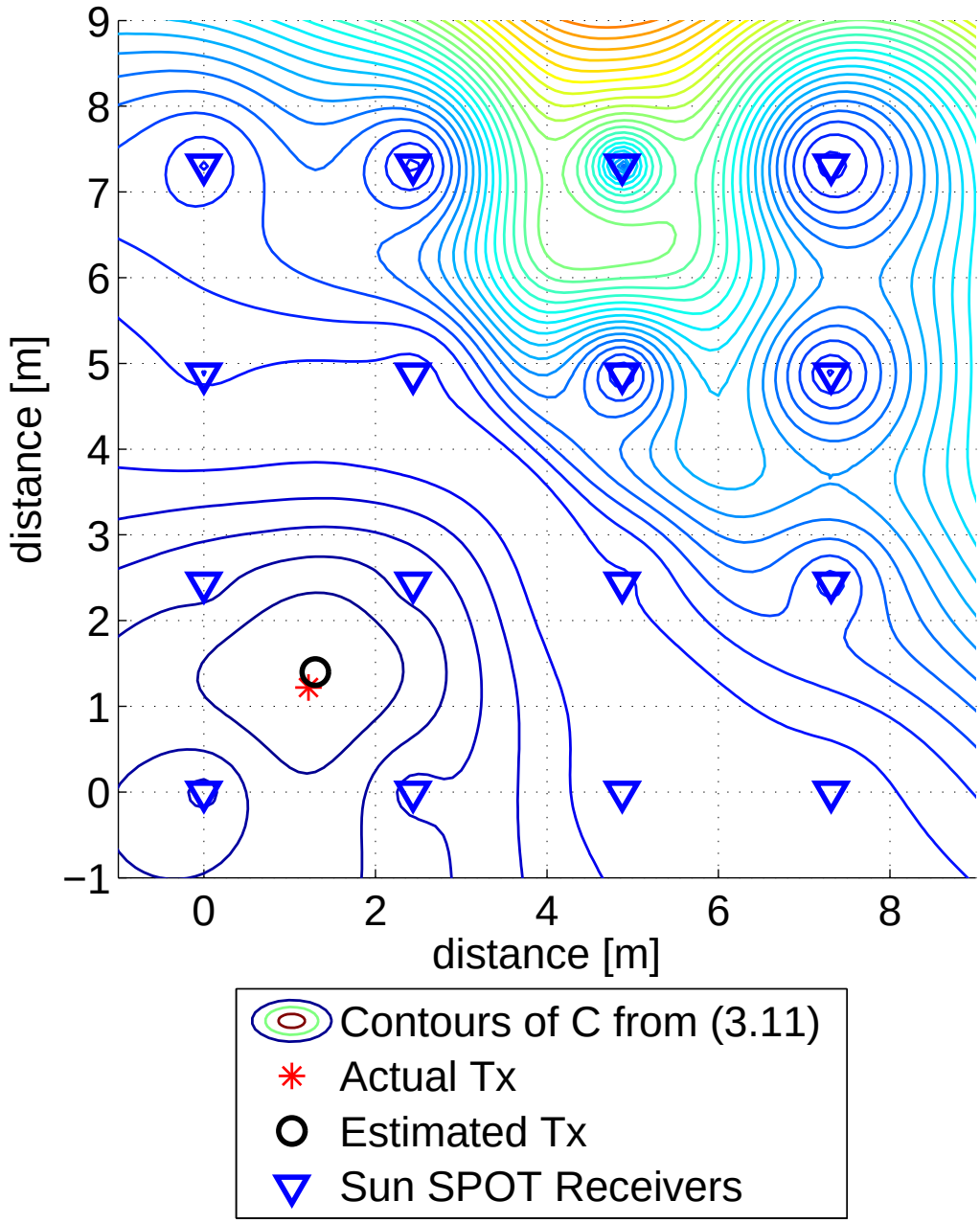


Figure 4.4: Non-jamming results from hardware testing Sun SPOTs in a four by four grid of sensors. Only one trial at one transmitter location is shown.

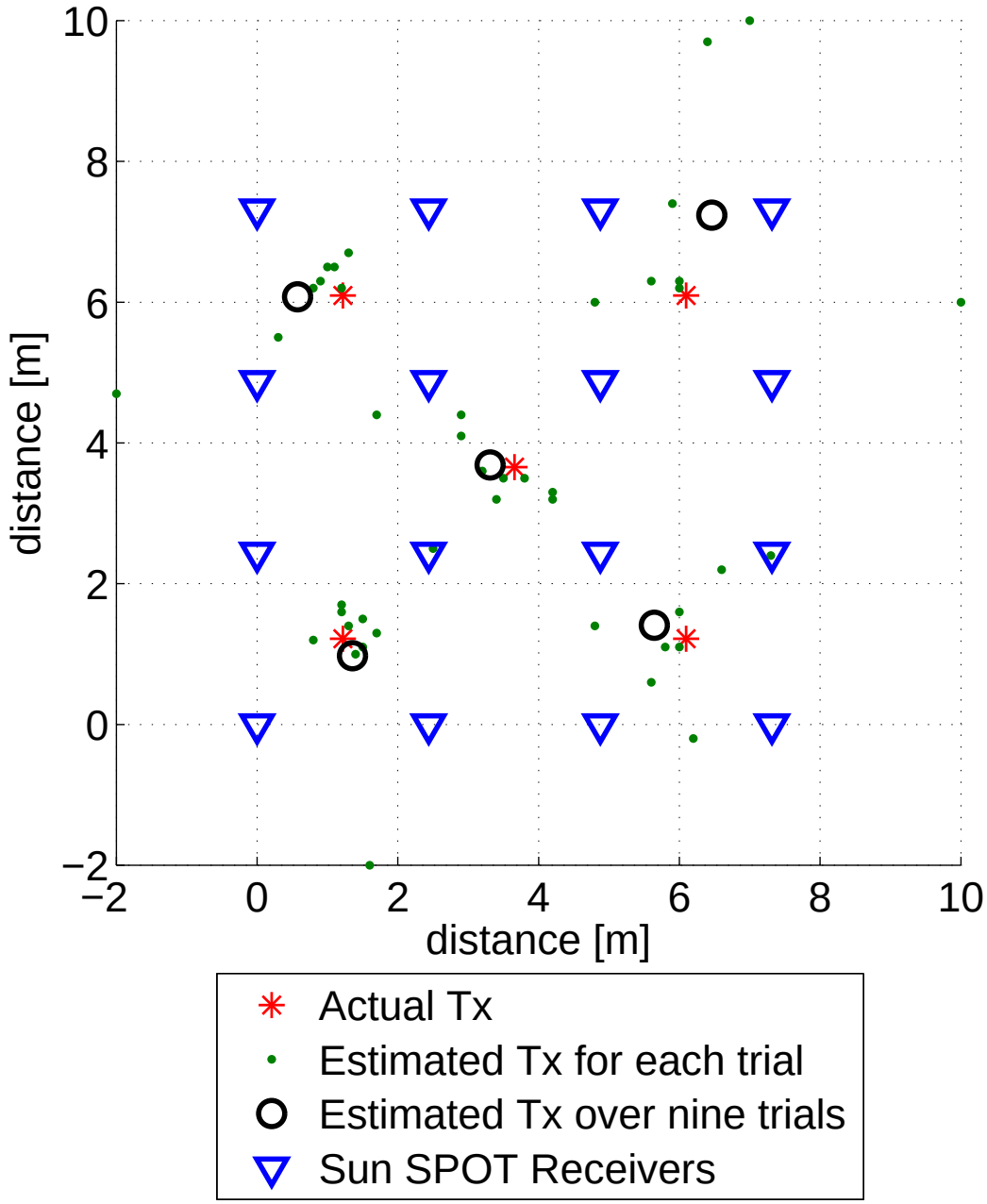


Figure 4.5: Non-jamming results from hardware testing Sun SPOTs in a four by four grid of sensors. The average estimated position over nine trials at each of the transmitters locations are shown.

directional antenna. The transmitter's location estimate in the area where the sensors are jammed is not as accurate as the transmitters that are surrounded by sensors. This data shows that in a cooperative sensor network the jamming effect is localized to the area where the sensors are jammed. More data on this is shown in Section 4.4.

Unlike the cooperative sensor network, in the non-cooperative sensor network, the receivers do not know the MAC address or modulation of the transmitter. The jamming results are discussed next in this section. Unlike the cooperative network, the jamming effects are not as localized in a non-cooperative network. Figure 4.10 demonstrates the effects of jamming a non-cooperative sensor network on one transmitter location. The jammer in this simulation and all the non-cooperative network simulations is an omni-directional jammer. Figure 4.11 shows the results for the five different transmitter locations. For each of the five transmitter locations, the jammer affected the receivers differently. For this reason, the figure does not show which receivers had $> 50\%$ power from the jammer. For each transmitter location, different receivers were affected. As the results show, all five transmitter location estimates were affected by the jammer. Since the jammer has approximately three dB more power than the transmitter, the jamming results moved the estimation closer to the jammers location. Higher power levels for the jammer were simulated, but the results of the estimated position for the transmitter at the various locations were all near the jammer. This is due to the fact that the receivers thought the jammer was the transmitter since most of the power was coming from the jammer.

4.4 Jamming Sun SPOT Sensor with Hardware

This section will cover the performance of the geolocation algorithm in a jamming environment using Sun SPOT sensors and the USRP2 as a jammer. There are three different antennas used for the hardware testing as discussed in Chapter III. The first antenna used is a 3 dB gain omni-directional antenna. This antenna was used to jam a five by five grid of Sun SPOTs. Figure 4.12 shows the effects the

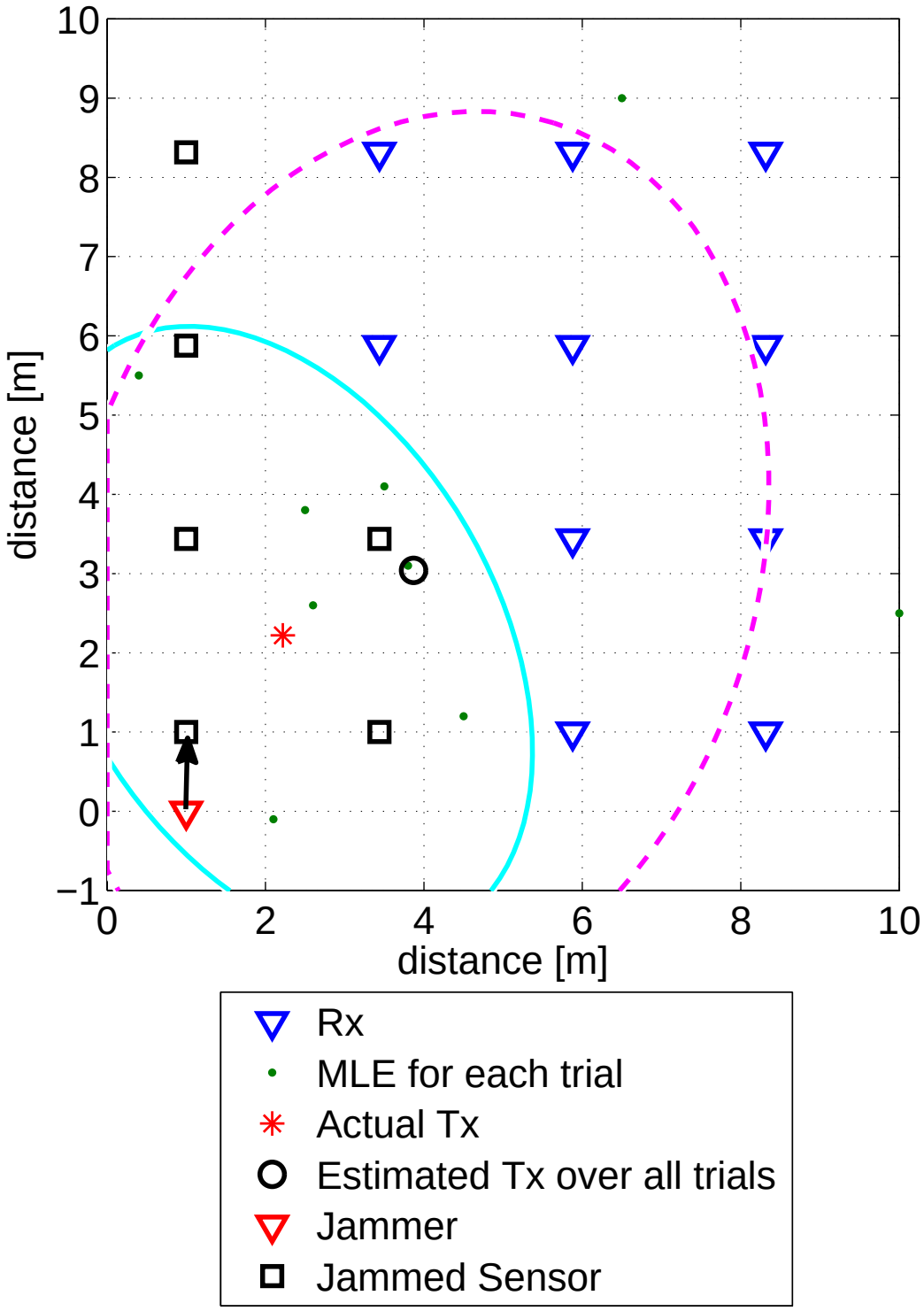


Figure 4.6: Jamming results from MATLAB simulation of a directional antenna in a four by four grid of cooperative network sensors. The average estimated position over 10 trials at transmitter location one is shown with the CRLB in cyan solid line and the Covariance in magenta dashed line, with $\eta = 2$ and $\sigma_{noise} = 6$.

