ABSTRACT

Title of dissertation: MODEL BASED OPTIMIZATION
AND DESIGN OF SECURE SYSTEMS

Waseem Ansar Malik, Doctor of Philosophy, 2014

Dissertation directed by: Prof. Nuno C. Martins
Department of Electrical and Computer Engineering
University of Maryland, College Park

Dr. Ananthram Swami
Computational and Information Sciences Directorate
Army Research Laboratory

Control systems are widely used in modern industry and find wide applications in power systems, nuclear and chemical plants, the aerospace industry, robotics, communication devices, and embedded systems. All these systems typically rely on an underlying computing and networking infrastructure which has considerable security vulnerabilities. The biggest threat, in this age and time, to modern systems are cyber attacks from adversaries. Recent cyber attacks have practically shut down government websites affecting government operation, undermined financial institutions, and have even infringed on public privacy. Thus it is extremely important to conduct studies on the design and analysis of secure systems. This work is an effort in this research direction and is mainly focused on incorporating security in the design of modern control systems.

In the first part of this dissertation, we present a linear quadratic optimal control problem subjected to security constraints. We consider an adversary which can make

partial noisy measurements of the state. The task of the controller is to generate control sequences such that the adversary is unable to estimate the terminal state. This is done by minimizing a quadratic cost while satisfying security constraints. The resulting optimization problems are shown to be convex and the optimal solution is computed using Lagrangian based techniques. For the case when the terminal state has a discrete distribution the optimal solution is shown to be nonlinear in the terminal state. This is followed by considering the case when the terminal state has a continuous distribution. The resulting infinite dimensional optimization problems are shown to be convex and the optimal solution is proven to be affine in the terminal state.

In the next part of this dissertation, we analyze several team decision problems subjected to security constraints. Specifically, we consider problem formulations where there are two decision makers each controlling a different dynamical system. Each decision maker receives information regarding the respective terminal states that it is required to reach and applies a control sequence accordingly. An adversary makes partial noisy measurements of the states and tries to estimate the respective terminal states. It is shown that the optimal solution is affine in the terminal state when it is identical for both systems. We also consider the general case where the terminal states are correlated. The resulting infinite dimensional optimization problems are shown to convex programs and we prove that the optimal solution is affine in the information available to the decision makers.

Next, a stochastic receding horizon control problem is considered and analyzed. Specifically, we consider a system with bounded disturbances and hard bounds on the control inputs. Utilizing a suboptimal disturbance feedback scheme, the optimization problem is shown to be convex. The problem of minimizing the empirical mean of the

cost function is analyzed. We provide bounds on the disturbance sample size to compute the empirical minimum of the problem. Further, we consider the problem where there are hard computational constraints and complex on-line optimization is not feasible. This is addressed by randomly generating both the control inputs and the additive disturbances. Bounds on sample sizes are provided which guarantee a notion of a probable near minimum. Model uncertainty is also incorporated into the framework and relevant bounds are provided which guarantee a probable near minimax value. This work finds many applications in miniature devices and miniature robotics.

In the final part of this dissertation, we consider a centralized intrusion detection problem with jointly optimal sensor placement. A team of sensors make measurements regarding the presence of an intruder and report their observations to a decision maker. The decision maker solves a jointly optimal detection and sensor placement problem. For the case when the number of sensors is equal to the number of placement points, we prove that uniform placement of sensors is not strictly optimal. We introduce and utilize a majorization based partial order for the placement of sensors. For the case when the number of sensors is less than or equal to six, we show that for a fixed local probability of detection (probability of false alarm) increasing the probability of false alarm (probability of detection) results in optimal placements that are higher on a majorization based partial order.

