AFRL-RI-RS-TR-2014-274

LOCALIZATION UNDER ADVERSARY MISDIRECTION

OCTOBER 2014

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the 88th ABW, Wright-Patterson AFB Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2014-274 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/ S /
JAMES PERRETTA
Branch Chief

/ S /
WARREN H. DEBANY, JR.
Technical Advisor, Information
Exploitation & Operations Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
OCTOBER 2014	FINAL TECHNICAL REPORT	JAN 2009 – SEPT 2014

4. TITLE AND SUBTITLE

LOCALIZATION UNDER ADVERSARY MISDIRECTION

5a. CONTRACT NUMBER
IN-HOUSE

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
AFOSR / 61102F

6. AUTHOR(S)

Lauren M. Huie-Seversky

5d. PROJECT NUMBER
23E2

5e. TASK NUMBER
IH

5f. WORK UNIT NUMBER
09

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/RIGB
525 Brooks Road
Rome NY 13441-4505

8. PERFORMING ORGANIZATION REPORT NUMBER

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

Air Force Research Laboratory/RIGB
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSOR/MONITOR'S REPORT NUMBER
AFRL-RI-RS-TR-2014-274

12. DISTRIBUTION AVAILABILITY STATEMENT

Approved for Public Release; Distribution Unlimited. PA# 88ABW-2014-3777
Date Cleared: AUG 14, 2014

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Wireless sensor networks are particularly versatile for performing a wide range of detection and estimation tasks for the identification, localization, and tracking of unknown phenomenon. The shared nature of the wireless medium presents a number of design challenges as the sensors transmitted data can be compromised both by natural artifacts such as noise and channel fading and by the intentional corruption due to an adversary. While much work has examined how noise and channel conditions impact estimation accuracy, much less attention has been given to the problem of corruption due to an intelligent adversary. This work considers the problem of estimating emitter location in the presence of an intelligent adversary. The localization problem is considered from two different viewpoints. We focus on the fundamental behavior of adversary-network strategies at the physical layer. Examination of an adversary at the physical layer is a rich space for discovering fundamental behavioral insights into security strategies for sensor networks. Strategies that both the network and the adversary should employ are developed, to see which side really has the upper hand. The adversary seeks to degrade and redirect the network while the networks goal is to mitigate effect of the adversary. These physical layer adversary attacks and defense strategies can be considered the last line of defense when higher-layer techniques fail.

15. SUBJECT TERMS
Localization, sensor networks, time difference of arrival, optimization, false information injection, estimation and detection theory

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			**LAUREN M. HUIE-SEVERSKY**
U	U	U	UU	73	19b. TELEPHONE NUMBER (*Include area code*) **315-330-3187**

Contents

List of Figures

List of Tables

1.0. Summary

Wireless sensor networks are particularly versatile for performing a wide range of detection and estimation tasks for the identification, localization, and tracking of unknown phenomenon. The shared nature of the wireless medium presents a number of design challenges as the sensors transmitted data can be compromised both by natural artifacts such as noise and channel fading and by the intentional corruption due to an adversary. While much work has examined how noise and channel conditions impact estimation accuracy, much less attention has been given to the problem of corruption due to an intelligent adversary. This work considers the problem of estimating emitter location in the presence of an intelligent adversary. The localization problem is considered from two different viewpoints. We focus on the fundamental behavior of adversary-network strategies at the physical layer. Examination of an adversary at the physical layer is a rich space for discovering fundamental behavioral insights into security strategies for sensor networks. Strategies that both the network and the adversary should employ are developed, to see which side really has the upper hand. The adversary seeks to degrade and redirect the network while the networks goal is to mitigate effect of the adversary. These physical layer adversary attacks and defense strategies can be considered the last line of defense when higher-layer techniques fail.

2.0. Introduction

Wireless sensor networks are particularly versatile for performing a wide range of detection and estimation tasks for the identification, localization, and tracking of unknown phenomenon. Detection problems use the measured data to determine *if* a particular event has occurred in applications such as determining the occurrence of rare events, intrusion monitoring, and signal detection. Whereas estimation problems use the measured data to determine the *value* of the unknown parameter in applications such as environmental monitoring, seismology, communication, speech, and image analysis [30].

A sensor network consists of two main parts: nodes that make measurements on the underlying phenomenon and a node (or set of nodes) that process the measured data. The sensors' measurements are transmitted and collectively processed in order to compute an estimate of the unknown parameter. A variety of methods exist for both communicating between nodes, and processing the measured data. The sensors can be configured using a centralized or distributed set-up. Under a centralized set-up, the sensor measurements are each transmitted to a central fusion center. In a distributed set-up, several local neighborhoods of sensors each independently make an interim parameter estimate. The estimates from all neighborhoods are then combined to determine the final estimate of the unknown parameter.

A number of challenges inherent in wireless applications can influence the network's parameter estimation. One of the most well studied issues is that of limited sensor battery life, which can exist across a variety of estimation tasks. The specific estimation task dictates the severity of energy constraints. For example, sensors may be used for sensing tasks in harsh environments, thus energy replacement might prove difficult. As a result, guaranteeing a sensor's lifetime in certain applications may be key in the design process. Another challenge that arises is that the sensors' transmitted data is subject to degradation from measurement noise and poor channel conditions. Still a worse problem is ensuring security in wireless networks, not only due to the open nature of a shared wireless medium but also due to the fact that the sensors are vulnerable to physical compromise. It is of interest to not only safeguard our networks against an eavesdropper monitoring transmitted messages but also to ensure that the estimation cannot be influenced by the intentional corruption by an adversary. While much work has examined how noise and channel conditions impact estimation accuracy, much less attention has been given to the problem of corruption due to an *intelligent* adversary.

Characterizing and analyzing an adversary's behavior as well as detecting and mitigating its impact on a network's parameter estimation is an important problem with widespread applications. There are a number of ways an intelligent adversary can impact parameter estimation across a broad range of applications. In the context of environmental monitoring, a heat source such as a match, can be placed in close proximity of a temperature sensor causing an false alert in either a fire alarm system, or forest fire monitoring system. Another application area is speech processing, where features such as pitch or frequency can be adjusted to disguise a voice precluding speaker identification. In image analysis, a group of pixels can be replaced with a different set of pixels, in order to completely remove an object of interest from the scene. In the case of localization, the sensor positioning information can be altered to make the network believe the source's location is actually somewhere other than its true value.

A parameter of particular interest is estimating the location of an emitter, which has a number of applications including 911 services, location based social networking, and location based advertising [17]. The general problem of source localization, is typically a two-step process. First the sensors make measurements of an intermediate location parameter (i.e. delay, angle, signal strength) as determined by their location method. Many localization methods exist such as time of arrival (TOA), time difference of arrival (TDOA), angle of arrival (AOA), and received signal strength (RSS). The noisy estimates of the location parameter are then transmitted to a central node, where they are combined to determine the final estimate of emitter location. Typically, non-linear least squares is used to estimate location where a set of non-linear equations is linearized and the estimate is iteratively improved. More recently, semidefinite programming has attracted attention for localization.

There are many opportunities for an adversary to compromise a localization network. For example, an adversary can inject false information by changing the position of sensors, corrupting the communication between the sensors and the fusion center, or by hijacking the node. Central to localization is obtaining accurate sensor positioning information. As a result, this work focuses on an adversary model that modifies

the reported sensor position. From this model we are able to show intuitive results of the developed strategies in terms of the sensor-emitter geometry. Alternatively, the sensors' measurements of the intermediate localization parameter, i.e. delay, angle or signal strength could also be corrupted. However, the intuition behind changing only the locating parameter and how it maps to the sensor-emitter positions is not as evident. One could also envision a more powerful adversary that has the ability to directly control the fusion center. This work considers adversary strategies to inject false information as well as network strategies to detect and mitigate those injections at the physical layer.

2.1. Strategies at the Physical Layer

The open nature of the wireless medium makes sensors susceptible to an adversary either by passive methods such as eavesdropping or by the active injection of data. While much work has focused on securing sensor networks at higher layers, we argue that examination of an adversary at the physical layer is a rich space for discovering fundamental behavioral insights into security strategies for sensor networks.

A significant effort has been devoted to securing sensor networks at higher network layers including encryption and authentication. Encryption methods strive to keep data secret while authentication seeks to ensure that received data is from an authorized user. Despite the existence of methods for securing sensor networks through encryption and authentication unauthorized access can still occur [5]. Ensuring the security of sensor networks is a particularly challenging problem due to overhead, cost, storage, and scalability issues required by these methods. Encryption methods may be too costly and require too much overhead due to their need for encryption key exchange and distribution [5]. In addition, end-to-end encryption is in general unrealistic for large sensor networks since the number of unique encryption keys necessary is likely to exceed the sensors' storage capacity [5]. To avoid such storage limitations, a hop-by-hop method could be used where only the sensor's nearest neighbor's keys are stored [5]. However, if a sensor was commandeered by the adversary, then encryption would fail for all traffic passing through that sensor [5]. Thus, the inherent mobile nature of sensor networks pose challenges for using such higher layer security methods.

This work considers the development of adversary-network strategies for source localization at the physical layer, due to its simplicity and the insights that can be obtained by a strict examination of the physically-based aspects of the problem. Consideration of how an adversary can affect the network's physical characteristics provides a simple and intuitive framework to discover insights into an adversary's behavior. These physical layer adversary attacks and defense strategies can be considered as either a complementary method or the last line of defense when higher-layer techniques such as encryption or authentication fail.

2.2. Related Work

Adversarial work has been considered in a number of different contexts. Our focus is its effect on localization. We begin by reviewing the general problem of localization and the large research effort devoted to both localization and tracking in non-adversarial settings. Next, adversarial work is discussed for a wide variety of sensor network applications and then we focus specifically on localization.

2.2.1. Non-adversarial Settings: Localization

The problem of estimating location is one that has existed for decades [52]. There have been two main research areas: sensor localization, and source localization. The problem of sensor localization seeks to determine a set of unknown sensor positions given a smaller set of known sensor positions commonly referred to as anchors or beacons. In source localization, the goal is to estimate the geographic location of an emitter.

Sensor Localization

Due to the nature of sensor deployment, all of the sensor positions may not be known exactly apriori. Position information is essential as it is often required to use the collected sensor data and in addition is the basis of many communication protocols [27]. A number of challenges arise in this scenario. Specifically, a lack of accurate positioning information can cause cumulative error, which poses a serious problem. Range-free localization methods are reviewed in [61], which can be categorized into: anchor-based schemes and anchor-free schemes. In anchor-based techniques, a smaller set of anchor nodes with known positions are

used to localize the remaining nodes. In [27] the authors propose a distributed multidimensional scaling (MDS) algorithm where local maps of adjacent sensors are determined along the path between anchors, avoiding cumulative errors. The effect of the fading channel on proximity measurements was considered, which indicates if two devices are within communication range [53]. A distributed, iterative algorithm to locate a set of sensors using the minimum number of anchor nodes was developed in [32]. In [1] the authors determine how to optimally place the anchor nodes. In anchor-free techniques, a controlled event at a known location, such as a light source or a radio transmission is used to determine the sensors' location. The authors in [55] develop a distributed algorithm to determine the set of sensor positions without the need for anchors. In [54] a sensor network is used to measure a time-varying isotrophic random field where the sensor data itself is used to estimate a map of the sensors' locations using manifold learning algorithms.

Source Localization

A number of methods exist for estimating location including angle of arrival (AOA), time of arrival (TOA), time difference of arrival (TDOA), and received signal strength (RSS). These methods will be described in detail in the sections that follow. Typically localization is a two step process where each sensor (or pair of sensors) makes a measurement of an intermediate localization parameter, i.e. angle, delay, or signal strength. The sensors' measurements and positions are then transmitted to a central node for processing to determine a final estimate of the emitter location.

Several methods exist for performing the final geo-location. The first approach is non-linear least squares (LS) estimation, where a non-linear set of equations is approximated by a linear equation. In [16], the authors consider the advantages of a Taylor series expansion in order to estimate location. This method requires an initial guess of location and improves the guess in an iterative fashion by determining the local least-sum-squared error. The measurements are linearized and then least squares minimization is used at each step of the iteration. If given a Gaussian distribution, the global minimum is the maximum likelihood (ML) solution. Recently, the use of semidefinite programming has become popular as an efficient method for an approximate solution. The use of semidefinite relaxation is a computationally efficient method for a range of difficult nonconvex problems [45]. Specifically, semidefinite programming has attracted interest for the nonconvex problem of localization [2, 48, 50]. In [48], a semidefinite program is developed for source localization for the received signal strength (RSS) method. Different from other SDP approaches that minimize the l_1 measurement error, [48] begins with the Maximum Likelihood estimate (MLE) and applies a minimax approximation allowing for a semidefinite relaxation.

A number of challenges arise in the localization scenario, in particular how to balance communication, with computing, and accuracy. One can consider a variety of different communication set-ups from centralized where every sensor transmits its measurement to a central fusion center, to distributed scenarios where local neighborhoods of sensors each make their own estimate of the unknown parameter. In [18] a distributed algorithm for source localization under RSS is presented, which uses the projection on convex sets method in a distributed fashion. The problem of localizing an acoustic source is considered in [3] using a distributed scheme by distributed projection on convex sets. A closed form is found to determine the projections and lends itself to an efficient solution. The authors in [47] consider locating an acoustic source in a distributed fashion and present a new weighted least squares method, which provides a reduction in computational complexity.

The effect of erroneous sensor positions on source localization was considered in [8, 19, 20, 56]. In [20] the authors considered sensor position errors for angle of arrival. The effect of erroneous sensors position on the Cramer Rao Lower Bound (CRLB) was considered under direction of arrival in [56]. The authors in [19] considered the effect of erroneous sensor positions on localization under the TDOA method. The receiver at each sensor has a random error. The authors derive the CRLB in the presence of sensor position errors, which is modeled as Gaussian noise. However, they do not consider that the sensor position has been intelligently optimized to degrade the network.

Tracking

Source and sensor localization generally considers that the sensors to be localized are stationary. A natural next step is to consider that the sensor is moving, i.e. tracking. Work in the tracking literature addresses

similar issues such as energy and bandwidth constraints. In [67] the authors develop an information driven framework where the resources of communication and computation are traded for a gain in information utility. The problem of sensor bias estimation and compensation for target tracking has been addressed in [40, 41].

2.2.2. Adversarial Settings in Sensor Networks

There are a number of works which consider the general problem of sensor networks in the presence of an adversary. Most notably the Byzantine sensor problem considers a sensor network in which an unknown percentage of nodes report fictitious observations, originally motivated by the Byzantine Generals problem [36].

The Byzantine generals problem considers a group of generals that must agree on whether or not to attack and can only communicate via messenger. Some of the generals are traitors and seek to prevent a consensus from being reached. Under this paradigm, a solution only exists if more than two-thirds of the generals are loyal.

The byzantine sensor scenario has been considered for the specific problems of distributed detection [46], source coding [34], network security [21,26], and power grid systems [33,35]. In [34] the authors consider the distributed source coding problem with Byzantine sensors. Each sensor transmits an encoded measurement to the decoder, which seeks to reconstruct the source message. Some of these nodes are Byzantine. The authors find achievable rate regions for variable-rate codes, deterministic fixed-rate codes, and randomized fixed-rate codes. In [26], the authors consider the effect of corrupt malicious packets on network coding. In particular, they develop the first distributed polynomial-time rate optimal network codes that hold with byzantine nodes. In [46] the authors consider a set of sensors some of which are Byzantine and a fusion center that employs a Neyman Pearson detector. The optimal attacking strategy is sought (from the adversary's viewpoint) where the worst case miss detection probability is minimized using Kullback-Leibler (KL) divergence. In [33, 35] a detector is developed to determine whether or not an adversary is present in power grid systems, where the adversary alters a sparse number of measurements. The network's detector is based on a rise in mean squared error (MSE).

The problem of localization in the presence of an adversary has also been considered in [7, 39]. In [39], a bias is introduced into the triangulation location estimates where the sensor to be localized has a set of measurements $\{x_i, y_i, d_i\}$ consisting of anchor locations and estimated distances from the sensor to each anchor. The adversary arbitrarily alters a percentage of the distance measurements such that the localization "votes" for some other location. The authors in [42] consider attacks on range based location discovery and develop attack tolerant estimation methods. In [7] a linear attack model based on signal attenuation and amplification is used under the received signal strength (RSS) method.

The problem of secure localization, where a sensor determines its own location in the presence of an adversary is considered in [37, 38]. The authors propose a range-independent localization algorithm and show its robustness against the wormhole attack, sybil attack, and compromised sensors. In [43] the authors consider the security of geographic routing and propose a location verification algorithm for attacks that falsify location information. In-region verification was considered in [59], where a set of verifiers must determine the validity of a sensor's location claim, that is whether or not it is in a particular region.

The problem of state estimation with an adversary is considered in [49] with application to target tracking. The adversary injects false information into a sensor's measurement and the performance of the Kalman filter is assessed. A target tracking system is considered, where the effect of the false information on the Kalman filter proves to be diminishing over time. Instead of estimating and removing the bias, in [49] the effect of the bias on state estimation performance over time is analyzed.

2.3. A Framework for Adversary-Network Strategies

Assessing security issues in sensor networks is an important problem, in particular behavior in contentious environments. Understanding the behavior of both the adversary and the network is necessary to characterize the complex interaction that exists between the competing objectives of the adversary that seeks to harm the network and the network that must ensure its security. In the design of adversary-network strategies, a number of fundamental questions arise. For example, How can the adversary inject false information?,

How powerful is the adversary?, What information should be injected?, How does the standard estimation processing handle adversary injections?

This work seeks to answer these questions and builds a framework that establishes a set of rules and objectives from both the viewpoint of the adversary and the network. First adversary methods for injecting false information into a network are described. Modeling the adversary is discussed, where the strength of the adversary is defined. The competing nature of the adversary-network strategies is explored.

2.3.1. Assumptions: Adversary Modeling

Due to the mobile nature of the wireless sensor networks, not only are the signal transmissions susceptible to tampering but the sensors themselves can also be physically compromised by an adversary. There are a number of ways in which an adversary can alter the sensor's transmitted signal data, or its location information through injection of false information. Examples of methods for injecting information include: altering the time of flight by inserting physical barriers or holding transmissions, inserting an absorbing barrier for received signal strength (RSS) based methods, and altering hop counts both directly and indirectly during the conversion of hop count to distance by jamming or changing transmission power [39]. In this work, it is assumed that the adversary has a means for injecting false data into the network.

Modeling the adversary's strength is an important design consideration. If the adversary is too strong, then it can completely overwhelm the network, making parameter estimation irrelevant. Further, strong adversary models are likely to be highly detectable to the estimation network and subject to resource constraints. An adversary may for example, have time limitations to perform the injection or limits on the reachable sensors that can be compromised due to physical barriers. Practically, it is likely that the adversary would face these obstacles simultaneously. To balance these trade-offs, we consider two limited adversary models: (1) spatial based restrictions and (2) content based restrictions. Under spatial based restrictions, we consider the most restrictive model of a single injection but that the adversary can inject any value into the sensor. Under content based restrictions, we consider that the adversary can corrupt every sensor but can only alter the injection by a small limited amount.

The adversary strategies must carefully consider the strength of its injections, where it must both harm the network and avoid detection by the locating network. This delicate balance can be considered from both the viewpoint of the adversary and the locating network. From the network's viewpoint, the worst case scenario is that of a "naive network" where the network is unaware an adversary is present and performs its estimation regardless, allowing the adversary to have maximum impact. As a first step towards network resilience, the network can employ an adversary detector such that if it detects an adversary, the estimation can be repeated at a later time when the adversary is no longer present or it may be able to add additional trusted sensors to decrease the relative percentage of corrupt nodes. For maximum network resilience, the network's goal is to perform its estimation task despite adversary injections ideally without suffering any degradation in accuracy.

2.4. Contribution

The overarching goal of this work is to provide a comprehensive examination of estimating emitter location in the presence of an intelligent adversary. Figure 1 shows both ends of the spectrum where the red arrow represents increasing adversary impact and the blue arrow represents increasing network resilience. Moving from left to right, are the strategies that are most resilient to an adversary (or have minimal adversary impact) and progress to those strategies that cause maximal harm to the network (or have minimal network resilience). Strategies from both the viewpoints of the adversary and network are developed to see which side really has the upper hand.

An overview of the key contributions of this thesis is given below by considering both ends of the spectrum, in terms of *Maximum Adversary Impact* and *Maximum Network Resilience*.

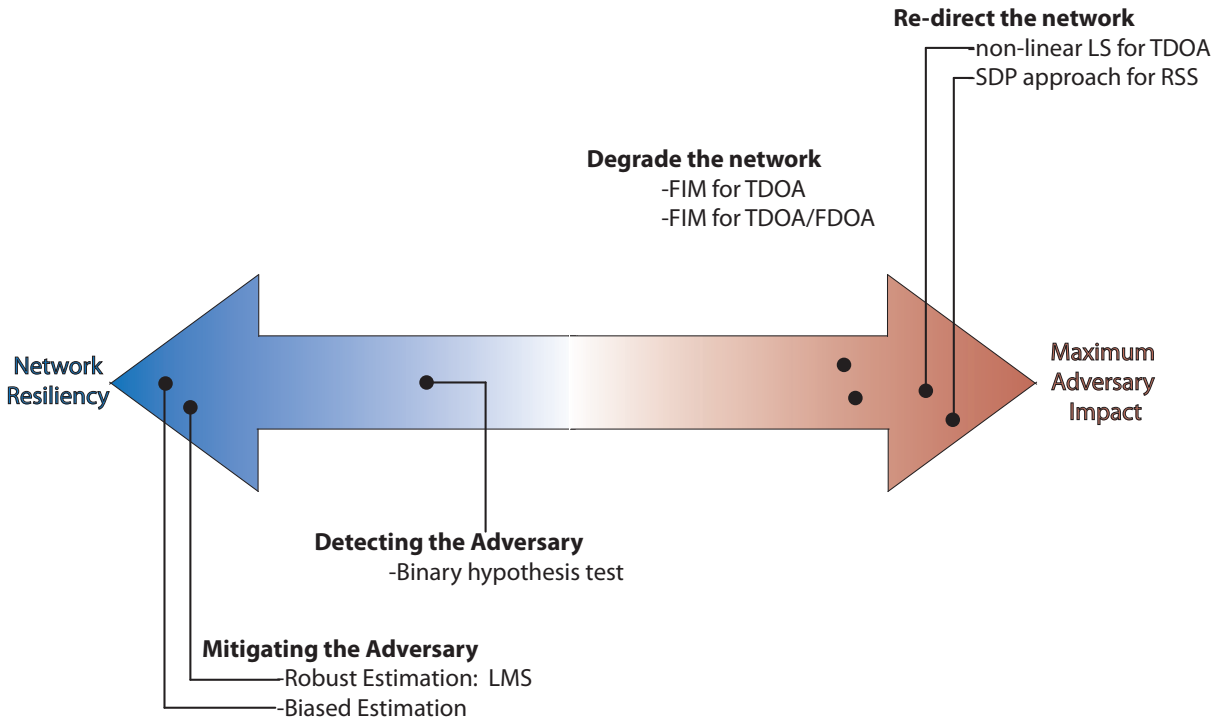


Figure 1: Overview of Adversary - Network Strategies

Maximum Adversary Impact: Adversary's Viewpoint

- **Degrading the Location Network's Accuracy:** We develop new adversary methods that degrade accuracy using the determinant of the Fisher Information as the distortion criteria.
  - A new method for adversary injection is developed where the false sensor position that should be injected is determined for networks using the highly accurate TDOA/FDOA method. We show that the network's location accuracy is significantly reduced independent of sensor-emitter geometry. *[L. Huie and M. Fowler, Emitter Location in the Presence of Information Injection, in the Proceedings of Conference on Information Science and Systems (CISS), 2010.]*
  - A new method is developed for degrading accuracy in stationary networks. We find a closed form solution for the false sensor position by exploiting semidefinite programming. It is shown that the adversary can remove the effect of a single sensor pair. The adversary achieves maximum impact in scenarios where the pair that contributes the most to the FIM is corrupted and when the number of sensors is small. *[L. Huie and M. Fowler, A Closed Form for False Location Injection under Time Difference of Arrival, in the Asilomar Conference on Signals, Systems, and Computers, 2010.]*
- **Redirecting the Estimate:** We develop a set of adversary strategies for redirecting the emitter location estimate a specified distance away from its true value. We develop a power limited adversary model under two types of restrictions: (1) spatial and (2) content.
  - *Spatial restriction:* For a single false sensor position injection, we show the emitter location estimate can be redirected away from its true value. The effectiveness of our strategy is shown for networks under a variety of estimation methods. *[L. M. Huie and M. Fowler, Biasing emitter*

location estimates via false location injection, in IEEE Workshop on Statistical Signal Processing (SSP), 2011]

– *Content restriction:* A bounded adversary is considered where the adversary is able to inject every sensor by a limited amount. We formulate the adversary's injection problem as a semidefinite program (SDP), where we introduce constraints on the allowable sensor displacement by the adversary. The resulting SDP is convex and has a global optimum solution.

Maximum Network Resiliency: Network's Viewpoint

- **Detecting the Adversary:** We derive a detection statistic to determine whether or not an adversary is present for the developed adversary strategies. We show the trade-off between the adversary's probability of detection and the strength of its injection using the receiver operating characteristic performance.
- **Mitigating the Adversary:** We develop strategies that mitigate the adversary's impact on the locating network. We show that the effectiveness of a locating network using non-linear least squares (LS) or least median squares (LMS) is dependent on the strength of the adversary and SNR. We show this relationship and provide direction on when each method is most appropriate. We derive two biased estimators under the TDOA method that hold under any sensor pairing scheme and reduce the MSE. The biased estimators exhibit the largest performance benefit in cases of low SNR.

2.5. Overview

Chapter 3.0. begins by providing a background on parameter estimation and describes the general problem of localization. Chapter 4.0. develops adversary strategies to degrade the network and explores how the adversary can degrade the network's location accuracy by minimizing the Fisher Information Matrix. Specifically, we focus on both TDOA and TDOA/FDOA localization methods [24, 25]. Chapter 5.0. designs adversary strategies to redirect the network's location estimate to some other location [23]. Both spatial and content restricted adversary models are considered. Chapter 6.0. considers network strategies to detect and mitigate the adversary. First an adversary detector is derived under the TDOA method and its effectiveness against both adversary strategies to: degrade and redirect the network is evaluated. Next, strategies to mitigate the effect of the adversary are explored using robust and biased estimation. Chapter 7.0. presents conclusions and areas for future work.

3.0. Estimating Location

This work considers the problem of parameter estimation where the unknown parameter of interest is the emitter location. The chapter begins by describing the general parameter estimation problem. Next the problem of emitter location is introduced and the data measurement model is described. We proceed by describing the design and use of an unbiased estimator to estimate location and show how to assess its performance using the Cramer Rao Lower Bound.

3.1. Parameter Estimation

The estimation of an unknown parameter is a core signal processing task with application across a wide variety of fields including communication, seismology, speech, and image analysis [30]. Given a collection of sensed measurements the goal is to estimate the parameters of interest. If the parameters of interest are deterministic and unknown, the problem is referred to as classical estimation. In the case that the parameters are random, it is called Bayesian estimation. Key to the design of a good estimator is how well the particular data set, which is a function of the unknown parameter can be represented in terms of probability density functions (pdfs). If the data does not match the mathematical model, then one cannot expect to obtain a good estimator.

Estimators can be divided into two broad categories: unbiased and biased. Unbiased estimators will on average, find the true value of the unknown parameter. Alternatively, a biased estimator allows for a reduction in variance through the introduction of a bias. Once an estimator is determined, it is important to assess its performance. A benchmark for assessing the performance of an estimator is the Cramer Rao Lower Bound (CRLB).

In this chapter, we focus on the development of unbiased estimators for emitter location. The use of biased estimators for emitter location will be discussed in Chapter 6.0.. The problem of estimating emitter location is introduced.

3.2. Location Estimation

A collection of N sensors is used to estimate the location of a stationary emitter located at $\mathbf{e} = [e_x \; e_y]$. The localization problem is generally a two-step process. The sensors first make measurements on an intermediate localization parameter such as delay, angle or signal strength. Then the measurements are combined through the design of an estimator to determine a single estimate of location, which is a function of the measured data.

3.2.1. Locating Methods

There exists a number of localization methods such as angle of arrival (AOA), received signal strength (RSS), time of arrival (TOA), and time difference of arrival (TDOA). A comparison of existing localization techniques can be found in [17, 52].

Under the Angle of Arrival method, the angle between sensors is used to determine the distance between nodes. AOA requires antenna arrays with a minimum distance spacing, requiring a larger node footprint. Performance suffers in the presence of multipath, non-line of sight (NLOS) conditions, and is sensitive to array precision.

The RSS method determines the distance between nodes by measuring the signal attenuation from the transmitter to each receiver. This method requires an accurate model of the channel pathloss. The simplicity of a RSS based location approach is attractive due to its simplicity as special hardware is not required. However, it comes at the cost of accuracy especially in the presence of noise, interference, and channel fades. As a result, this method is typically used for coarse position estimation.

Under the TOA method, each receiver obtains a time delayed version of the original transmitted signal. The delays from all receivers are then used to estimate location. As a result, perfect synchronization between the transmitter and each of the receivers is required. A TOA approach is therefore commonly used in cellular networks where specialized timing and synchronization hardware is deployed and controlled.

Table 1: Comparison of Localization Methods

Localization Method	**Trade-offs**
RSS	Simple implementation but sensitive to inaccurate channel modeling, interference, fading
AOA	Minimum distance spacing, sensitive to multipath, NLOS, and array positioning
TOA	Requires perfect synchronization between the source and each receiver
TDOA	Requires perfect synchronization between receivers
FDOA	Adds complexity but provides an increase in accuracy for mobile sensors

The Time Difference of Arrival (TDOA) method requires that all the sensors be paired. Each sensor receives a time delayed version of the transmitted message. One of the sensors in each pair transmits its measurement to its paired sensor. An estimate of the delay is determined by cross correlation. The TDOA method eliminates the need for synchronization between the transmitter and only requires that the receivers are synchronized. As a result, the TDOA method provides greater flexibility while maintaining the benefit of high accuracy. For these reasons, TDOA is widely used in wireless sensor networks both due to its greater flexibility over methods like TOA, and greater accuracy over RSS and AOA. Further TDOA methods can be augmented by additionally applying the frequency difference of arrival (FDOA) method to increase accuracy [20], which is typical for networks with non-stationary sensors.

A summary of the trade-offs of each method is given in Table 1.

3.2.2. Measurement Model

Once the sensors make their measurements on the intermediate localization parameter, they are transmitted along with the sensor positioning information to a fusion center. The fusion center processes these measurements and determines an estimate of the emitter's geographic location $\hat{\mathbf{e}}$. In the most general form, the noisy localization measurements from all sensors are given by

$$\mathbf{x} = \mathbf{s}(\mathbf{e}) + \mathbf{n} \tag{1}$$

where $\mathbf{s}$ is the true value of the localization parameters or "signals", parameterized by the emitter location $\mathbf{e}$, and $\mathbf{n}$ is the additive Gaussian noise. Given the noisy measurements, an estimate $\hat{\mathbf{e}}(\mathbf{x})$ is determined, where its functional dependence on the collected data is specified. Since the estimator $\hat{\mathbf{e}}(\mathbf{x})$, is a random variable it is of interest to not only determine the estimator value, which is specific to the data set, but to also quantify the accuracy of the estimator. Next, different types of estimators are discussed. Then the Cramer Rao Lower Bound is explored as a benchmark on estimator performance.