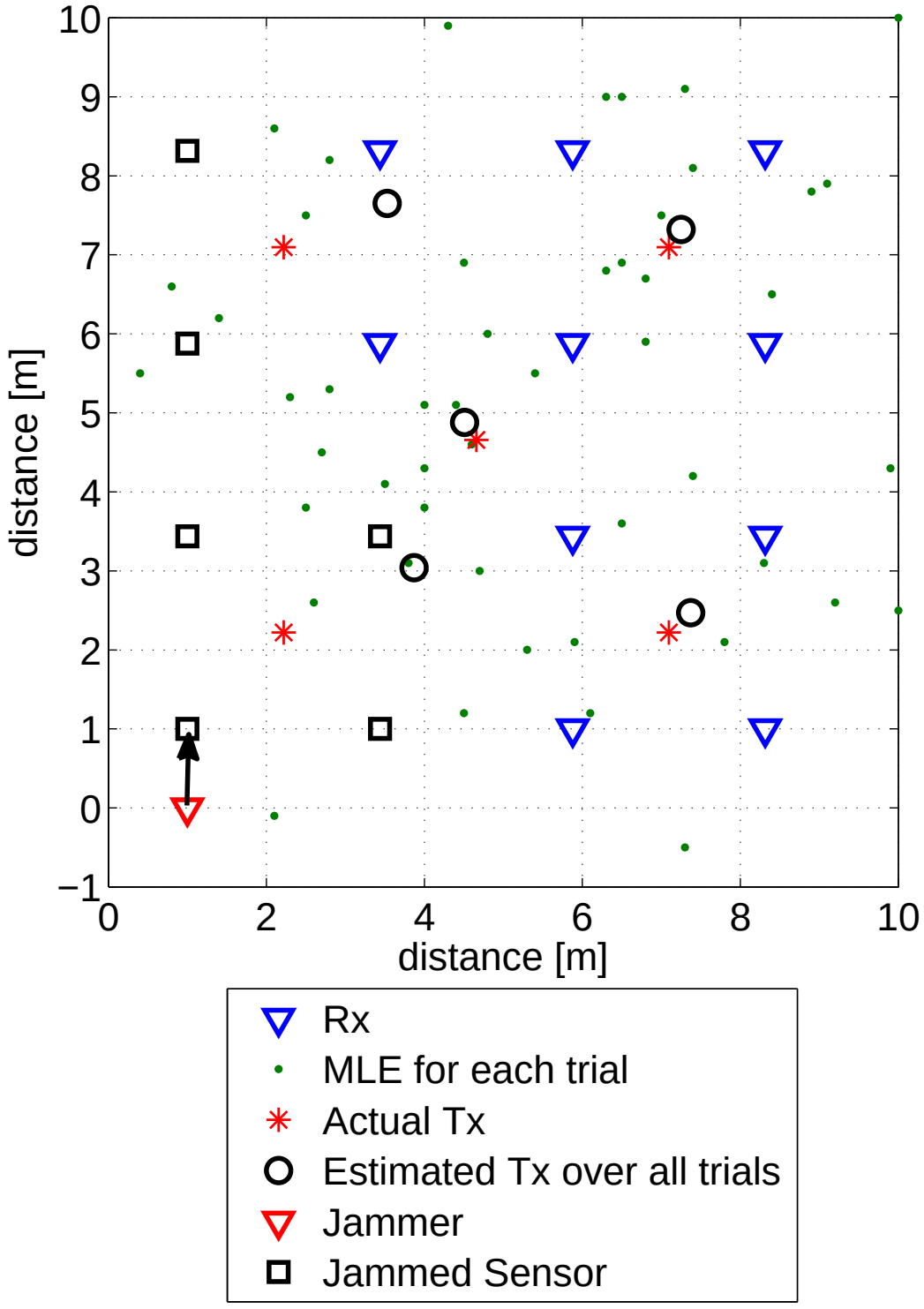


Figure 4.7: Jamming results from MATLAB simulation of a directional antenna in a four by four grid of cooperative network sensors. The average estimated position over 10 trials at each of the transmitters locations are shown, with $\eta = 2$ and $\sigma_{noise} = 6$.

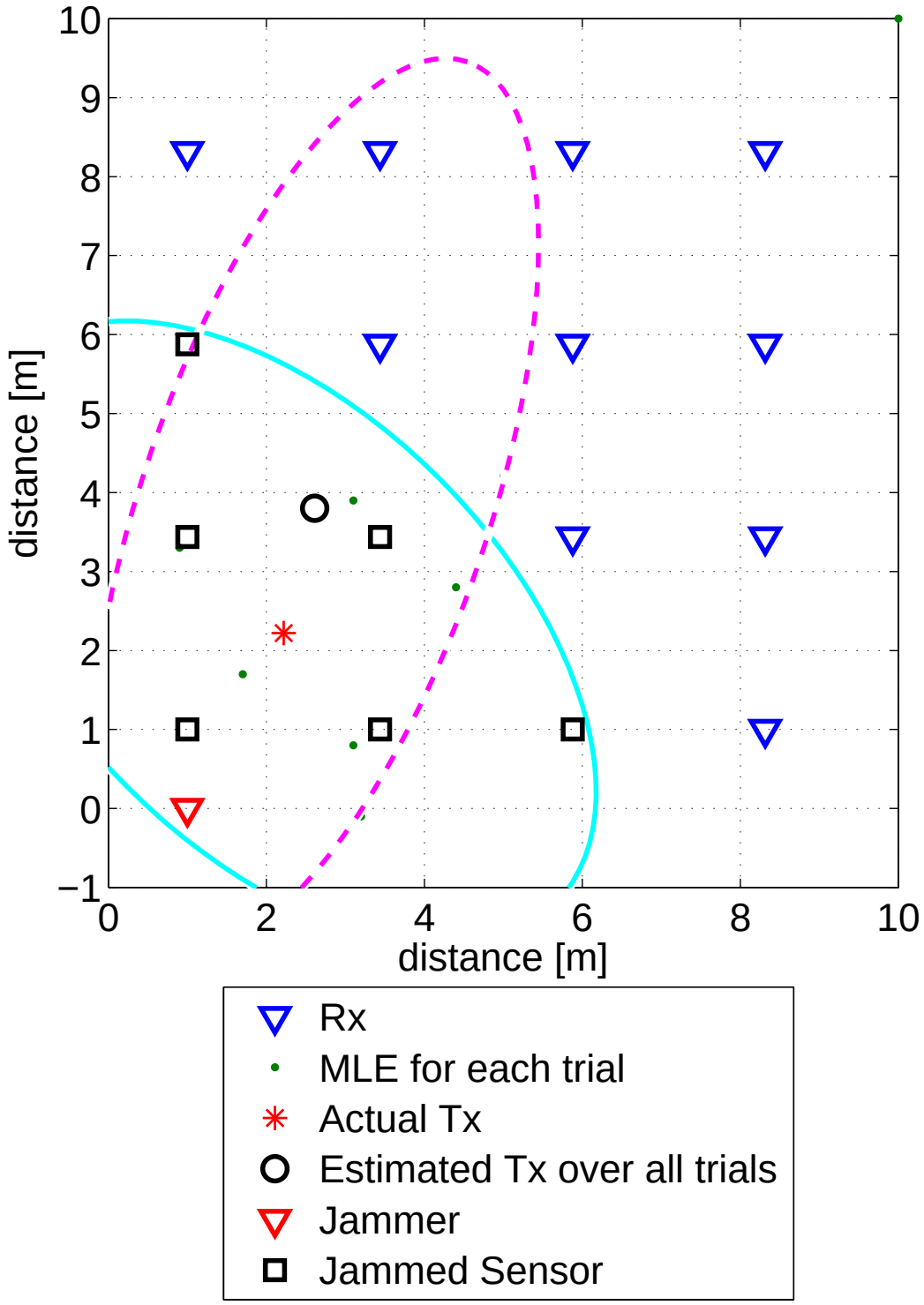


Figure 4.8: Jamming results from MATLAB simulation of an omni-directional antenna in a four by four grid of cooperative network sensors. The average estimated position over 10 trials at transmitter location one is shown with the CRLB in cyan solid line and the Covariance in magenta dashed line, with $\eta = 2$ and $\sigma_{noise} = 6$.

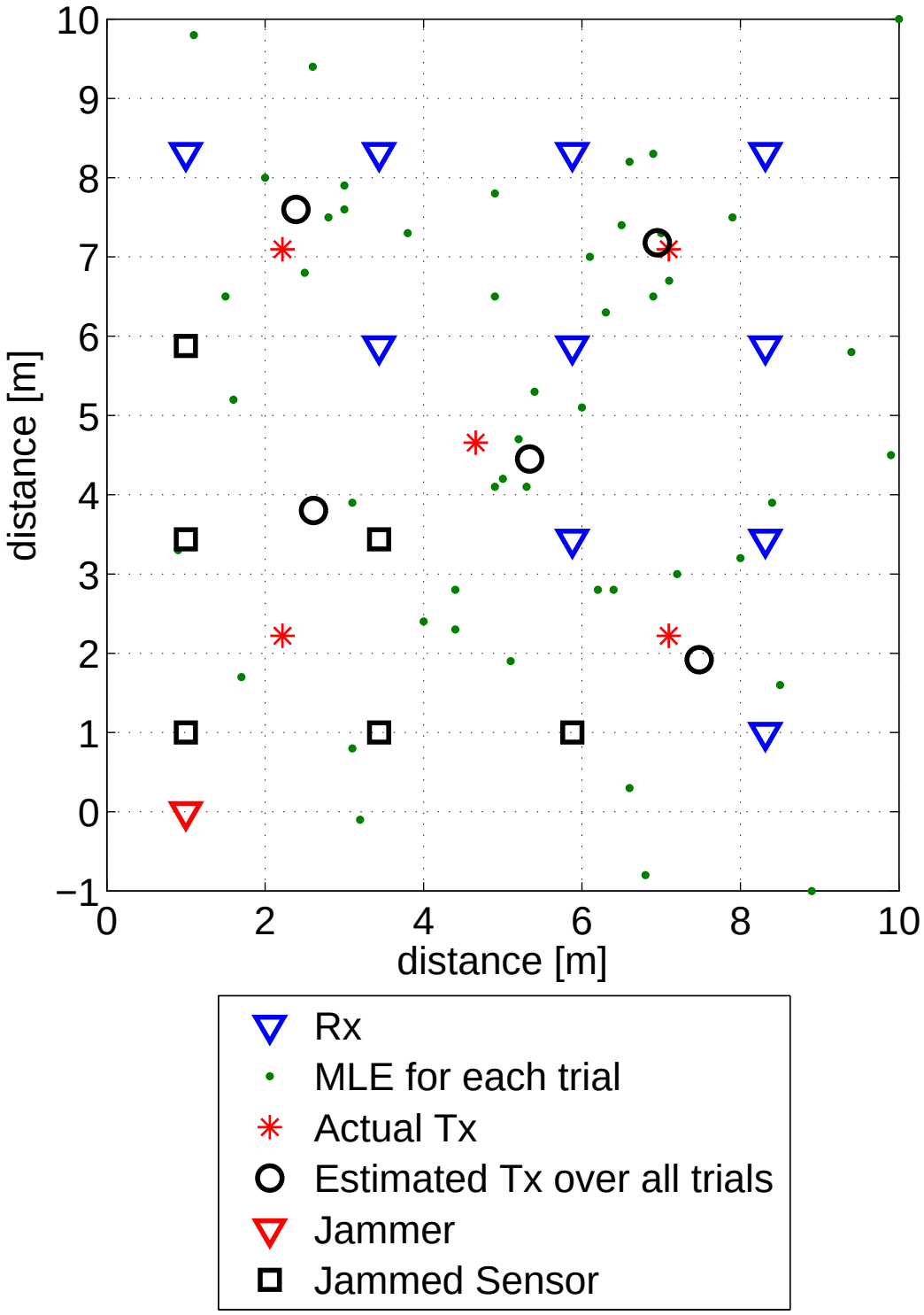


Figure 4.9: Jamming results from MATLAB simulation of an omni-directional antenna in a four by four grid of cooperative network sensors. The average estimated position over 10 trials at each of the transmitters locations are shown, with $\eta = 2$ and $\sigma_{noise} = 6$.