MODEL BASED OPTIMIZATION AND DESIGN OF SECURE SYSTEMS

by

Waseem Ansar Malik

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2014

Advisory Committee:
Professor Nuno C. Martins, Chair/Advisor
Doctor Ananthram Swami, Co-Advisor
Professor Steven I. Marcus
Professor Sennur Ulukus
Professor Nikhil Chopra

© Copyright by
Waseem Ansar Malik
2014

Dedication

This dissertation is dedicated to my mother ~ ***Zarina Ahmed***

Acknowledgments

First and foremost, I would like to express my thanks and deep gratitude to my creator and the almighty being, Allah Subhanahu Wa Ta'ala, for the granting me the gift of life and for sustaining me over the course of my life. I really appreciate the knowledge, wisdom, and the guidance imparted to me by his religion. Faith in my religion enabled me to lead a highly disciplined life and is probably the main reason behind the timely completion of this dissertation. No words can be enough for my gratitude and thanks to my creator. "Verily, unto God do we belong and, verily, unto Him we shall return." (Al Baqrah: Chapter 2, Verse 156).

I would like to thank my advisor Prof. Nuno C. Martins for his help, advice, and guidance over the past 6 years. I would not have been able to complete this dissertation without his support and supervision. Prof. Martins not only encouraged me but also taught me how to think deeply about hard mathematical problems. He imparted his mathematical rigor, clarity of thought, and the ability to dissect a hard problem into tractable sub-problems to me through the many interactions and meetings we had over the years. In addition, his mathematical brilliance and technical sophistication provided my research with significant impetus over the years. I learned from him the formulation of complex research problems, the methodology to tackle a hard research problem, and the physical interpretation of technical theoretical results. I really want to thank him for taking an unproven student under his wings and for developing and polishing my research skills over the course of my PhD. He took great interest in my academic and personal development and his suggestions and sincere advice have helped me tremendously over the years. He

has always been extremely kind with his time and has always made himself available to discuss my research. He not only gave me intellectual freedom to pursue my own research ideas but also shared his deep insights and advanced knowledge in the fields of systems, optimization, and control. I really appreciate his help, time, and advice and words cannot do justice to what he has done for me during my graduate years.

I would also like to thank my advisor Dr. Ananthram Swami for his help and advice over the course of my PhD. I have benefited tremendously by interacting with him at the Army Research Laboratory. He has always been extremely kind with his time and has always made himself available to meet me despite his busy schedule and commitments. I have learned a lot from Dr. Swami over the past few years. He has been extremely helpful in the formulation of my research problems and has helped me a lot in developing the ability to ask the right research questions. I have benefited a lot from his exceptional technical abilities, research acumen, and vast experience in solving problems in control and communications. His emphasis of always keeping the bigger picture in mind helped me a lot in my technical and research development. He took great interest in my academic and research development and always encouraged me to take advanced courses in mathematics, control theory, and statistics. I really appreciate his help and support over the course of my PhD. This work would not have been possible without his supervision, guidance, and support.

I would like to thank Prof. Steven I. Marcus, Prof. Sennur Ulukus, and Prof. Nikhil Chopra for serving on my dissertation committee. I really appreciate their help, time, and kindness in this regard. In addition, I would like to thank Prof. Marcus for teaching me courses on linear control theory and stochastic control theory. I would also

like to thank Prof. Andre Tits for all the academic support, for his counseling, and his sincere advice over the years. Taking his course on signals and systems during my undergraduate education radically changed my outlook on electrical engineering and I subsequently decided to pursue an advanced degree in systems and control. I would also like to acknowledge and thank Prof. Krishnaprasad for teaching me courses in nonlinear control, optimal control, and adaptive control. I learned mathematical statistics from Prof. Eric Slud of the Department of Mathematics. It was a pleasure to take his sequence of courses in statistical inference. I owe him a lot of gratitude for teaching me various advanced statistical techniques which helped me a lot in my research. Finally, I would like to thank all the faculty at the University of Maryland for teaching me many courses over the years. I benefited tremendously from your classes, advanced knowledge, and expertise in your respective fields of research. I would also like to acknowledge the faculty at Islamabad Model College for Boys (IMCB) G-10/4. I really appreciate your help, time, and the interest that you showed in my development. I spent ten wonderful years under your tutelage and guidance. I have utilized the skills and the passion for learning that you instilled in me during my early academic years all my life. Some words cannot describe how thankful I am to all of you. May Allah reward you for the kindness and the generosity that you showed me over the years.