3.2.3. Types of Estimators

In general, the Minimum Variance Unbiased Estimator (MVUE) may not exist or may be difficult to obtain. Fortunately, in such cases, one can use the Maximum Likelihood Estimator (MLE). The MLE for a vector is the value that maximizes the likelihood function $p(\mathbf{x};\mathbf{e})$ over all possible values of $\mathbf{e}$. A very useful property of the MLE is its asymptotic behavior. For large data sizes, the MLE is asymptotically distributed as

$$\hat{\mathbf{e}} \overset{a}{\sim} \mathcal{N}\left(\mathbf{e},\ \mathbf{J}^{-1}(\mathbf{e})\right). \tag{2}$$

The MLE is a useful practical estimator as it can be easily computed given the pdf $p(\mathbf{x};\mathbf{e})$. Even if a closed form does not exist, it can be obtained numerically using a grid search or by iterative approaches like Newton Raphson.

In cases where the pdf is unknown and the signal is deterministic, the least squares estimator (LSE) can be used. The LSE minimizes the squared difference between the data and the assumed signal i.e.

$$\hat{\mathbf{e}} = \min_{\tilde{\mathbf{e}}} ||\mathbf{x} - \mathbf{s}(\tilde{\mathbf{e}})||^2 \tag{3}$$

In the case of Gaussian noise, the LSE and MLE give the same solution. If the location parameter $\mathbf{s}(\tilde{\mathbf{e}})$ is a non-linear function of $\tilde{\mathbf{e}}$, then the MLE must be found numerically. The Gauss-Newton method [30] can be used to iteratively find the LS solution where non-linear LS is typically used to estimate location [62].

3.2.4. Estimator Accuracy

As with any estimation problem, it is of interest to determine bounds on the maximum accuracy attainable by the estimator. The Cramer Rao Lower Bound (CRLB) is the performance benchmark for unbiased estimators [30]. An unbiased estimator that achieves the CRLB is the Minimum Variance Unbiased Estimator. The CRLB gives a lower bound on the variance of unbiased estimators provided the following regularity condition is satisfied

$$E\left[\frac{\partial \ln p(\mathbf{x};\mathbf{e})}{\partial \mathbf{e}}\right] = 0 \quad \forall\ \mathbf{e}. \tag{4}$$

Thus, the variance is bounded by the CRLB,

$$\mathrm{var}(\hat{\mathbf{e}}) \geq \frac{1}{-E\left[\frac{\partial^2 \ln p(\mathbf{x};\mathbf{e})}{\partial^2 \mathbf{e}}\right]} \tag{5}$$

where the denominator is the Fisher Information. The FIM and the CRLB matrices are inversely related [30].

For the general Gaussian case of $\mathbf{x} = \mathbf{s}(\mathbf{e}) + \mathbf{n}$ where $\mathbf{x} \sim \mathcal{N}(\boldsymbol{\mu}(\mathbf{e}), \mathbf{C}(\mathbf{e}))$, the Fisher Information is given by

$$[\mathbf{J}(\mathbf{e})]_{i,j} = \left[\frac{\partial \boldsymbol{\mu}(\mathbf{e})}{\partial \mathbf{e}_i}\right]^T \mathbf{C}^{-1}(\mathbf{e}) \left[\frac{\partial \boldsymbol{\mu}(\mathbf{e})}{\partial \mathbf{e}_i}\right] + \frac{1}{2}\mathrm{tr}\left\{\mathbf{C}^{-1}(\mathbf{e}) \frac{\partial \mathbf{C}(\mathbf{e})}{\partial \mathbf{e}_i} \mathbf{C}^{-1}(\mathbf{e}) \frac{\partial \mathbf{C}(\mathbf{e})}{\partial \mathbf{e}_j}\right\} \tag{6}$$

In source localization, the unknown parameter is deterministic. Thus, the second term in (6) is zero.

3.2.5. Utility of the Fisher Information Matrix

The Fisher Information Matrix (FIM) plays a key role in a wide range of parameter estimation tasks in which the geometry of the sensor network is of particular importance. In the context of emitter location estimation, the FIM is preferred over other distortion measures, such as mean squared error, due to its ability to intrinsically capture the geometry of the sensor-emitter geometry [6, 15, 22]. Highly accurate location estimates can be achieved when the FIM is maximized, where more information is better. As a result, a number of applications seek formulations that maximize the FIM. For example, optimal sensor placement has been considered for various applications in [28, 63] where the determinant of the FIM is maximized. The FIM has also been used for other applications such as sensor pairing [22], fault tolerant vehicle guidance [65], and bit allocation [6]. In [6], the trace of the FIM is maximized to find the optimal bit allocation for data compression. The trace of the FIM is maximized in [22] to find the best sensor pairings for location estimation.

The Fisher Information Matrix is a useful distortion criteria for emitter location. To gain insight into how the location error is oriented in the x-y plane, an error ellipse interpretation of the FIM can be used [13]. Figure 2 provides a notional illustration of the error ellipse with overlaid emitter location estimates. By defining the error $\boldsymbol{\epsilon} = \mathbf{e} - \hat{\mathbf{e}}$, the error ellipse is given by $\boldsymbol{\epsilon}^T \mathbf{J} \boldsymbol{\epsilon} = k$ where $k = -2\ln(1 - P_e)$ and $0 \leq P_e \leq 1$. The error vector falls within this ellipse with probability P_e. The eigenvectors of the FIM dictate the major and minor axes of the error ellipse and the reciprocal square roots of the eigenvalues dictate the lengths of the axes as shown in Figure 2. For example, the 95% error ellipse specifies that 95% of the location estimates lie within the ellipse.

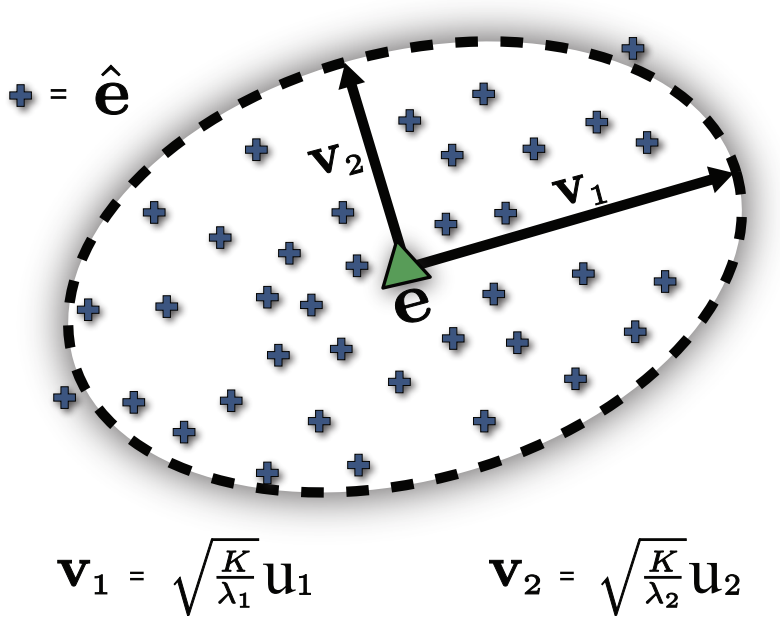


Figure 2: Error ellipse interpretation of the FIM.

3.3. The FIM for Adversary Modeling

The error ellipse interpretation of the FIM leads to two fundamentally different adversary strategies. First, we consider an adversary that seeks to minimize the network's accuracy. Chapter 4.0. explores degrading the network's accuracy by minimizing the FIM, which is equivalent to maximizing the error ellipse as shown in red in Figure 3(a). In Chapter 5.0. a different strategy is considered where the adversary's goal is to move an emitter location estimate a specified distance away from its true value as shown in Figure 3(b).

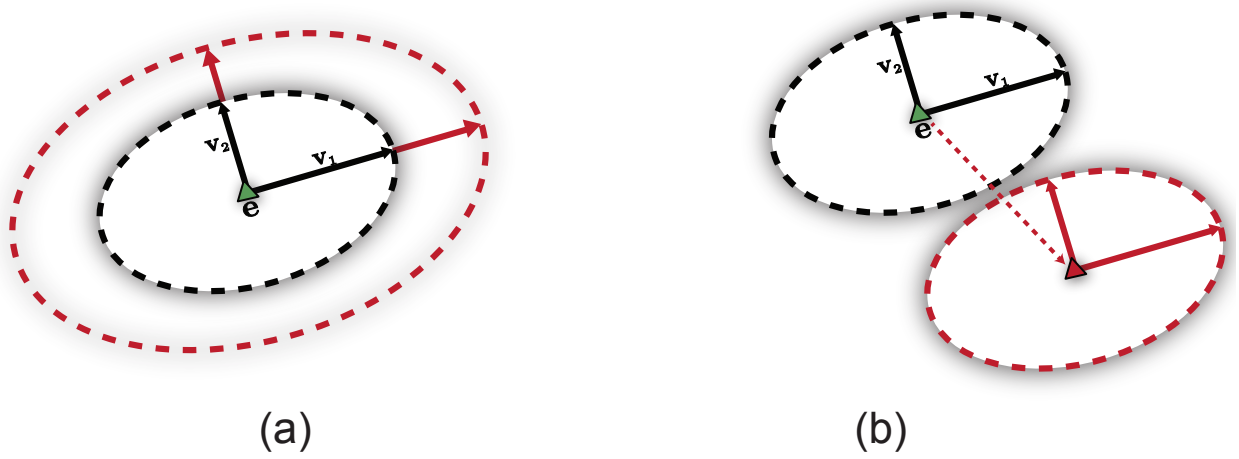


Figure 3: Adversary strategies motivated by the error ellipse: (a) degrades the FIM (b) redirects the estimate

This work considers that the adversary can inject false information into the network, more specifically

that the sensors' positions are corrupted. The adversary strategies will determine what false information should be injected while the network strategies will determine how to detect and mitigate these injections. The effect of an adversary's injection on both the FIM and on the non-linear LS estimate will be explored in more detail in Chapters 4.0. and 5.0.. Figure 4 shows the input parameters that a network uses for location processing, both to determine the FIM, and the LS emitter location estimate. In the presence of an adversary, some of the sensors' positions may be compromised as highlighted in red.

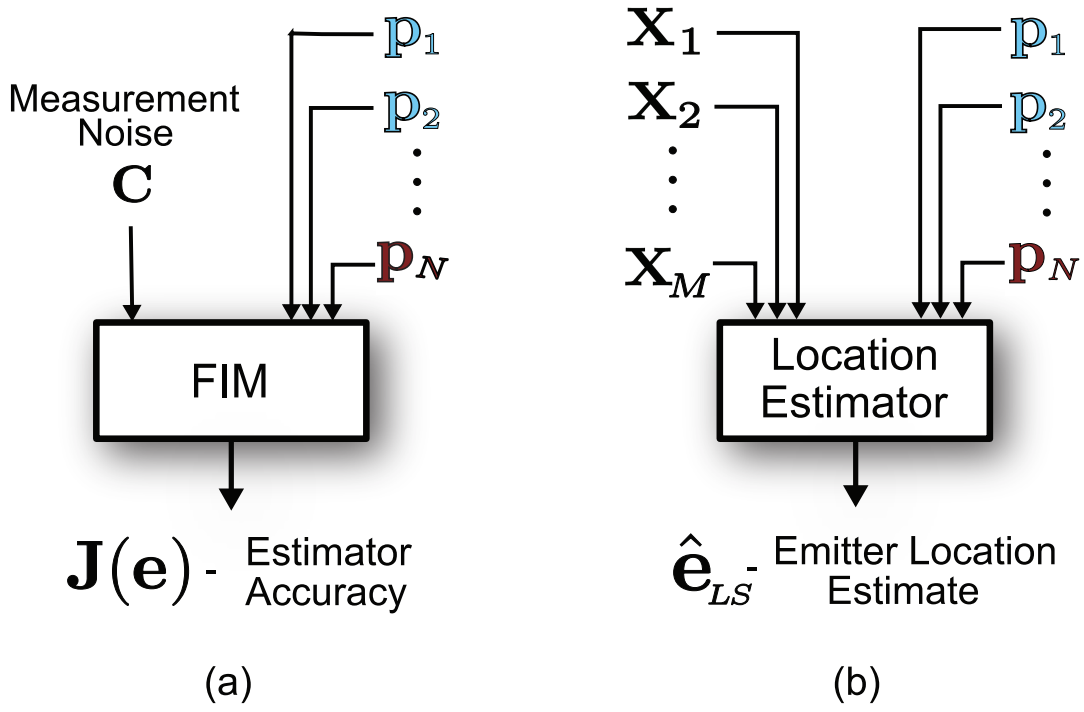


Figure 4: Location processing with false sensor position reports (shown in red).

4.0. Methods: Adversary Strategies to Degrade the Network

This chapter considers the viewpoint of the adversary and designs strategies to degrade the locating network. The strategies are motivated by the error ellipse interpretation of the Fisher Information Matrix where the network's location accuracy is minimized (or equivalently its error ellipse is maximized) as shown in Figure 5(a). First, the worst case scenario for the adversary is considered where the network employs the highly accurate TDOA/FDOA method. Then, the case of stationary sensors is explored under the TDOA method, which is particularly vulnerable to compromise by the adversary. Figure 5(b) shows the input parameters required by the network to determine its FIM where the adversary injects a false sensor position.

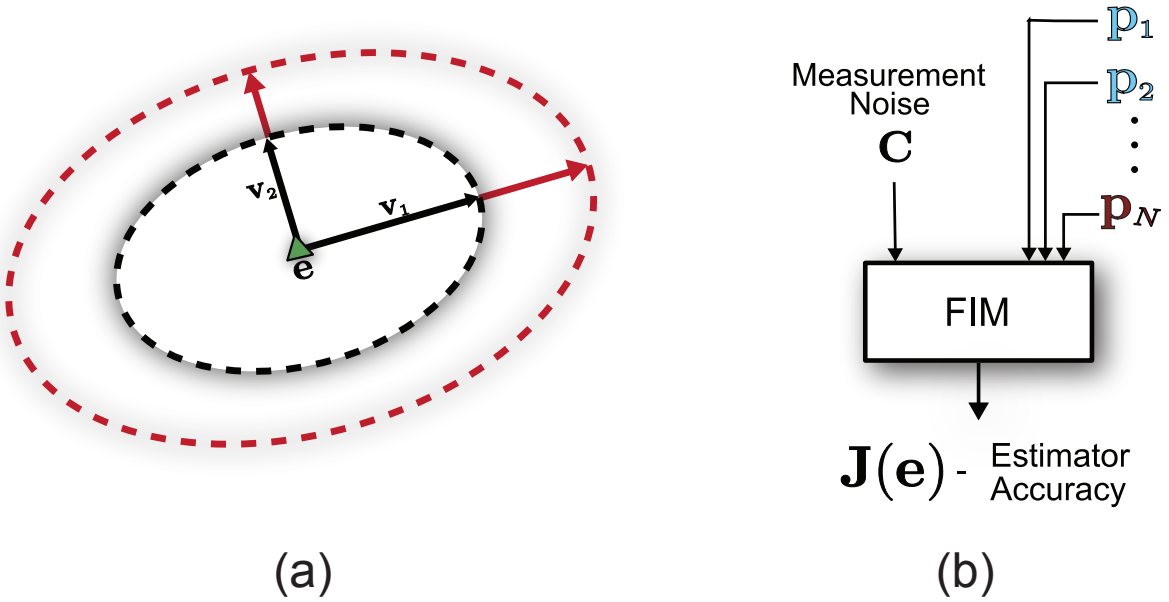


Figure 5: An adversary degrades the FIM.

We consider that the adversary seeks a pessimistic assessment and minimizes the network's best case performance. More specifically, we consider that the adversary minimizes the FIM evaluated at the true value of emitter location. The FIM computed using an estimate will provide less information about the emitter as compared with that calculated using the true value of emitter location. Therefore, by minimizing the FIM computed with the true emitter location, the adversary minimizes the network's best case (largest possible) FIM, which is the worst case scenario from the adversary's viewpoint.

A number of different functions of the FIM can be minimized, where the two primary choices are the determinant and the trace. For optimal sensor placement, the determinant of the FIM was maximized in [28, 63]. The trace of the FIM was used due to its computational simplicity [64]. However, in [51] it was shown that using the trace of the FIM resulted in a different solution than with the optimal sensor configuration obtained by maximizing the determinant. Thus, we consider the determinant of the FIM as our objective function.

4.1. Minimizing the FIM under TDOA/FDOA

The main contribution of this section is the development of an adversary strategy for minimizing the location accuracy under the time and frequency difference of arrival (TDOA/FDOA) method. The injection problem

is formulated as the minimization of the determinant of the Fisher Information Matrix (FIM). The false sensor position to inject is determined. We show that it significantly reduces the accuracy of the emitter location estimate independent of the sensor-emitter geometry.

4.1.1. Time and Frequency Difference of Arrival Method

TDOA/FDOA methods [60, 62] are commonly used for emitter location. This section describes the system model for estimating location under the time and frequency difference of arrival method. Given a collection of N sensors the location of a stationary emitter, $\mathbf{e}$ is sought. The sensors are paired apriori into $m = 1, ..., M = \frac{N}{2}$ pairs such that no pair shares a common sensor. The sensors are assumed to have a constant velocity. The actual TDOA and FDOA of the m^{th} sensor pair are given by

$$\tau_m = \frac{1}{c}\left(||\mathbf{p}_i - \mathbf{e}|| - ||\mathbf{p}_j - \mathbf{e}||\right) \tag{7}$$

$$\omega_m = \frac{f_e}{c}\left(\frac{(\mathbf{p}_i - \mathbf{e})^T \dot{\mathbf{p}}_i}{||\mathbf{p}_i - \mathbf{e}||} - \frac{(\mathbf{p}_j - \mathbf{e})^T \dot{\mathbf{p}}_j}{||\mathbf{p}_j - \mathbf{e}||}\right) \tag{8}$$

where sensors i and j are paired, and $\mathbf{p}_i$, $\mathbf{p}_j$ and $\dot{\mathbf{p}}_i$, $\dot{\mathbf{p}}_j$ are the x-y positions and velocities of sensors i and j, respectively. The frequency of the emitter is f_e and c is the speed of light.

Each sensor pair makes a TDOA/FDOA estimate, $\hat{\boldsymbol{\theta}}_m = [\hat{\tau}_m \;\; \hat{\omega}_m]^T$ by cross correlating their measured signal data. Typically, the signal data will be transferred from one sensor in the pair to the other over a data link. The noisy measurements are modeled by additive estimation errors

$$\hat{\boldsymbol{\theta}}_m = \begin{bmatrix} \hat{\tau}_m \\ \hat{\omega}_m \end{bmatrix} = \begin{bmatrix} \tau_m \\ \omega_m \end{bmatrix} + \begin{bmatrix} \Delta_{\tau_m} \\ \Delta_{\omega_m} \end{bmatrix} \quad \forall\, m \tag{9}$$

where Δ_{τ_m} and Δ_{ω_m} are the random TDOA and FDOA measurement errors of the m^{th} pair, respectively. The TDOA/FDOA measurements are obtained using the Maximum Likelihood (ML) estimator [60]. From the asymptotic properties of the ML estimator [30], the distribution of $[\Delta_{\tau_m} \;\; \Delta_{\omega_m}]^T$ is zero-mean Gaussian with covariance matrix $\mathbf{C}_m$ for $m = 1, ..., M$.

In order to assess the location accuracy the FIM [30] is used as the distortion criteria where more information is better [22] and is given by

$$\mathbf{J} = \mathbf{H}^T \mathbf{C}^{-1} \mathbf{H} \tag{10}$$

$$= \sum_{m=1}^{M} \mathbf{H}_m^T \mathbf{C}_m^{-1} \mathbf{H}_m \tag{11}$$

where $\mathbf{H} = [\mathbf{H}_1; \ldots; \mathbf{H}_M]$ is the Jacobian of the TDOA/FDOA with respect to the emitter location and $\mathbf{C} = diag\{\mathbf{C}_1 \ldots \mathbf{C}_M\}$ is the covariance matrix of the noise process that corrupts the TDOA/FDOA measurements. The Jacobian of the m^{th} pair is the derivative of the m^{th} pair's TDOA/FDOA with respect to the emitter location and is given by

$$\mathbf{H}_m = \frac{\partial \boldsymbol{\theta}_m}{\partial \mathbf{e}} = \begin{bmatrix} \frac{\partial}{\partial \mathbf{e}}(\tau_m) \\ \\ \frac{\partial}{\partial \mathbf{e}}(\omega_m) \end{bmatrix} \tag{12}$$

where

$$\frac{\partial(\tau_m)}{\partial \mathbf{e}} = \frac{1}{c}\left[\frac{\mathbf{p}_i - \mathbf{e}}{||\mathbf{p}_i - \mathbf{e}||} - \frac{\mathbf{p}_j - \mathbf{e}}{||\mathbf{p}_j - \mathbf{e}||}\right]^T \tag{13}$$

$$\begin{aligned}\frac{\partial(\omega_m)}{\partial \mathbf{e}} &= \frac{f_e}{c}\left[\frac{[\mathbf{p}_i - \mathbf{e}]^T \dot{\mathbf{p}}_i [\mathbf{p}_i - \mathbf{e}]^T}{||\mathbf{p}_i - \mathbf{e}||^3} - \frac{\dot{\mathbf{p}}_i^T}{||\mathbf{p}_i - \mathbf{e}||}\right] \\ &- \frac{f_e}{c}\left[\frac{[\mathbf{p}_j - \mathbf{e}]^T \dot{\mathbf{p}}_j [\mathbf{p}_j - \mathbf{e}]^T}{||\mathbf{p}_j - \mathbf{e}||^3} - \frac{\dot{\mathbf{p}}_j^T}{||\mathbf{p}_j - \mathbf{e}||}\right].\end{aligned} \tag{14}$$

The FIM is a function of the noise covariance matrix, and the Jacobian, which is a function of the sensors' positions and the true emitter location. The locating network does not know the true emitter location but can evaluate the FIM by estimating the location from a small amount of initially shared data or from a coarse location estimate from a cueing sensor system [22].

In order to gain insights into the geometric aspects of this problem, we specify an ellipse that shows how the location error is oriented in the x-y plane as in [14]. The ellipse interpretation of the FIM is used where the eigenvectors dictate the major and minor axes of the error ellipse and the reciprocal square roots of the eigenvalues dictate the lengths of the axes. Further, the error ellipse can be decomposed into a set of ellipses, where each ellipse represents an individual sensor pair's contribution. This geometric interpretation is shown in Figure 6 for a specific sensor-emitter geometry. In Figure 6, two pairs of sensors seek to locate the emitter where the error ellipses of each pair's contribution are shown in blue (Pair 1) and black (Pair 2). Geometrically, the total resultant error ellipse $\mathbf{J}^{-1}$ is the ellipse inscribed in the intersection of the two individual pairs' ellipses as shown in red. Thus, for a highly accurate location estimate, the total resultant error ellipse should be small and correspond to a large FIM. Conversely, if the goal is to decrease accuracy, the false sensor position should result in a large error ellipse indicating less Fisher Information. With this motivation we now formulate our information injection problem.

4.1.2. Problem Formulation

Geometrically, the adversary's goal is to maximize the total resultant error ellipse, or similarly the partial ellipses due to the true and false pairs should have the largest intersection possible. As a result, minimizing the area of the ellipse is an intuitive choice for the objective function. Therefore, we choose the determinant of the FIM as it measures the area of an ellipse [6]. The false sensor position that should be injected which minimizes the location network's FIM is given by

$$\min_{\mathbf{p}_f} \quad \det\{\mathbf{J}\} = \det\left\{\mathbf{H}^T\mathbf{C}^{-1}\mathbf{H}\right\} \tag{15}$$

where the sensor position to be falsified is $\mathbf{p}_f$.

The Jacobian matrix, $\mathbf{H}$ is a function of the false position, $\mathbf{p}_f$. Since only one sensor is falsified, only the corrupt sensor pair's Jacobian matrix changes. To ensure that the non-corrupt pairs' Jacobian matrices do not change, an equality constraint is introduced. Further, since $\mathbf{H}$ is a function of the false position a change of variables is used to minimize the problem over $\mathbf{H}$ instead of $\mathbf{p}_f$. Thus, the problem is reformulated as

$$\min_{\mathbf{H}} \quad \det\left\{\mathbf{H}^T\mathbf{C}^{-1}\mathbf{H}\right\} \tag{16}$$

$$\text{s.t.} \quad \mathbf{DH} = \mathbf{E} \tag{17}$$

where both $\mathbf{D}$ and $\mathbf{E}$ are constant matrices specifying the fixed entries of $\mathbf{H}$. We solve for the problem in (16)-(17) numerically using a grid-based approach.

4.1.3. Numerical Results

The det(**FIM**) is evaluated over a fine grid, except at the actual emitter location where $\mathbf{p}_f = \mathbf{u}$. Figure 7 shows the value of the $\det\left\{\mathbf{H}^T\mathbf{C}^{-1}\mathbf{H}\right\}$ at each grid location on a log scale for the sensor-emitter geometry

in Figure 6. The position with the minimum value of the det(**FIM**) is selected as the false sensor position to be injected. The ten false positions $\mathbf{p}_f$ which yield the smallest values of the det $\left\{\mathbf{H}^T\mathbf{C}^{-1}\mathbf{H}\right\}$ are identified in Figure 7 by an '**x**'.

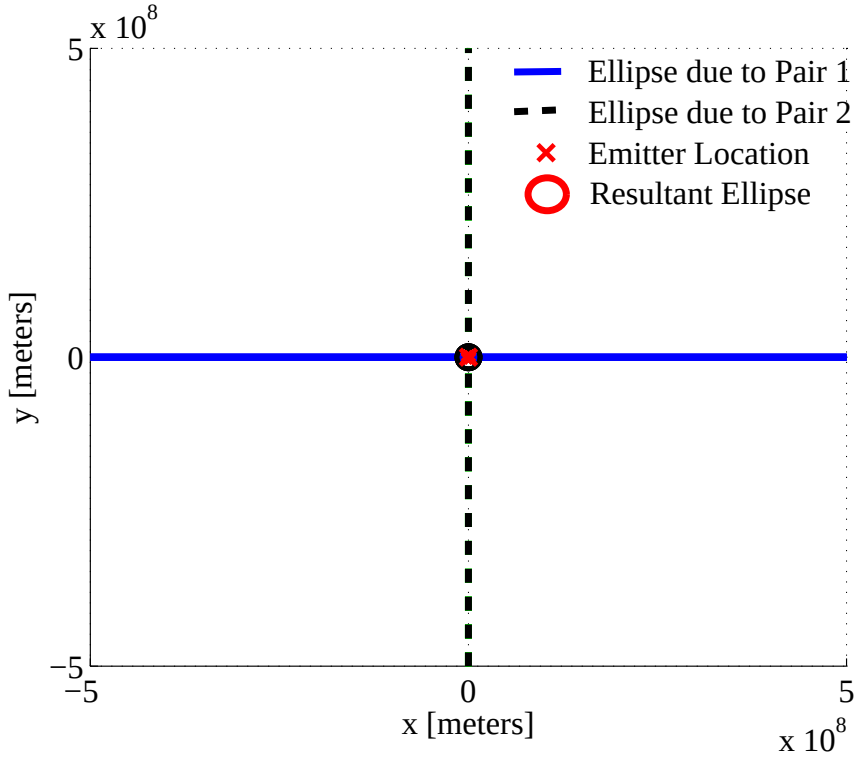
Decreasing Accuracy for a Specific Sensor-Emitter Geometry

The selection of the false sensor position is examined for the sensor-emitter geometry shown in Figure 6. To gain insight into the behavior of the falsified FIM the individual sensor pair's error ellipses are plotted. As shown in Figure 8 the position that minimizes the FIM is the one that maximizes the resultant error ellipse such that the false pair's ellipse has as much area in common with the ellipse of the true pair as possible.

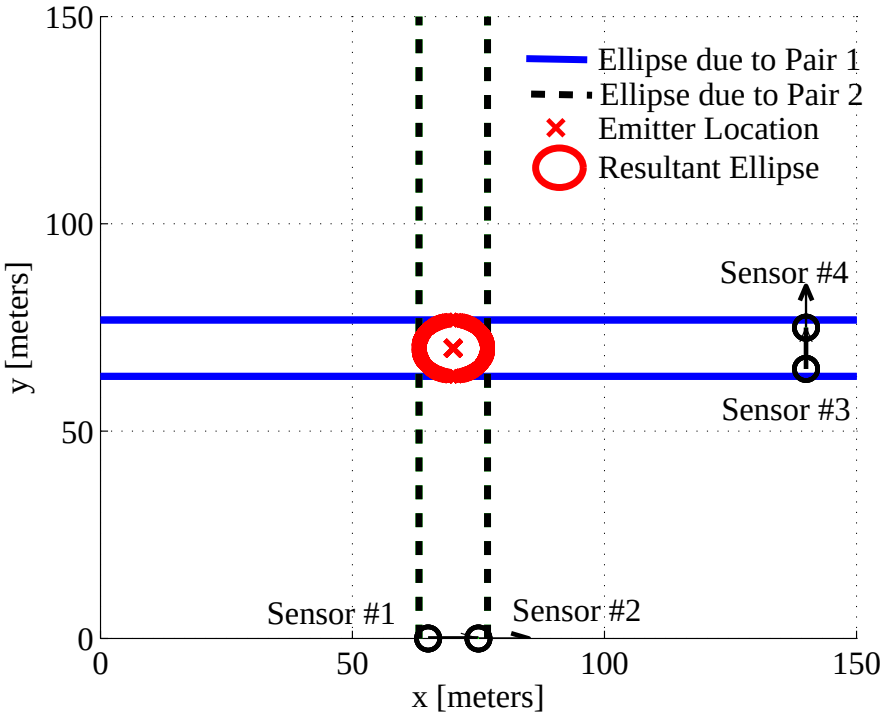
For this geometry, the falsified pair's ellipse aligns with the true pair's ellipse as shown in Figure 8. In Figure 9 the ellipses with and without information injection are overlaid. Observe that the resultant error ellipse under information injection degenerates and approaches a line, while the resultant ellipse without information injection constitutes a smaller area indicating the location accuracy has been substantially decreased.

Decreasing Accuracy across Sensor-Emitter Geometries

Our method is able to decrease emitter location estimation accuracy across sensor-emitter geometries of varying quality as measured by the geometric dilution of precision (GDOP). The GDOP indicates the quality of a particular sensor-emitter geometry and is given by $\frac{\sqrt{trace\{\mathbf{J}\}}}{c\sigma_s}$ where $c\sigma_s$ is the square root of the mean square ranging error [62]. Smaller values of GDOP indicate better location accuracy [68]. The determinant of the FIM is evaluated over a fine grid for 500 random sensor-emitter geometries uniformly generated in a 200m x 200m field, with values of GDOP ≤ 6. For each geometry, the relative percent error between the *det*(**FIM**) with and without false information injection is computed and averaged according to its GDOP value. In Figure 10, the average relative percent error in the *det*(**FIM**) is plotted versus GDOP and shows that our method is able to significantly decrease the location accuracy for both high and low quality geometries.