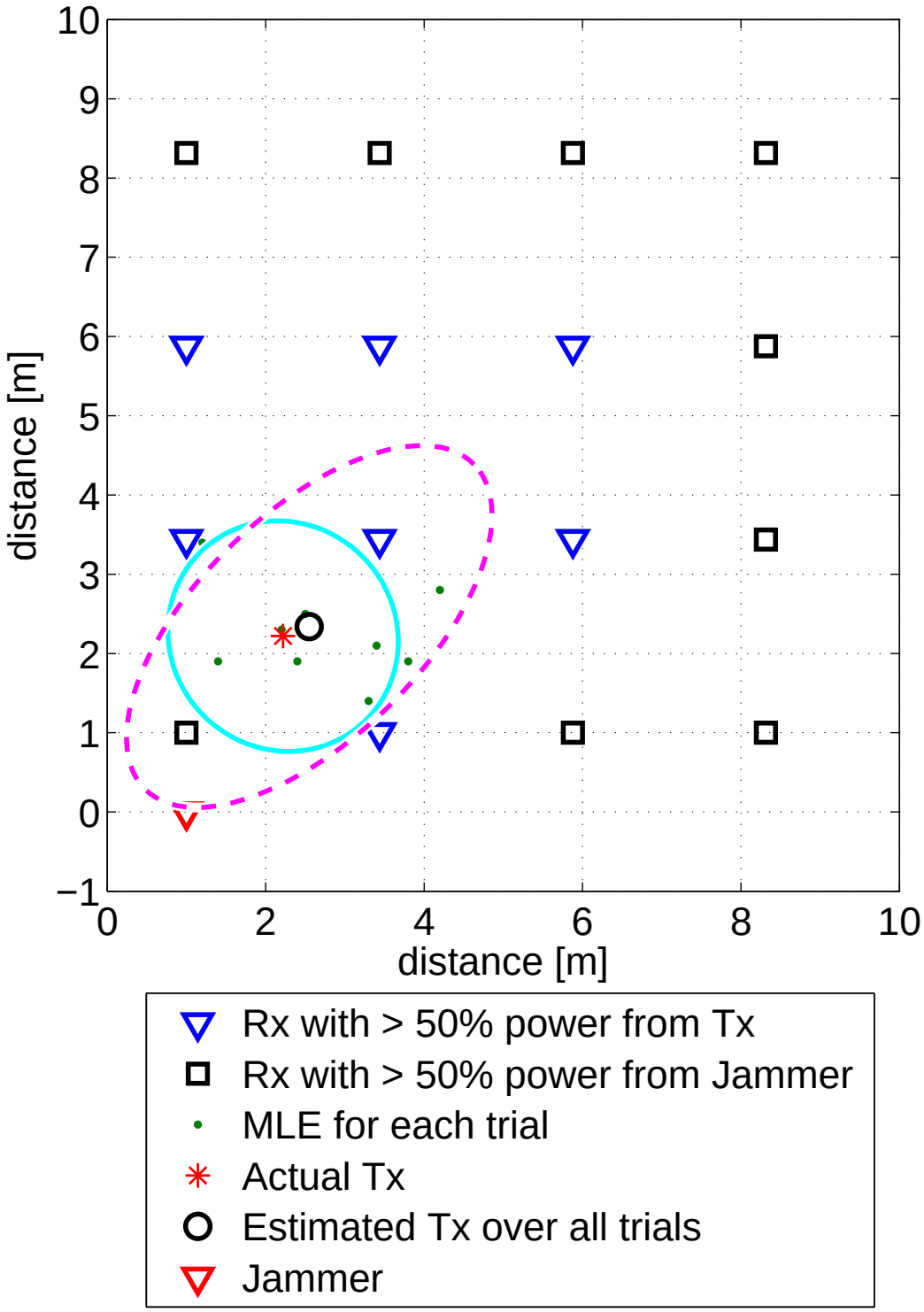


Figure 4.10: Jamming results from MATLAB simulation of an omni-directional antenna in a four by four grid of non-cooperative network sensors. The average estimated position over 10 trials at transmitter location one is shown with the CRLB in cyan solid line and the Covariance in magenta dashed line, with $\eta = 2$ and $\sigma_{noise} = 6$.

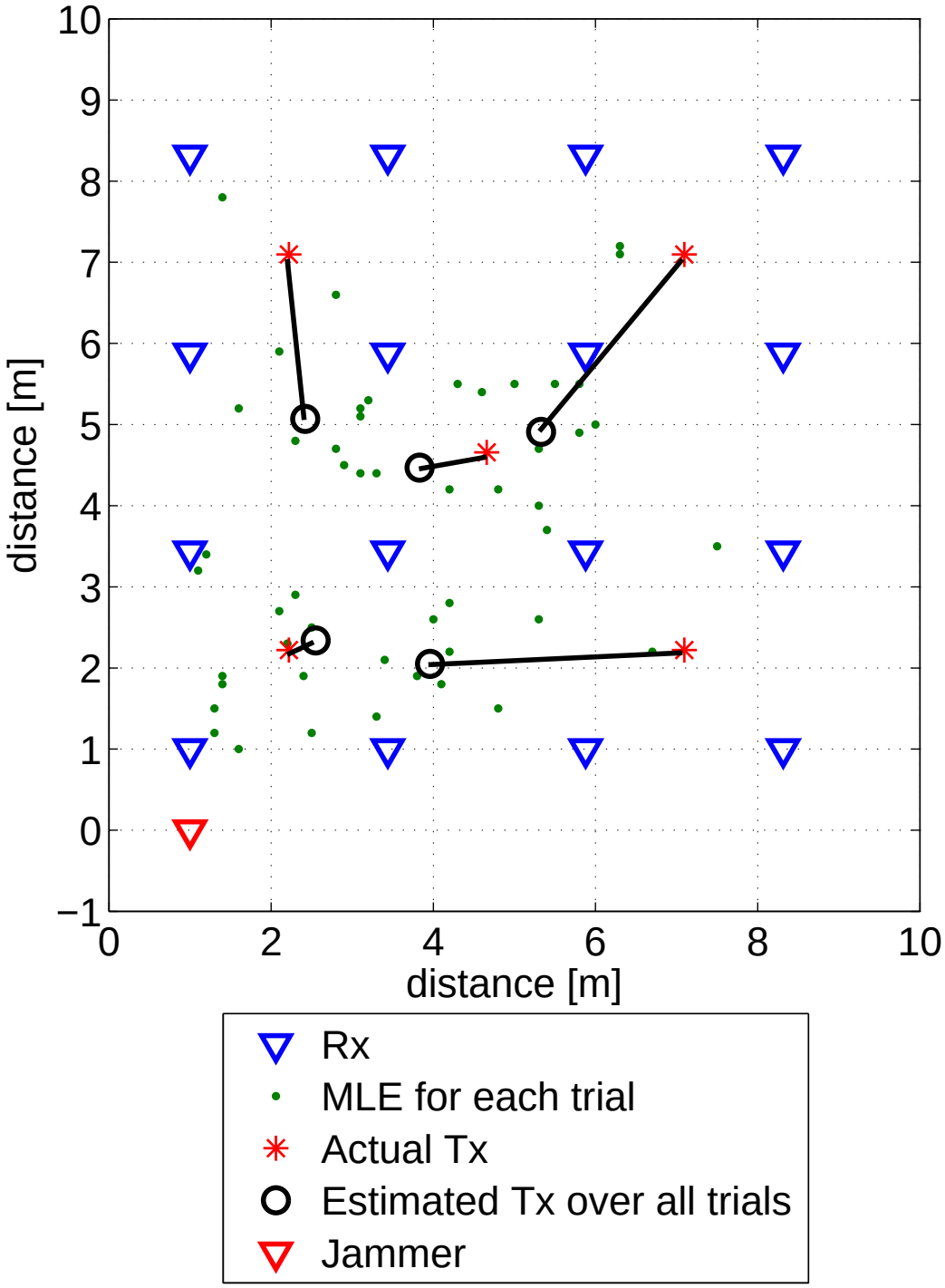


Figure 4.11: Jamming results from MATLAB simulation of an omni-directional antenna in a four by four grid of non-cooperative network sensors. The average estimated position over 10 trials at each of the transmitters locations are shown, with $\eta = 2$ and $\sigma_{noise} = 6$.

omni-directional jammer had on the Sun SPOT network for the transmitter located at location 1 near the jammer. Figure 4.13 shows the effects the omni-directional jammer had on the Sun SPOT network for all five transmitter locations. The estimated position near the transmitter at location 1 is actually the estimated position for the transmitter at location 4. Some of the Sun SPOTS were not reporting which is why there are some shown as jammed even though they are not near the jammer. The effects of jamming the Sun SPOT sensors are very similar to the simulations done with MATLAB. Most of the error is where the Sun SPOTS are jammed around a transmitter. The one anomaly is the bottom right estimation is not accurate even though the Sun SPOTs were not jammed around the transmitter.

Another antenna tested is the Kent Electronics, WA5VJB, 900 - 2600 MHz log periodic antenna. This antenna was used to direct the energy of the jammer like a directional antenna. The antenna is not designed specifically for the 2.4 GHz band and did not have a high gain pattern. The results in Figure 4.14 show that the Sun SPOT receivers near the jammer were jammed. The Sun SPOT receivers on the top row were not reporting during the time of jamming the transmitter at this location and were not jammed by the jammer. These results are from one test and are not averaged over a number of trials. In Figure 4.15, the results are averaged over three jamming trials conducted with different Sun SPOT configurations on three different days. The results for the transmitter at location 1 look like they are accurate, but they are averaged from an estimated location below and two estimated locations above the transmitter. The three independent trials can also be seen in Figure 4.15. No jammed Sun SPOT receivers are shown in the figure since each independent trial had a different amount of Sun SPOT receivers jammed. Three trials are not enough to get a good average for the jammed location estimation.