I would like to thank my family members especially my mother, Zarina Ahmed. This thesis is dedicated to my mother. She has always been there for me and has always encouraged me to take advantage of any academic opportunity that comes up in my life. Her love, care, and devotion for me is not something that can be measured by worldly standards or metrics. She was a constant source of encouragement and support during

my graduate years. I can never repay or forget the love and care that she has given me during the course of my life. She has always been extremely proud of my academic ambitions and has always provided me with all the resources that could help me succeed in my course work and research. During my PhD years she would always make arrangements that would facilitate my studies and always took active responsibility for the various chores in my life. Her love, care, sympathy, advice, prayers, and supplications are greatly admired and appreciated. My words can never do any justice to what she has done for me in my life. It is one of the main goals of my life to make her proud and to keep her happy for the rest of my life. I also want to thank my brothers Naveed Ansar Malik and Malik Azam Sultan. They always been there for me and have helped me a lot both physically and psychologically during my education. The love, advice, and help of my sisters Sadia Ansar and Maria Ansar is greatly appreciated. I have learned a lot about life through them. My sister Maria has followed my footsetps and has started a MD/PhD program in UTMB. I am extremely proud of her and wish her all the best in her academic career. My niece Khadija and my nephews Zaid and Musa are always a source of encouragement and fun. I owe deep gratitude to my family and without their help I would not have been able to complete my dissertation.

I would like to acknowledge the Army Research Laboratory, the Department of Defense STEP Program, the Office of Naval Research AppEl center at UMD (Task E12) research grant, the National Science Foundation CPS (CNS 0931878) research grant, the Air Force Office of Scientific Research (FA95501110182) grant, and the A James Clark School of Engineering Graduate Fellowship program for funding and supporting my graduate education and research.

I would also like to thank my office mates and colleagues; James Ferlez, Alborz Alavian, Bhaskar Ramasubramanian, Graham Aldredge, Kun Lin, Osman Yagan, Yongqianq Wang, Anthony Fanous, Tingyue Gan, Nof Abuzainab, Meiyun He, and Paul Tschirhart for all the discussions, support, and encouragement. The technical discussions with James were very helpful and I want to thank him for all his help. I would like to acknowledge my research group members; Eduardo Arvelo, Gabriel Lipsa, Serban Sabau, Marcos Vasconcelos, David Ward, and Shinkyu Park for their support and time. In particular, I appreciate their patience and their time in listening to my lectures on "The Probability Method". I would like to acknowledge my friends; Abdel Hameed Badawy, Mohammed Fathy, Mohamed Kashef, Khaleed El Wazeer, Ahmed Arafa, Mahmoud Gad, and Mohamed Baidas for their help, support, and for organizing prayers in the ECE department. I would also like to acknowledge my UET scholar friends; Hamza Shakeel, Awais Khawar, Shafiq Ur Rahman, Tamoor Gandapur, and Muhammad Akbar for their time, help, and support. Further, I would like to acknowledge my childhood friends; Fawad Ahmed Malik, Umar Jawaid, Syed Owais Ahmed, and Rizwan Mansoor. The long discussions with the UET scholars were memorable and were quite relaxing during stressful times. I specifically want to mention and thank Shafiq Ur Rahman for his help, time, kindness and cheerful attitude. I thoroughly enjoyed my adventures with Shafiq and Umar and thank them for that. I would also like to acknowledge all my friends at IMCB who always encouraged me to strive for the best. They provided me with a competitive academic environment which really sharpened my academic aptitude. I realy appreciate the help and support of my undergraduate friends and colleagues; Fahad Mahmood, Musharraf Nazir, Burhan Sadiq, Quadeer Ahmed, Chetan Bansal, Thameem Ullah Khan, Imran Shamim, Hassan

Sahibzada, Tanvir Ahmed, Farooq Saleem, Bilal Raja, Haris Raja, and Muhammad Adnan Walid. I appreciate the help and advice of Burhan Sadiq during many math classes at UMD. The jovial and funny personalities of Fahad and Adnan are greatly appreciated. I would like to thank my good friends; Khurram Raza, Ali Iqudus, Daanish Maqbool, Hira Siddiqui, Hamid Khalid, and Sadia Zaheer for their hospitality, encouragement, and support. Last but definitely not the least, I would like to thank Chaudhry Hassan Afzal for his out of the box thinking, career advice, funny jokes, and unique personality. I wish all of my friends and family the best in their lives and careers. May Allah grant you whatever you seek in this life!