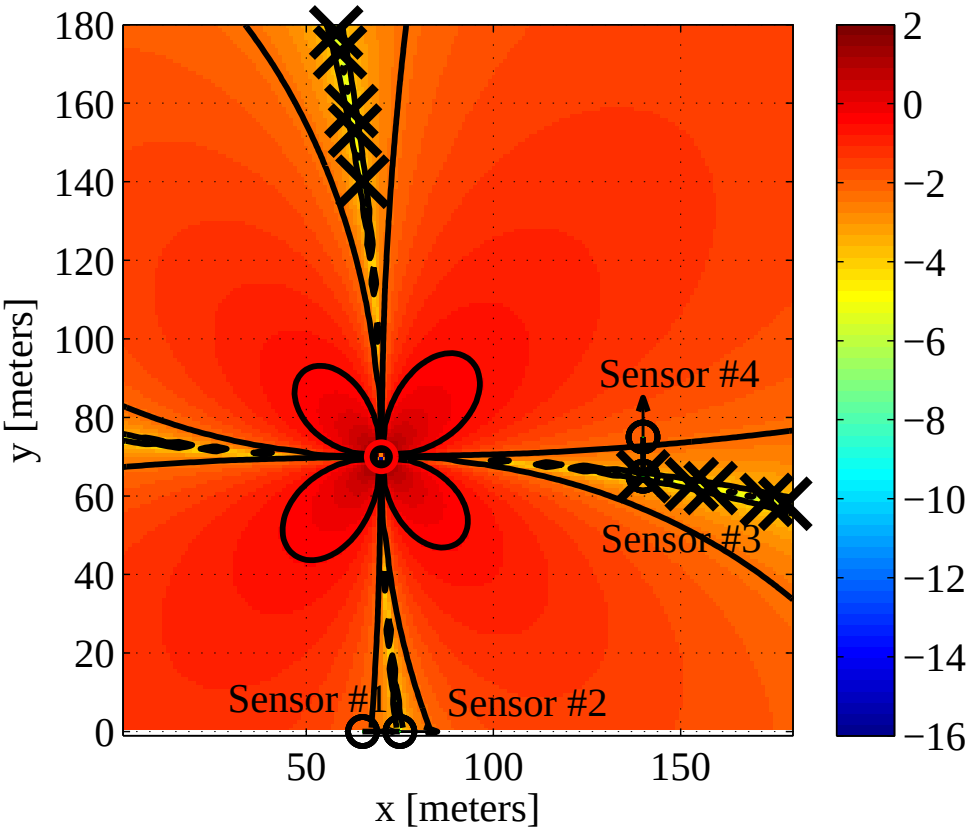


(a) Zoomed Out

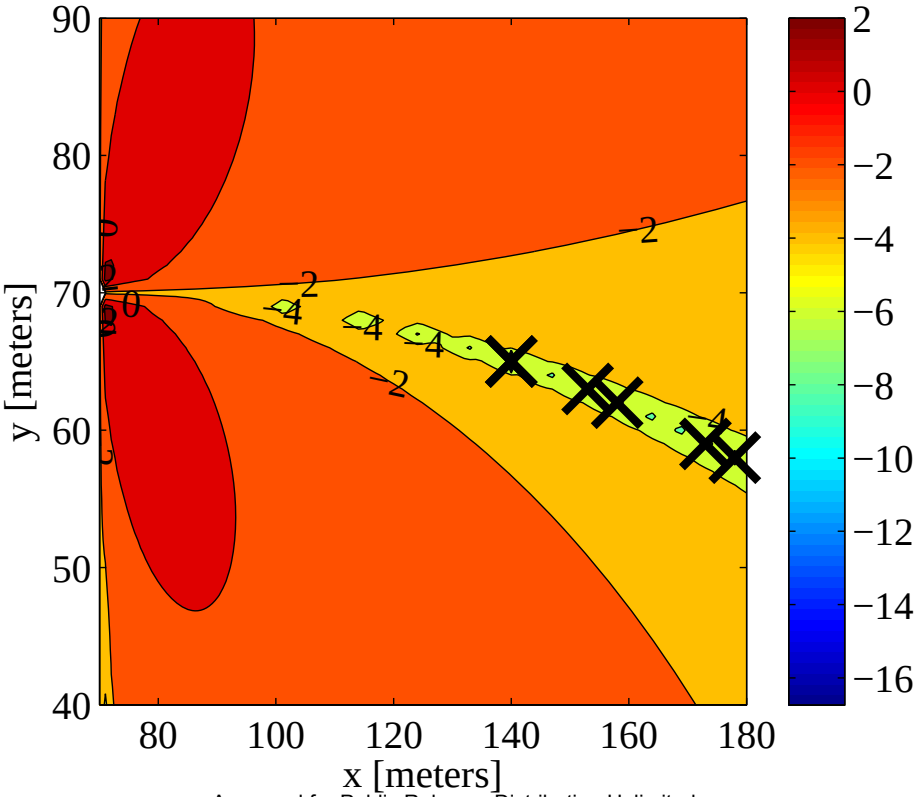


(b) Zoomed In

Figure 6: Ellipse Interpretation: The error ellipses due to Pair 1 (Sensors 1 & 2) and Pair 2 (Sensors 3 & 4) are shown in blue (solid) and black (dashed), respectively. The total resultant error ellipse (red) is inscribed in the intersection. SNR=10dB and $f_e = 3x10^9$.



(a)



(b)

Figure 7: Evaluation of det (**FIM**) over a grid on a log scale. SNR=10dB and $f_e = 3x10^9$ (a) Normal view (b) Close-Up

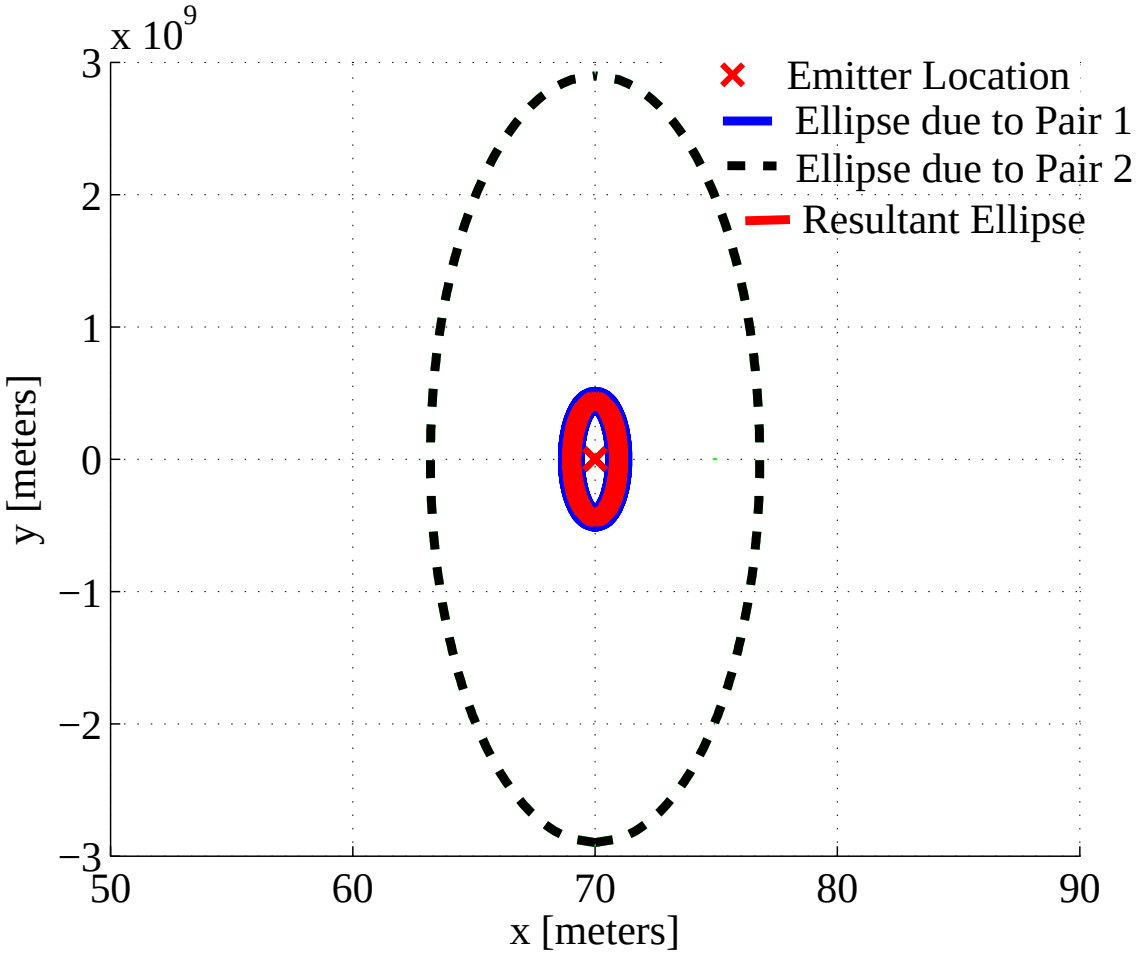


Figure 8: Injecting a false sensor position: Sensor 1 is falsified by injecting the false position [140 65]. The error ellipses due to the false sensor pair (solid blue) and true sensor pair (dashed black) are aligned.

4.2. Minimizing the FIM for TDOA

Unfortunately, minimizing the FIM under the TDOA/FDOA method does not lead to a closed form solution. In this section, we consider minimizing the FIM under the TDOA method. While the TDOA/FDOA method can improve the location accuracy as compared with using TDOA only, a stationary network is perhaps the most vulnerable to an adversary and is deserving of a thorough investigation.

The main contribution of this adversary strategy is the development of a method for degrading network accuracy under TDOA. We develop a closed form solution for the false sensor position. The physical implication of our minimizing accuracy strategy is that the adversary can at most eliminate the contribution of the corrupted sensor pair and as will be seen in Chapter 6.0., does so with no risk of detection by the network.

4.2.1. System Model under Time Difference of Arrival

In a two-dimensional scenario at least two pairs of sensors are needed under the time difference of arrival (TDOA) method. The sensors are paired apriori into $M = \frac{N}{2}$ pairs and no two pairs share a common sensor. Each pair of sensors defines a hyperbola where the foci are the sensor positions [62]. The TDOA of the m^{th} sensor pair is

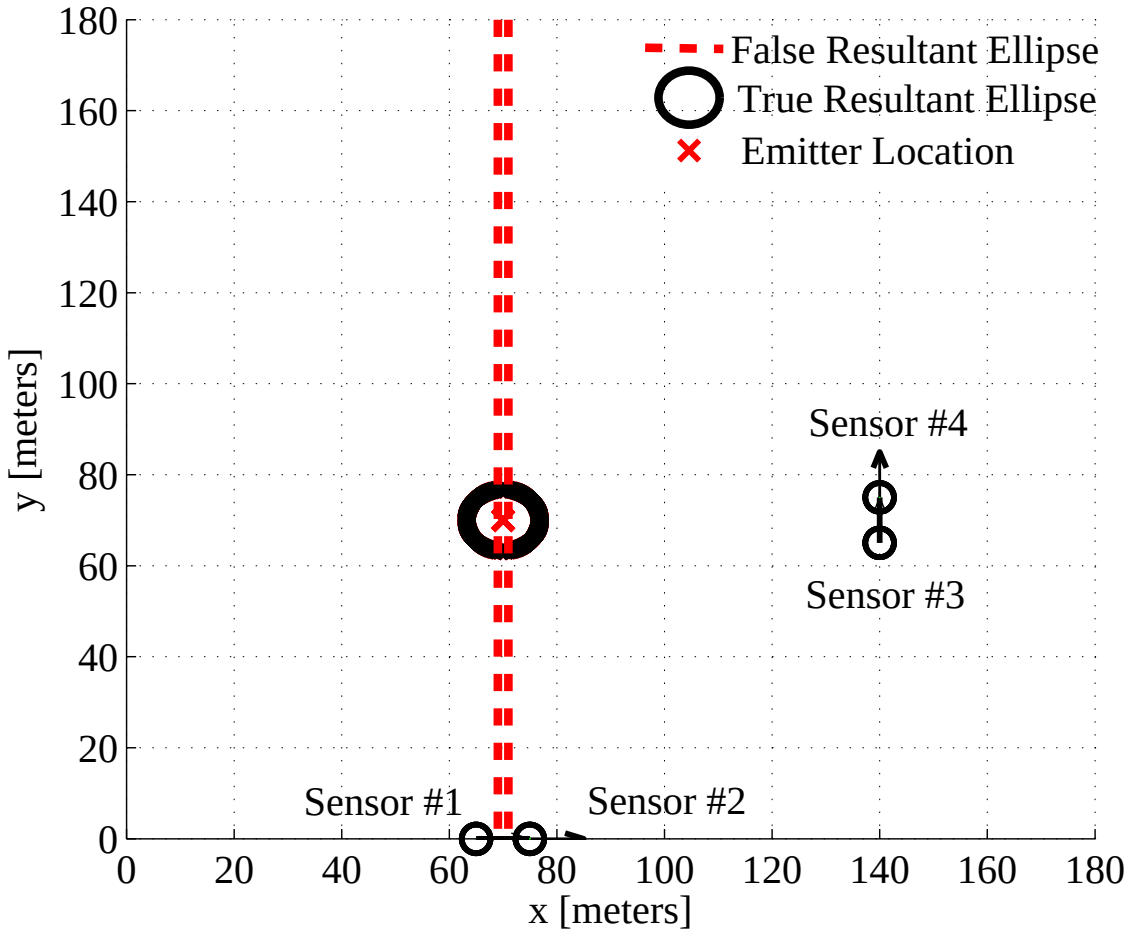


Figure 9: Comparison of the resultant error ellipses with (red dashed) and without (black solid) information injection.

$$\tau_m(\mathbf{e}) = \frac{1}{c}\left(||\mathbf{e}-\mathbf{p}_i|| - ||\mathbf{e}-\mathbf{p}_j||\right) \tag{18}$$

where $\mathbf{p}_i$, $\mathbf{p}_j$ are the positions of sensors i and j of the m^{th} pair, and c is the speed of light.

Each sensor pair makes their TDOA estimate, $\hat{\tau}_m$, by cross correlating their measured signal data. The measurements are corrupted by additive estimation errors

$$\hat{\tau}_m = \tau_m(\mathbf{e}) + n_m \quad m = 1, \ldots, M, \tag{19}$$

where n_m is the m^{th} pair's random TDOA measurement error. The TDOA measurements are obtained using the maximum likelihood (ML) estimator. From the asymptotic properties of the ML estimator [30], the distribution of n_m is taken as zero-mean Gaussian with variance σ_m^2 for $m = 1, ..., M$. All estimated TDOAs and reported sensor positions are sent to a single node for location processing which is assumed not be the corrupted sensor.

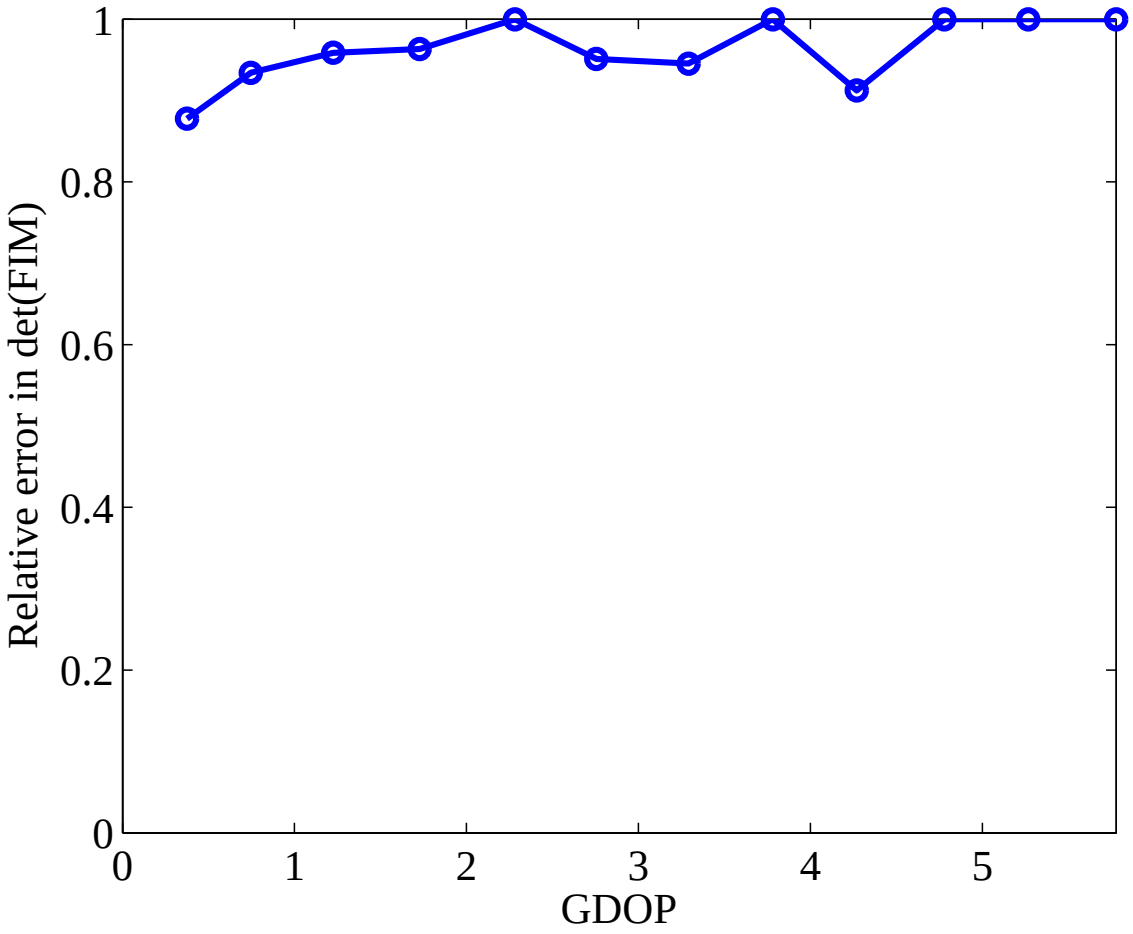


Figure 10: Relative percent error in location accuracy for different geometries with varying GDOP. SNR=10dB, $c\sigma_s = 1$.

4.2.2. Assessing Location Accuracy

The estimated TDOA $\hat{\boldsymbol{\tau}} = \boldsymbol{\tau}(\mathbf{e}) + \mathbf{n}$ is comprised of a deterministic signal vector $\boldsymbol{\tau}(\mathbf{e})$ parameterized by $\mathbf{e}$ and corrupted by Gaussian noise $\mathbf{n}$, with covariance matrix $\mathbf{C}$. The FIM is given by

$$\mathbf{J}(\mathbf{e}) = \frac{\partial \boldsymbol{\tau}(\mathbf{e})^T}{\partial \mathbf{e}} \mathbf{C}^{-1} \frac{\partial \boldsymbol{\tau}(\mathbf{e})}{\partial \mathbf{e}} \tag{20}$$

where $\frac{\partial \boldsymbol{\tau}(\mathbf{e})}{\partial \mathbf{e}} \triangleq \mathbf{H}$ is the Jacobian matrix and is positive semidefinite [30]. The Jacobian is given by

$$\mathbf{H} = \begin{bmatrix} \frac{\partial}{\partial \mathbf{e}}(\tau_1) \\ \vdots \\ \frac{\partial}{\partial \mathbf{e}}(\tau_{\mathrm{M}}) \end{bmatrix} \tag{21}$$

where the derivative of the m^{th} pair's TDOA is

$$\frac{\partial(\tau_m)}{\partial \mathbf{e}} = \frac{1}{c}\left[\frac{\mathbf{e}-\mathbf{p}_i}{||\mathbf{e}-\mathbf{p}_i||} - \frac{\mathbf{e}-\mathbf{p}_j}{||\mathbf{e}-\mathbf{p}_j||}\right]. \tag{22}$$

4.2.3. Minimizing the Network's Accuracy

This adversary strategy seeks to minimize the location network's estimation accuracy. The single false sensor position to inject, $\mathbf{p}_f$ is sought that minimizes the locating network's FIM and is given by

$$\arg\min_{\mathbf{p}_f} \ \det\left(\mathbf{H}^T\mathbf{C}^{-1}\mathbf{H}\right) \tag{23}$$

where $\mathbf{H}$ is a function of the false position, $\mathbf{p}_f$ as in (21)-(22). For notational convenience, we consider that the last pair M is corrupted by the adversary and is composed of the rogue sensor reporting a false position, $\mathbf{p}_f$ and a valid sensor reporting its true position, $\mathbf{p}_t$.

The FIM can be expressed as the linear combination of each pair's contribution to the FIM,

$$\begin{aligned}
\mathbf{J} &= \mathbf{H}^T\mathbf{C}^{-1}\mathbf{H} = \sum_{m=1}^{M}\frac{1}{\sigma_m^2}\mathbf{h}_m\mathbf{h}_m^T && (24)\\
&\overset{(a)}{=} \sum_{m=1}^{M}\tilde{\mathbf{h}}_m\tilde{\mathbf{h}}_m^T && (25)\\
&\overset{(b)}{=} \tilde{\mathbf{h}}_M\left(\mathbf{p}_f\right)\tilde{\mathbf{h}}_M^T\left(\mathbf{p}_f\right)+\mathbf{A} && (26)
\end{aligned}$$

where $\mathbf{H} = \left[\mathbf{h}_1^T;\ \mathbf{h}_2^T;\ldots;\mathbf{h}_M^T\right]$, $\mathbf{h}_m^T = \frac{\partial\tau_m}{\partial\mathbf{e}}$ is a 1×2 row vector, and σ_m^2 is the variance of the m^{th} TDOA pair. Each submatrix $\mathbf{h}_m\mathbf{h}_m^T$ in (24) is pair m's contribution to the Fisher Information Matrix. In (25), (a) follows from letting $\tilde{\mathbf{h}}_m = \frac{1}{\sigma_m}\mathbf{h}_m$, and in (26), (b) follows from noting the functional dependency on $\mathbf{p}_f$ and defining $\mathbf{A} = \sum_{m=1}^{M-1}\tilde{\mathbf{h}}_m\tilde{\mathbf{h}}_m^T$ which is due the remaining $(M-1)$ valid sensor pairs and is positive semidefinite. The outer product of the derivative of the corrupt pair's TDOA is defined as $\mathbf{Y}\left(\mathbf{p}_f\right) = \tilde{\mathbf{h}}_M\left(\mathbf{p}_f\right)\tilde{\mathbf{h}}_M^T\left(\mathbf{p}_f\right)$.

Replacing into (23) and since the $\log(\cdot)$ is monotonically increasing in its argument gives,

$$\begin{aligned}
\arg\min_{\mathbf{Y}(\mathbf{p}_f)} \quad & \log\left(\det\left(\mathbf{Y}\left(\mathbf{p}_f\right)+\mathbf{A}\right)\right) && (27)\\
\text{s.t.} \quad & \mathbf{Y}\left(\mathbf{p}_f\right)\succeq\mathbf{0} && (28)
\end{aligned}$$

where (28) is the positive semidefinite requirement.

The log determinant has been used as a smooth surrogate for rank minimization. For simplicity the rank of the FIM is discussed for two sensor pairs. We consider the case of two sensor pairs ($\mathbf{p}_1$ & $\mathbf{p}_2$) and ($\mathbf{p}_3$ & $\mathbf{p}_4$) where $\mathbf{A}$ is rank one, which implies the sum in (26) is at least rank one. Since the $\text{Rank}\left(\mathbf{Y}+\mathbf{A}\right) \leq \text{Rank}\left(\mathbf{Y}\right)+\text{Rank}\left(\mathbf{A}\right)$, there are two possibilities for $\mathbf{Y}$. For the $\text{Rank}\left(\mathbf{Y}\right) = \text{Rank}\left(\mathbf{Y}+\mathbf{A}\right) = 1$, requires that the row and column spaces of $\mathbf{Y}$ and $\mathbf{A}$ are dependent, which implies that both sensor pairs give the same contribution to the FIM. This is the case, for example, if the unit vectors pointing from the emitter to the sensors in both pairs are equal, i.e. $\mathbf{p}_1$ & $\mathbf{p}_3$ lie along the same line as the emitter and so do $\mathbf{p}_2$ & $\mathbf{p}_4$. Since the rogue can only alter one sensor position, it is not likely that the network would position a sensor from each pair along the same line from the emitter, since it is a poor geometry for localization. Otherwise, given any arbitrary geometry it may not be possible to ensure there is a solution such that the $\text{Rank}\left(\mathbf{Y}+\mathbf{A}\right) = 1$. If the $\text{Rank}\left(\mathbf{Y}\right) = 0$, this restriction is not imposed. Later this constraint is introduced and a closed form is obtained.

The objective function in (27) is linearized using the Taylor Series Expansion about $\mathbf{Y}_k$,

$$\log\left(\det\left(\mathbf{Y}\left(\mathbf{p}_f\right)+\mathbf{A}\right)\right) \approx \log\left(\det\left(\mathbf{Y}_k+\mathbf{A}\right)\right)+\text{tr}\left\{\mathbf{B}_k\cdot\left[\mathbf{Y}\left(\mathbf{p}_f\right)-\mathbf{Y}_k\right]\right\} \tag{29}$$

where $\mathbf{B}_k = \left(\mathbf{Y}_k+\mathbf{A}\right)^{-1}$. A similar linearization procedure was used for the rank minimization problem [12]. The constants in (29) can be ignored since they do not affect the minimization. Minimizing (29) gives a sequence of semidefinite programs (SDP)s

$$\mathbf{Y}_{(k+1)} = \underset{\mathbf{Y}(\mathbf{p}_f)}{\arg\min} \ \ \mathrm{tr}\left\{\mathbf{B}_k \mathbf{Y}\left(\mathbf{p}_f\right)\right\} \tag{30}$$

which are each convex [4].

From the construction of $\mathbf{Y}$, the matrix can have rank 0 or 1. By imposing zero rank, $\mathbf{Y}^*(\mathbf{p}_f) = \mathbf{0}_{2\times 2}$ and $\mathbf{h}_{\mathrm{M}}^* = \mathbf{0}_{2\times 1}$ and no iterations are needed since the rank of the objective function is zero and cannot be reduced further.

The solution $\mathbf{h}_M^* = \mathbf{0}_{2\times 1}$ can also be found using the following alternate proof. Suppose that $\mathbf{A}$ is positive definite, which requires at least three sensor pairs and that at least two non-corrupt pairs are capable of locating the emitter. Manipulating the determinant of (26) gives

$$\begin{aligned}
\det\left(\tilde{\mathbf{h}}_M \tilde{\mathbf{h}}_{\mathrm{M}}^T + \mathbf{A}\right) &= \det\left(\mathbf{A}\right)\det\left(\mathbf{I}_{2\times 2} + \mathbf{A}^{-1}\tilde{\mathbf{h}}_M \tilde{\mathbf{h}}_M^T\right) && (31)\\
&\overset{(a)}{=} \det\left(\mathbf{A}\right)\det\left(\left(\mathbf{I}_{2\times 2} + \mathbf{A}^{-1}\tilde{\mathbf{h}}_M \tilde{\mathbf{h}}_M^T\right)^T\right) && (32)\\
&\overset{(b)}{=} \det\left(\mathbf{A}\right)\det\left(\mathbf{I}_{2\times 2} - \left(-\tilde{\mathbf{h}}_M \tilde{\mathbf{h}}_M^T \mathbf{A}^{-1}\right)\right) && (33)\\
&\overset{(c)}{=} \det\left(\mathbf{A}\right)\det\left(\begin{bmatrix} 1 & -\tilde{\mathbf{h}}_M^T\mathbf{A}^{-1} \\ \tilde{\mathbf{h}}_M & \mathbf{I}_{2\times 2}\end{bmatrix}\right) && (34)\\
&= \det\left(\mathbf{A}\right)\det\left(1\right)\det\left(\mathbf{I}_{2\times 2} - \tilde{\mathbf{h}}_M\left(-\tilde{\mathbf{h}}_M^T\mathbf{A}^{-1}\right)\right) && (35)\\
&\overset{(d)}{=} \det\left(\mathbf{A}\right)\det\left(\mathbf{I}_{2\times 2}\right)\det\left(1 - \left(-\tilde{\mathbf{h}}_M^T\mathbf{A}^{-1}\right)\mathbf{I}_{2\times 2}\tilde{\mathbf{h}}_M\right) && (36)\\
&= \det\left(\mathbf{A}\right)\det\left(1 + \tilde{\mathbf{h}}_M^T\mathbf{A}^{-1}\mathbf{I}_{2\times 2}\tilde{\mathbf{h}}_M\right) && (37)\\
&= \det\left(\mathbf{A}\right)\left(1 + \tilde{\mathbf{h}}_M^T\mathbf{A}^{-1}\tilde{\mathbf{h}}_M\right) && (38)
\end{aligned}$$

where (a) follows from $\det(\mathbf{X}) = \det(\mathbf{X}^T)$, (b) from $\mathbf{A}$=$\mathbf{A}^T$, (c) from block matrix representation, and (d) from $\det\begin{bmatrix}\mathbf{A} & \mathbf{B}\\ \mathbf{C} & \mathbf{D}\end{bmatrix} = \det\left(\mathbf{D}\right)\det\left(\mathbf{A} - \mathbf{B}\mathbf{D}^{-1}\mathbf{C}\right) = \det\left(\mathbf{A}\right)\det\left(\mathbf{D} - \mathbf{C}\mathbf{A}^{-1}\mathbf{B}\right)$.

The constant in (38) can be removed as it does not affect the minimization yielding,

$$\underset{\tilde{\mathbf{h}}_M}{\arg\min} \quad \left(1 + \tilde{\mathbf{h}}_M^T\mathbf{A}^{-1}\tilde{\mathbf{h}}_M\right) \tag{39}$$

where $\tilde{\mathbf{h}}_M^* = \mathbf{0}_{2\times 1}$.

Observe that $\mathbf{h}_{\mathrm{M}}$ is not a one-to-one function of $\mathbf{p}_f$ so multiple values of $\mathbf{p}_f^*$ exist that yield the same value of $\mathbf{Y}^*(\mathbf{p}_f)$. Nonetheless, a closed form solution is obtained for the false sensor position,

$$\frac{\mathbf{p}_f^* - \mathbf{e}}{||\mathbf{p}_f^* - \mathbf{e}||} = \frac{\mathbf{p}_t - \mathbf{e}}{||\mathbf{p}_t - \mathbf{e}||}. \tag{40}$$

The solution in (40) dictates the unit vector pointing from the emitter $\mathbf{e}$, to the valid true sensor $\mathbf{p}_t$, should equal the unit vector pointing from the emitter to the rogue corrupted sensor $\mathbf{p}_f$. Therefore, any position along the vector through $\mathbf{p}_t$ maximally degrades estimation accuracy. Figure 11 shows a numerical example, where the positions that minimize the determinant of the FIM are marked with an "**x**".

The solution $\mathbf{Y}^*(\mathbf{p}_f) = \mathbf{0}_{2\times 2}$ suggests the *best* the adversary can do is remove the effect of the rogue corrupted pair. In the case of two pairs of sensors, $\det\left(\tilde{\mathbf{h}}_1\tilde{\mathbf{h}}_1^T\right) = 0$, where with 50% of corrupted TDOA measurements the estimating network cannot recover. This limit has been shown in other adversarial work [46].