The third antenna used for jamming the Sun SPOT Receivers is the Hawking HiGain Directional Corner Antenna with 15 dB of gain and a 90° beam width. This antenna had a larger effect than the other antennas. The same amount of power from the USRP2 went into the antenna. Figure 4.16 shows the results for the jamming

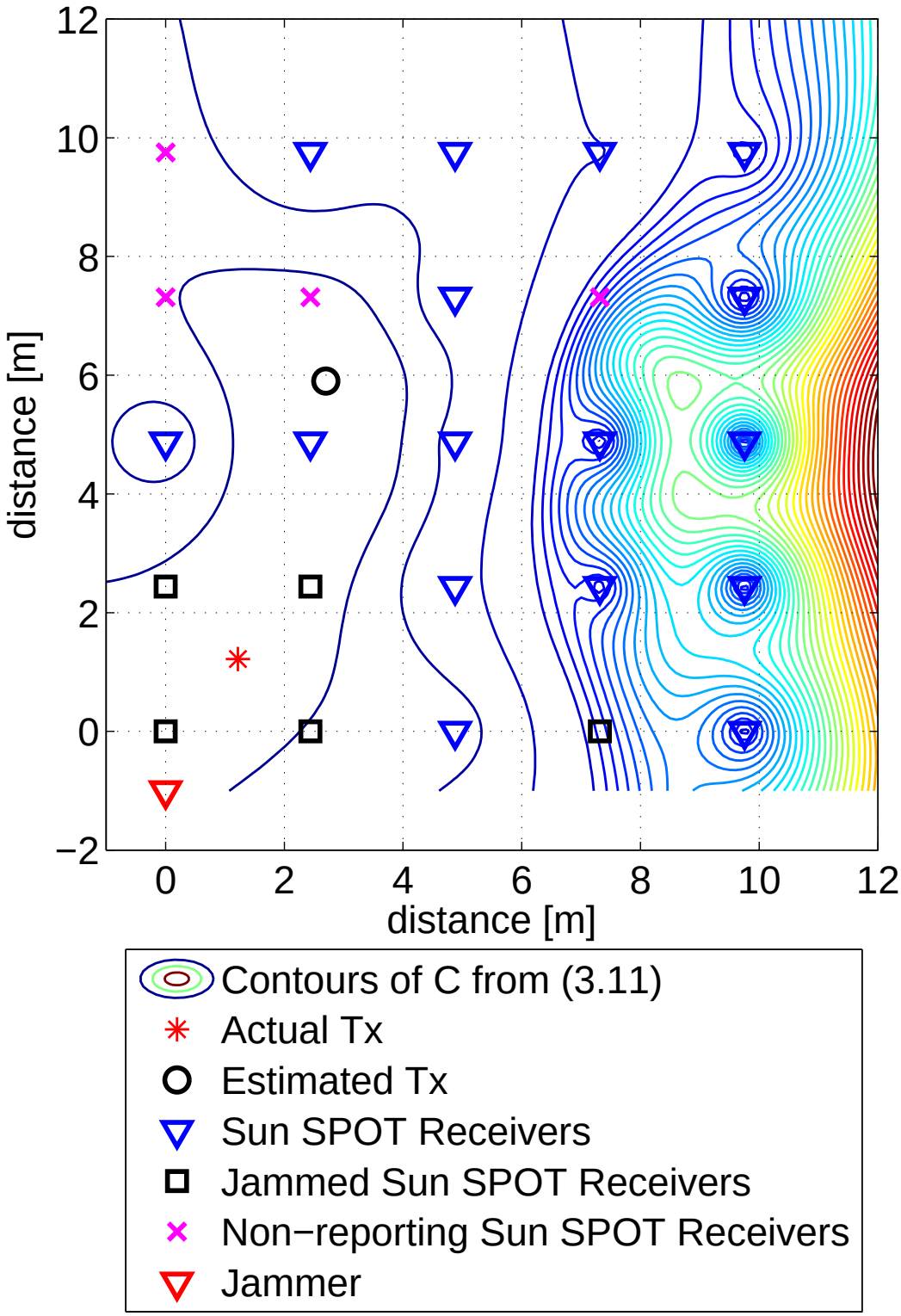


Figure 4.12: Jamming results from hardware jamming with the USRP2 and an omni-directional antenna in a five by five grid of Sun SPOT receivers at location one.

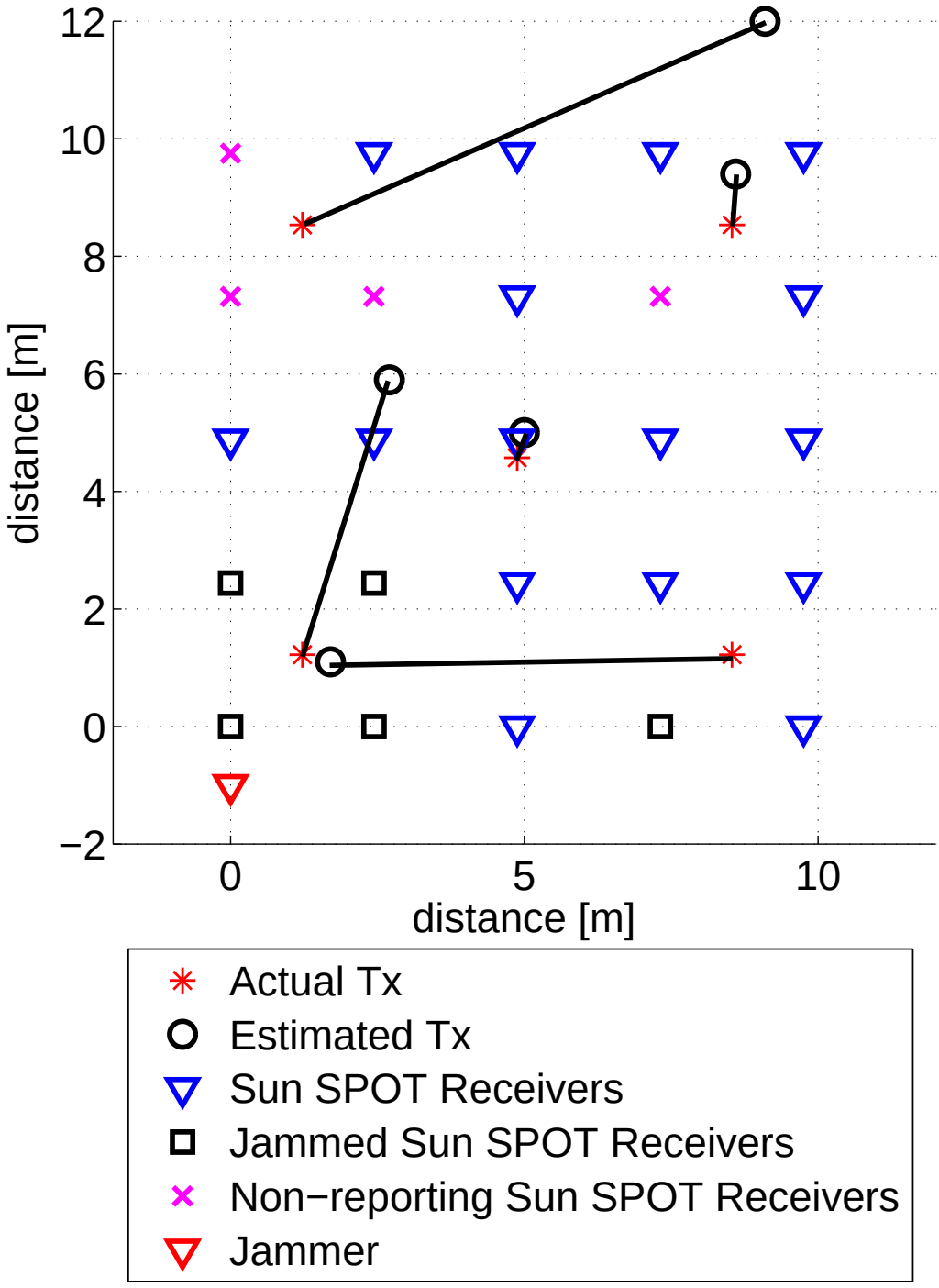


Figure 4.13: Jamming results from hardware jamming with the USRP2 and an omni-directional antenna in a five by five grid of Sun SPOT receivers at all five locations.

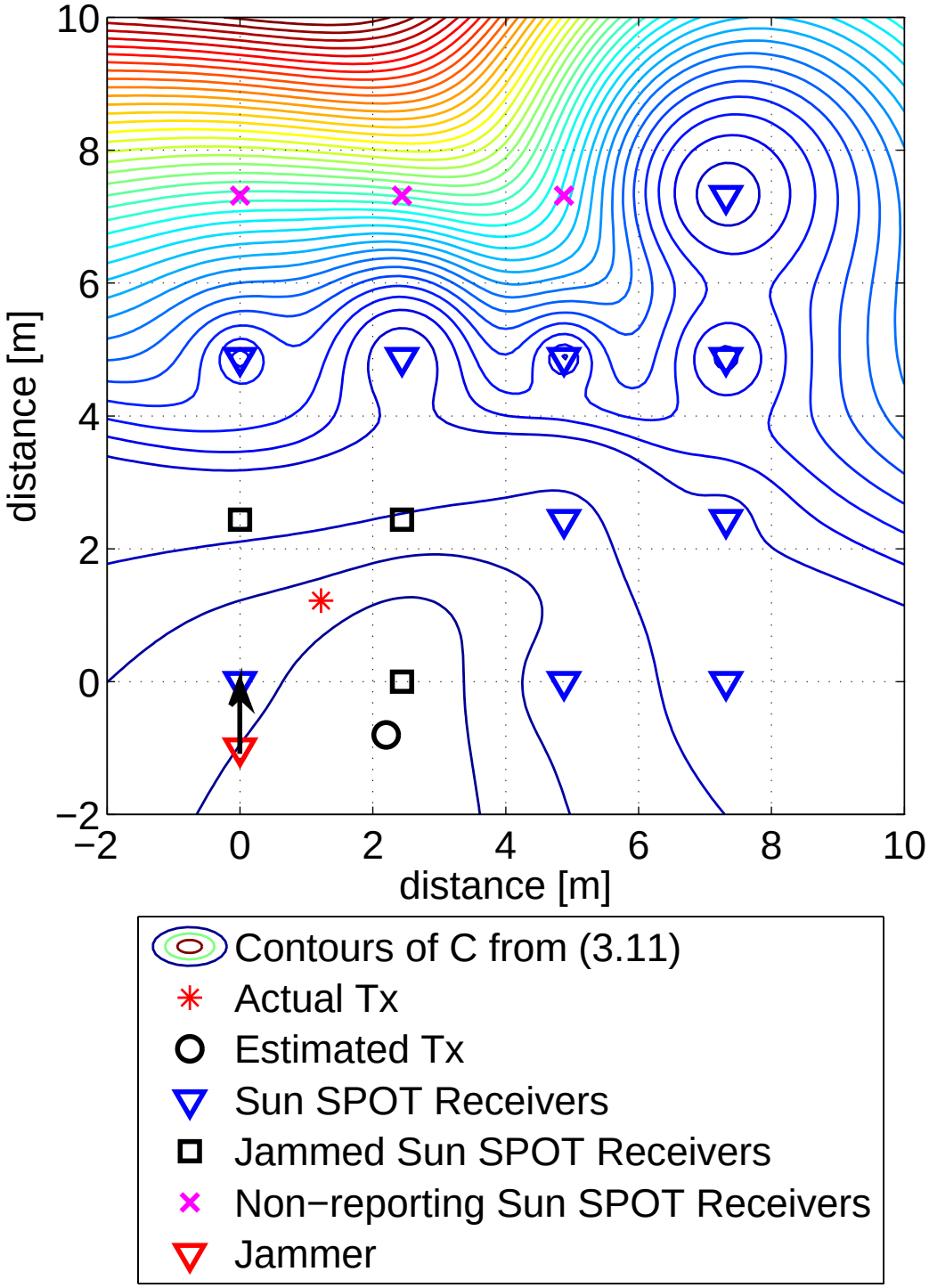


Figure 4.14: Jamming results from hardware jamming with the USRP2 and a log periodic antenna in a four by four grid of Sun SPOT receivers at location one.