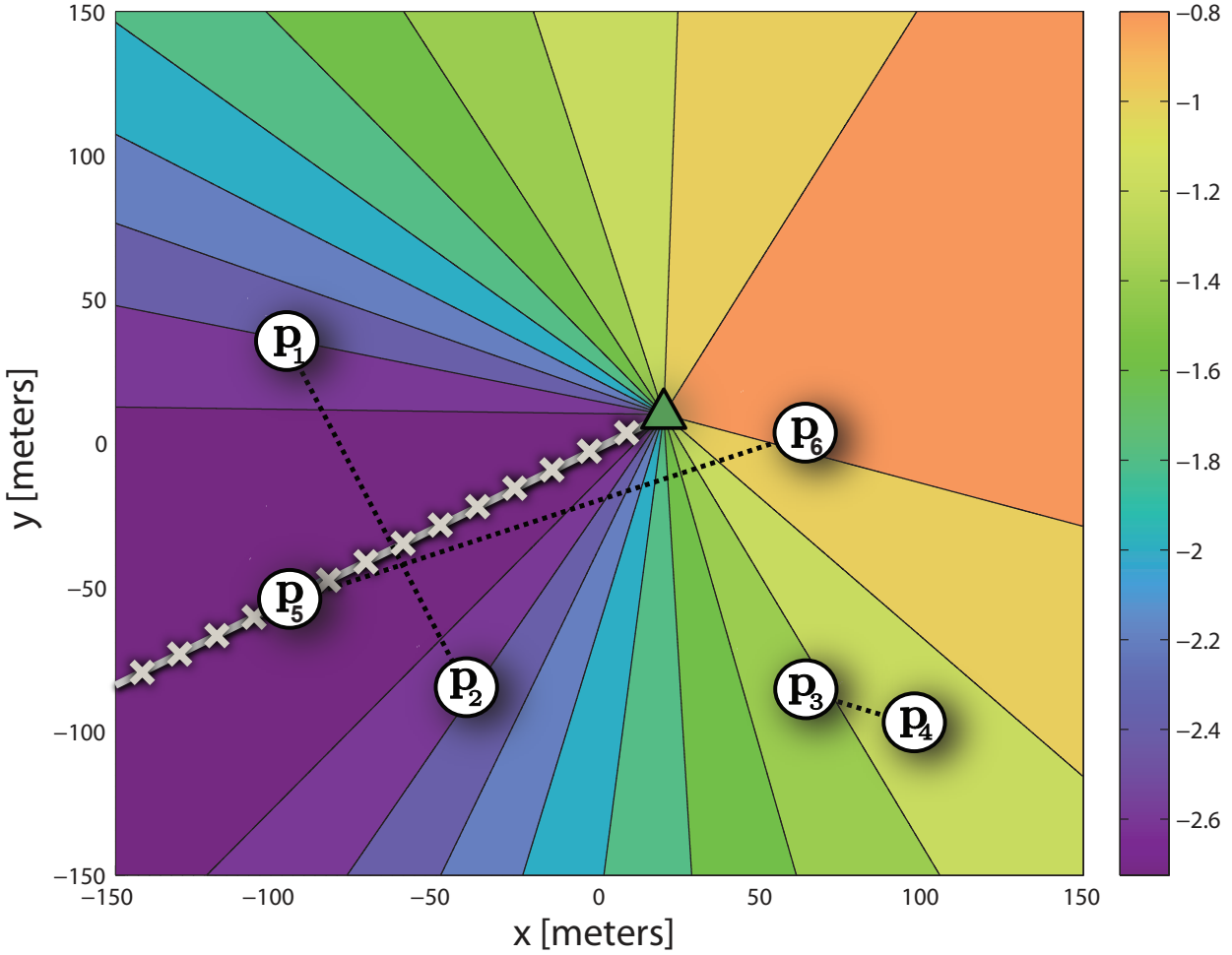


Figure 11: Evaluation of the determinant of the FIM over a 300m × 300m field for six sensors which are paired as shown by the black dotted line. The solution set of false sensor positions are marked with an "**x**" where $\mathbf{p}_t$ is sensor 5 and sensor 6 is corrupted. The emitter is located at [20 10].

4.3. Impact of Minimizing the FIM on non-linear LS Estimation

Minimizing the estimation accuracy of the network increases the variance of the estimation error. Specifically, the accuracy is decreased to that of the remaining $(M-1)$ non-corrupt sensor pairs. Thus, the solution in (40) is equivalent to only using the non-corrupt pairs to perform the emitter location. This performance reduction to $(M-1)$ pairs also applies to the least squares estimate. We begin by examining the non-linear LS estimate update [30] given by

$$\hat{\mathbf{e}}_{k+1} = \mathbf{e}_k + \left(\mathbf{H}_{\mathbf{e}_k}^T \mathbf{H}_{\mathbf{e}_k}\right)^{-1} \mathbf{H}_{\mathbf{e}_k}^T \boldsymbol{\Delta}, \tag{41}$$

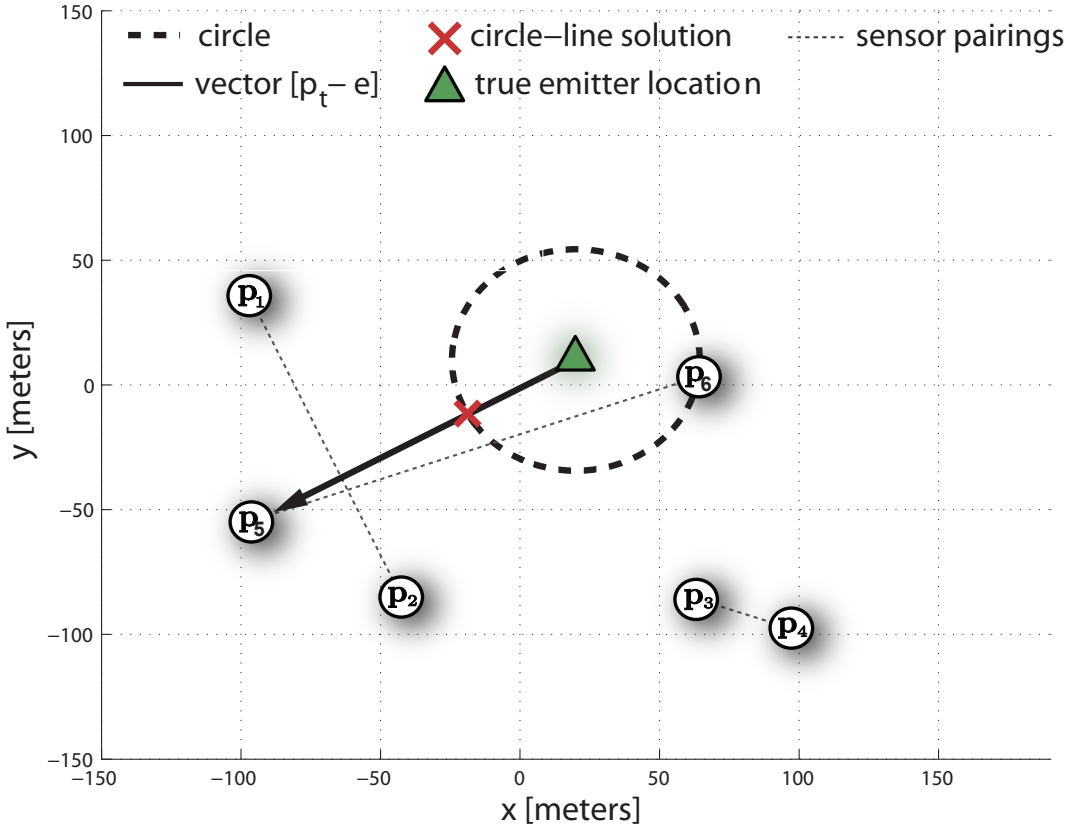
where $\hat{\mathbf{e}}_{k+1}$ is the $(k+1)$ update of the unknown parameter (emitter location), the Jacobian, $\mathbf{H}_{\mathbf{e}_k}$ is the derivative of the TDOA w.r.t. the emitter's location given that the k^{th} estimate is correct, and $\boldsymbol{\Delta} = \hat{\boldsymbol{\tau}} - \boldsymbol{\tau}(\mathbf{e}_k)$ is the residual TDOA given the k^{th} estimate. For M sensor pairs, the Jacobian is (dropping the subscript) $\mathbf{H} = \left[\mathbf{h}_1^T; \ldots; \mathbf{h}_{M-1}^T; \mathbf{h}_M^T\right]$ where $\mathbf{h}_m$ is the derivative of the TDOA of the m^{th} pair w.r.t. the emitter's location and $\mathbf{h}_m^T$ is the m^{th} row of $\mathbf{H}$. The product $\mathbf{H}^T\mathbf{H}$ can be written as the sum of each pair's contribution, $\mathbf{H}^T\mathbf{H} = \mathbf{h}_1\mathbf{h}_1^T + \mathbf{h}_2\mathbf{h}_2^T + \cdots + \mathbf{h}_M\mathbf{h}_M^T$. Assuming that the last pair M contains the corrupt rogue sensor and by substituting ${\mathbf{h}_M^*}^T = \bar{\mathbf{0}}_{1\times 2}$, the Jacobian becomes $\mathbf{H} = \left[\mathbf{h}_1^T; \ldots; \mathbf{h}_{M-1}^T; \bar{\mathbf{0}}_{1\times 2}\right]$. The product $\mathbf{H}^T\mathbf{H}$ becomes

$$\mathbf{H}^T\mathbf{H} = \underbrace{\mathbf{h}_1\mathbf{h}_1^T + \mathbf{h}_2\mathbf{h}_2^T + \cdots + \mathbf{h}_{M-1}\mathbf{h}_{M-1}^T}_{\text{due to non-corrupt pairs}} + \bar{\mathbf{0}}_{2\times 2} \tag{42}$$

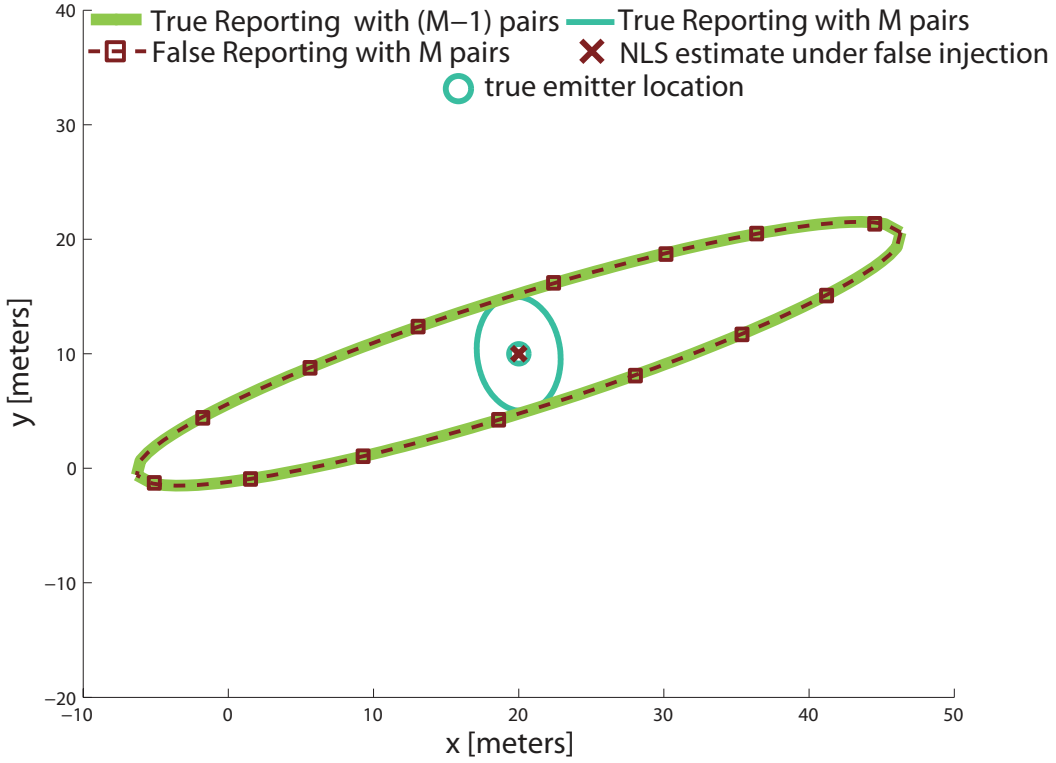
indicating that the non-linear LS estimate is computed using only the non-corrupt pairs' Jacobian submatrices. Thus, (40) can increase the variance to the level that would occur if only the $(M-1)$ non-corrupt pairs were used for location processing.

Figure 12 shows an example of this result where the network in 12 (a) is injected with a false sensor position along (40). Sensor 6 is injected with the position at the intersection of the circle and line shown by the red "x". The utility of this solution will be discussed later in Section 6.0. from a detection viewpoint since it does not change the TDOA. Figure 12 (b) shows several error ellipses based on the sensor configuration in 12 (a). The ellipses without injection, labeled *true reporting* are shown for both M and $(M-1)$ sensor pairs in blue and green, respectively. The ellipse given the false sensor position reported from 12 (a) is shown by the red ellipse. Observe that the performance of the FIM solution under false reporting is equal to that using only the $(M-1)$ non-corrupt pairs. We see that while the FIM minimizing solution degrades the variance of the estimator, a single NLS estimate may be quite accurate.

The physical implication of the FIM minimizing strategy is that the adversary can remove the contribution of the corrupted pair, which is most effective when the M^{th} pair contributes the most to the FIM or for networks with a small number of sensor pairs. If the adversary is able to inject any sensor in the network it should determine which pair contributes the most to the FIM to have the largest impact on the network.



(a) System setup. Six sensors are paired as shown by the dotted line. The emitter is located at [20 10]. The solution from (40) lies along the line through the black arrow. The dashed circle shows the sensor positions that do not alter the corrupt sensor pair's TDOA.



(b) Effect of false reports on the error ellipse and non-linear LS estimate. The non-linear LS estimate given the false position in 12(a) is shown by a red "x".

Figure 12: Impact of the adversary's injection in (40). The FIM strategy can increase the variance to that of the $(M-1)$ non-corrupt pairs.

4.4. Discussion

This chapter develops adversary strategies to minimize the locating network's accuracy. Motivated by the two-dimensional interpretation of the Fisher Information Matrix we consider minimizing the determinant of the FIM, which is equivalent to maximizing the error ellipse. Intuitively, the more accurate the network's localization i.e. the smaller its error ellipse, the stronger the injection must be by the adversary. From this observation we formulate two strategies, first under the highly accurate TDOA/FDOA and then for stationary networks under TDOA. We show that under TDOA/FDOA our solution significantly reduces the network's accuracy independent of sensor-emitter geometry. However, it does not lend itself to a closed form. A closed form solution is derived under TDOA, where the physical implication behind this solution is that the best the adversary can do is to remove the effect of the corrupted sensor pair.

The developed strategies were limited to corruption of a single sensor. It is of interest to examine how the strategies can be extended to the multi-sensor case as well as determining which sensors should be corrupted. Directions for future work include consideration of more than one corrupt sensor, and determining which sensors should be compromised given that only a limited number may be corrupted. Another direction is consideration of a time horizon where the adversary can inject false information over multiple time shots.

Investigation of the FIM minimizing strategies on the network's LS processing suggests that while the adversary can make the ellipse quite large, it can increase the variance only to that of the non-corrupt pairs. We are motivated to develop new adversary redirection strategies which are explored in the next chapter.

5.0. Methods: Adversary Strategies to Redirect the Locating Network

This chapter designs adversary strategies to redirect the locating network's estimate a specified distance away from its true value. The problem is again approached by considering the error ellipse interpretation as shown in Figure 13(a). However, now we seek a strategy that redirects the emitter a specified distance away from its true value. Figure 13(b) shows the parameters that the network uses to determine its location estimate where the adversary injects a false sensor position.

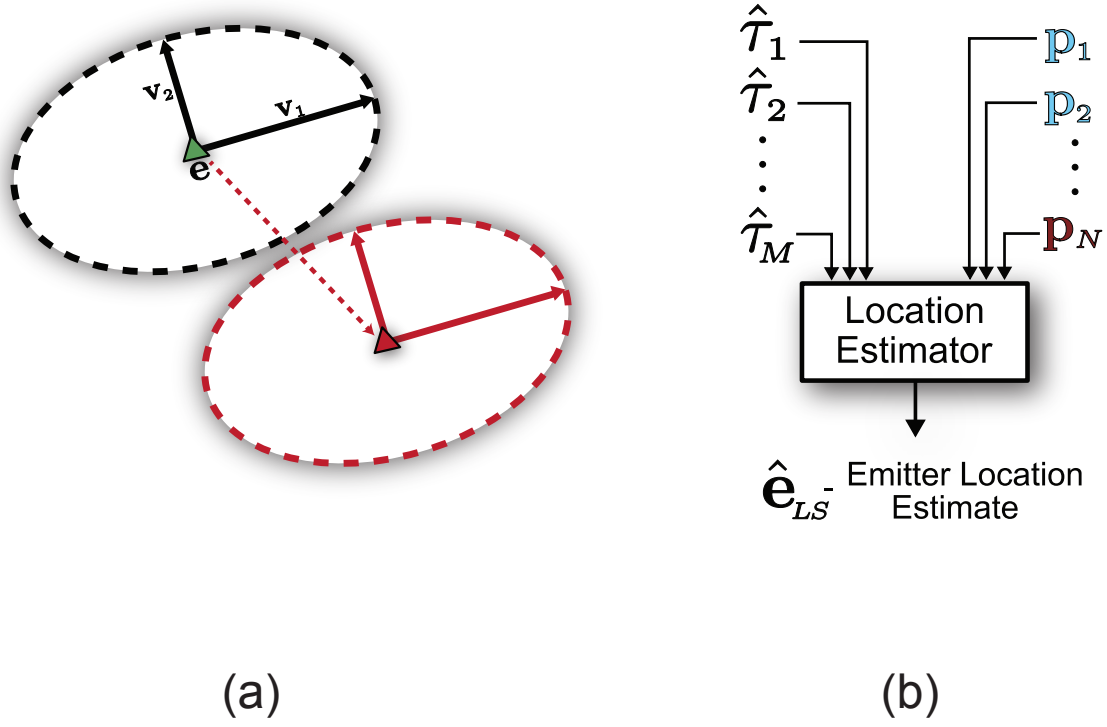


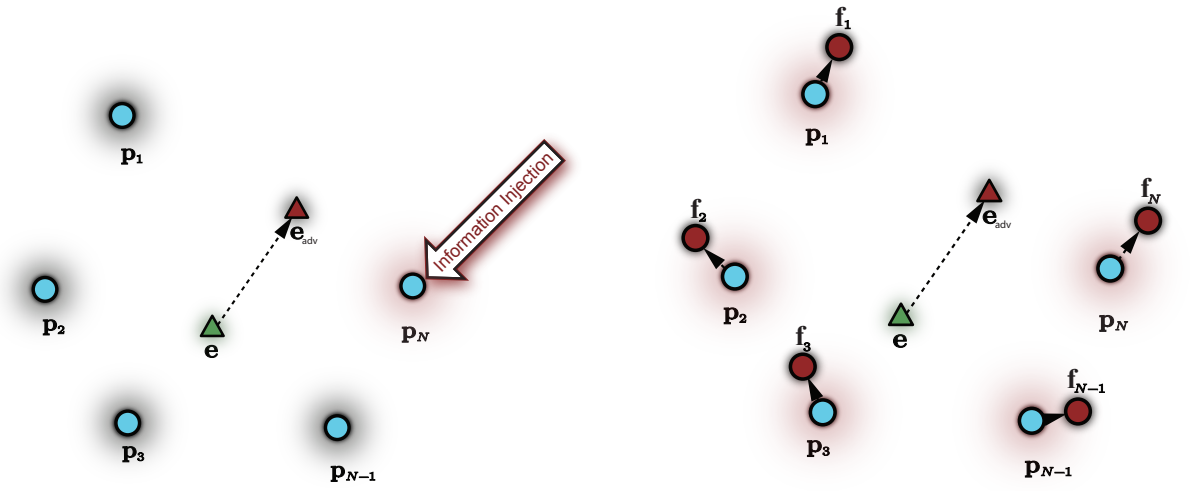
Figure 13: An adversary redirects the location estimate.

Clearly, if the adversary is able to inject every node in the network with unlimited value then the network's estimation will not be able to recover. Modeling the strength of the adversary is explored. On the one hand, the stronger the adversary's model, the more seriously it can impact the network's localization at the cost of detectability. On the other hand, the adversary likely has limited resources with which to redirect the network. We define a more realistic scenario of a power-limited adversary and define the adversary's strength in terms of how many nodes are injected as a *spatial restriction* and what is injected as a *content restriction* as shown in Figure 14.

5.1. Redirection with a Spatial Restriction

The main contribution of this section is an adversary strategy to estimate redirection under the TDOA method using only a single false injection. The adversary seeks to redirect the emitter location estimate to a new position

$$\hat{\mathbf{e}}_r(\theta) = \mathbf{e} + r\left[\cos(\theta) \quad \sin(\theta)\right]^T, \tag{43}$$



(a) spatial restriction

(b) content restriction

Figure 14: Modeling the adversary's strength: (a) spatial restriction-one injection with unlimited value and (b) content restriction-all sensors are injected with bounded value

where r is the desired offset and θ is any value in $[0,\ \ 2\pi]$ shown by the dashed circle in Figure 15. The adversary allows the location estimate to be at any value of θ, and therefore must also be considered in the optimization.

5.1.1. Problem Formulation

To determine the false sensor position, the LS cost of the TDOA residuals is minimized given the adversary's desired condition in (43). The problem can be formulated as

$$\arg\min_{\mathbf{p}_f,\theta} \sum_{m=1}^{M-1} \left(\bar{\tau}_m\left(\hat{\mathbf{e}}_r\left(\theta\right)\right) - \tau_m\right)^2 + \left(\bar{\tau}_M\left(\hat{\mathbf{e}}_r\left(\theta\right),\ \mathbf{p}_f\right) - \tau_M\right)^2 \tag{44}$$

where $\bar{\tau}_m\left(\hat{\mathbf{e}}_r(\theta)\right)$ and $\bar{\tau}_M\left(\hat{\mathbf{e}}_r(\theta),\ \mathbf{p}_f\right)$ are the TDOA values for the possible values of $\mathbf{p}_f$ and θ, and τ_m is the true value of TDOA of the m^{th} pair in (18). For simplicity of notation we drop the functional dependence of the TDOAs on $\hat{\mathbf{e}}_r(\theta)$ to θ noting that all parameters in (43) except θ are known. The problem in (44) is non-linear and due to the rank deficiency of the Jacobian matrix the Gauss-Newton method cannot be used. The Jacobian is given by

$$\mathbf{H} \quad = \quad \begin{bmatrix} \frac{\partial\bar{\tau}_1(\theta)}{\partial\theta} & \frac{\partial\bar{\tau}_1(\theta)}{\partial\mathbf{p}_f} \\ \vdots & \vdots \\ \frac{\partial\bar{\tau}_M(\theta,\mathbf{p}_f)}{\partial\theta} & \frac{\partial\bar{\tau}_M(\theta,\mathbf{p}_f)}{\partial\mathbf{p}_f} \end{bmatrix} \tag{45}$$

where $\frac{\partial\bar{\tau}_m(\theta)}{\partial\mathbf{p}_f} = \bar{\mathbf{0}}_{1\times 2} \quad \forall m \neq M$. The Jacobian is $M\times 3$ and is clearly rank degenerate. To remedy this problem a change of variables can be used where $R_f = ||\hat{\mathbf{e}}_r\left(\theta\right) - \mathbf{p}_f||$. Thus, (44) can be re-written as

$$\arg\min_{R_f,\theta} \sum_{m=1}^{M-1} \left(\bar{\tau}_m\left(\theta\right) - \tau_m\right)^2 + \left(\bar{\tau}_M\left(\theta,\ R_f\right) - \tau_M\right)^2 \tag{46}$$

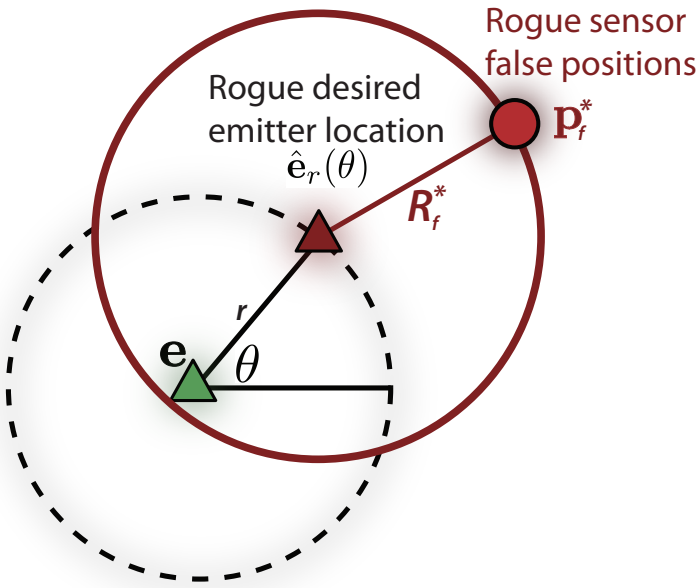


Figure 15: The adversary redirects the emitter location estimate.

where $\bar{\tau}_M(\theta,\ R_f) = \frac{1}{c}\left[||\hat{\mathbf{e}}_r(\theta) - \mathbf{p}_t|| - R_f\right]$. The set of false positions that minimize the LS cost in (46) is described by a circle with center $\hat{\mathbf{e}}_r(\theta)\,|_{\theta=\theta^*}$ and radius R_f^* as shown in Figure 15. Thus, any point on this circle is a solution for the false sensor position. The solution of (46) is found by evaluating over a fine grid of 2000m, although it is expected that this could be solved using other methods such as gradient-based methods, or using particle swarm optimization techniques. While the goal of the adversary is to find the false sensor position to drive the estimate to the desired location, depending on the value of the desired adversary offset and the sensor-emitter geometry of the non-corrupt pairs, the desired location estimate may not be achieved exactly by (44).

5.1.2. Impact on the Locating Network

To evaluate the effectiveness of this strategy the false sensor position solution from (46) is reported to the locating network and the emitter location is estimated. To this end, our approach is evaluated for both traditional non-linear LS and for robust statistical methods, specifically least median squares (LMS).

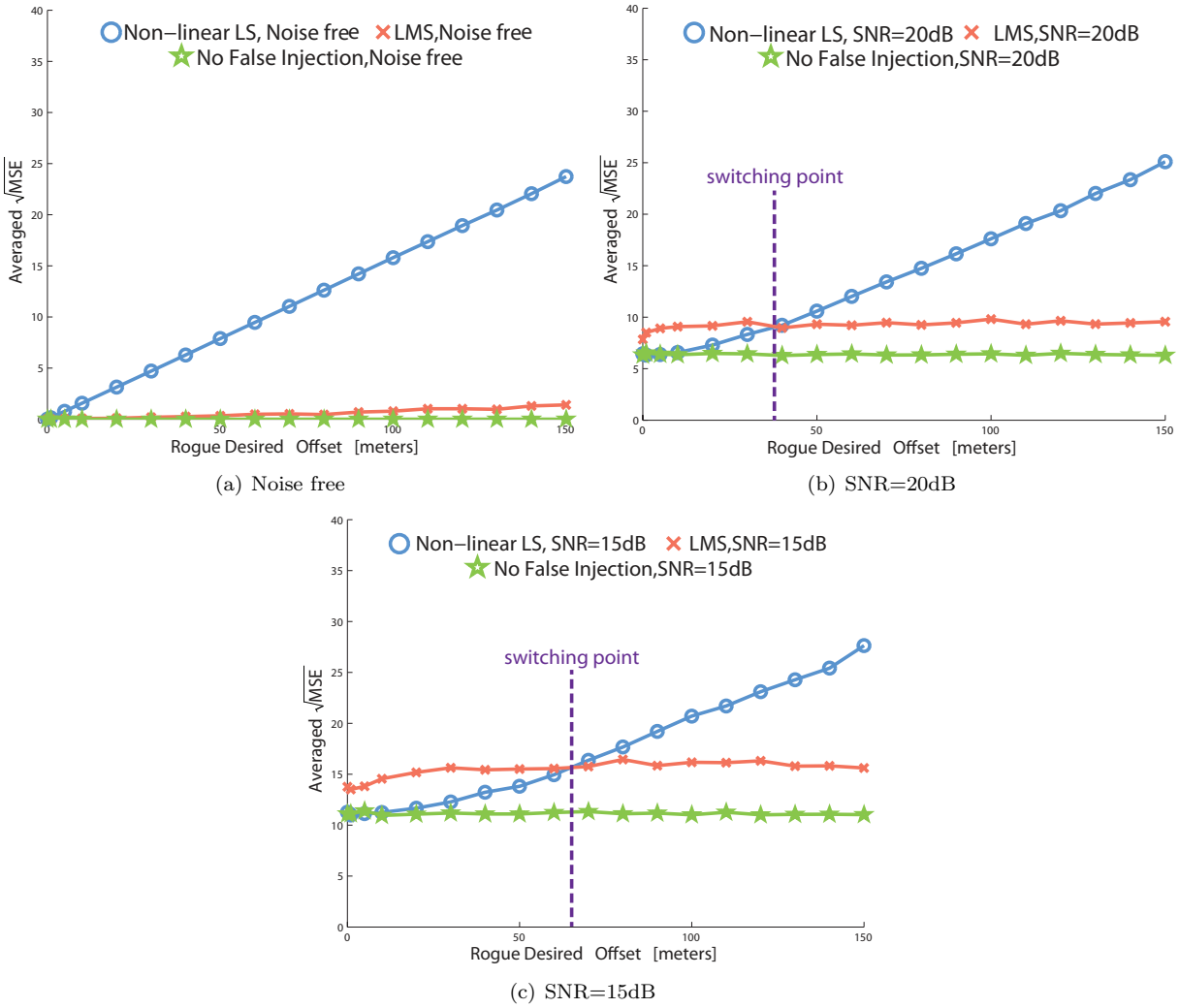
The performance of LMS has been shown in [57]. Although no closed form exists for LMS, [58] provides an efficient method. There are two main steps, (1) clustering the measurements into subsets to obtain a set of weights, and (2) reweighting the measurements and solving for the final estimate using weighted LS.

Given X total measurements, K subsets are randomly chosen, each with n samples. For each subset j an estimate $\hat{\boldsymbol{\theta}}_j$ is found and the squared residuals r_{ij}^2 for each estimate is determined across all X measurements. The cluster with the smallest median of the squared residuals is used to determine the weights for each measurement,

$$w_i = \begin{cases} 1 & |\frac{r_i}{s_o}| \leq \gamma \\ 0 & \text{otherwise} \end{cases} \tag{47}$$

where $s_o = 1.48826\left(1 + \frac{5}{X-P}\right)\sqrt{\text{med}_i r_i^2\left(\hat{\boldsymbol{\theta}}\right)}$, P is the dimension of the unknown parameter, and γ is a threshold chosen as in [58]. Given these weights, weighted LS is then used to find the final location estimate.