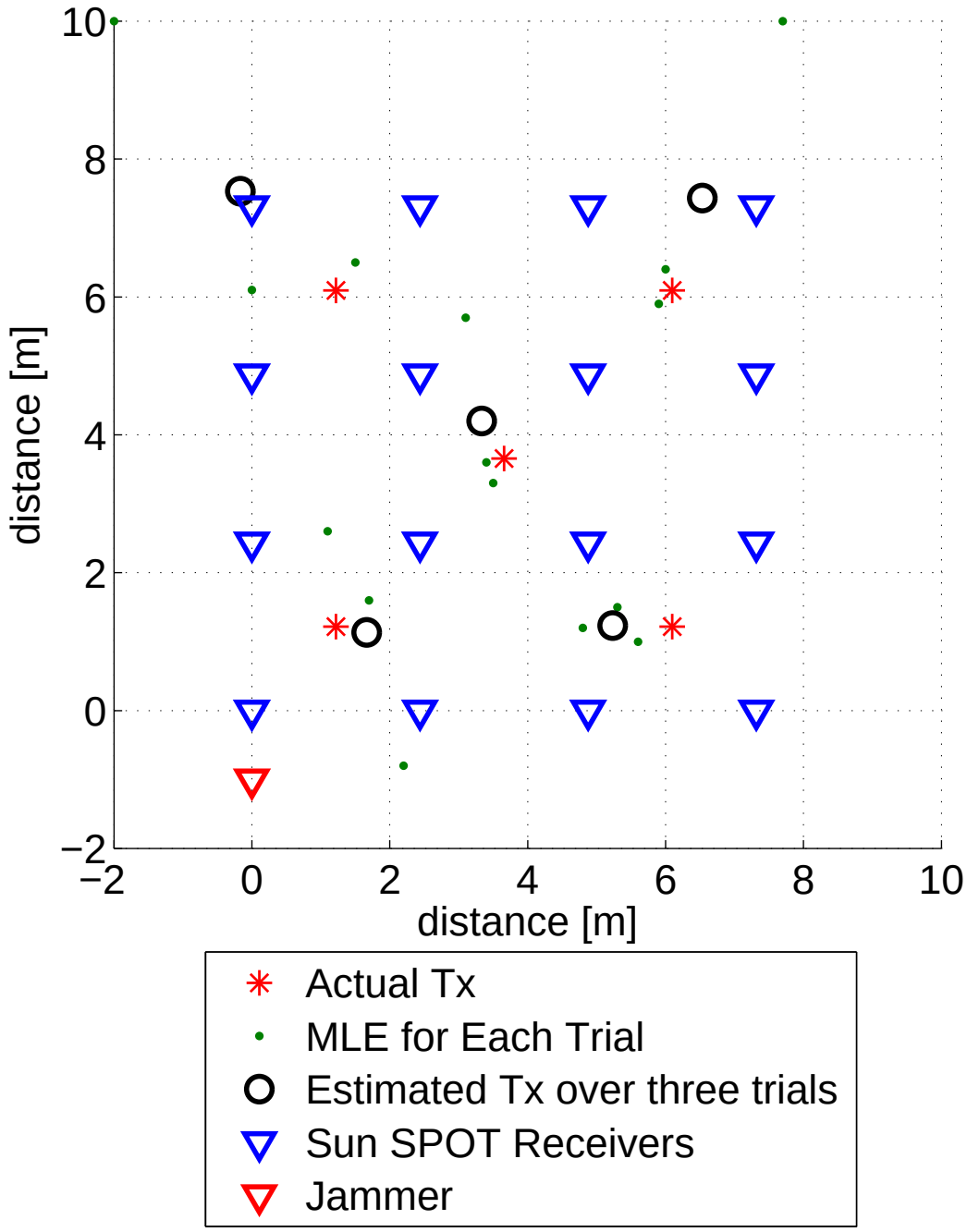


Figure 4.15: Jamming results from hardware jamming with the USRP2 and a log periodic antenna in a four by four grid of Sun SPOT receivers showing the average over three independent jamming trials at all five locations.

scenario where the jammer is pointed down the row of Sun SPOT receivers and the transmitter is at location 1. Since the antenna is designed for the 2.4 GHz spectrum and is a directional antenna, the effects were dramatic. Most of the Sun SPOT receivers in the 90° beam width were jammed. Figure 4.17 shows the estimated position for all five transmitter locations. The only location that was not affected by the jammer is the transmitter at location 4. This is due to the fact that there were still receivers around that transmitter. Figure 4.18 shows the estimated position for all five transmitter locations averaged over two trials. The results are similar and shows that all the receivers in the 90° beam width were jammed. The results from the directional antenna show that with the same transmit power the jammer can be more efficient depending on what antenna is used.

4.5 Comparison between Jamming and Non-Jamming

This section compares the difference between jamming and non-jamming geolocation performance. Table 4.2 shows the comparison on the difference between the non-jamming and jamming results using the log periodic antenna. This table also shows how far off the jamming and clear air collection is from the reference transmitter location. Figure 4.19 shows the results of jamming with a log periodic antenna averaged over three trials. The estimation for transmitter one seems accurate, but the individual trials were below and above the actual location. The average happened to be in the correct spot. Transmitter location two shows that the jammed estimation is not as accurate as the clear air estimation. Each individual trial shows that the jamming has an effect on the geolocation solution. If more trials were conducted, there would be a better statistical accuracy to compare the jamming against the non-jamming results.

Next the results for the directional antenna are shown in Figure 4.20. As the figure shows, the jamming effects for the directional antenna are obvious compared to the log periodic antenna. The directional antenna has a higher gain and narrower beam width focusing the same power from the jammer more efficiently than the log

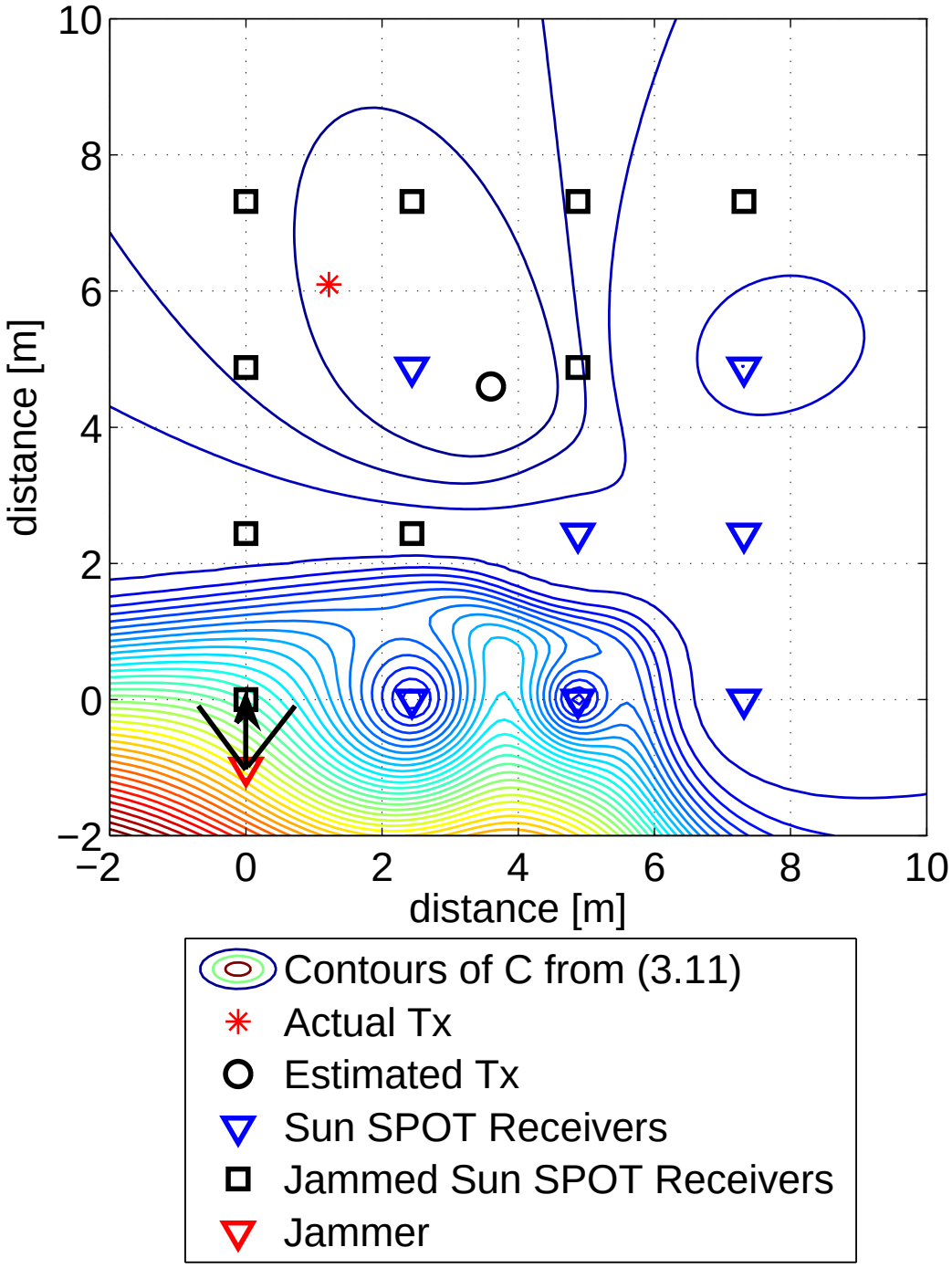


Figure 4.16: Jamming results from hardware jamming with the USRP2 and a HiGain directional antenna in a four by four grid of Sun SPOT receivers showing the estimated location for the transmitter at location 2.

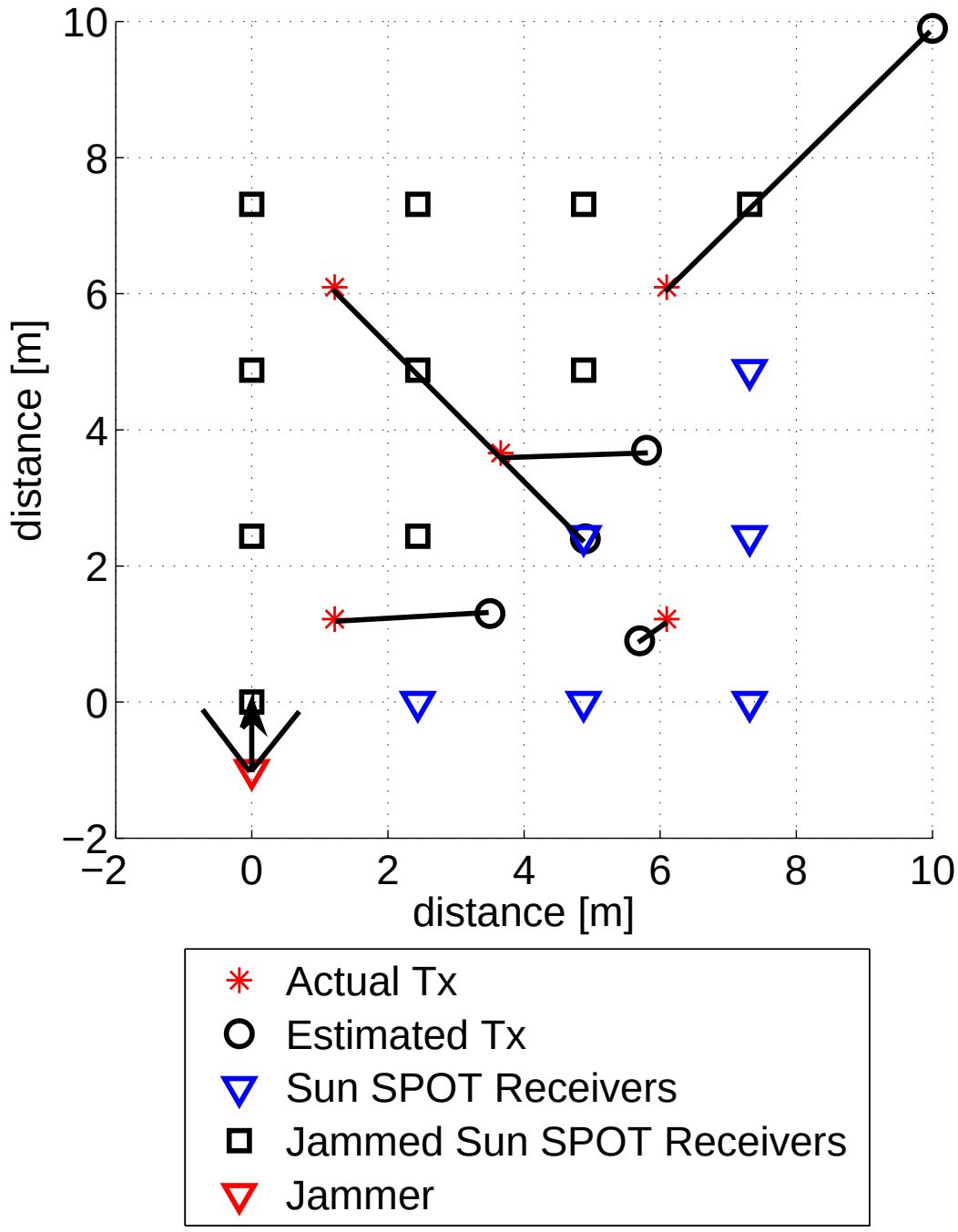


Figure 4.17: Jamming results from hardware jamming with the USRP2 and a HiGain directional antenna in a four by four grid of Sun SPOT receivers showing all five transmitter locations.