The performance is evaluated as a function of the MSE averaged across 2000 sensor-emitter geometries randomly generated in a 1000m×1000m field for ten sensor pairs. Figure 16 shows the averaged square root MSE in the presence of false injection under non-linear LS and LMS for varying SNR. The baseline square



(a) Noise free

(b) SNR=20dB

(c) SNR=15dB

Figure 16: Mean squared error performance for non-linear LS and LMS. A total of 2000 sensor-emitter geometries were considered, each with 20 sensors.

root MSE without injection is shown for comparison. We observe that by using only a single false sensor position the adversary can: (1) increase the error under both NLS and LMS, and (2) under LMS the error is increased by roughly a constant. Interestingly, in the presence of noise, we observe a switching point (shown by the dashed line) between the NLS and LMS methods similar to [39]. From the network's perspective, NLS offers the smallest rise in MSE for small adversary offsets while LMS offers the best protection given larger adversary offsets. This switching point is a function of SNR and the value of the adversary desired offset. From the network's viewpoint choosing LMS is not always appropriate in order to minimize the MSE. From the adversary's viewpoint, this switching point can be used to guide the selection of the desired offset to cause the largest rise in MSE.

5.2. Redirection with a Content Restriction

We consider that the adversary is able to perturb every sensor by a small amount where the goal is to redirect the localization estimate to a specified location away from its true value as shown in Figure 17. Specifically, we consider the problem of redirecting the network's location estimate under varying levels of adversary control with respect to the distance the sensors can move. The main contribution of this strategy is a method to determine the set of false sensor positions for the adversary's redirection problem with bounds

on the distance each sensor can move.

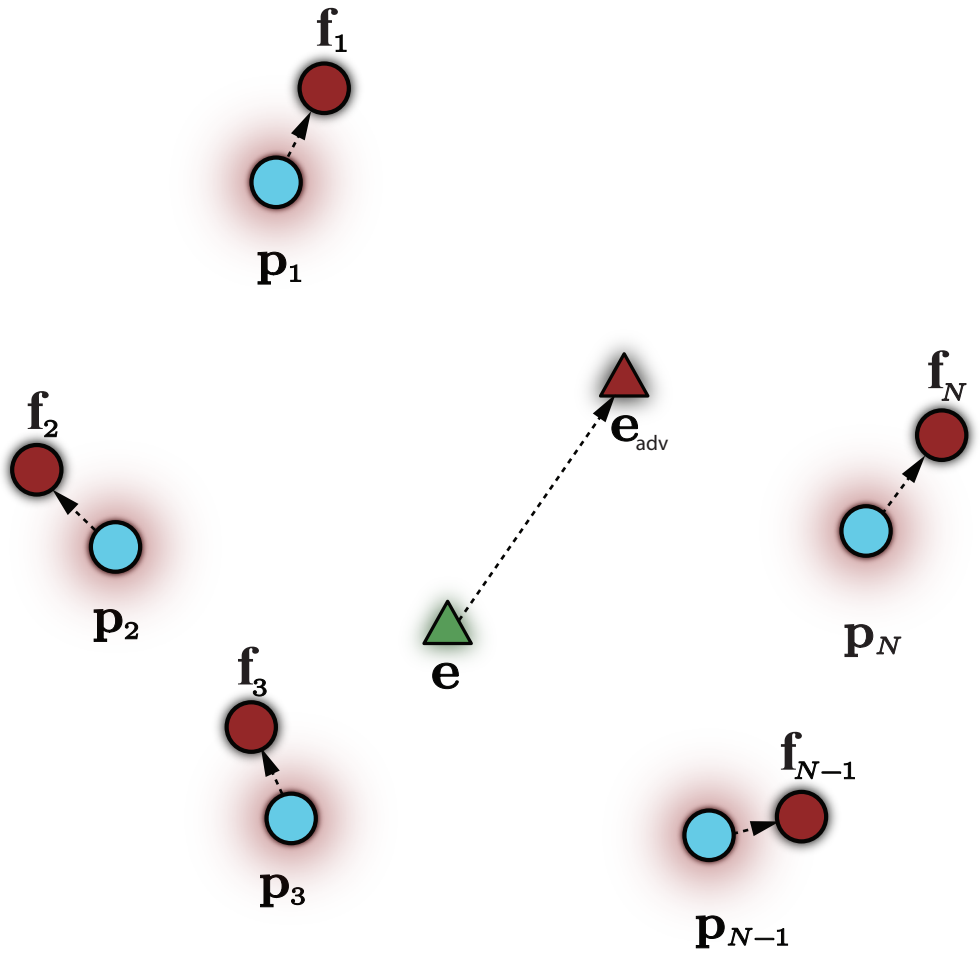


Figure 17: Overview: An adversary seeks a false sensor positions $\{f_i\}$, redirecting the locating network's estimate to $\mathbf{e}_{\text{adv}}$ subject to bounds on the distance each sensor can move.

We explore the adversary redirection problem using received signal strength (RSS) and develop a semidefinite programming approach to solve for the false sensor positions. Different levels of adversary control are considered and two cases are explored where (1) each sensor is allowed to move up to a prescribed distance, and (2) a penalty is imposed to restrict the distance certain sensors can move. The effectiveness and efficiency of our approach is evaluated using mean squared error and by measuring total sensor displacement.

5.2.1. System Model under Received Signal Strength

A collection of N sensors is tasked with estimating the emitter's location, $\mathbf{e}$ with dimension d using the RSS method. Under this method, the sensors measure their RSS and transmit their measurements to a fusion center where the estimate, $\hat{\mathbf{e}}$ is determined. The Maximum Likelihood estimator is a practical method of estimating the unknown quantity [30]. In [48], a minimax approximation of the MLE is used to form a semidefinite program. The system model under RSS is now reviewed.

Each sensor measures its received signal strength (RSS). The noise free signal at sensor i is

$$s_i = \frac{P_{\text{tx}}}{||\mathbf{p}_i - \mathbf{e}||^{\beta}} \ \forall \ i \tag{48}$$

where P_{tx} is the transmit power, $\mathbf{p}_i$ is the i^{th} sensor position, $\mathbf{e}$ is the emitter location, and β is the pathloss exponent. Lognormal fading is considered, where the signal received at each sensor in dB is

$$10\log\left(s_i\right) = 10\log\left(P_{\text{tx}}\right) - 10\beta\log\left(||\mathbf{p}_i - \mathbf{e}||\right) + n_i \tag{49}$$

where $n_i \sim \mathcal{N}\left(0, \sigma^2\right)$ and $s_i = \frac{P_{\text{tx}} 10^{\frac{n_i}{10}}}{||\mathbf{p}_i - \mathbf{e}||^\beta}$. The RSS measurements from all sensors are combined to estimate $\mathbf{e}$ and can be estimated using the Maximum Likelihood estimator. The Maximum Likelihood estimate of emitter location is given by

$$\hat{\mathbf{e}} = \arg\min_{\tilde{\mathbf{e}}} \quad \sum_{i=1}^{N} \left(\ln\, s_i - \ln\left(\frac{P_{\text{tx}}}{||\mathbf{p}_i - \tilde{\mathbf{e}}||^\beta} \right) \right)^2, \tag{50}$$

which is a non-linear least squares (LS) problem.

In [48] the MLE in (50) is rewritten as a minimax problem by replacing the l_2 norm with the l_∞ norm

$$\hat{\mathbf{e}} = \arg\min_{\tilde{\mathbf{e}}} \quad \max_{i=1,\ldots,N} \quad \left| \ln\, \left(q_i\, ||\mathbf{p}_i - \tilde{\mathbf{e}}||^2 \right) \right| \tag{51}$$

where $q_i = \left(\frac{s_i}{P_{\text{tx}}}\right)^{\frac{2}{\beta}}$. Thus, (51) can be written as a semidefinite program (SDP)

$$\min_{\mathbf{E},\, t} \quad t \tag{52}$$

$$\text{s.t.} \quad -t < q_i\, \text{tr}\left\{\mathbf{P}_i \mathbf{E}\right\} - 1 < t \;\; \forall\, i \tag{53}$$

$$\mathbf{E} \succeq \mathbf{0} \tag{54}$$

$$\mathbf{E}\left(d{+}1, d{+}1\right) = 1 \tag{55}$$

where $\mathbf{E} = \bar{\mathbf{e}}\bar{\mathbf{e}}^T$, $\bar{\mathbf{e}} = \left[\tilde{\mathbf{e}}^T\ 1\right]$, $\mathbf{P}_i = \begin{bmatrix} \mathbf{I} & -\mathbf{p}_i \\ -\mathbf{p}_i^T & \mathbf{p}_i^T \mathbf{p}_i \end{bmatrix}$ $\forall\, i$.

The solution $\bar{\mathbf{e}}^*$ is extracted from $\mathbf{E}^*$ through Gaussian randomization [45]. A set of L Gaussian random vectors with covariance matrix $\mathbf{E}^*$ are generated satisfying the constraints in the optimization problem. The vector that minimizes the objective function is taken as the solution $\bar{\mathbf{e}}^*$. Thus, the emitter location estimate can be easily extracted from $\bar{\mathbf{e}}^*$. In the next section we explore the adversary's redirection problem under the received signal strength method exploiting the use of a SDP approach.

5.2.2. Adversary Redirection

The goal of the adversary is to redirect the location estimate to $\mathbf{e}_{\text{adv}}$. We consider two variations on the adversary redirection problem. First we formulate the problem for the case of *maximum distance constraints*, where the sensors can each move up to a prescribed distance $\sqrt{\alpha}$. The problem is formulated as a semidefinite program where the distance constraints are incorporated as inequalities. We then modify our formulation for the case of *penalized distance constraints*, where each sensor is assigned a weight penalizing its movement.

Maximum Distance Constraints

We first explore the adversary redirection problem where each sensor is allowed to move up to $\sqrt{\alpha}$ meters. This redirection problem is given by

$$\min_{\{\mathbf{f}_i\}_{i=1}^N} \quad \sum_{i=1}^{N} \left(\ln\, s_i - \ln\left(\frac{P_{\text{tx}}}{||\mathbf{f}_i - \mathbf{e}_{\text{adv}}||^\beta} \right) \right)^2 \tag{56}$$

$$\text{s.t.} \quad ||\mathbf{p}_i - \mathbf{f}_i||^2 \leq \alpha \;\forall\; i \tag{57}$$

where $\mathbf{p}_i$ are the true sensor positions, $\mathbf{f}_i$ are the false sensor positions, $\mathbf{e}_{\text{adv}}$ is the adversary desired emitter location, and $\sqrt{\alpha}$ is a bounding radius on the distance each sensor can move.

The objective function has a similar form to (50), allowing for a semidefinite programming approach. The problem in (56)-(57) becomes

$$\begin{aligned}
\min_{t,\ \mathbf{F}_i\ \forall\ i} \quad & t && (58)\\
\text{s.t.} \quad & -t < q_i\ \text{tr}\left\{\mathbf{F}_i\mathbf{E}_{\text{adv}}\right\} - 1 < t\ \forall\ i && (59)\\
& \text{tr}\left\{\mathbf{F}_i\mathbf{P}_i\right\} \leq \alpha\ \forall\ i && (60)\\
& \mathbf{F}_i \succeq \mathbf{0}\ \forall\ i && (61)\\
& \mathbf{F}_i\left(d{+}1, d{+}1\right) = 1\ \forall\ i && (62)
\end{aligned}$$

where $\mathbf{E}_{\text{adv}} = \begin{bmatrix} \mathbf{I} & -\mathbf{e}_{\text{adv}} \\ -\mathbf{e}_{\text{adv}}^T & \mathbf{e}_{\text{adv}}^T\mathbf{e}_{\text{adv}} \end{bmatrix}$, $\mathbf{F}_i = \bar{\mathbf{f}}_i\bar{\mathbf{f}}_i^T$, $\bar{\mathbf{f}}_i = \begin{bmatrix}\mathbf{f}_i^T & 1\end{bmatrix}\ \forall\ i$. Thus, we have a SDP where $\mathbf{f}_i^*$ is extracted from $\mathbf{F}_i^*$. Figure 18 shows an example system model with the false position solution for varying values of $\mathbf{e}_{\text{adv}}$.

Penalized Distance Constraints

The adversary may have additional information dictating how the sensors can be moved. In the second case, we introduce a penalty term in order to further restrict the movement of all or a subset of sensors. For example, certain sensors in the network may be more difficult to move due to physical barriers or may be more heavily monitored for tampering by the locating network. Thus, we introduce a penalty term associating a cost to the adversary for moving a given sensor.

The redirection problem with penalized constraints is

$$\begin{aligned}
\min_{\{\mathbf{f}_i\}_{i=1}^N} \quad & \sum_{i=1}^{N}\left(\ln s_i - \ln\left(\frac{P_{\text{tx}}}{||\mathbf{f}_i - \mathbf{e}_{\text{adv}}||^{\beta}}\right)\right)^2 + \sum_{i=1}^{N}\lambda_i||\mathbf{p}_i - \mathbf{f}_i||^2 && (63)\\
\text{s.t.} \quad & ||\mathbf{p}_i - \mathbf{f}_i||^2 \leq \alpha\ \forall\ i && (64)
\end{aligned}$$

where $\mathbf{p}_i$ are the true sensor positions, $\mathbf{f}_i$ are the false sensor positions, $\sqrt{\alpha}$ is a bounding radius on the distance each sensor can move, and λ_i is the penalty weight for moving sensor i.

Using a change of variables and by rewriting the problem in epigraph form gives

$$\begin{aligned}
\min_{t_1,t_2,\ \mathbf{F}_i\ \forall\ i} \quad & t_1 + t_2 && (65)\\
\text{s.t.} \quad & \sum_{i=1}^{N}\left(\ln\ \left(q_i\text{tr}\left\{\mathbf{F}_i\mathbf{E}_{\text{adv}}\right\}\right)\right)^2 < t_1 && (66)\\
& \sum_{i=1}^{N}\lambda_i\text{tr}\left\{\mathbf{F}_i\mathbf{P}_i\right\} \leq t_2 && (67)\\
& \text{tr}\left\{\mathbf{F}_i\mathbf{P}_i\right\} \leq \alpha\ \forall\ i && (68)\\
& \mathbf{F}_i \succeq \mathbf{0}\ \forall\ i && (69)\\
& \mathbf{F}_i\left(d{+}1, d{+}1\right) = 1\ \forall\ i. && (70)
\end{aligned}$$

By replacing the l_2 norm in (66) with the l_∞ norm, the problem can be written as a semidefinite program where (63)-(64) becomes

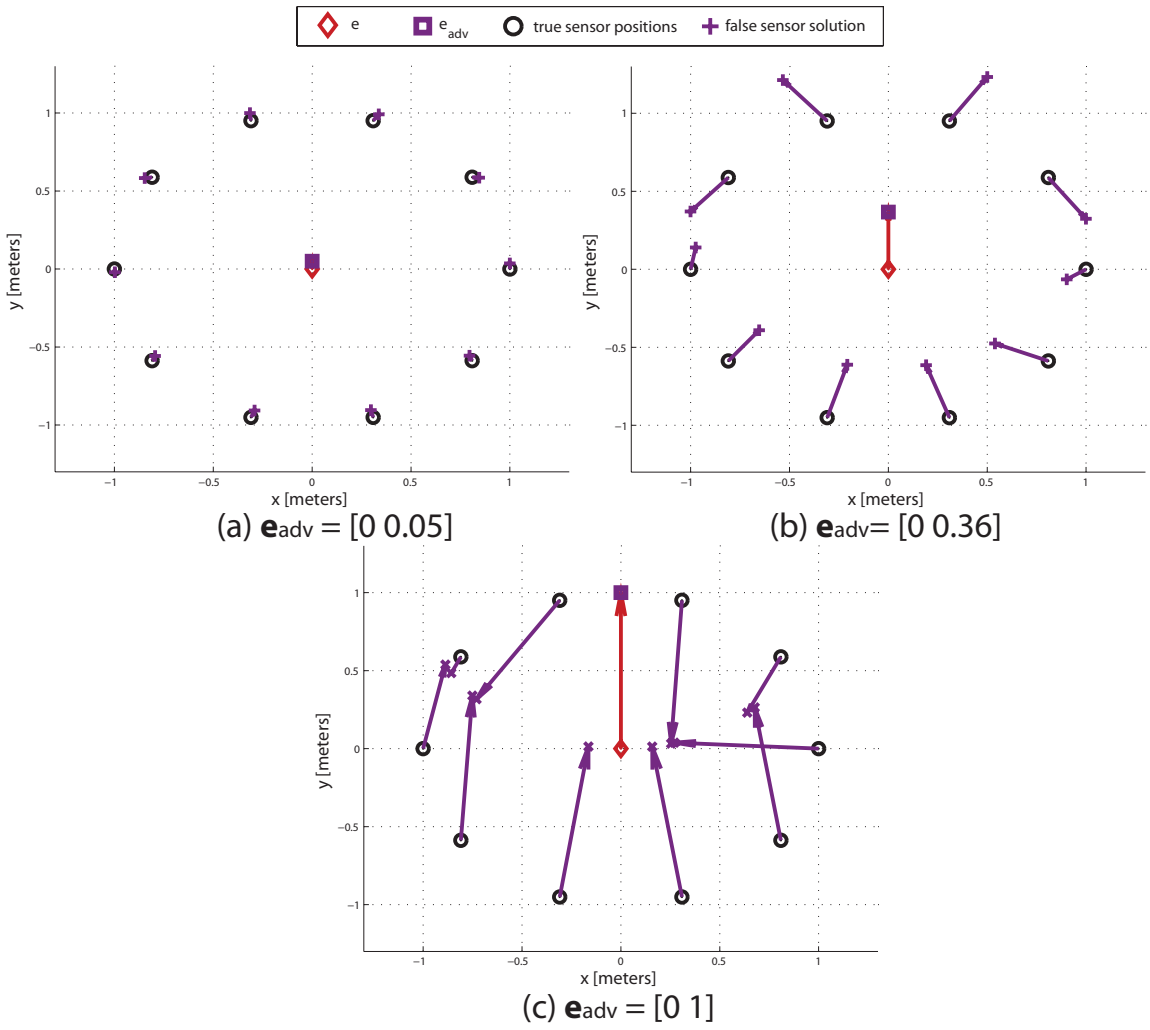


Figure 18: Maximum distance constraints: Examples of true and falsified sensor positions for varying offset distances, where $N = 10$ sensors.

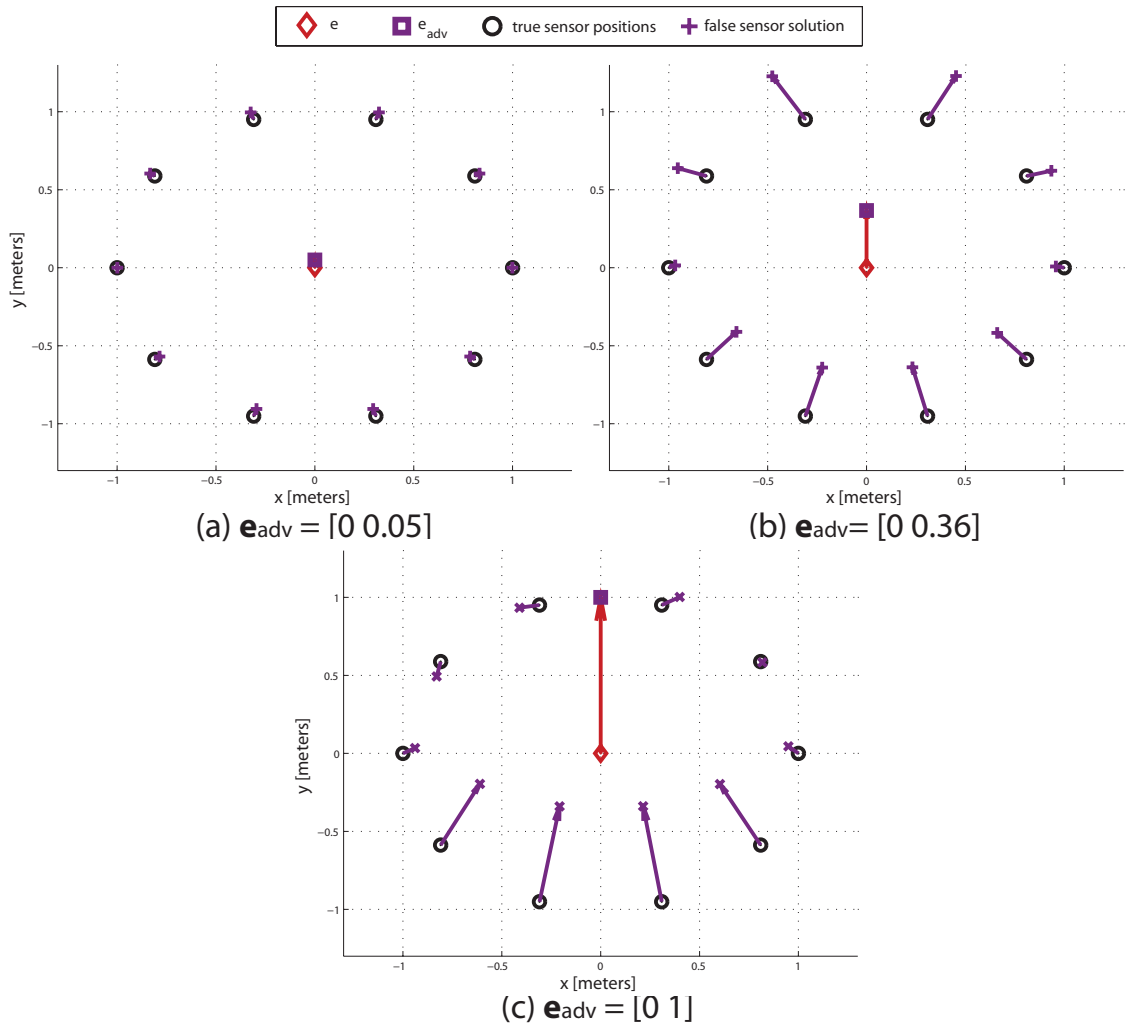


Figure 19: Penalized distance constraints: Examples of true and falsified sensor positions for varying offset distances, where $N = 10$ sensors.

$$\min_{t_1,t_2,\ \mathbf{F}_i\ \forall\ i} \quad t_1 + t_2 \tag{71}$$

$$\text{s.t.} \quad -t_1 < q_i \text{tr}\left\{\mathbf{F}_i \mathbf{E}_{\text{adv}}\right\} - 1 < t_1\ \forall\ i \tag{72}$$

$$\sum_{i=1}^{N} \lambda_i \text{tr}\left\{\mathbf{F}_i \mathbf{P}_i\right\} \leq t_2 \tag{73}$$

$$\text{tr}\left\{\mathbf{F}_i \mathbf{P}_i\right\} \leq \alpha\ \forall\ i \tag{74}$$

$$\mathbf{F}_i \succeq \mathbf{0}\ \forall\ i \tag{75}$$

$$\mathbf{F}_i\left(d+1, d+1\right) = 1\ \forall\ i \tag{76}$$

where $\mathbf{E}_{\text{adv}} = \begin{bmatrix} \mathbf{I} & -\mathbf{e}_{\text{adv}} \\ -\mathbf{e}_{\text{adv}}^T & \mathbf{e}_{\text{adv}}^T \mathbf{e}_{\text{adv}} \end{bmatrix}$, $\mathbf{F}_i = \bar{\mathbf{f}}_i \bar{\mathbf{f}}_i^T$, $\bar{\mathbf{f}}_i = \begin{bmatrix} \mathbf{f}_i^T & 1 \end{bmatrix}\ \forall\ i$. Figure 19 shows the false position solution for varying adversary desired locations $\mathbf{e}_{\text{adv}}$ with increasing distance from the true location.

5.2.3. Numerical Results: Evaluating Effectiveness and Efficiency of the Adversary's Redirection

This section evaluates the effectiveness and the efficiency of the adversary's redirection. The adversary determines the set of false sensor positions to inject for the maximum distance constraints (58)-(62) and for the penalized constraints in (71)-(76). For both cases, the false positions are reported to the location network's estimation algorithm outlined in (52)-(55).

To determine the effectiveness of our method, we evaluate the mean squared error between the adversary's desired emitter location and the network's estimate given the injected false positions, $||\mathbf{e}_{\text{adv}} - \hat{\mathbf{e}}_{\text{inj}}||^2$. To measure the efficiency of our solution, as a baseline, we compare against the trivial case of a translation where the adversary moves each sensor by $||\mathbf{d}||$ resulting in a total of $N||\mathbf{d}||$ meters. For our numerical simulations we set $\beta = 3$, $P_{\text{tx}} = 1000$, and perform 1000 Monte-Carlo runs.

Effectiveness: Mean Squared Error

We determine the MSE$=||\mathbf{e}_{\text{adv}} - \hat{\mathbf{e}}_{\text{inj}}||^2$, where $\hat{\mathbf{e}}_{\text{inj}}$ is the location estimate under the false injection. The performance of the semidefinite programming approach for localization without an adversary is used as a baseline for performance.

For the case of *maximum distance constraints*, the average MSE performance of our perturbation method is shown in Figure 20(a) for varying adversary desired locations. The traces from bottom to top correspond to values of $\mathbf{e}_{\text{adv}}$ with increasing distance from the true location $\mathbf{e}$. Observe that the MSE performance is on the same order as that of our baseline case, without injection and that it can be achieved for a wide range of adversary desired offsets. As the adversary's desired location moves farther away from its true value, the

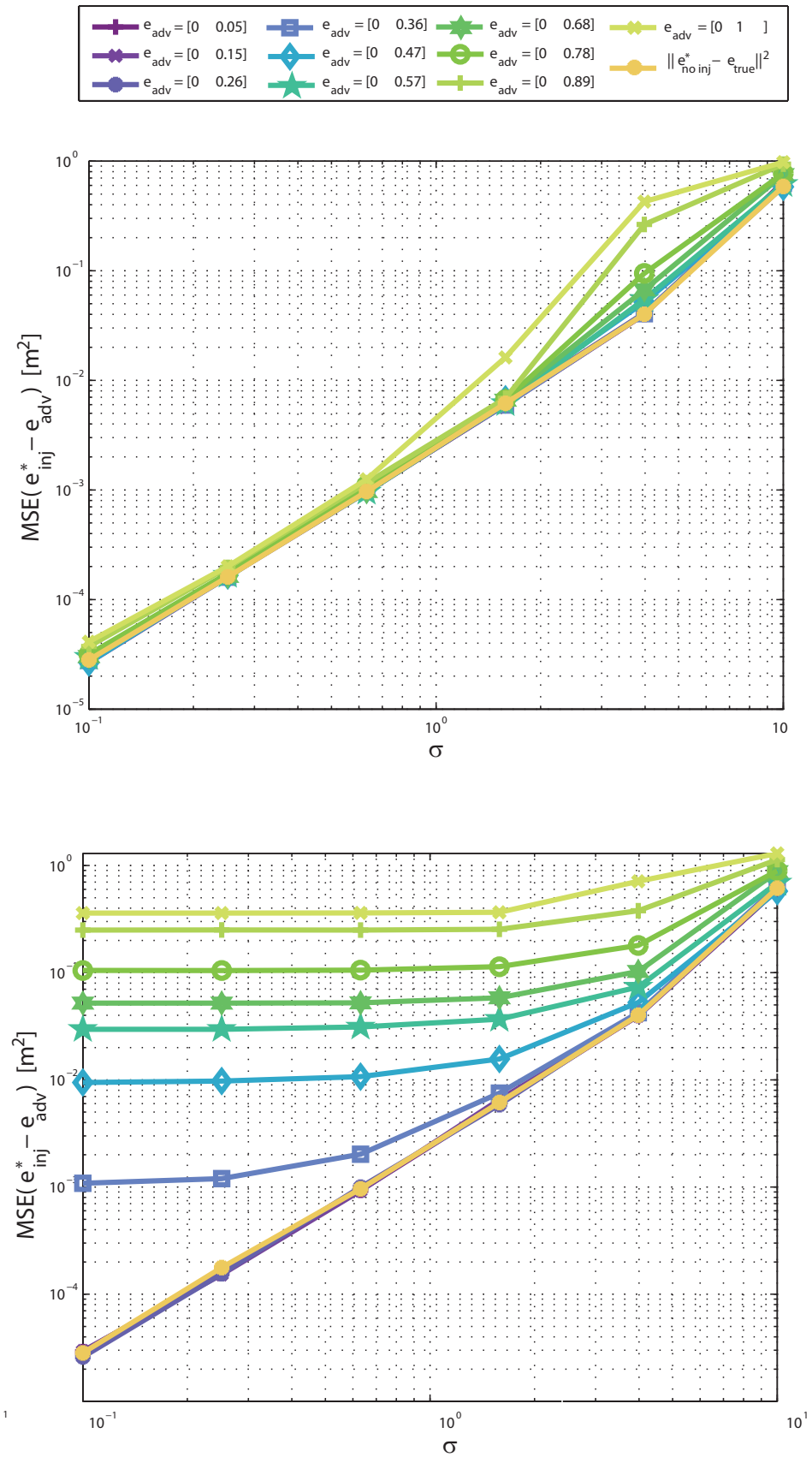


Figure 20: Average MSE performance for varying adversary desired locations: (a) Maximum distance constraints and (b) Penalized distance constraints.

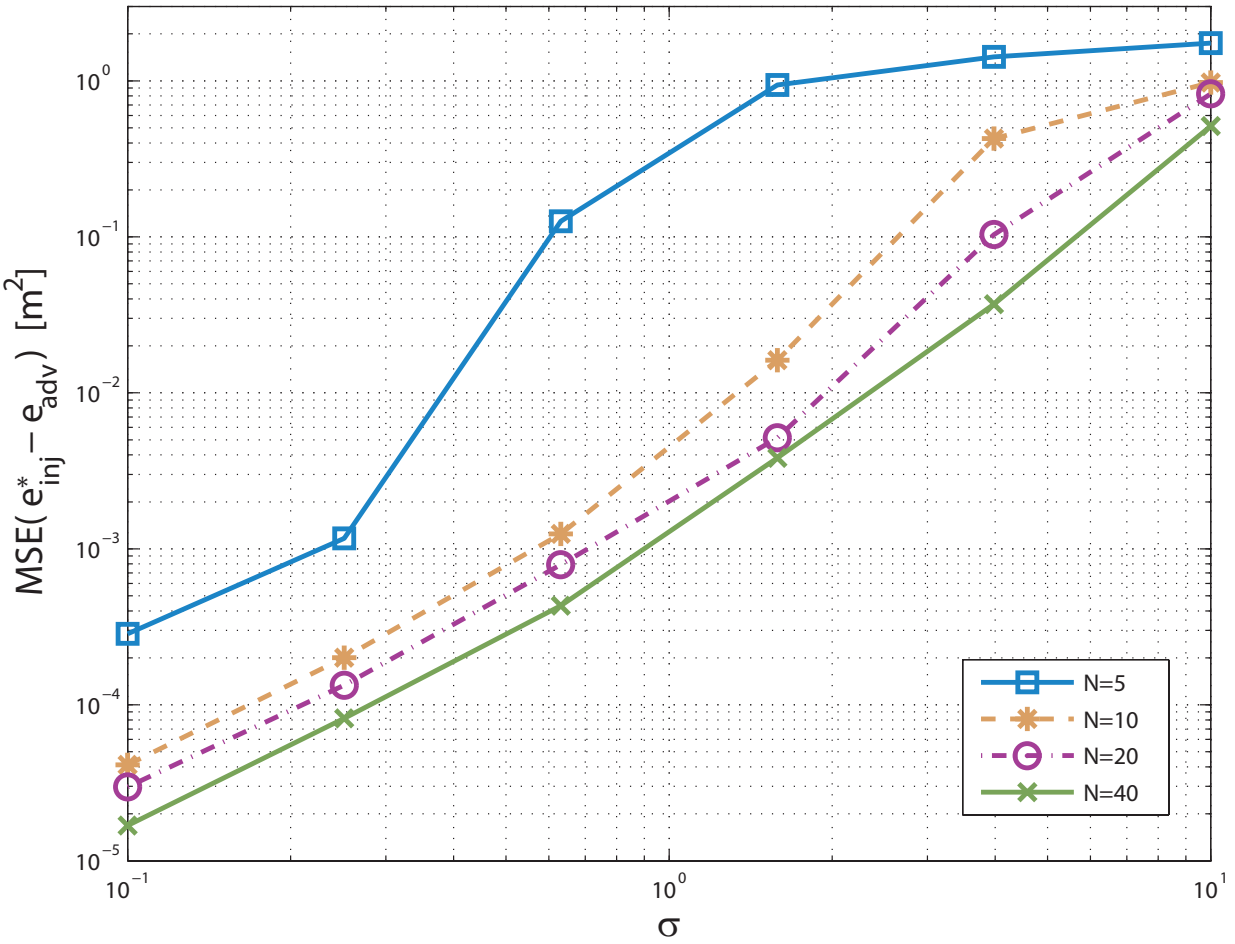


Figure 21: Average MSE performance for varying N and a fixed adversary desired location.