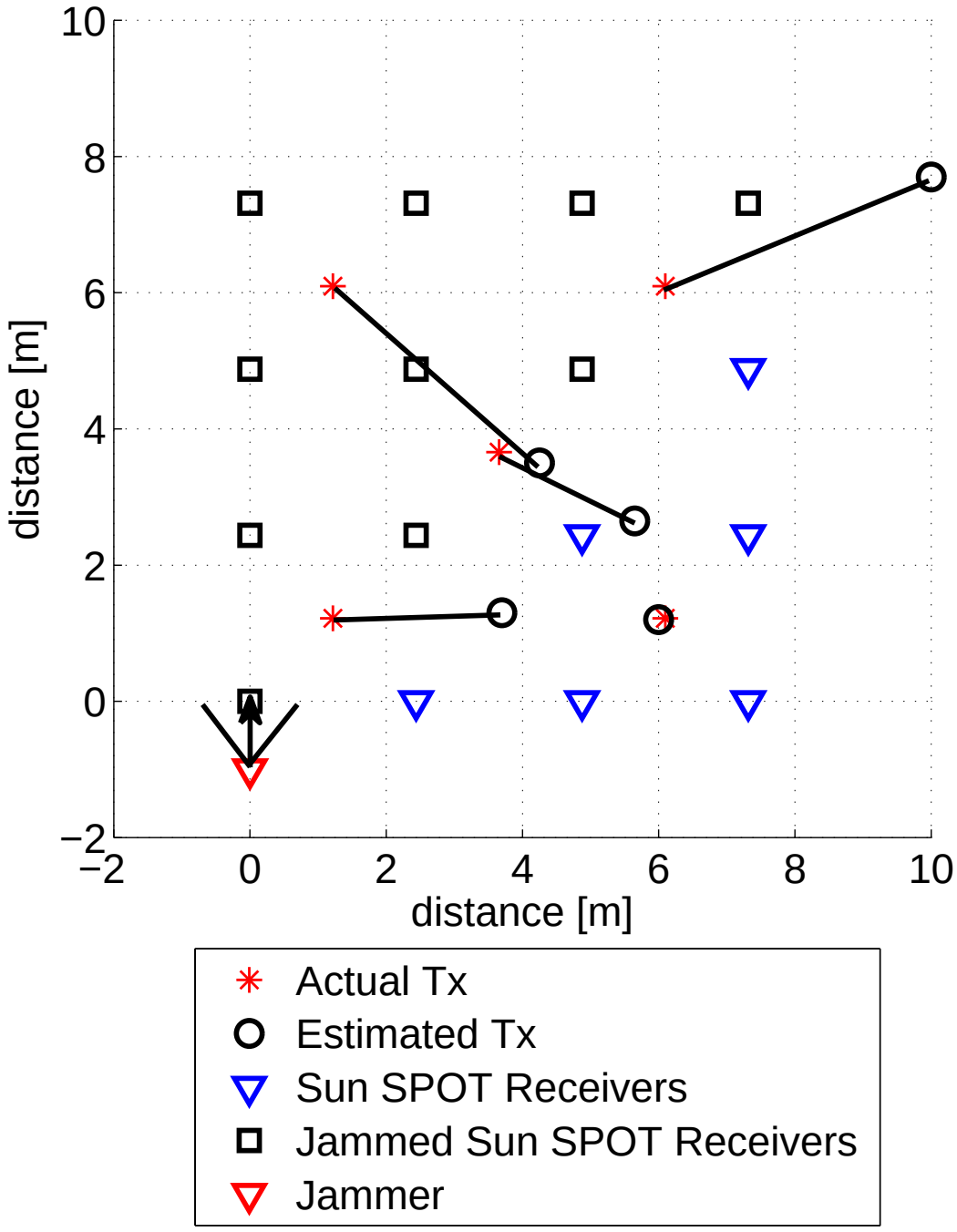


Figure 4.18: Jamming results from hardware jamming with the USRP2 and a HiGain directional antenna in a four by four grid of Sun SPOT receivers showing all five transmitter locations averaged over two trials.

Table 4.2: Data for the log periodic jammer

Tx Location	Clear Air Error from Reference	Jamming Error from Reference	Jamming Error from Clear Air Results	RMSE in X direction	RMSE in Y direction
Tx 1	0.28 m	0.46 m	0.35 m	0.71 m	1.75 m
Tx 2	0.64 m	2.00 m	1.64 m	2.24 m	2.58 m
Tx 3	1.20 m	1.41 m	0.21 m	1.10 m	2.61 m
Tx 4	0.49 m	0.86 m	0.45 m	0.95 m	0.25 m
Tx 5	0.35 m	0.63 m	0.51 m	0.39 m	1.42 m

periodic antenna. Table 4.3 gives the numerical results shown in Figure 4.20. The data shows that the transmitters in the beam width of the jammer were affected while the transmitter outside the beam width was not affected. Even though there is only one jamming trial, the effects of the jamming are easily seen. More trials would be required to get a good statistical comparison between the jamming and non-jamming.

In Figure 4.21, there is only one jamming trial and one non-jamming trial. Table 4.4 gives the numerical results for the five by five grid shown in Figure 4.21. There are not enough trials of non-jamming or jamming to get a good statistical comparison. The results do show that the jamming solution is not as accurate as the non-jamming solution. Another issue with the five by five grid of Sun SPOT sensors is that the Sun SPOTs randomly kept going out in the clear air data collection along with the jamming collection. This did not happen with the four by four grid of Sun SPOTs. An older and different version of the software controlling the Sun SPOTs was used for the four by four grid. This version of the control software was more stable but was limited to 16 Sun SPOT receivers. More trials were planned for the five by five grid, but this issue was not resolved and a good statistical data set would not have been able to be collected.

Table 4.5 gives the percentages of the difference between the jamming and clear air results for all three antenna types. As the data shows, the HiGain Directional antenna had the largest impact on the estimation performance of the Sun SPOT WSN. For example, at location 1 the jammer using the HiGain Directional antenna

Table 4.3: Data for the directional jammer

Tx Location	Clear Air Error from Reference	Jamming Error from Reference	Jamming Error from Clear Air Results	RMSE in X direction	RMSE in Y direction
Tx 1	0.28 m	2.48 m	2.37 m	2.50 m	0.08 m
Tx 2	0.64 m	3.99 m	4.49 m	3.17 m	3.03 m
Tx 3	1.20 m	4.22 m	3.57 m	3.90 m	3.50 m
Tx 4	0.49 m	0.10 m	0.41 m	0.44 m	0.42 m
Tx 5	0.35 m	2.23 m	2.56 m	2.00 m	1.79 m

Table 4.4: Data for the omni-directional jammer

Tx Location	Clear Air Error from Reference	Jamming Error from Reference	Jamming Error from Clear Air Results	RMSE in X direction	RMSE in Y direction
Tx 1	2.37 m	4.91 m	7.27 m	1.48 m	4.68 m
Tx 2	1.59 m	8.61 m	7.03 m	7.88 m	3.47 m
Tx 3	0.78 m	0.87 m	0.99 m	0.07 m	0.87 m
Tx 4	3.59 m	6.84 m	10.33 m	6.83 m	0.12 m
Tx 5	0.34 m	0.45 m	0.22 m	0.12 m	0.43 m

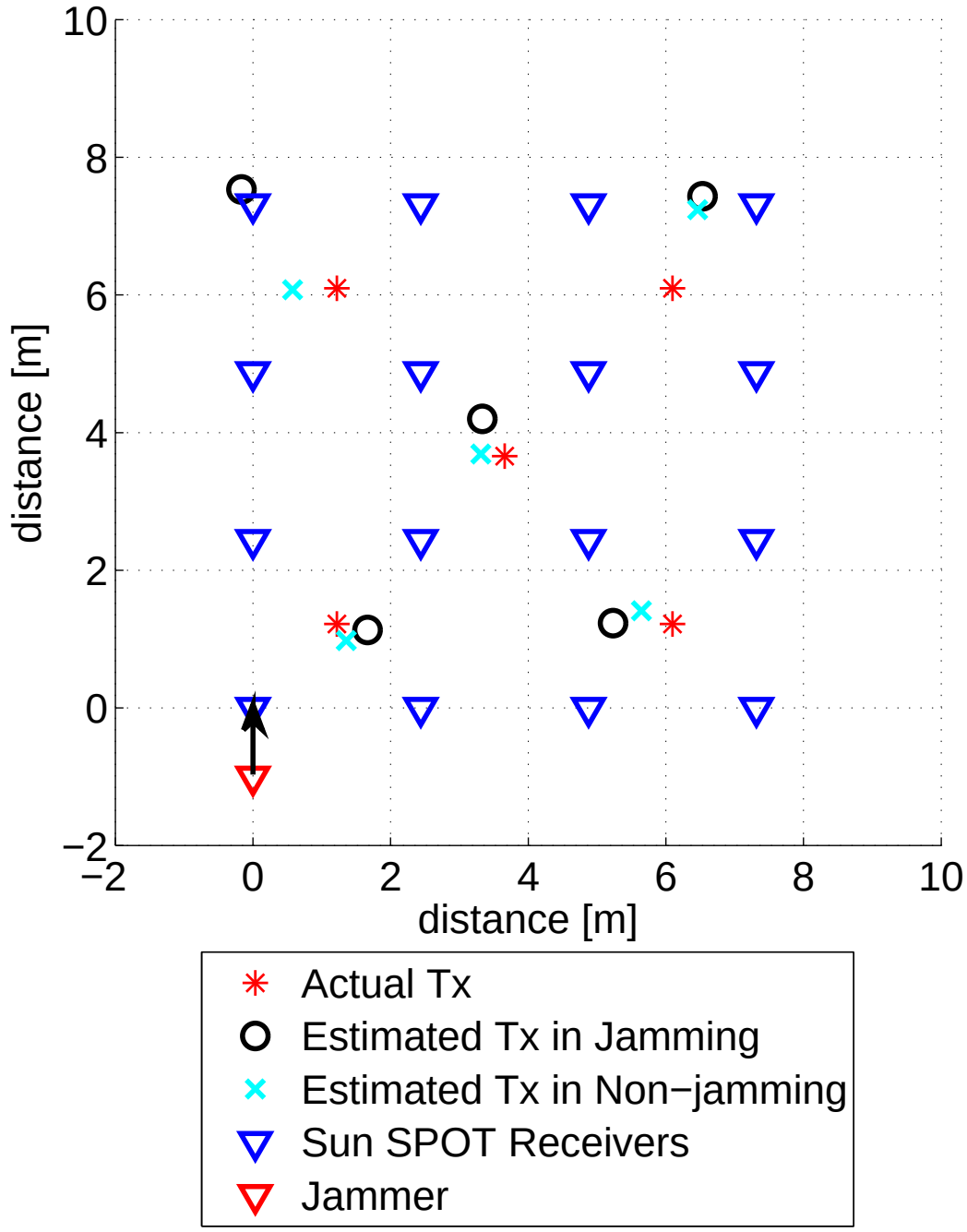


Figure 4.19: Jamming results from hardware jamming with the USRP2 and a log periodic antenna in a four by four grid of Sun SPOT receivers averaged over three trials compared to non-jamming results.

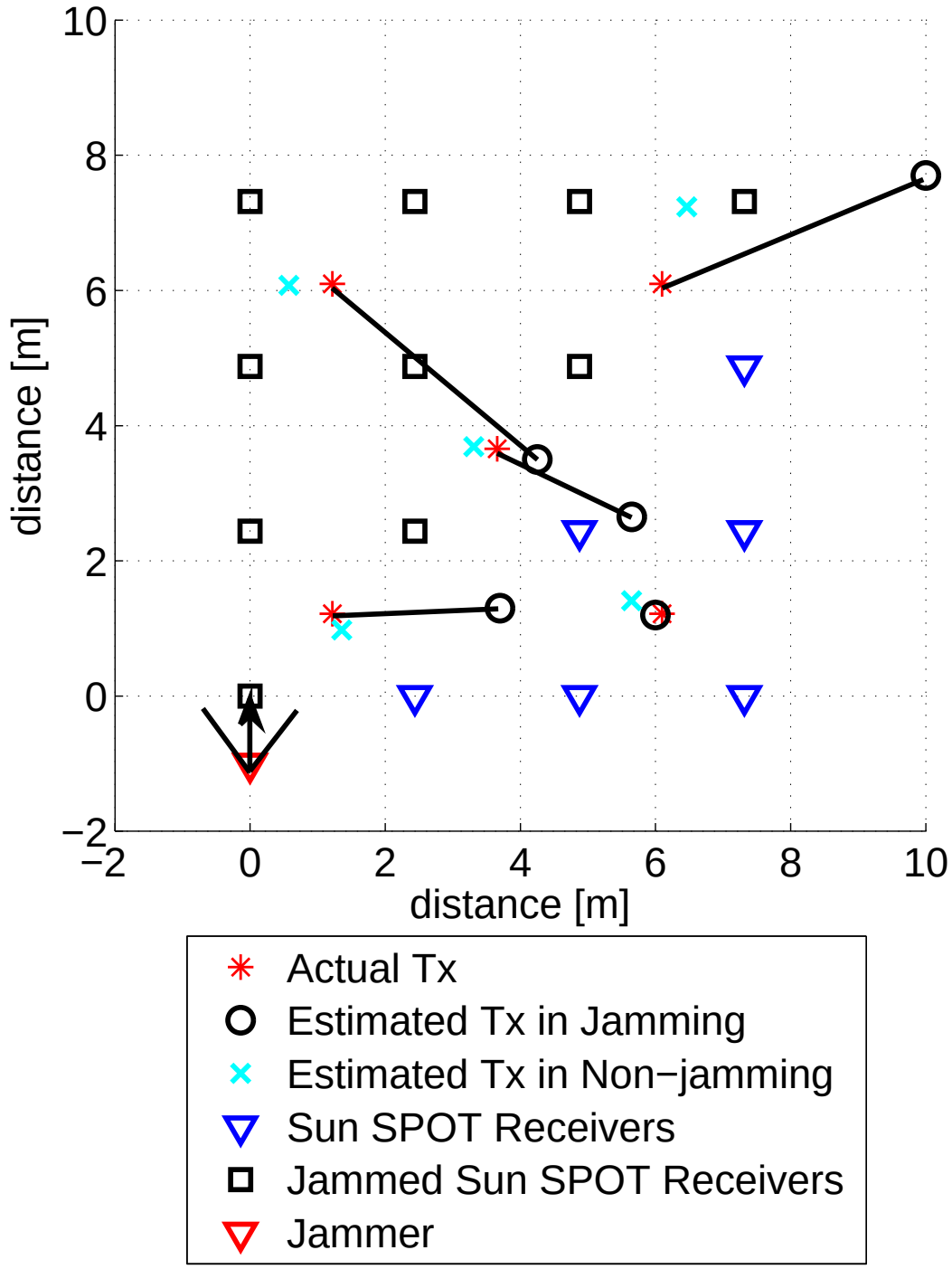


Figure 4.20: Jamming results from hardware jamming with the USRP2 and a HiGain directional antenna in a four by four grid of Sun SPOT receivers averaged over two trials compared to non-jamming results.

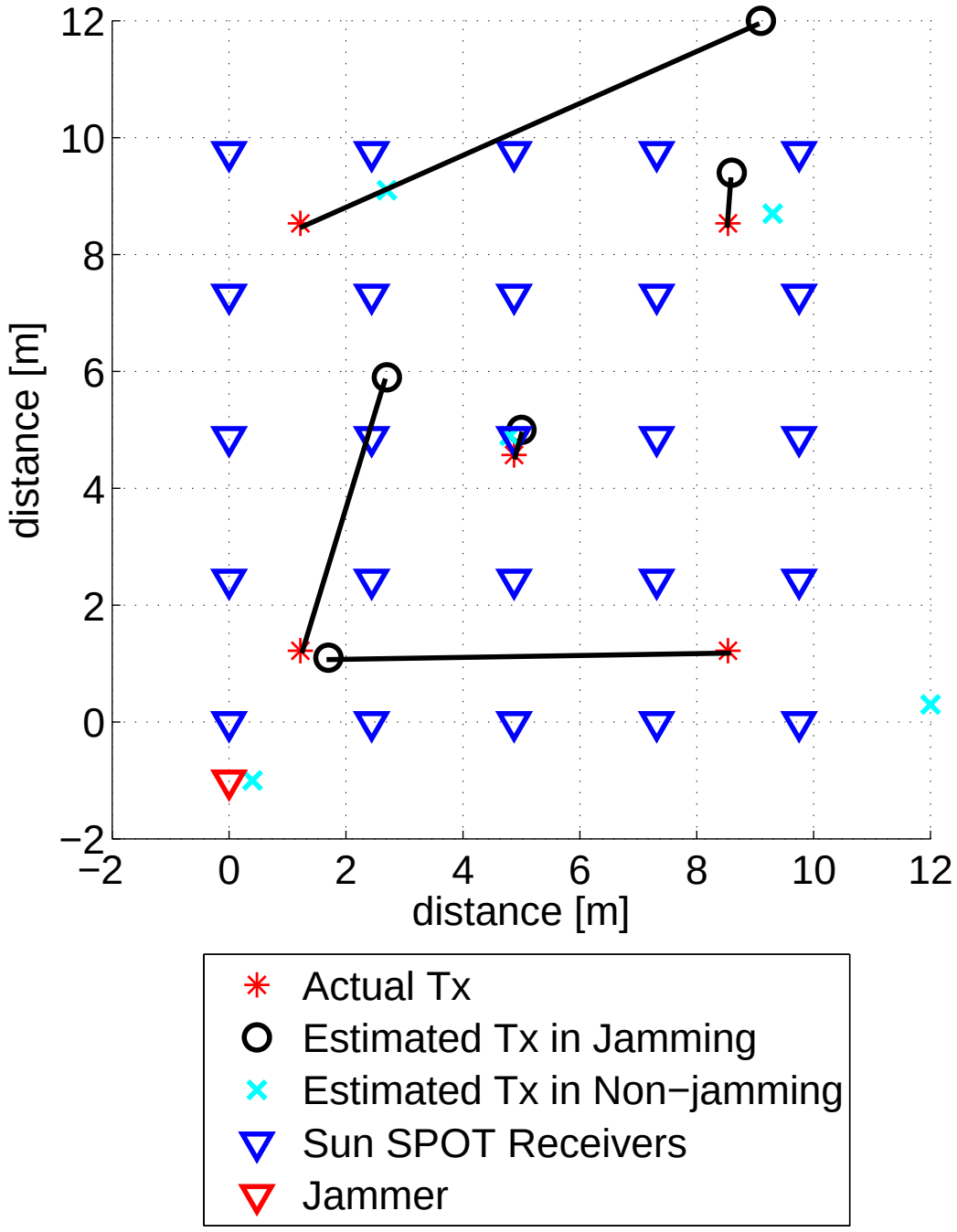


Figure 4.21: Jamming results from hardware jamming with the USRP2 and a omni-directional antenna in a five by five grid of Sun SPOT receivers compared to non-jamming results.

Table 4.5: Jamming estimation difference compared to non-jamming

Tx Location	% Error from Non-jamming using Directional	% Error from Non-jamming using Log Periodic	% Error from Non-jamming usign Omni-directional
Tx 1	795%	64%	108%
Tx 2	519%	210%	443%
Tx 3	252%	17%	11%
Tx 4	-80%	76%	91%
Tx 5	542%	82%	32%

had approximately 795% or 8 times worse estimation than the clear air estimation. This data shows that the more efficient and effective jammer combination is using the HiGain Directional antenna. The HiGain Directional antenna produced a less accurate estimation which leades to a greater percent estimation error. The exception is location four with approximately an 80% better estimation than the non-jamming test. This is due to the fact that there were only a limited number of trials conducted and that location four was not affected by the jammer. Also, the estimation happened to be almost exactly on the correct location for the transmitter.

The performance increase of the HiGain Directional antenna over the log periodic antenna is significant. For transmitter location one, the performance increase is approximately 11 times greater than the log periodic antenna. Table 4.6 gives the data for all five transmitter locations and the average performance increase excluding transmitter location 4. The data shows that in all but one location the HiGain Directional antenna performed better than the log periodic antenna. This is due to the fact that the HiGain antenna is designed specifically for the 2.4 GHz ISM band and has larger gain than the other antennas. The reason the estimation for transmitter location 4 was less accurate for the log periodic antenna is mainly due to the number of trials conducted. If there were a sufficient number of hardware trials conducted, the results should be similar for transmitter location 4.

Table 4.6: Performance increase of the HiGain antenna over the log periodic antenna

Tx Location	Performance increase over log periodic antenna
Tx 1	1136%
Tx 2	147%
Tx 3	1352%
Tx 4	-206%
Tx 5	564%
Average	800%

4.6 Basestation Results

The basestation is the Sun SPOT unit connected to the laptop through a USB cable. This specially configured Sun SPOT unit collects all the reports from the Sun SPOT receivers and stores them in a data file on the laptop. This one Sun SPOT unit is the device which communicates with all of the Sun SPOT receivers and if the connection is disrupted, no data will be collected from the network. This fact was observed the first time the USRP2 was tested as a jammer on the Sun SPOTs. The jammer was approximately two meters from the Sun SPOT basestation connected to the laptop collecting the data from the Sun SPOT receivers. Within a second of the jammer being turned on all the reports from the receivers stopped and it was determined the jammer blocked the signals from reaching the Sun SPOT used as a basestation. In order to test the jammer with the sensor network, the laptop and Sun SPOT basestation were moved to the other side of the WSN opposite the jammer, approximately 12 meters away from the jammer. This allowed testing to resume and data was able to be collected.

The jamming of the basestation showed a weakness in the Sun SPOT WSN that was not considered in this research before hardware testing began. This result showed another way to disrupt a WSN using less energy and more efficient jamming. Depending on what the end results of jamming are determined to be, either reducing the accuracy of the estimation or blocking the estimation, jamming the basestation

can stop the geolocation estimation and result in no data collected. This can be a more efficient way of jamming a WSN if the user just wants to block the geolocation estimation from occurring. The results from this test concluded that within a matter of seconds, the data from the entire Sun SPOT network can be blocked while the jammer is within close proximity to the Sun SPOT basestation. This can be very challenging since an attacker would have to know where the basestation collecting the data from the WSN is located. This method of jamming would be difficult for an attacker to perform.

Another observation relating to the basestation is that when the jammer is turned on the report rate from the receivers reduces dramatically. The number of reports that the basestation receives per second is reduced. In order to achieve the same number of reports per transmitter location as the non-jamming results, it took at least twice as long. The amount of reports per second and the multi-hop of the data across the Sun SPOT receivers should be researched in the future.

Due to some software control issues with the USRP2 with Simulink, the jammer was intermittent. At first the jammer was working and then unexpectedly the jammer stopped working. A few weeks later the jammer began to work again. No changes were made to the control software and there was no explanation on what fixed the issues happening in the preceding weeks. After a couple of months testing the jammer stopped working again for no explained reason. There was trouble with Simulink compiling the code to the USRP2. Once that issue was resolved, the jammer still would not operate. Because of these issues there was a lack of data collection after the jammer stopped working in November. If these issues had not happened more data would have been collected to get better statistical results for comparison.

V. Conclusions and Future Work

This Section details conclusions that were drawn from the results of this research. Future research project possibilities are also presented here based on the research outlined in Chapter III and Chapter IV.

5.1 Summary

The goal of this research is to determine the effects of jamming on Sun SPOT sensors used in a sensor network for geolocation. The sensor network was first simulated in MATLAB to get an idea of how the Sun SPOTs would respond to jamming. A cooperative WSN and a non-cooperative WSN were simulated to see the effects on the two different types of networks. After the networks were simulated, a jammer was introduced into the simulation. A number of jamming trials were conducted and the data was processed using the geolocation estimation algorithm outlined in Chapter III. This data was used to help create the set-up for the hardware jamming experiments.