MSE increases. This increase occurs as the adversary desired location moves towards the boundary of the convex hull formed by the sensors.

Figure 21 shows the MSE performance for a fixed $\mathbf{e}_{\text{adv}}$ with a varying number of sensors. Observe that as the number of sensors increases, the MSE decreases. The additional sensors increase the network's density resulting in a decrease in error.

For the case of *penalized distance constraints* the average MSE performance of our perturbation method is shown in Figure 20(b), where $\lambda_i = 0.5$. Observe that for adversary desired locations with a smaller displacement from the true value we can achieve the same MSE as location performance without an adversary. As the adversary's desired location moves farther away from the emitter's true value, it is more difficult to achieve the adversary desired emitter location. Next we explore this behavior further and examine the trade-off between MSE and total sensor displacement.

Efficiency: Total Distance Required

We examine the efficiency of our approach by measuring the total displacement required by our SDP method. One solution for this problem is to simply translate each sensor by $\mathbf{d} = \mathbf{e}_{\text{adv}} - \mathbf{e}$. However, this translation requires that all the sensors be moved a total distance of $N||\mathbf{d}||$ as shown in Figure 22. We compare the displacement of our approach against the case of translating all sensors a total of $N||\mathbf{d}||$ meters and find our distance bounds provide a significant savings in the total sensor displacement.

Figure 23 shows the total distance moved for the case of maximum distance constraints. As the distance

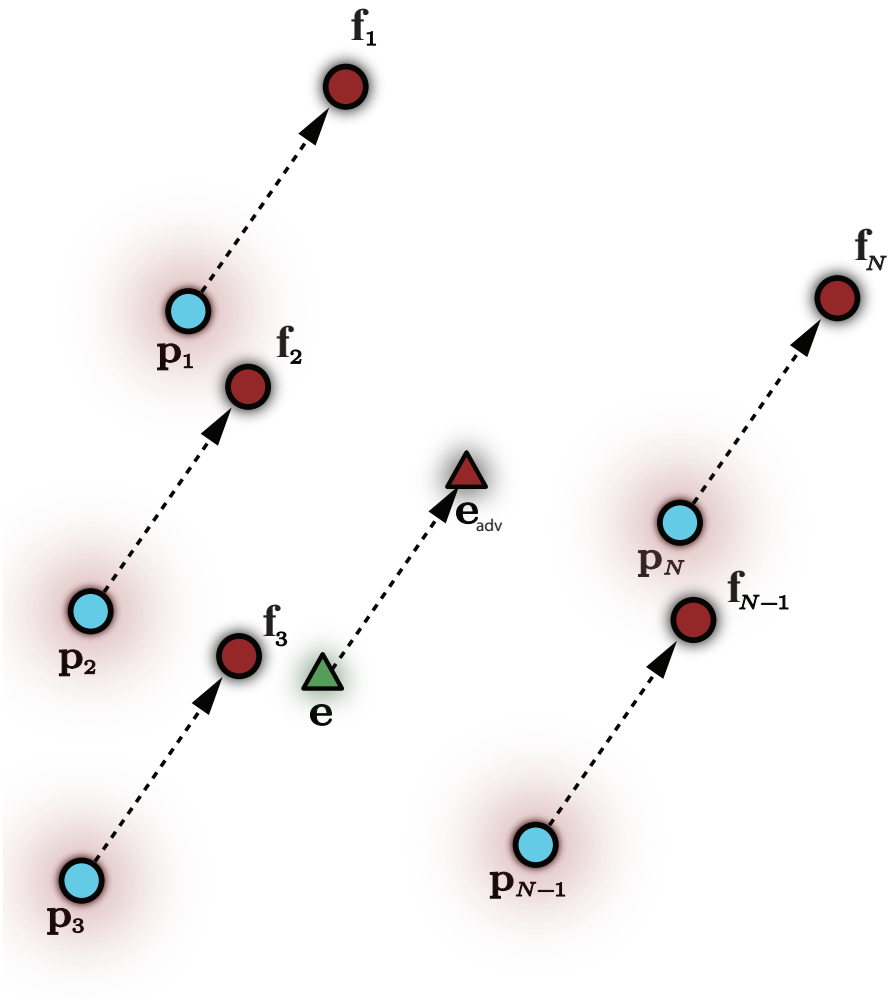


Figure 22: Translation Example

between the adversary desired location and its true value increases, the total distance required by our approach increases at a much slower rate. Our method obtains a significant savings over the trivial translation case in terms of total distance moved. Further, this savings increases as the number of sensors increases.

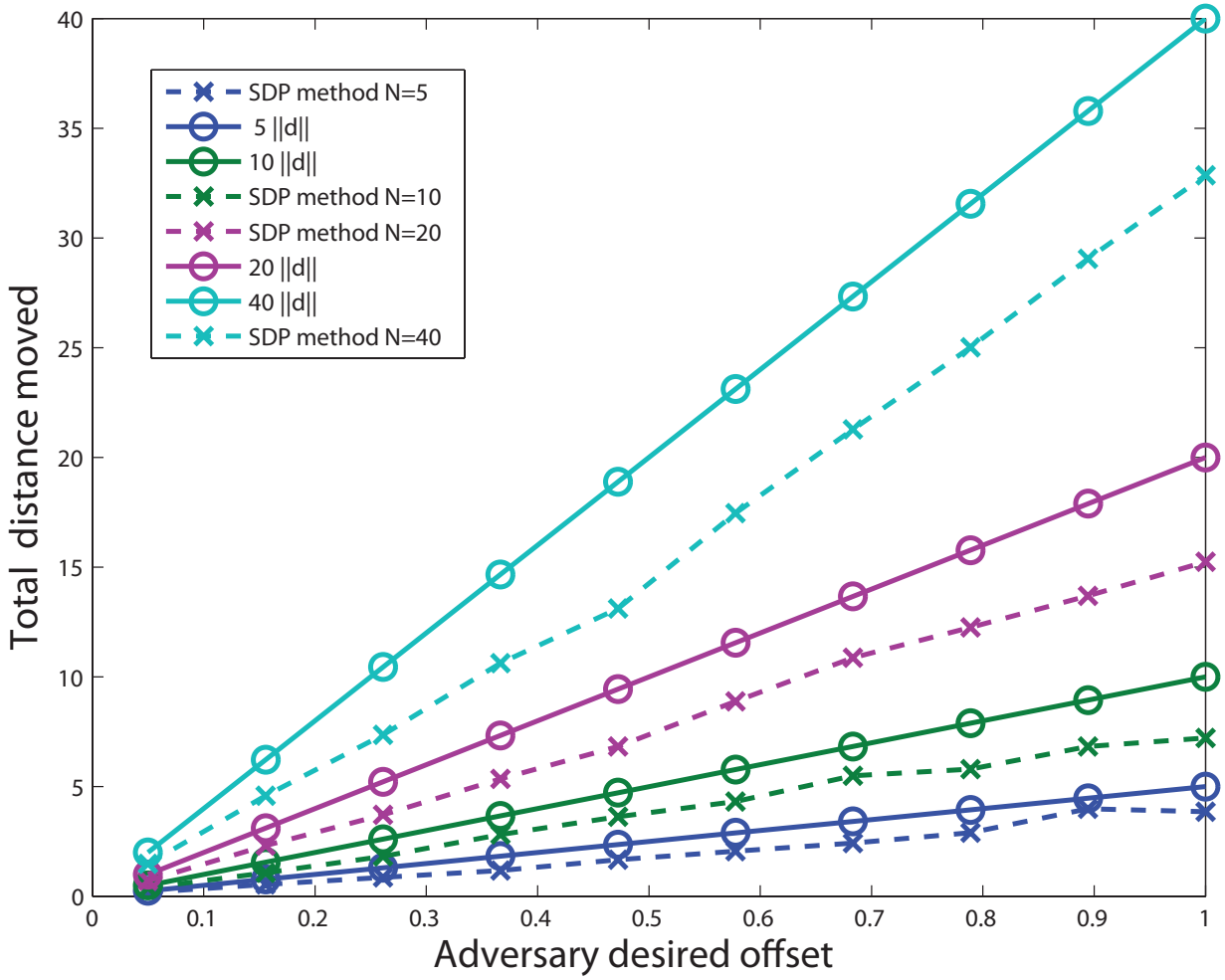


Figure 23: Total distance required for maximum distance constraints with a varying number of sensors.

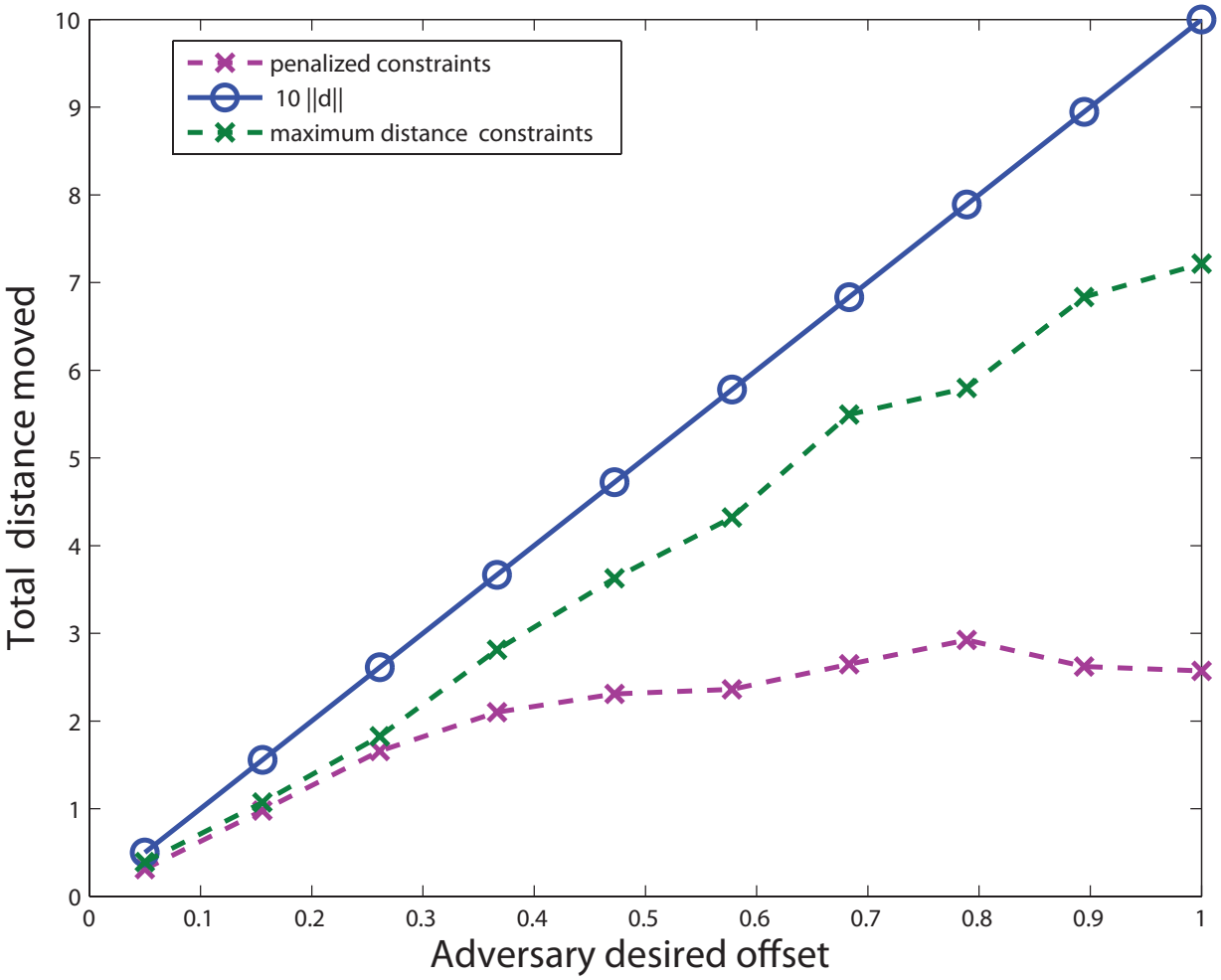


Figure 24: Total distance required using penalized constraints for $N = 10$ sensors.

Figure 24 shows the total distance required for the case of penalized constraints for a fixed number of sensors. Observe a significant savings in the total distance required over the case of maximum distance constraints. Also, note the trade-off between the MSE and the total distance required in Figure 20(b), where significant savings in the total distance can be achieved with a cost in MSE performance.

5.3. Discussion

This chapter develops adversary strategies to redirect the emitter location estimate. In the previous chapter, it was shown that the effect of the Fisher Information minimizing solution on the LS estimation processing is that only the M–1 non-corrupt pairs are used in the non-linear LS processing. From this observation and the error ellipse interpretation, we formulate two strategies that consider varying levels of adversary strength under a spatial restriction and content restriction. We show that under a spatial restriction, our solution introduces significant bias into the network. We formulate the scenario of a content restriction as a convex program using semidefinite program approach.

Directions for future work include exploration of sparsity under both spatial and content restrictions. Other directions include consideration of a time horizon where the adversary may have an injection budget and seeks to optimally inject false information over multiple time slots.

6.0. Methods: Network Strategies for Detecting and Mitigating the Adversary

The adversary strategies presented in Sections 4.0. and 5.0. assumed that the locating network was either unaware or unable to detect the adversary, resulting in maximum impact of the injection. This chapter explores the scenario where the locating network is aware an adversary may be present and develops strategies to detect and mitigate the adversary.

The first step towards network resilience is the ability to detect an adversary. We derive a detector to determine whether the adversary is present under both adversary strategies: (1) to minimize the FIM (Section 4.0.) and (2) to redirect the location estimate (Section 5.0.). Moving towards network resilience, the network's objective is not only to detect the adversary but also mitigate the effect of its the injection, i.e. operate without a degradation in accuracy. Two mitigating strategies are developed using robust and biased estimation.

6.1. Introduction to Detection Theory

Core to any detection problem is to determine whether a signal is present or absent [31]. This simple case can be framed as a binary hypothesis test,

$$\begin{array}{ll} H_0 : \mathbf{x} = \mathbf{n} & \text{signal absent} \\ H_1 : \mathbf{x} = \mathbf{s} + \mathbf{n} & \text{signal present} \end{array} \tag{77}$$

where $\mathbf{x}$ is the observed data, $\mathbf{n}$ is noise, and $\mathbf{s}$ is the signal of interest.

Determining an optimal detector depends on how much is known about the probability density functions (pdf) of both the signal and noise characteristics. They may be deterministic, or random with known or unknown parameters. In the case the pdfs under both hypotheses are completely known, the Neyman-Pearson test can be used. The Neyman-Pearson test seeks to maximize the probability of detection subject to a false alarm rate. The likelihood ratio test (LRT) decides in favor of H_1 if

$$L(\mathbf{x}) = \frac{p(\mathbf{x}; H_1)}{p(\mathbf{x}; H_0)} > \gamma \tag{78}$$

where

$$P_{\text{FA}} = \int_{\mathbf{x}: l(\mathbf{x}) > \gamma} p(\mathbf{x}; H_0)\, d\mathbf{x} = \alpha \tag{79}$$

In practice, however, the pdfs may not be known exactly, prohibiting design of optimal detectors. Cases where the pdfs have unknown parameters are referred to as *composite hypothesis testing*. There are two main approaches: (1) Bayesian where a prior pdf is assigned and (2) estimation of the unknown parameters for a LRT. The latter, generalized likelihood ratio test (GLRT) is used frequently in practice since it does not require such harsh assumptions and is easy to implement. Although the GRLT is not an optimal detector, it has been shown to perform well. The GLRT is given by

$$L_{\text{G}}(\mathbf{x}) = \frac{p\left(\mathbf{x}; \hat{\boldsymbol{\theta}}_1, H_1\right)}{p\left(\mathbf{x}; \hat{\boldsymbol{\theta}}_0, H_0\right)} > \gamma \tag{80}$$

where $\hat{\boldsymbol{\theta}}_i$ is the MLE of $\boldsymbol{\theta}_i$ assuming H_i is true.

The goal of hypothesis testing is to correctly decide on a particular hypothesis. One method of summarizing a detector's performance is using a receiver operating characteristic (ROC). The ROC plots probability of detection versus the probability of false alarm. All ROC curves should be greater than the 45 degree line as it corresponds to a fair coin flip.

Table 2: Evaluation of the RHS of (86) evaluated under both hypotheses averaged over 2000 geometries each with 20 sensors.

		H_0 (no adversary $\mathbf{p}_{\text{rep}} = \mathbf{p}_{\text{act}}$)	H_1 (adversary is present $\mathbf{p}_{\text{rep}} \neq \mathbf{p}_{\text{act}}$)
SNR	noise free	3.2e-16	9.4e-09
	20 dB	4.2e-08	6.4e-08
	15 dB	7.4e-08	1e-07

6.2. Adversary Detector for TDOA

The main contribution of this section is the development of an adversary detector under the TDOA method. A simple binary hypothesis test is developed and it is observed that the test is a function of the true emitter location, which is unknown to the locating network. By substituting the emitter location estimate for its true value, and observing that certain parameters can be approximated as zero, the network's hypothesis test is derived.

In order to detect the adversary, consider a test on the residual TDOA by comparing the measured TDOAs where $\hat{\boldsymbol{\tau}} \sim \mathcal{N}\left(\boldsymbol{\tau}(\mathbf{e}, \mathbf{p}_{\text{act}}), \sigma^2 \mathbf{I}\right)$ with TDOAs computed using the reported sensor positions, $\boldsymbol{\tau}(\mathbf{e}, \mathbf{p}_{\text{rep}})$.

The network does not know the emitter location exactly but has an estimate $\hat{\mathbf{e}}$. By taking $\boldsymbol{\tau}(\mathbf{e}, \mathbf{p}_{\text{rep}}) \approx \boldsymbol{\tau}(\hat{\mathbf{e}}, \mathbf{p}_{\text{rep}})$, the binary hypothesis test is given by

$$H_o : \hat{\boldsymbol{\tau}} - \boldsymbol{\tau}(\hat{\mathbf{e}}, \mathbf{p}_{\text{rep}}) \approx \hat{\boldsymbol{\tau}} - \boldsymbol{\tau}(\mathbf{e}, \mathbf{p}_{\text{act}}) = \mathbf{n} \sim \mathcal{N}(\mathbf{0}, \sigma^2 \mathbf{I}) \tag{81}$$

$$H_1 : \hat{\boldsymbol{\tau}} - \boldsymbol{\tau}(\hat{\mathbf{e}}, \mathbf{p}_{\text{rep}}) \approx \mathbf{n} + \underbrace{\boldsymbol{\tau}(\mathbf{e}, \mathbf{p}_{\text{act}}) - \boldsymbol{\tau}(\mathbf{e}, \mathbf{p}_{\text{rep}})}_{\mathbf{r}} \sim \mathcal{N}(\mathbf{r}, \sigma^2 \mathbf{I}) \tag{82}$$

where $\mathbf{r}$ is the difference in TDOA due to the adversary's injection, $\mathbf{r} \neq \mathbf{0}$, and $||\mathbf{r}||_0 = 1$ indicates there is only one non-zero element of $\mathbf{r}$.

To write the test in (81)-(82) requires that: (1) $\boldsymbol{\tau}(\hat{\mathbf{e}}, \mathbf{p}_{\text{rep}}) \approx \boldsymbol{\tau}(\mathbf{e}, \mathbf{p}_{\text{rep}})$ and (2) $\mathbf{r} = \boldsymbol{\tau}(\mathbf{e}, \mathbf{p}_{\text{act}}) - \boldsymbol{\tau}(\mathbf{e}, \mathbf{p}_{\text{rep}})$ is the relevant detection quantity.

1. We examine the value of $\boldsymbol{\tau}(\hat{\mathbf{e}}, \mathbf{p}_{\text{rep}}) - \boldsymbol{\tau}(\mathbf{e}, \mathbf{p}_{\text{rep}})$ under both hypotheses. The m^{th} row, consisting of sensors i and j gives

$$[(\boldsymbol{\tau}(\mathbf{e}, \mathbf{p}_{\text{rep}}) - \boldsymbol{\tau}(\hat{\mathbf{e}}, \mathbf{p}_{\text{rep}}))]_m = \frac{1}{c}(||\mathbf{e} - \mathbf{p}_i|| - ||\hat{\mathbf{e}} - \mathbf{p}_i||) - \frac{1}{c}\left(||\mathbf{e} - \mathbf{p}_j|| - ||\hat{\mathbf{e}} - \mathbf{p}_j||\right). \tag{83}$$

   From the reverse triangle inequality, shown in Figure 25 (a)

$$|\, ||\mathbf{e} - \mathbf{p}_i|| - ||\hat{\mathbf{e}} - \mathbf{p}_i||\, | \;\leq\; ||\mathbf{e} - \hat{\mathbf{e}}|| \tag{84}$$

$$|\, |\mathbf{e} - \mathbf{p}_j|| - ||\hat{\mathbf{e}} - \mathbf{p}_j||\, | \;\leq\; ||\mathbf{e} - \hat{\mathbf{e}}||. \tag{85}$$

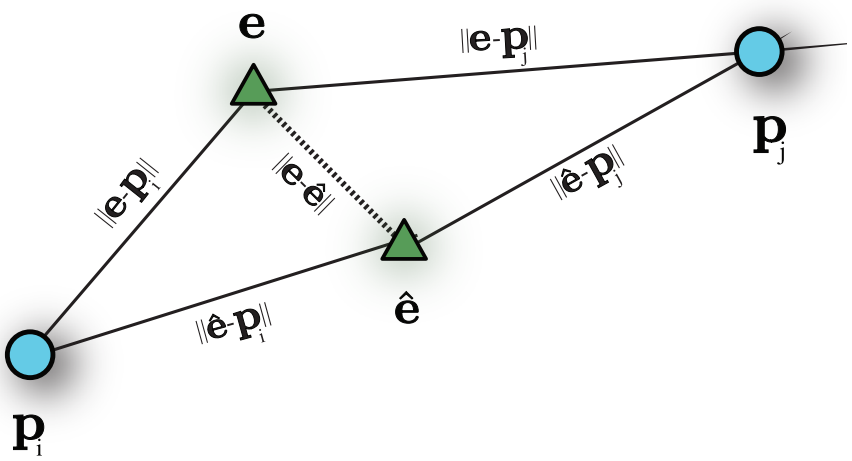
   Thus, both $||\mathbf{e} - \mathbf{p}_i|| - ||\hat{\mathbf{e}} - \mathbf{p}_i||$ and $||\mathbf{e} - \mathbf{p}_j|| - ||\hat{\mathbf{e}} - \mathbf{p}_j||$ lie in the interval, $[-||\mathbf{e} - \hat{\mathbf{e}}||, +||\mathbf{e} - \hat{\mathbf{e}}||]$. Taking the difference in (83) gives,

$$|\boldsymbol{\tau}(\mathbf{e}, \mathbf{p}_{\text{rep}}) - \boldsymbol{\tau}(\hat{\mathbf{e}}, \mathbf{p}_{\text{rep}})| \leq \frac{2}{c}||\mathbf{e} - \hat{\mathbf{e}}||\mathbf{1}_{M \times 1} \tag{86}$$

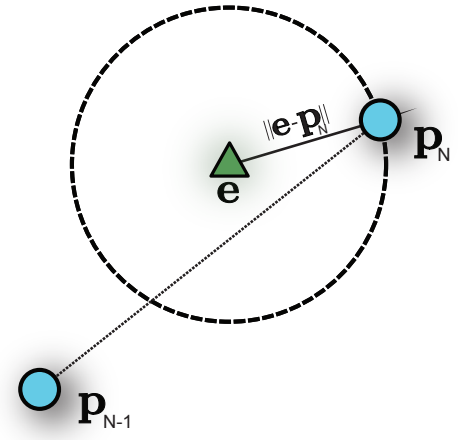
   where the upper bound depends on the distance between the estimate and its true value. The error is dependent on SNR and the adversary strategy used. The maximum value of the RHS of (86) across strategies is shown in Table 2 under both hypotheses. It is observed that (86) is upper bounded by a small value such that $\boldsymbol{\tau}(\hat{\mathbf{e}}, \mathbf{p}_{\text{rep}}) \approx \boldsymbol{\tau}(\mathbf{e}, \mathbf{p}_{\text{rep}})$.

2. Given that $\boldsymbol{\tau}(\hat{\mathbf{e}}, \mathbf{p}_{\text{rep}}) \approx \boldsymbol{\tau}(\mathbf{e}, \mathbf{p}_{\text{rep}})$, the rise in TDOA is

$$\mathbf{r} = \boldsymbol{\tau}(\mathbf{e}, \mathbf{p}_{\text{act}}) - \boldsymbol{\tau}(\mathbf{e}, \mathbf{p}_{\text{rep}})\,. \tag{87}$$



(a) Sensors $\mathbf{p}_i$ and $\mathbf{p}_j$ are paired. The true emitter location and its estimate are given by $\mathbf{e}$ and $\hat{\mathbf{e}}$.



(b) Sensors $\mathbf{p}_{\text{N-1}}$ and $\mathbf{p}_{\text{N}}$ are paired.

Figure 25: (a) Illustration of the reverse triangle inequality in (84)-(85) and (b) Illustration of the rise in TDOA.

Since there is only one-non-zero entry of $\mathbf{r}$, the actual value of the rise in TDOA given that the N^{th} sensor is corrupted is

$$\mathbf{r}_{\text{non-zero}} \quad = \quad \frac{1}{c}\left(||\mathbf{e}-\mathbf{p}_f||-||\mathbf{e}-\mathbf{p}_N||\right). \tag{88}$$

Consider the implication of (88) shown by the pair of sensors in Figure 25(b). Any point along the circle with radius $||\mathbf{e}-\mathbf{p}_N||$ selected as the false position $\mathbf{p}_f$ receives the signal at the same time as $\mathbf{p}_N$. Thus, there is no change in TDOA for any sensor position selected along this circle. Clearly, the value of (88) cannot be ignored as the corrupt pair's TDOA will change as $\mathbf{p}_f$ moves away from the circle in either direction along the vector from $\mathbf{e}$ to $\mathbf{p}_N$. As a result, we see that $\mathbf{r}$ is the relevant detection quantity.

Figure 26 shows the detection problem set-up with the network's known parameters: the measured

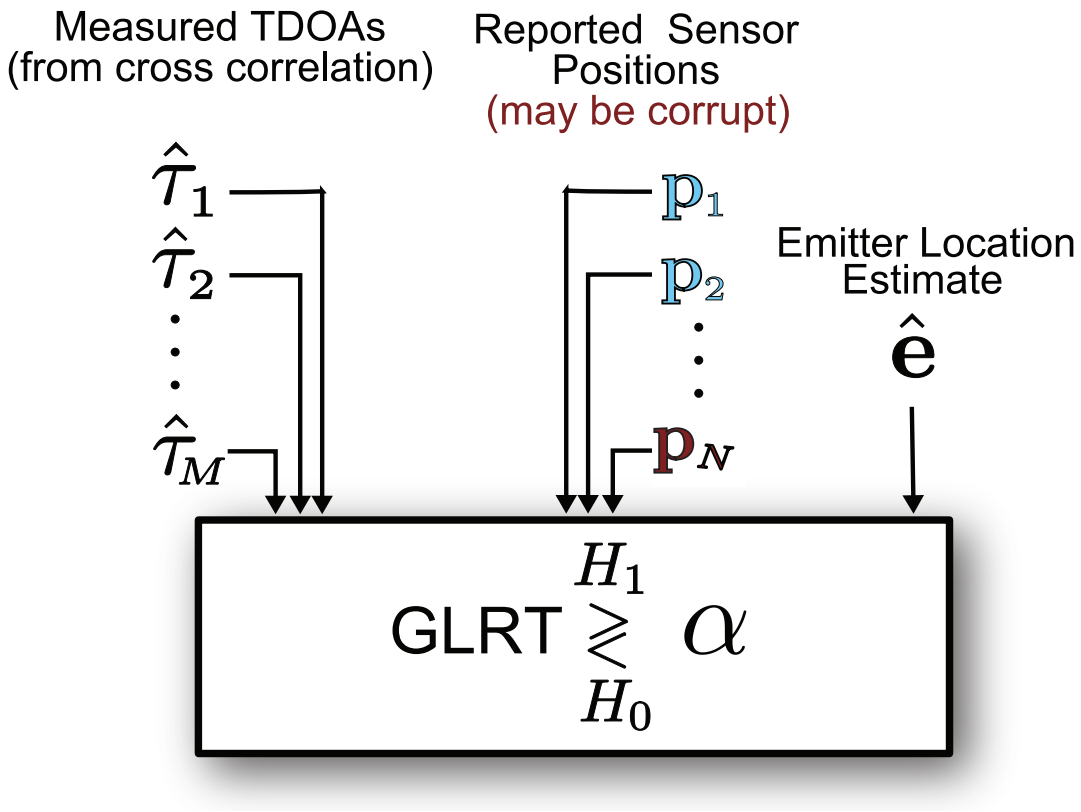


Figure 26: Detection Problem Setup - Locating Network's Known Parameters.