The next step of the research was to develop and create a simple noise jammer using a USRP2. The USRP2 was controlled using Simulink from MATLAB 2011a. This control was new and there were issues with the software interface through Simulink to the USRP2. Support for the USRP2 has changed in the latest version of MATLAB 2011b. Special software from MathWorks needs to be downloaded and installed for the USRP2 to communicate in Simulink. The RFX2400 daughterboard has not been tested in the latest version of Simulink and may not work according to MathWorks. The jammer did work for a time and data was collected on 10 different days over four months before the jammer stopped working. After the data was collected, the data was processed through the geolocation algorithms using MATLAB. From this the estimates were compared to non-jamming results and the reference location for the transmitters.

5.2 Conclusions

First the hardware results show that jamming does have an effect on geolocation estimation produced by the Sun SPOT sensors similar to the results in the simulations. The MATLAB simulations gave an expected outcome on how the Sun SPOT sensors would react in a jamming environment and provided a baseline to compare the results with. The hardware results showed that by jamming the Sun SPOT receivers near the transmitter, the estimation accuracy of the transmitter's location was reduced by up to 795% or 8 times depending on the antenna used. The results also showed that the effects were localized to the area affected by the jammer which varied depending on the antenna used. To disrupt a cooperative WSN like the Sun SPOTs, the jammer would have to be very powerful, very close to the WSN or just powerful enough to block the basestation. For the non-cooperative network, the simulation results showed that the effects of jamming were not localized and that all the transmitter locations were affected by the jammer. Also as the power of the jammer increased, the estimation for the transmitters location moved toward the location of the jammer.

One area of interest discovered during testing was the type of antenna made a huge difference in the performance of the jammer. All three of the antennas used were designed to operate in the 2.4 GHz spectrum, but only one was designed specifically for the ISM band of the 2.4 GHz spectrum. The Hawking HiGain Directional Corner Antenna with 15 dB of gain and a 90° beam width performed better than the other two antennas. The HiGain antenna performed approximately 8 times better than the log periodic antenna, excluding transmitter location 4, which resulted in a less accurate estimation for the transmitter. The HiGain antenna had the same amount of transmit power from the USRP2 as the other antennas, but was more efficient in focusing the power out of the antenna. This allowed the USRP2 acting as a noise jammer to disrupt more Sun SPOT receivers in the path of the HiGain antenna. This shows that the antenna used for the jammer has a major impact on the efficiency and lethality of the jammer. If power is a consideration, a more efficient antenna will help offset the lower power coming from the jammer.

Another observation from this research is that the type of WSN has an effect on the results from jamming. When compared to a non-cooperative WSN, a cooperative WSN is protected more from jamming since the sensors are able to communicate with each other and communicate with the transmitter. In this type of WSN the effects of jamming are localized based on the location of the jammer and the beam width of the antenna used for jamming. In a non-cooperative WSN the effects of jamming are greater than in the cooperative WSN because the transmitter is not communicating with the receivers in the WSN. Since the transmitter is not part of the network, when the jammer is transmitting, the receivers in the WSN mistake the jammer as another transmitter. The results of jamming in a non-cooperative WSN are not localized and affect the transmitter at all possible locations in the non-cooperative WSN.

5.3 Future Work

There are a few areas of this research that should be explored further. The first area is changing the control software from Simulink to GNU Radio software and its newer graphical interface GRC. Simulink has some control and programming issues that affected the amount of experimental results that were available for this research. Using GNU Radio should allow the USRP2 to be a more diverse and capable jammer.

Another area to explore is using two or more USRP2 radios connected together by using the Multiple Input Multiple Output (MIMO) port on the USRP2's. This will allow the user to expand the jammers bandwidth and create diverse signals using multiple USRP2 radios with up to eight antennas. Along with MIMO a reactive jammer should be considered as the next step in this research. Having a jammer that could detect a signal and then start jamming would make the jammer a more efficient device. Other types of jammers would also be beneficial to look into. A random jammer would be harder to detect and could give different results than the other types of jammers.

A hardware test for a non-cooperative WSN would be the next step in testing the USRP2 jammer. The testing of the USRP2 jammer in this research used Sun

SPOT sensors that communicated with each other as a cooperative WSN. Getting data from a non-cooperative WSN would be beneficial and allow comparison with the simulations that were conducted for a non-cooperative WSN.

Bibliography

1. Blossom, E. "Exploring GNU Radio", 2004. URL `http://www.gnu.org/software/gnuradio/doc/exploring-gnuradio.html`. [Accessed 09-November-2011].

2. Brown, T. X., James, J. E. and Sethi, A. "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks". *Proceedings of the 7th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 120 –130. 2006.

3. Butler, M. *Low Cost, Low Complexity Sensor Design for Non-Cooperative Geolocation via RSS*. Master's of Science, Air Force Institute of Technology, 2950 Hobson Way, WPAFB, OH 45433-7765, March 2012.

4. Chiang, M. W., Zilic, Z., Radecka, K., and Chenard, J.-S. "Architectures of Increased Availability Wireless Sensor Network Nodes". *International Test Conference Proceedings*, 1232 – 1241. October 2004.

5. Commander, C. W., Pardalos, P. M., Ryabchenko, V., Shylo, O., Uryasev, S. and Zrazhevsky, G. "Jamming communication networks under complete uncertainty". *Optimization Letters*, 2:53–70, 2008. URL `http://dx.doi.org/10.1007/s11590-006-0043-0`.

6. Cook, D. J. and Das, S. K. *Smart environments: technologies, protocols, and applications*. John Wiley & Sons, Inc., Hoboken, New Jersey, first edition, 2005. ISBN 0-471-54448-5.

7. Ettus, M. "Universal Software Radio Peripheral (USRP) Rev. 2", 2011. URL `http://www.ettus.com/`. [Accessed 07-October-2011].

8. Ettus Research. "TX and RX Daughterboards For the USRP Software Radio System", 2011. URL `http://www.ettus.com/downloads/ettus_daughterboards.pdf`. [Accessed 07-October-2011].

9. Ettus Research. "USRP2 Motherboard Datasheet", 2011. URL `http://www.ettus.com/downloads/ettus_ds_usrp2_v5.pdf`. [Accessed 07-October-2011].

10. Hardy, T. *Malicious and Malfunctioning Node Detection via Observed Physical Layer Data*. Master's of Science, Air Force Institute of Technology, 2950 Hobson Way, WPAFB, OH 45433-7765, March 2011.

11. Hatke, G. F. "Adaptive Array Processing for Wideband Nulling in GPS Systems". *Conference Record of the Thirty-Second Asilomar Conference on Signals, Systems Computers*, volume 2, 1332 –1336. November 1998.

12. Hawking Technologies, Inc. "Hi-Gain 15dBi Corner Antenna", 2011. URL `http://hawkingtech.com/index.php/products/178-antennas.html`. [Accessed 26-October-2011].

13. Kay, S. M. *Fundamentals of Statistical Signal Processing: Estimation Theory*. Prentice-Hall PTR, 1993. ISBN 0-13-345711-7.

14. Kent Electronics. "Printed Circuit Board Antenna-Specification Data", 2011. URL `http://www.wa5vjb.com/pcb-pdfs/LogPerio900.pdf`. [Accessed 26-October-2011].

15. Li, M., Koutsopoulos, I. and Poovendran, R. "Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks". *26th IEEE International Conference on Computer Communications*, 1307 –1315. May 2007.

16. Martin, R. K. and Thomas, R. W. "Algorithms and bounds for estimating location, directionality, and environmental parameters of primary spectrum users". *IEEE Transactions on Wireless Communications*, 8(11):5692 –5701, November 2009.

17. Martin, R. K., King, A. S., Thomas,R. W. and Pennington, J. "Practical limits in RSS-based positioning". *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2488 –2491. May 2011.

18. Martin, R. K., Thomas, R. W. and Wu, Z. "Using spectral correlation for non-cooperative RSS-based positioning". *IEEE Statistical Signal Processing Workshop (SSP)*, 241 –244. June 2011.

19. Martin, R. K., Thomas, R. W., King, A. S., Lenahan, R., Pennington, J. and Lawyer, C. "Modeling and Mitigating Noise and Nuisance Parameters in Received Signal Strength Positioning". *Submitted to IEEE Transactions on Signal Processing*, November 2011.

20. Nerguizian, C., Belkhous, S., Azzouz, A., Nerguizian, V. and Saad, M. "Mobile robot geolocation with received signal strength (RSS) fingerprinting technique and neural networks". *IEEE International Conference on Industrial Technology*, volume 3, 1183 – 1185. December 2004.

21. Patwari, N., Ash, J. N., Kyperountas, S., Hero III, A. O., Moses,R. L. and Correal, N. S. "Locating the nodes: cooperative localization in wireless sensor networks". *IEEE Signal Processing Magazine*, 22(4):54 – 69, July 2005.

22. Sayed, A. H., Tarighat, A. and Khajehnouri, N. "Network-based wireless location: challenges faced in developing techniques for accurate wireless location information". *IEEE Signal Processing Magazine*, 22(4):24 – 40, July 2005.

23. Sun, G., Chen, J., Guo, W. and Liu, K. J. R. "Signal processing techniques in network-aided positioning: a survey of state-of-the-art positioning designs". *IEEE Signal Processing Magazine*, 22(4):12 – 23, July 2005.

24. Sun Microsystems. "Sun SPOT Quick Start Tutorial The Basestation in Action", 2011. URL `http://www.sunspotworld.com/docs/Green/Tutorial/Basestation.html`. [Accessed 15-October-2011].

25. Sun SPOT World. "Frequently Asked Questions", 2011. URL `http://www.sunspotworld.com/docs/general-faq.html`. [Accessed 07-October-2011].

26. Sun, Y. and Wang, X. "Jammer Localization in Wireless Sensor Networks". *5th International Conference on Wireless Communications, Networking and Mobile Computing*, 1 –4. September 2009.

27. Tabassam, A. A., Ali, F. A., Kalsait, S. and Suleman, M. U. "Building Software-Defined Radios in MATLAB Simulink - A Step Towards Cognitive Radios". *Computer Modelling and Simulation (UKSim), 2011 UKSim 13th International Conference on*, 492 –497. April 2011.

28. The MathWorks, IncF. "USRP2 Transmitter MATLAB 2011a Help File. Communications System Toolbox/Demos/Simulink Demos/USRP2 Transmitter", 28 March 2011.

29. Wei, X., Wang, L., and Wan, J. "A New Localization Technique Based on Network TDOA Information". *6th International Conference on Telecommunications Proceedings*, 127 –130. June 2006.

30. Wilson, J. S. *Sensor technology handbook, Volume 1.* Newnes, Burlington, MA, illustrated edition, 2005. ISBN 0-7506-7729-5.

31. Xu, W., Ma, K., Trappe, W. and Zhang, Y. "Jamming sensor networks: attack and defense strategies". *Network, IEEE*, 20(3):41 – 47, May-June 2006.

32. Xu, W., Trappe, W., Zhang, Y. and Wood, T. "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks". *MobiHoc 2005 Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, 46 – 57. May 2005.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
22–03–2012	Master's Thesis	Sept 2010 — Mar 2012

4. TITLE AND SUBTITLE

The Effects of Cognitive Jamming
on Wireless Sensor Networks used for Geolocation

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Huffman, Michael A, Captian, USAF

5d. PROJECT NUMBER

12G136

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/GE/ENG/12-21

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

Air Force Research Laboratory
Attn: AFRL RYRE (Dr. Vasu Chakravarthy)
2241 Avionics Circle
WPAFB, OH 45433
(937) 785-5579 ext 4245
Vasu.Charkravarthy@wpafb.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/RYRE

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

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approval for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The increased use of Wireless Sensor Networks (WSN) for geolocation has led to the increased reliance of this technology. Jamming, protecting and detecting jamming in a WSN are areas of study that have increased in interest because of this. To learn more about the effects of jamming, this research uses simulations and hardware to test the effects of jamming on a WSN. For this research the hardware jamming was tested using a Universal Software Radio Peripheral (USRP) version 2 to assess the effects of jamming on a cooperative network of Java Sun SPOTs. This research combined simulations and data collected from hardware experiments to see the effects of jamming on cooperative and non-cooperative geolocation.

15. SUBJECT TERMS

cooperative, non-cooperative geolocation, jamming, wireless sensor networks

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. Richard K. Martin (ENG)
U	U	U	UU	89	19b. TELEPHONE NUMBER *(include area code)* (937) 255–3636 x4625; Richard.Martin@afit.edu