TDOAs, the reported sensor positions (which may be corrupt), and the emitter location estimate. The generalized likelihood ratio test (GRLT) decides in favor of H_1 if

$$L(\hat{\boldsymbol{\tau}} - \boldsymbol{\tau}(\hat{\mathbf{e}}, \mathbf{p}_{\text{rep}})) = \frac{\max_{\mathbf{r}} p(\hat{\boldsymbol{\tau}} - \boldsymbol{\tau}(\hat{\mathbf{e}}, \mathbf{p}_{\text{rep}}); \mathbf{r}, H_1)}{p(\hat{\boldsymbol{\tau}} - \boldsymbol{\tau}(\hat{\mathbf{e}}, \mathbf{p}_{\text{rep}}), H_0)} > \alpha \tag{89}$$

The log likelihood ratio is

$$\Lambda = \min_{\mathbf{r}} \quad -\frac{1}{2\sigma^2}\left(-2\left[\hat{\boldsymbol{\tau}} - \boldsymbol{\tau}(\hat{\mathbf{e}}, \mathbf{p}_{\text{rep}})\right]^T \mathbf{r} + \mathbf{r}^T \mathbf{r}\right) \underset{H_0}{\overset{H_1}{\gtrless}} \ln \alpha \tag{90}$$

Rearranging gives

$$\Lambda = \min_{\mathbf{r}} \quad -2\left[\hat{\boldsymbol{\tau}} - \boldsymbol{\tau}(\hat{\mathbf{e}}, \mathbf{p}_{\text{rep}})\right]^T \mathbf{r} + \mathbf{r}^T \mathbf{r} \underset{H_1}{\overset{H_0}{\lessgtr}} -2\sigma^2 \ln \alpha \tag{91}$$

Due to the sparsity constraint on $\mathbf{r}$, the problem is

$$\min_{\mathbf{r}} \quad -2\left[\hat{\boldsymbol{\tau}} - \boldsymbol{\tau}(\hat{\mathbf{e}}, \mathbf{p}_{\text{rep}})\right]^T \mathbf{r} + \mathbf{r}^T \mathbf{r} \tag{92}$$

$$\text{s.t.} \quad ||\mathbf{r}||_0 = 1 \tag{93}$$

Since there is only one non-zero entry of $\mathbf{r}$, defined as $\mathbf{r}_i$ the problem can be written as

$$\min_i \min_{\mathbf{r}_i} \quad -2\left[\hat{\boldsymbol{\tau}} - \boldsymbol{\tau}(\hat{\mathbf{e}}, \mathbf{p}_{\text{rep}})\right]_i \mathbf{r}_i + \mathbf{r}_i^2 \tag{94}$$

where solving the inner optimization problem gives

$$\mathbf{r}_i^* = \left[\hat{\boldsymbol{\tau}} - \boldsymbol{\tau}\left(\hat{\mathbf{e}}, \mathbf{p}_{\text{rep}}\right)\right]_i . \tag{95}$$

Replacing into (94) gives

$$\Lambda = \max_i \; -\frac{\left(\left(\hat{\boldsymbol{\tau}} - \boldsymbol{\tau}\left(\hat{\mathbf{e}}, \mathbf{p}_{\text{rep}}\right)\right)_i\right)^2}{\sigma^2} \underset{H_1}{\overset{H_0}{\gtrless}} -2\ln\,\alpha \tag{96}$$

$$= \max_i \; \frac{\left(\left(\hat{\boldsymbol{\tau}} - \boldsymbol{\tau}\left(\hat{\mathbf{e}}, \mathbf{p}_{\text{rep}}\right)\right)_i\right)^2}{\sigma^2} \underset{H_0}{\overset{H_1}{\lessgtr}} 2\ln\,\alpha \tag{97}$$

6.2.1. Evaluating P_{D} under each Adversary Strategy

We evaluate the detection performance by computing the test in (97). Under each adversary strategy, the probability of detection and false alarm are estimated. For each geometry, the false sensor position is determined according to the adversary strategy where 1000 Monte-Carlo runs are performed and then averaged over 2000 geometries.

Minimizing Network Accuracy

The set of sensor positions along the line in (40) all minimize the Fisher Information. However, each sensor position results in a different detection performance. Figure 27 shows that any falsified sensor position at the same distance from the emitter as the sensor's true position does not change the value of TDOA as shown by the dashed circle. The sensor positions from (40) are marked with an "**x**". The intersection of the dashed circle and line solution in (40) is the false sensor position that not only minimizes the FIM but also does not alter the corrupt pair's TDOA value and is shown in red.

Figure 28(a) shows the receiver operating characteristic (ROC) curves for increasing distances away from the circle-line intersection point. The intersection point corresponds to $\mathbf{r} = 0$ in the binary hypothesis set-up. The corresponding ROC curve is the 45 degree line indicating the locating network should flip a coin to decide if an adversary is present. Since the corrupt pair's TDOA is the same as if the rogue sensor was reporting its true value, the injection is undetectable to the network. Figure 28(a) shows that as the distance from the circle-line intersection point increases, so does the probability of detection.

Redirecting the Emitter Location Estimate

Figure 28(b) shows the ROC curve for varying values of the adversary desired offset. As the adversary desired offset increases, the probability of detection increases. This is expected since a larger adversary offset causes a larger TDOA residual making the adversary more detectable to the network.

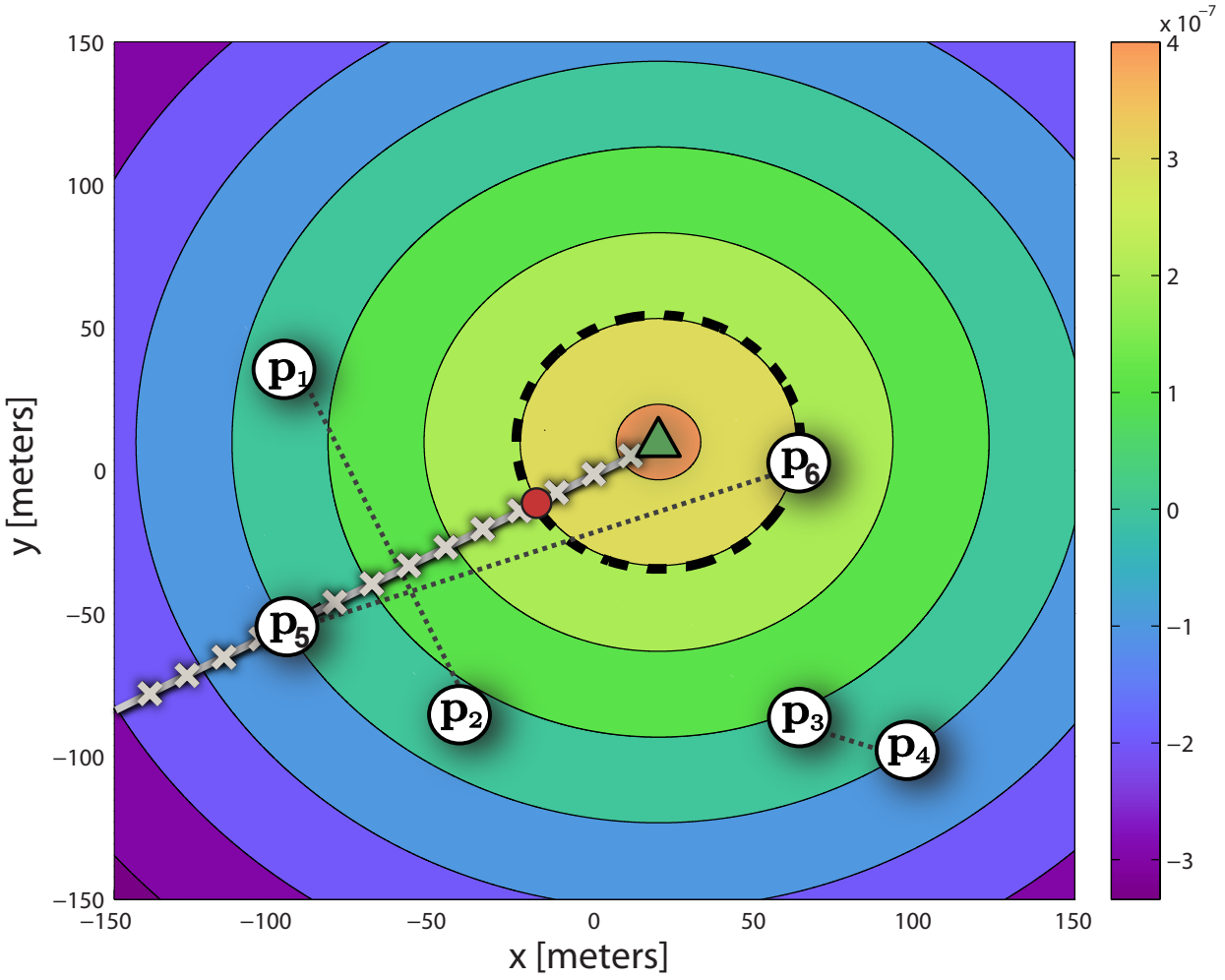
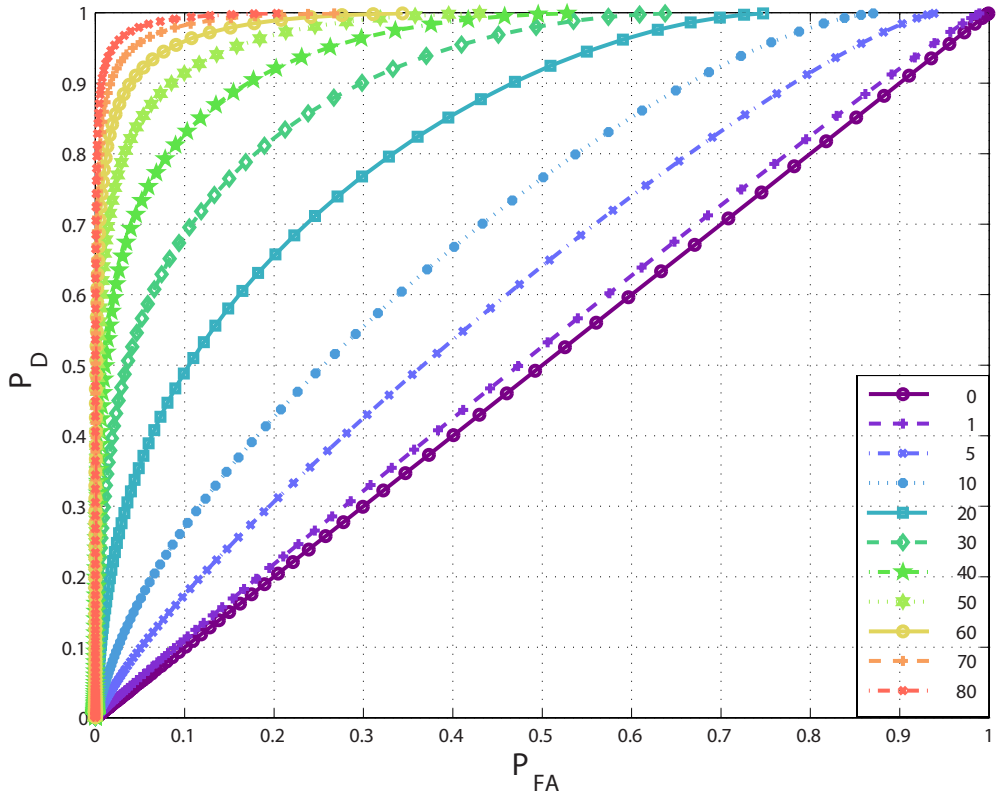
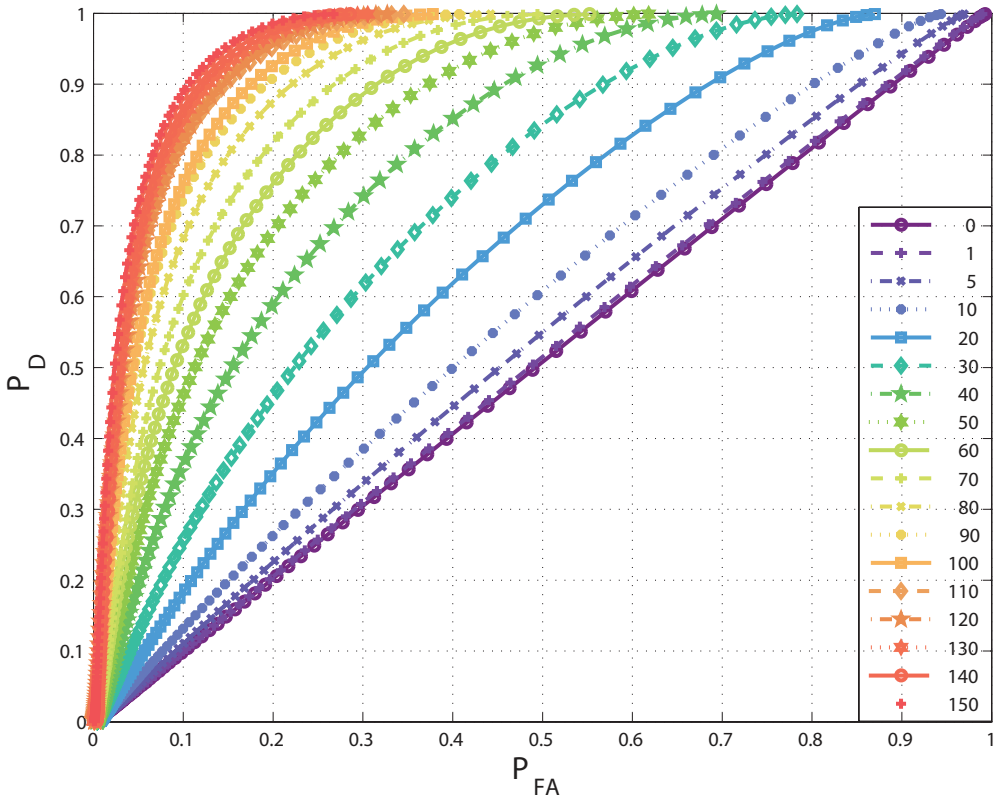


Figure 27: Evaluation of the TDOA over grid locations. Six sensors are used and are paired as shown by the dotted line. The emitter is located at [20 10]. A total of 2000 sensor-emitter geometries were considered, each with 20 sensors.



(a)



(b)

Figure 28: Receiver Operating Characteristics under both Adversary Strategies: (a) Minimizing accuracy strategy, SNR= 20dB. Each curve is a different adversary desired offset distance from the intersection point, (b) Redirecting Strategy, SNR= 20dB. Each curve is a different adversary desired offset distance. A total of 2000 sensor-emitter geometries were considered, each with 20 sensors.

6.3. Mitigating the Adversary

The first half of this chapter discussed the locating network's goal to detect the presence of an adversary. While this is a necessary first step, the network's ultimate goal of resiliency is to perform its estimation mission even in spite of such corruption.

Two methods for mitigating the adversary are introduced. We consider the use of biased estimation. Then, we develop mitigation strategies using tools from robust estimation and biased estimation. We show the relationship between MSE and the strength of the adversary's injection and indicate when the locating network should use either non-linear LS or LMS to most effectively remove the influence of the injection. Two biased estimators are developed under TDOA, where we remove the restriction of a reference sensor in previous work. Specifically, the minimax trace MSE and minimax matrix MSE biased estimators for TDOA are derived, which hold under any sensor pairing scheme.

6.3.1. Robust Estimation: Beyond Least Squares Estimation

It is well known that least squares (LS) estimation is susceptible to outliers. In fact, even a single outlier can greatly impact the estimator, which is known as a breakdown or leverage point [58]. A natural consideration is the use of robust statistical techniques [29,57,58] to remove the sensitivity to outliers. In robust regression, the goal is to develop estimators that are not strongly influenced by outliers.

Instead of minimizing the sum of squared residual in least squares estimation, another operator such as absolute value or the median can be used [57]. In least absolute values regression or l_1 regression, the sum of absolute values is minimized. Disappointingly, the breakdown point of this estimator is not greater than 0%. A number of other robust estimators have been proposed including those from Wald, Nair and Shrivastava, Bartlett, Brown, Mood, the median of pair slopes, the resistant line, R-estimators, and L-estimators. Despite numerous methods, they do not exceed a breakdown point greater than 30% for simple regression. Sigiegel suggested an iterative method using repeated medians. This estimator required significant computation as it is necessary to determine all subsets of the observations. Thus, the sum in the classical LS estimator is replaced by the median of the squared residuals, known as Least Median Squares (LMS). It is well known that the breakdown point of LMS is up to 50%. We focus on LMS as our robust estimator of choice.

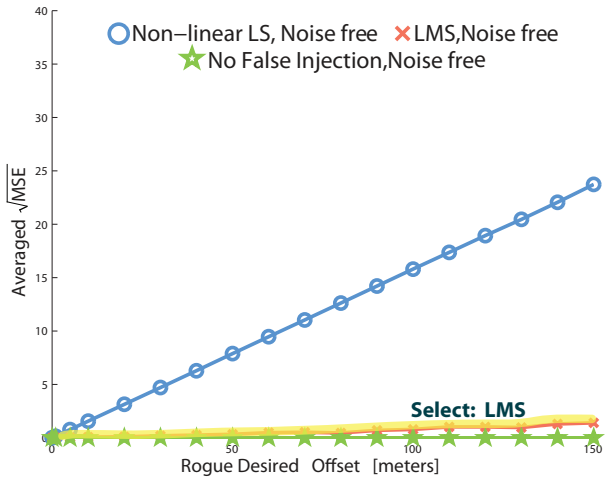
Robust Estimation Strategy: When to use LMS

In Chapter 5.0. the use of robust estimation, specifically LMS was considered. Figure 29 shows the same MSE performance of a locating network that uses non-linear LS or LMS estimation but is now considered from the network's viewpoint as highlighted in yellow. Observe that the strength of the adversary's injection dictates whether non-linear LS or LMS is a more effective mitigating strategy. In the presence of noise, Figure 29 (b)-(c) each show that for smaller adversary offsets, non-linear LS should be used as the mitigating strategy and for higher offsets LMS should be selected. The value of the adversary's strength at the cross-over point of the red and blue traces dictates when the network should use each strategy. This switching point is also clearly a function of the SNR.

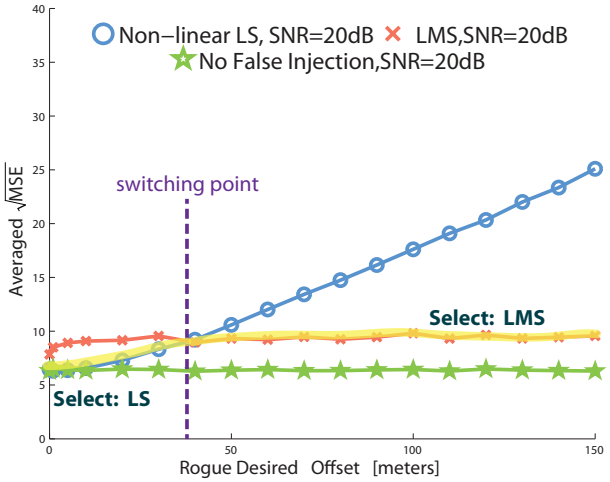
6.3.2. Beyond Unbiased Estimation

Despite the fact that the unbiased property may be intuitively pleasing, it finds an estimator whose optimality is based on the difference between $\hat{\boldsymbol{\theta}}$ and its average value versus $\hat{\boldsymbol{\theta}}$ and its true value. The use of biased estimation over traditional unbiased approaches has attracted interest due to its ability to reduce the variance by increasing the bias. However, for practical problems, it is not known what the bias should be. Simply choosing a bias is not very useful since an estimate can be found to yield a zero bias and variance, i.e. for a fixed $\boldsymbol{\theta}_0$, choose $\hat{\boldsymbol{\theta}} = \boldsymbol{\theta}_0$ which is not useful unless we have $\boldsymbol{\theta}_0$. As such, a bias must be determined such that the resulting MSE is guaranteed for all values of the unknown parameter. In [10], these issues are discussed and the author finds it is possible to choose a bias that results in a lower MSE than the Cramer Rao Bound (CRB) for all values of the parameter.

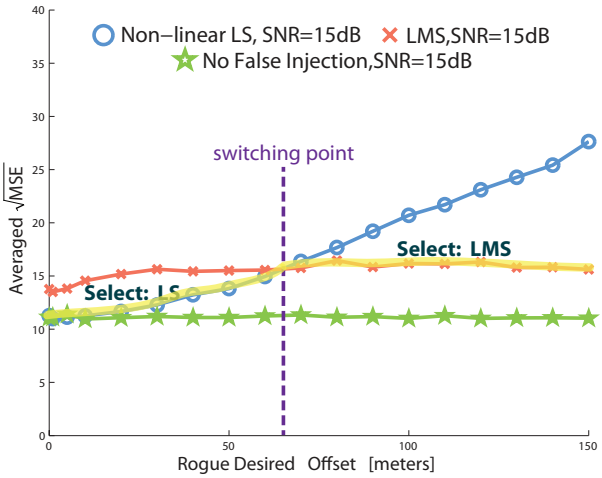
There are two main approaches for design of biased estimators. The first biased estimator uses a minimax trace MSE (MXTM) approach, which is known to obtain a smaller trace MSE than the worst case MSE of the least squares estimator. The MXTM method, however, does not make any guarantees about the



(a) Noise free



(b) SNR=20dB



(c) SNR=15dB

Figure 29: Mean squared error performance for non-linear LS and LMS. A total of 2000 sensor-emitter geometries were considered, each with 20 sensors.

component-wise error. The second biased estimator uses a minimax matrix MSE (MXMM) approach, which ensures that the component-wise MSE is less than that of the traditional LS estimator [11].

A biased estimator is developed for the emitter location problem under the time difference of arrival (TDOA) method that holds for any sensor pairing scheme. The most closely related work determines a biased estimator for TDOA using minimax trace MSE approach under a centralized sensor set-up where each sensor is paired with a reference sensor [9]. While the reference sensor can be carefully chosen to ensure a good sensor-emitter geometry, it is not ideal to have a fully centralized set-up. From a fault tolerant viewpoint, a single reference sensor can be easily compromised whether due to a hardware failure or by an intelligent adversary. Compromise of the reference sensor can seriously impact the network's location estimate since every TDOA measurement is affected. This fault tolerant consideration is especially important in case where an adversary is present in the network. If the adversary corrupts the reference sensor, then the network would be severely compromised. We remove the restriction of using a reference sensor, enabling the use of any sensor pairing scheme. A set of biased estimators for TDOA are developed, which allows for any arbitrary sensor pairing scheme. The biased estimators show a reduction in MSE for low SNR.

6.3.3. Related Work

In [44, 66], a biased estimator is designed for source localization under the time of arrival (TOA) method. In [66] the authors compare the performance of linear least squares estimation, linear biased estimation, and affine biased estimation. In terms of MSE, the affine biased estimator performs best, then the linear biased estimator, and finally the linear least squares estimator. In [44], the performance of the linear least squares estimator is compared with the MXTM and MXMM approaches. The trace method provides a smaller trace MSE as compared with the LS estimator while the matrix method provides a smaller trace MSE and a smaller component-wise MSE over the LS estimator. In [9], source localization with TDOA was considered and a biased estimator developed. The authors use the MXTM approach, which provides an improvement in accuracy.

6.3.4. System Model under Time Difference of Arrival

The TDOA model has been given in previous chapters, where the TDOA measurement of pair m is given by

$$\hat{\tau}_m = \frac{1}{c}\left(||\mathbf{p}_i - \mathbf{e}|| - ||\mathbf{p}_j - \mathbf{e}||\right) + n_m \tag{98}$$

and the noise from all pairs , $\mathbf{n} \sim \mathcal{N}(\mathbf{0}, \mathbf{C})$.

The MXTM method under TDOA is derived in [9] and is outlined as follows. Each sensor is paired with a common reference sensor, Sensor 1. The noisy distance measurements are given by

$$d_{k1} = ||\xi_k - \xi_0|| - ||\xi_1 - \xi_0|| + n_{k1}, \quad k = 2, \ldots, M \tag{99}$$

where ξ_k is the position of the k^{th} sensor. By re-arranging and squaring both sides of (99),

$$\left(\xi_k - \xi_1\right)^T \xi_0 + d_{k1}\rho = \frac{1}{2}\left[\left(\xi_k - \xi_1\right)^T \left(\xi_k + \xi_1\right) - d_{k1}^2\right] + e_k \tag{100}$$

where $e_k = n_{k1}\left(||\xi_k - \xi_0|| + \frac{n_{k1}}{2}\right)$ is the noise. The LS system is given by

$$\mathbf{G}\boldsymbol{\theta} = \mathbf{h} + \mathbf{e} \tag{101}$$

where $\boldsymbol{\theta} = \left[\xi_0^T \rho\right]^T$, $\mathbf{G} = \begin{bmatrix} \xi_2^T - \xi_1^T & d_{21} \\ \vdots & \vdots \\ \xi_M^T - \xi_1^T & d_{M1} \end{bmatrix}$, $\mathbf{h} = \begin{bmatrix} \left(\xi_2 - \xi_1\right)^T \left(\xi_2 + \xi_1\right) - d_{21}^2 \\ \vdots \\ \left(\xi_M - \xi_1\right)^T \left(\xi_M + \xi_1\right) - d_{M1}^2 \end{bmatrix}$, and $\mathbf{e} = [n_{21}||\xi_2 - \xi_0||, \ldots, n_{M1}||\xi_M - \xi_0||]^T$. This approach only holds for the case where each sensor is paired with the same reference sensor. While the choice of the reference sensor can certainly be optimized, from a fault tolerant perspective an independent pairing scheme is preferable.

6.3.5. TDOA estimation under independent sensor pairings

The least squares equations of emitter location can be written by either: (1) squaring the quantity in (102) and writing a set of LS equations, or by (2) taking the Taylor series approximation. We use the latter form to remove the dependency on the reference sensor.

The noisy distance measurements are given by

$$\tilde{d}_m = d_m + v_m \;\forall\; m \tag{102}$$

where $d_m = \left(||\mathbf{p}_i - \mathbf{e}|| - ||\mathbf{p}_j - \mathbf{e}||\right)$ is the true distance between sensors in the m^{th} pair. The additive noise on the TDOAs are distributed as $\mathcal{N}(\mathbf{0}, \mathbf{C})$. Thus, the noise on the distance measurement is $\mathbf{v} \sim \mathcal{N}(\mathbf{0}, \Sigma)$ where $\Sigma = c^2\mathbf{C}$. Re-arranging and denoting the functional dependence on $\mathbf{e}$ gives

$$f_m(\mathbf{e}) = d_m(\mathbf{e}) = \tilde{d}_m - v_m \tag{103}$$

where the goal is to estimate $\mathbf{e}$ from the set of measurements $\left\{\tilde{\mathbf{d}}_m\right\}_{m=1}^{M}$. Let $\mathbf{e}_g$ be the guess of emitter location and $\mathbf{e} = \mathbf{e}_g + \boldsymbol{\delta}$. Using a Taylor Series Expansion gives

$$f_m(\mathbf{e}) \approx f_m(\mathbf{e}_g) + \frac{\partial}{\partial \mathbf{e}} f_m(\mathbf{e}) \Big|_{\mathbf{e}=\mathbf{e}_g} [\mathbf{e} - \mathbf{e}_g] \tag{104}$$

$$= f_m(\mathbf{e}_g) + \frac{\partial}{\partial \mathbf{e}} f_m(\mathbf{e}) \Big|_{\mathbf{e}=\mathbf{e}_g} \boldsymbol{\delta} \tag{105}$$

where $f_m(\mathbf{e}_g) = (||\mathbf{e}_g - \mathbf{p}_i|| - ||\mathbf{e}_g - \mathbf{p}_j||)$ and $\frac{\partial}{\partial \mathbf{e}} f_m(\mathbf{e})\Big|_{\mathbf{e}=\mathbf{e}_g} = \left[\frac{\mathbf{e}_g - \mathbf{p}_i}{||\mathbf{e}_g - \mathbf{p}_i||} - \frac{\mathbf{e}_g - \mathbf{p}_j}{||\mathbf{e}_g - \mathbf{p}_j||}\right]^T$. Thus, we have the following linear Gaussian model

$$\mathbf{y}(\mathbf{e}_g) = \mathbf{B}(\mathbf{e}_g)\boldsymbol{\delta} + \mathbf{v} \tag{106}$$

where $\mathbf{B}(\mathbf{e}_g) = \begin{bmatrix} \frac{\partial}{\partial \mathbf{e}} f_1(\mathbf{e}) \Big|_{\mathbf{e}=\mathbf{e}_g} \\ \vdots \\ \frac{\partial}{\partial \mathbf{e}} f_M(\mathbf{e}) \Big|_{\mathbf{e}=\mathbf{e}_g} \end{bmatrix}$ $\mathbf{y}(\mathbf{e}_g) = \begin{bmatrix} \tilde{d}_1 - f_1(\mathbf{e}_g) \\ \vdots \\ \tilde{d}_M - f_{\mathrm{M}}(\mathbf{e}_g) \end{bmatrix}$ and $\boldsymbol{\delta}$ is unknown.

The LS equations in (106) can be solved iteratively where the k^{th} iteration gives $\hat{\boldsymbol{\delta}}^{(k)} = \left(\mathbf{B}^{(k)\ T}\Sigma^{-1}\mathbf{B}^{(k)}\right)^{-1}\mathbf{B}^{(k)\ T}\Sigma^{-1}\mathbf{y}^{(k)}$ and the guess of emitter location is updated as $\mathbf{e}_g^{(k+1)} = \mathbf{e}_g^{(k)} + \hat{\boldsymbol{\delta}}^{(k)}$. The optimization is repeated until convergence i.e. $\boldsymbol{\delta} \to \mathbf{0}$. Let i denote the iteration of convergence where the estimate is taken as

$$\hat{\mathbf{e}} = \mathbf{e}_g^{(i+1)} = \boldsymbol{\Gamma}^{(i)}\mathbf{y}^{(i)} \tag{107}$$

and $\boldsymbol{\Gamma}^{(i)} = \left(\tilde{\mathbf{B}}^T\Sigma^{-1}\tilde{\mathbf{B}}\right)^{-1}\tilde{\mathbf{B}}^T\Sigma^{-1}$. The Taylor series allows us to obtain a linear form of the problem allowing us to exploit the biased estimation formulation for linear Gaussian models.

6.3.6. Biased Estimation for the Linear Gaussian Model

If the bias is restricted to be linear then the unbiased estimator results can be used to find biased estimators that reduce the MSE and has the form,

$$\hat{\boldsymbol{\theta}}_b = \left(\mathbf{I} + \hat{\mathbf{M}}\left(\hat{\boldsymbol{\theta}}\right)\right)\hat{\boldsymbol{\theta}} \tag{108}$$

where $\mathbf{M}$ is the biased matrix sought and $\hat{\boldsymbol{\theta}}_u$ & $\hat{\boldsymbol{\theta}}_b$ are the unbiased and biased estimates, respectively. In general, the bias matrix, $\mathbf{M}$ is a function of the unknown parameter. The unknown parameter may be substituted with its Maximum Likelihood estimate where the bias matrix can then be determined in an iterative fashion.

$$\hat{\boldsymbol{\theta}}_k = \left(\mathbf{I} + \hat{\mathbf{M}}\left(\hat{\boldsymbol{\theta}}\right)\right)\hat{\boldsymbol{\theta}}_{k-1} \tag{109}$$

To find $\mathbf{M}$, for the vector case, the following minimax problem can be considered,

$$\mathbf{M}^* = \arg\min_{\mathbf{M}} \max_{\boldsymbol{\theta}\epsilon\boldsymbol{U}} \left\{\mathrm{MSE}\left(\hat{\boldsymbol{\theta}}_b\right) - \mathrm{MSE}\left(\hat{\boldsymbol{\theta}}_u\right)\right\} \tag{110}$$

where U is a constraint set on $\boldsymbol{\theta}$. If $\boldsymbol{\theta}$ is known to be within a sphere or an ellipse then the constraint will reduce the overall MSE. Although this parameter may not be known it can be estimated via blind minimax estimation where the constraint set is first estimated using the data and then the minimax problem is solved.

There are two types of biased estimators: (1) the Minimax Trace MSE (MXTM) method and (2) the Minimax Matrix MSE (MXMM) method.

The MXTM estimator is given by

$$\hat{\mathbf{e}}_{\text{MXTM}} = \frac{L^2}{L^2 + \text{tr}\left(\mathbf{J}^{-1}\left(\mathbf{e}\right)\right)}\hat{\mathbf{e}}_{\text{LS}} \tag{111}$$

where $\mathbf{J}^{-1}\left(\mathbf{e}\right)$ is the inverse Fisher Information Matrix (FIM) of the unknown parameter and L is a radius such that $||\mathbf{e}|| \leq L$. The FIM of the linear model is $\mathbf{J}\left(\mathbf{e}\right) = \mathbf{H}\left(\mathbf{e}\right)^T \Sigma^{-1}\mathbf{H}\left(\mathbf{e}\right)$ where the Jacobian is unknown due to its dependence on the unknown emitter location. We take the FIM as, $\mathbf{H}\left(\mathbf{e}_g^i\right)^T \Sigma^{-1}\mathbf{H}\left(\mathbf{e}_g^i\right)$ resulting from the convergence of the LS update. Since $||\mathbf{e}||$ is not known exactly, it can be replaced by its LSE, $||\hat{\mathbf{e}}_{\text{LS}}|| \leq L$.

Although the MXTM method guarantees a smaller total MSE for the worst case estimate, its component-wise MSE can be larger than that of the LS estimator [11]. As this is not desirable, the MXMM method can be used, which ensures that the component wise MSE is less than that of the LS estimator. This savings comes with the price of a small increase in the total trace MSE. The MXMM in [11] is

$$\min_{\hat{\mathbf{e}}} \quad \max_{\mathbf{e},\mathbf{W}} \qquad \text{trace}\left(\mathbf{W}\mathbf{M}\left(\hat{\mathbf{e}}\right)\right) : ||\mathbf{e}||_T \leq L, \mathbf{0} \preceq \mathbf{W} \prec \mathbf{I} \tag{112}$$

$$\text{s.t.} \qquad \mathbf{M}\left(\hat{\mathbf{e}}\right) \preceq \mathbf{M}\left(\hat{\mathbf{e}}_{LS}\right), \forall ||\mathbf{e}||_T \leq L \tag{113}$$

where the constraint ensures that the MSE dominates that of the LS estimator, ensuring a smaller component-wise MSE. The solution is

$$\hat{\mathbf{e}}_{\text{MXMM}} = \mathbf{K}\hat{\mathbf{e}}_{\text{LS}}. \tag{114}$$

where the bias matrix $\mathbf{K}$ can be formulated as a SDP

$$\begin{aligned}
\min_{\mathbf{K},\mathbf{X},\lambda} \quad & \text{trace}\left(\mathbf{X}\right) + L^2\lambda \\
\text{s.t.} \quad & \begin{bmatrix} \lambda\mathbf{T} & \mathbf{I}-\mathbf{K} \\ \left(\mathbf{I}-\mathbf{K}\right)^T & \mathbf{I} \end{bmatrix} \succeq \mathbf{0} \\
& \begin{bmatrix} \mathbf{Q}-\mathbf{X} & \mathbf{I}-\mathbf{K} \\ \left(\mathbf{I}-\mathbf{K}\right)^T & \frac{1}{L^2}\mathbf{T} \end{bmatrix} \succeq \mathbf{0} \qquad (115) \\
& \begin{bmatrix} \mathbf{X} & \mathbf{K} \\ \mathbf{K}^T & \mathbf{Q}^{-1} \end{bmatrix} \succeq \mathbf{0} \qquad (116)
\end{aligned}$$

6.3.7. Numerical Results

The performance of our biased estimators is plotted under varying SNR levels for both the total trace MSE and the component-wise MSE. The numerical simulations average the performance over 2000 sensor-emitter geometries where $L = ||\mathbf{e}||$ and $\mathbf{T} = \mathbf{I}$.

In Figure 30 the trace MSE performance is compared for the LS, MXTM and MXMM estimators. The performance of the unbiased and biased estimators are very similar for high SNR levels. For low SNR levels performance of the biased estimators exhibit a significant performance gain. In Figure 31 the x-component MSE performance is compared for the LS, MXTM and MXMM estimators. The MXMM estimator gives a smaller MSE than the MXTM method for low SNR. In

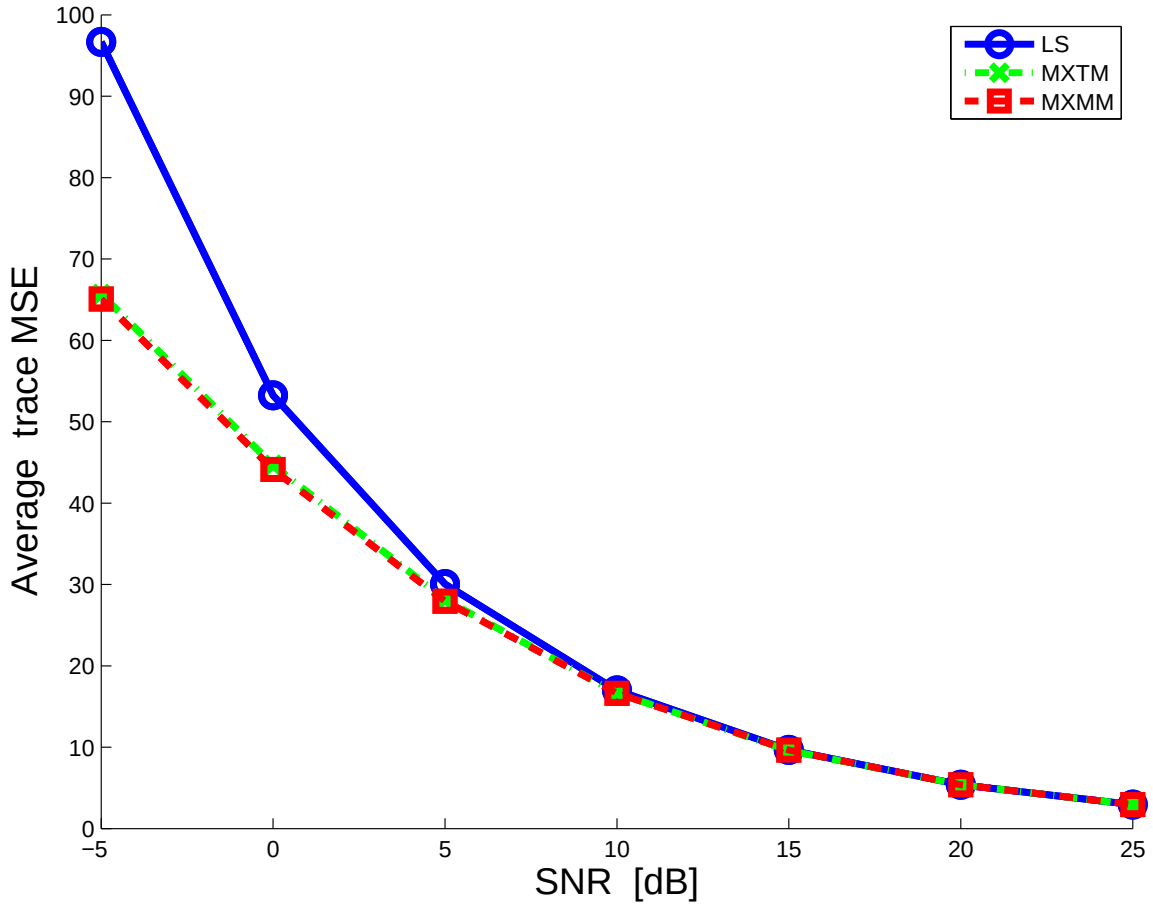


Figure 30: Root-trace MSE vs. SNR

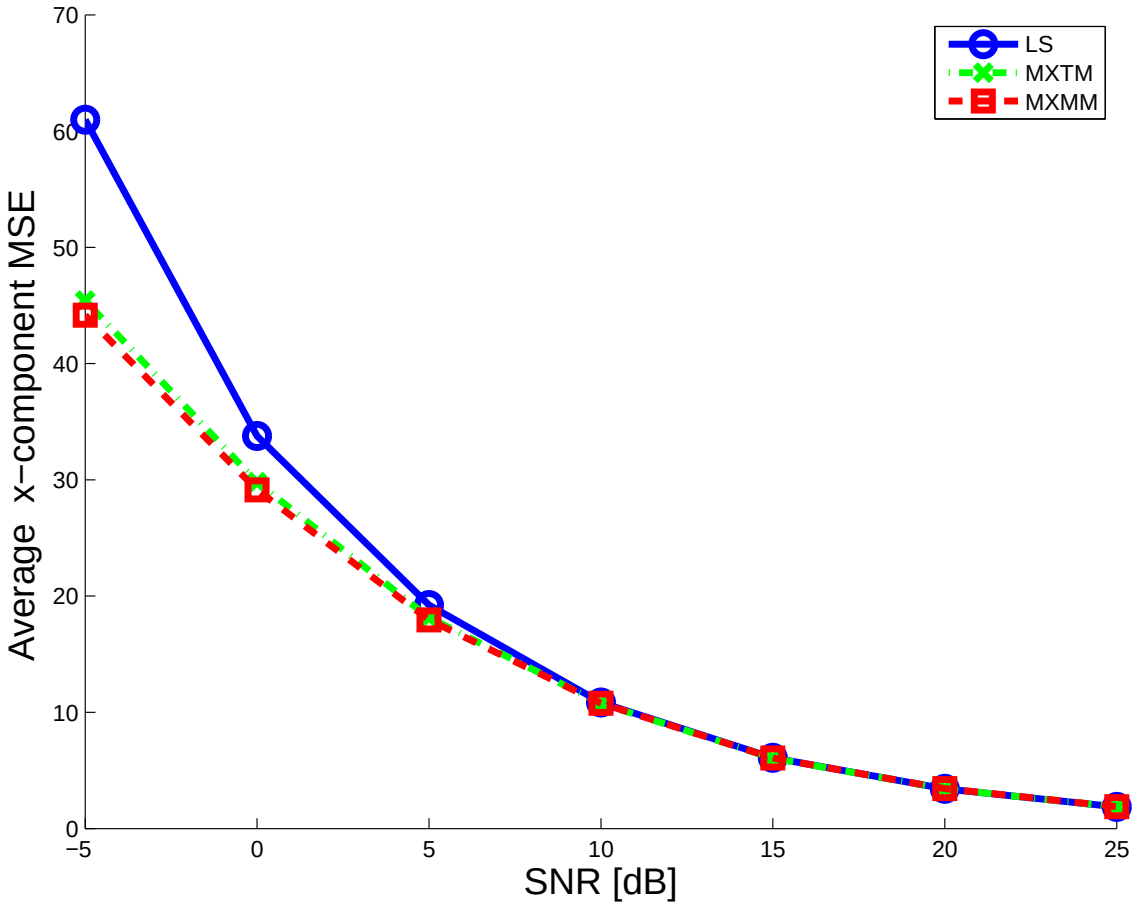


Figure 31: Root-MSE of the x-component vs. SNR

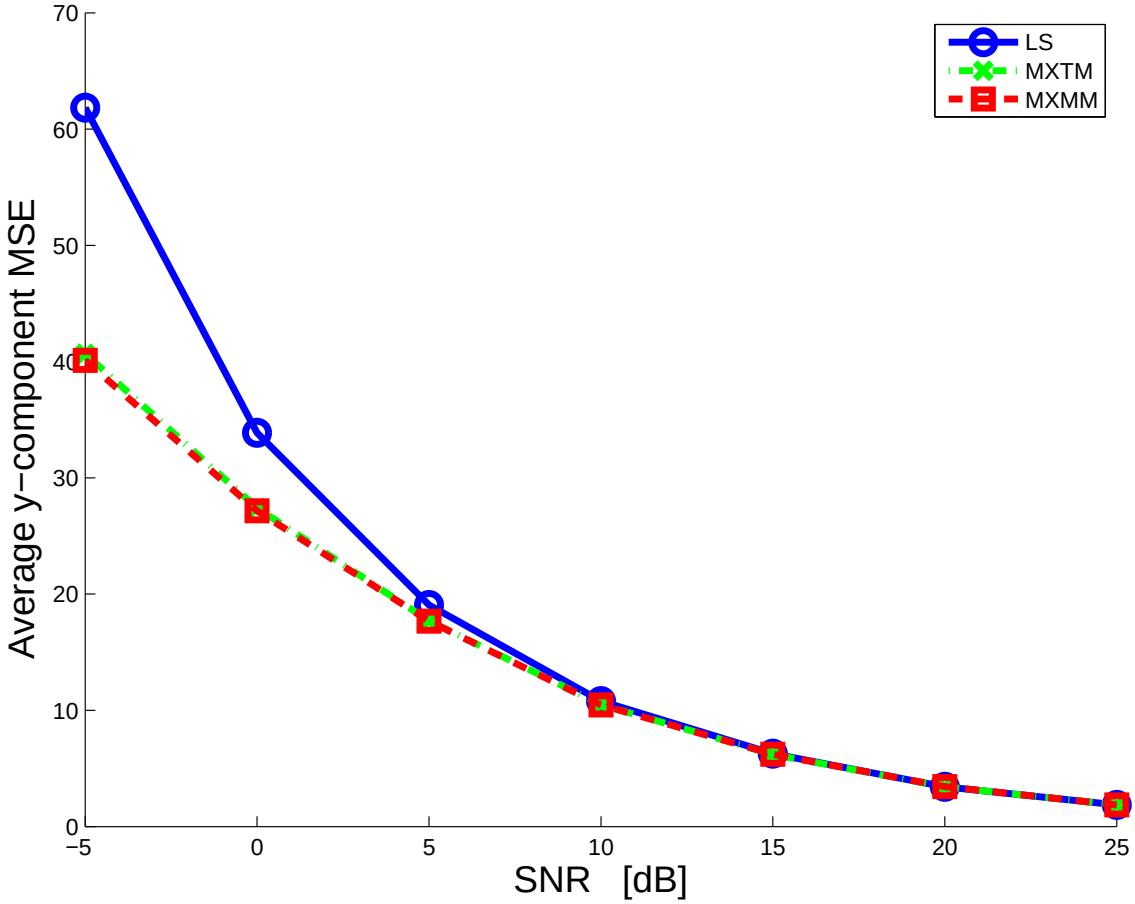


Figure 32: Root-MSE of the y-component vs. SNR

Figure 32 the y-component MSE performance is compared for the LS, MXTM and MXMM estimators.

6.4. Discussion

This chapter develops network strategies to detect and mitigate the adversary. We begin by deriving a detector to determine whether or not an adversary is present. Detection is just the first step, thus two strategies are developed to mitigate the effect of the injection on the network's localization using robust and biased estimation.

Directions for future work includes determining adversary detectors for all other localization methods. This work considered biased linear estimators. Another direction is to consider a larger class of biased estimators such as affine estimators.

7.0. Conclusions

Addressing security issues in contentious environments is a challenging problem. Development of bounds on the achievable performance from both the point of view of the adversary and the network have not been explored from a holistic view prior to this work.

This research addresses the complex relationship between two competing players in the wireless setting. The problem of localization with an intelligent adversary is explored. A novel framework is developed which designs adversary and network strategies ranging from maximum adversary impact to network resilience.

We begin by considering the Fisher Information Matrix and develop two new adversary strategies to degrade the network by minimizing the Fisher Information by exploiting its equivalence with maximizing the area of the location error ellipse. The FIM strategy essentially causes the non-linear least squares estimation to determine its estimate using only those non-corrupt sensor pairs. The utility of these adversary strategies are key for networks with a small number of sensor pairs or when the corrupted sensor pair contributes the most to the sensor emitter geometry. Although the FIM strategy allows an adversary to make the error ellipse large, it does not guarantee that a particular non-linear least squares estimate of location is far away from the true value of emitter location. A different set of adversary strategies are developed, which redirect the location estimate a specified distance away from its true value. We model the strength of the adversary and develop the power-limited adversary by defining the idea of a spatial restriction and a content restriction.

Next we consider the viewpoint of the network, where the first step is to detect the adversary and then second is to mitigate the effect of its injection. An adversary detector is derived and evaluated under both adversary strategies: (1) to minimize the Fisher Information and (2) to redirect the location estimate. It is observed that the detectability of the adversary is directly related to the power of its injection. Strategies for mitigating the adversary are developed using tools from robust estimation and biased estimation. The robust strategy indicates when to use non-linear LS or LMS is a function of the strength of the adversary's injection and the SNR. Biased estimators are derived that reduce the MSE under any sensor pairing scheme.

7.1. Future Research Directions

The work in this thesis inspires a number of new research directions. We considered modeling the adversary's strength in terms of both a spatial restriction and a content restriction. An interesting direction would be to consider the notion of sparsity in the adversary modeling. In the first case, the adversary is free to inject content with unlimited bounds but it can only inject a single node. In the latter, the adversary can inject every node but may only perturb the nodes by a small amount. Suppose, for example that the adversary can inject a sparse number of nodes with any content injection it chooses. Similarly, in the content restriction model perhaps the adversary can only slightly perturb a sparse number of nodes. Exploration of these scenarios are key to modeling an adversary that only has access to certain regions of the network.

Another research direction is to investigate the current framework with a time horizon, where the adversary and network would each employ their strategies, with varying levels of apriori knowledge on the other player's capabilities. One can consider that each side is aware of the other's presence and has a fixed deadline to either perform the location or harm the network. Both the adversary and network would each select different strategies based on how much time remains until the deadline. In addition, if each party knows that the other has a certain time window to respond then this would also affect their strategy selection. These time constrained scenarios suggest consideration of a game theoretic formulation.

This work focuses on the application of emitter location. Another research direction is to consider this framework for a variety of different parameter estimation problems such as speaker identification, image analysis, and environmental monitoring. It would be interesting to see how the developed strategies can be applied to these alternative problem domains.

The adversary-network framework developed in this work considers both ends of the spectrum, where the adversary's goal is to maximally impact the network and network's goal of resiliency is to operate despite an adversary's injection. Our framework applies to a wide set of sensor network tasks. Assessing this competing behavior is key to any network operations in contentious environments.

8.0. References

[1] J.N. Ash and R.L. Moses. On optimal anchor node placement in sensor localization by optimization of subspace principal angles. In *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 2289–2292, 2008.

[2] P. Biswas, T.C. Liang, K.C. Toh, Y. Ye, and T.C. Wang. Semidefinite programming approaches for sensor network localization with noisy distance measurements. *IEEE Transactions on Automation Science and Engineering*, 3(4):360–371, 2006.

[3] D. Blatt and A.O. Hero. Energy-based sensor network source localization via projection onto convex sets. *IEEE Transactions on Signal Processing*, 54(9):3614–3619, 2006.

[4] S.P. Boyd and L. Vandenberghe. *Convex optimization*. Cambridge university press, 2004.

[5] H. Chan and A. Perrig. Security and privacy in sensor networks. *IEEE Computer Society*, 36(10):103–105, 2003.

[6] M. Chen and M.L. Fowler. Data compression for multi-parameter estimation for emitter location. *IEEE Transactions on Aerospace and Electronic Systems*, 46(1):308–322, 2010.

[7] Y. Chen, W. Trappe, and R.P. Martin. Attack detection in wireless localization. *26th IEEE International Conference on Computer Communications (INFOCOM)*, pages 1964–1972, 2007.

[8] Y.M. Chen, J.H. Lee, and C.C. Yeh. Two-dimensional angle-of-arrival estimation for uniform planar arrays with sensor position errors. In *IEE Proceedings on Radar and Signal Processing*, volume 140, pages 37–42. IET, 1993.

[9] C.R. Comsa, A.M. Haimovich, S.C. Schwartz, Y.H. Dobyns, and J.A. Dabin. Time difference of arrival based source localization within a sparse representation framework. *in 45th Annual Conference on Information Sciences and Systems (CISS)*, pages 1–6, 2011.

[10] Y.C. Eldar. *Rethinking Biased Estimation*, volume 1. Now Publishers Inc, 2008.

[11] Y.C. Eldar. Universal weighted mse improvement of the least-squares estimator. *IEEE Transactions on Signal Processing*, 56(5):1788–1800, 2008.

[12] M. Fazel, H. Hindi, and S.P. Boyd. Log-det heuristic for matrix rank minimization with applications to Hankel and Euclidean distance matrices. *in the Proceedings of the American Control Conference*, 3:2156–2162, 2003.

[13] M.L. Fowler. Analysis of single-platform passive emitter location with terrain data. *IEEE Transactions on Aerospace and Electronic Systems*, 37(2):495–507, 2001.

[14] M.L. Fowler. Analysis of single-platform passive emitter location with terrain data. *IEEE Transactions on Aerospace and Electronic Systems*, 37(2):495–507, 2001.

[15] M.L. Fowler. New distortion measures for data compression for emitter location. *in Thirty-Fifth Asilomar Conference on Signals, Systems, and Computers*, 1:658–662, 2001.

[16] W.H. Foy. Position-location solutions by taylor-series estimation. *IEEE Transactions on Aerospace and Electronic Systems*, (2):187–194, 1976.

[17] I. Guvenc and C.C. Chong. A survey on toa based wireless localization and nlos mitigation techniques. *IEEE Communications Surveys & Tutorials*, 11(3):107–124, 2009.

[18] A.O. Hero III and D. Blatt. Sensor network source localization via projection onto convex sets (pocs). In *IEEE International Conference on Acoustics, Speech, and Signal Processing ICASSP*, volume 3, pages iii–689. IEEE, 2005.

[19] KC Ho, L. Kovavisaruch, and H. Parikh. Source localization using tdoa with erroneous receiver positions. In *Proceedings of the 2004 International Symposium on Circuits and Systems, 2004. ISCAS'04.*, volume 3, pages III–453. IEEE.

[20] KC Ho, X. Lu, and L. Kovavisaruch. Source localization using tdoa and fdoa measurements in the presence of receiver location errors: Analysis and solution. *IEEE Transactions on Signal Processing*, 55(2):684–696, 2007.

[21] T. Ho, B. Leong, R. Koetter, M. Médard, M. Effros, and D.R. Karger. Byzantine modification detection in multicast networks with random network coding. *IEEE Transactions on Information Theory*, 54(6):2798–2803, 2008.

[22] X. Hu and M.L. Fowler. Sensor Selection for Multiple Sensor Emitter Location Systems. *IEEE Aerospace Conference*, pages 1–10, 2008.

[23] L.M. Huie and M.L. Fowler. Biasing emitter location estimates via false location injection. *IEEE Statistical Signal Processing Workshop (SSP)*, pages 249–252, 2011.

[24] L.M. Huie and M.L. Fowler. Emitter Location in the Presence of Information Injection. *in the Proceedings of Conference on Information Science and Systems, CISS*, March 2010.

[25] L.M. Huie and M.L. Fowler. A Closed Form for False Location Injection under Time Difference of Arrival. *in 44th Asilomar Conf. on Signals, Systems and Computers*, Nov 2010.

[26] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Médard. Resilient network coding in the presence of byzantine adversaries. In *26th IEEE International Conference on Computer Communications INFOCOM 2007.*, pages 616–624. IEEE, 2007.

[27] X. Ji and H. Zha. Sensor positioning in wireless ad-hoc sensor networks using multidimensional scaling. In *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, volume 4, pages 2652–2661. IEEE, 2004.

[28] D.C. Kammer and M.L. Tinker. Optimal placement of triaxial accelerometers for modal vibration tests. *Mechanical Systems and Signal Processing*, 18(1):29–41, 2004.

[29] S.A. Kassam and H.V. Poor. Robust techniques for signal processing: A survey. *Proceedings of the IEEE*, 73(3):433–481, 1985.

[30] S.M. Kay. *Fundamentals of statistical signal processing: estimation theory*. Prentice Hall, 1993.

[31] S.M. Kay. Fundamentals of statistical signal processing, volume ii: Detection theory. *Upper Saddle River (New Jersey)*, 7, 1998.

[32] U.A. Khan, S. Kar, and J.M.F. Moura. Distributed sensor localization in random environments using minimal number of anchor nodes. *IEEE Transactions on Signal Processing*, 57(5):2000–2016, 2009.

[33] O. Kosut, L. Jia, R.J. Thomas, and L. Tong. Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures. *2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 220–225, 2010.

[34] O. Kosut and L. Tong. Distributed source coding in the presence of Byzantine sensors. *IEEE Transactions on Information Theory*, 54(6):2550–2565, 2008.

[35] Thomas RJ Kosut O., Jia L. and Tong L. Limiting False Data Attacks on Power System State Estimation. *Proceedings of Conference on Information Science and Systems, Princeton University*, 2010.

[36] L. Lamport, R. Shostak, and M. Pease. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401, 1982.

[37] Loukas Lazos and Radha Poovendran. Serloc: Secure range-independent localization for wireless sensor networks. In *Proceedings of the 3rd ACM workshop on Wireless security*, pages 21–30. ACM, 2004.

[38] Loukas Lazos and Radha Poovendran. Serloc: Robust localization for wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 1(1):73–100, 2005.

[39] Z. Li, W. Trappe, Y. Zhang, and B. Nath. Robust statistical methods for securing wireless localization in sensor networks. *Proc. of the 4 th Int. Symp. on Information Processing in Sensor Networks (IPSN)*, pages 91–98, 2005.

[40] X. Lin and Y. Bar-Shalom. Multisensor target tracking performance with bias compensation. *IEEE Transactions on Aerospace and Electronic Systems*, 42(3):1139–1149, 2006.

[41] X. Lin, Y. Bar-Shalom, and T. Kirubarajan. Multisensor multitarget bias estimation for general asynchronous sensors. *IEEE Transactions on Aerospace and Electronic Systems*, 41(3):899–921, 2005.

[42] Donggang Liu, Peng Ning, An Liu, Cliff Wang, and Wenliang Kevin Du. Attack-resistant location estimation in wireless sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, 11(4):22, 2008.

[43] Ke Liu, Nael Abu-Ghazaleh, and Kyoung-Don Kang. Location verification and trust management for resilient geographic routing. *Journal of Parallel and Distributed Computing*, 67(2):215–228, 2007.

[44] Z. Lu, X. Zhang, and Q. Wan. Biased time-of-arrival-based location dominating linear-least-squares estimation. In *2010 2nd International Conference on Signal Processing Systems (ICSPS)*, volume 2, pages V2–313. IEEE, 2010.

[45] Z.Q. Luo, W. Ma, A.M.C. So, Y. Ye, and S. Zhang. Semidefinite relaxation of quadratic optimization problems. *IEEE Signal Processing Magazine*, 27(3):20–34, 2010.

[46] S. Marano, V. Matta, and L. Tong. Distributed detection in the presence of Byzantine attacks. *IEEE Transactions on Signal Processing*, 57(1):16–29, 2009.

[47] C. Meesookho, U. Mitra, and S. Narayanan. On energy-based acoustic source localization for sensor networks. *IEEE Transactions on Signal Processing*, 56(1):365–377, 2008.

[48] C. Meng, Z. Ding, and S. Dasgupta. A semidefinite programming approach to source localization in wireless sensor networks. *IEEE Signal Processing Letters*, 15:253–256, 2008.

[49] R. Niu and L. Huie. System state estimation in the presence of false information injection. In *IEEE Statistical Signal Processing Workshop (SSP)*, pages 385–388. IEEE, 2012.

[50] R.W. Ouyang, A.K.S. Wong, and C.T. Lea. Received signal strength-based wireless localization via semidefinite programming: Noncooperative and cooperative schemes. *IEEE Transactions on Vehicular Technology*, 59(3):1307–1318, 2010.

[51] C. Papadimitriou, J.L. Beck, and S.K. Au. Entropy-based optimal sensor location for structural model updating. *Journal of Vibration and Control*, 6(5):781–800, 2000.

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

[53] N. Patwari and A.O. Hero III. Using proximity and quantized rss for sensor localization in wireless networks. In *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*, pages 20–29. ACM, 2003.

[54] N. Patwari and A.O. Hero III. Manifold learning algorithms for localization in wireless sensor networks. In *IEEE International Conference on Acoustics, Speech, and Signal Processing ICASSP*, volume 3, pages iii–857. IEEE, 2004.

[55] N.B. Priyantha, H. Balakrishnan, E. Demaine, and S. Teller. Anchor-free distributed localization in sensor networks. In *Proceedings of the 1st international conference on Embedded networked sensor systems*, pages 340–341. ACM, 2003.

[56] Y. Rockah and P. Schultheiss. Array shape calibration using sources in unknown locations–part ii: Near-field sources and estimator implementation. *IEEE Transactions on Acoustics, Speech and Signal Processing*, 35(6):724–735, 1987.

[57] P.J. Rousseeuw. Least median of squares regression. *Journal of the American statistical association*, 79(388):871–880, 1984.

[58] P.J. Rousseeuw and A.M. Leroy. *Robust regression and outlier detection*. John Wiley & Sons Inc, 1987.

[59] Naveen Sastry, Umesh Shankar, and David Wagner. Secure verification of location claims. In *Proceedings of the 2nd ACM workshop on Wireless security*, pages 1–10. ACM, 2003.

[60] S. Stein. Differential delay/Doppler ML estimation with unknown signals. *IEEE Transactions on Signal Processing*, 41(8):2717–2719, 1993.

[61] Radu Stoleru, Tian He, and John A Stankovic. Range-free localization. *Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks*, pages 3–31, 2007.

[62] D.J. Torrieri. Statistical Theory of Passive Location Systems. *IEEE Transactions on Aerospace and Electronic Systems*, AES-20(2):183–198, 1984.

[63] D. Uciński and M. Patan. D-optimal design of a monitoring network for parameter estimation of distributed systems. *Journal of Global Optimization*, 39(2):291–322, 2007.

[64] F.E. Udwadia. Methodology for optimal sensor locations for parameters identification in dynamic systems. *Journal of Engineering Mechanics*, 120(2):368–390, 1994.

[65] N.E. Wu, Y. Guo, K. Huang, M.C. Ruschmann, and M.L. Fowler. Fault-tolerant tasking and guidance of an airborne location sensor network. *International Journal of Control Automation and Systems*, 6(3):351–363, 2008.

[66] Z. Xiao and W. Qun. Accurate localization using biased estimation. In *2010 Sixth International Conference on Natural Computation (ICNC)*, volume 7, pages 3558–3561. IEEE, 2010.

[67] F. Zhao, J. Shin, and J. Reich. Information-driven dynamic sensor collaboration for tracking applications. *IEEE Signal processing magazine*, 19(2):61–72, 2002.

[68] J. Zhu. Calculation of geometric dilution of precision. *IEEE Transactions on Aerospace and Electronic Systems*, 28(3):893–895, 1992.

List of Abbreviations

TOA	Time of Arrival
TDOA	Time Difference of Arrival
FDOA	Frequency Difference of Arrival
AOA	Angle of Arrival
RSS	Received Signal Strength
LS	Least Squares
MLE	Maximum Likelihood Estimate
CRLB	Cramer Rao Lower Bound
KL	Kullback-Leibler
MSE	Mean Squared Error
SDP	Semidefinite programming
LMS	Least Median Squares
PDF	Probability Density Function
NLOS	Non-Line Of Sight
MVUE	Minimum Variance Unbiased Estimator
FIM	Fisher Information Matrix
GDOP	Geometric Dilution of Precision
LRT	Likelihood Ratio Test
GLRT	Generalized Likelihood Ratio Test
ROC	Receiver Operating Characteristic
SNR	Signal to Noise Ratio
LMS	Least Median Squares
MXTM	Minimax Trace MSE
MXMM	Minimax Matrix MSE