Table of Contents

List of Figures

Chapter 1: Introduction

In the past two decades, the advent of advanced data sharing technologies has not only revolutionized modern systems but also how we socially interact with one another. People from all parts of the globe have connected like never before to form one global village. In the past, innovation and technology used to be restricted to a few societies and it took decades for new inventions to reach all parts of the globe. However, this is no longer the case due to modern data sharing capabilities. Even if a device cannot practically be available in some parts of the world it's methodology, functionality, and usage can widely be known and is readily accessible. The Internet and social media have enabled users to instantly share information and have completely changed the face of modern technology. However, the ease with which crucial information regarding any system can be accessed has also created security vulnerabilities which adversaries can exploit to undermine and potentially damage a system.

The biggest threats to modern technology in this age and time are cyber attacks from adversaries. Recent cyber attacks have practically shut down government websites affecting government operation, undermined financial institutions, and have even infringed on public privacy. These threats effect both on a macro level in terms of affecting big corporations, governments, and public institutions and on a micro level in terms of affecting

people through identity thefts and privacy violations.

Past research in the field of system security was mainly focused on designing robust algorithms and to prevent hacking of computers. While pursuit of such research is worthwhile in its own right an emerging trend is to design security protocols for systems which have control, networking, and communication capabilities. These problems are multidisciplinary and offer the aspiring researcher with many paradigms of exploration. The recent focus, in academia as well as the industry, towards this field of research is mainly due to new and emerging threats to industrial systems. It should be noted that control systems are widely used in modern industry and find wide applications in power systems, nuclear and chemical plants, the aerospace industry, robotics, communication devices, and embedded systems. All these systems typically rely on an underlying computing and networking infrastructure which has considerable security vulnerabilities.

Last year alone, according to the Department of Homeland Security, industrial systems faced nearly 200 attacks where many of these were of a serious nature (See [1] and [2] for more details). A majority of these attacks targeted sensitive installations, like energy and water plants, and the attackers even employed a sophisticated search engine to find thousands of exposed systems. As mentioned in the Los Angeles Times, cyber espionage and cyber attacks pose a greater threat to national security than terrorism [3]. According to Forbes [4], "For the first time, the growing risk of computer-launched foreign assaults on U.S. infrastructure, including the power grid, transportation hubs and financial networks, was ranked higher in the U.S. intelligence communitys annual review of worldwide threats than worries about terrorism". In light of these discussions, it is essential to conduct studies on the design and analysis of secure systems. This thesis is

an effort in this research direction mainly focused on the incorporation of security in the design of modern control systems.

There are two main types of problems that can be addressed within the framework of incorporating security in modern control system design. One line of problems involve securing the system from an adversary which can make measurements regarding system operation. The other type of problems focus on the issue of detecting the presence of adversaries, within the environment of a system, and then taking actions to eliminate future threats from such adversaries. The first approach can be considered to be shoring up one's defenses against an attack and the second involves detecting and eliminating an adversary before an attack can take place. Problem formulations and affiliated solution methodologies exploring both these areas of research will be considered in detail in subsequent chapters.

We first consider the type of problems where we design a controller which is secure enough to withstand potential attacks from an adversary. This is done by incorporating security constraints in the design of a linear quadratic control problem. It should be noted that classical control systems were designed without considering such security constraints, network attacks, and other system failures. Therefore, one cannot rely on classical control techniques when designing controllers for any application employing *cyber-physical* systems.

The term cyber-physical systems is generically used to describe all such physical systems which rely on a communication network and have computational capabilities. Research in cyber physical systems is a growing field which offers lots of opportunities and challenges for both academia as well as the industry. Cyber physical systems

are expected to play a major role in the design of next generation engineering systems which will posses a higher level of functionality, security, and reliability than the systems which are currently in operation today [5]. Research problems within this area are highly multi-disciplinary and offer many opportunities for research and development in control systems, network communications, computer security, biomedical engineering, the health care industry, smart grid research, renewable energy sources, transportation systems, and many other application areas.

Using the aforementioned system framework we solve linear quadratic control problems subjected to security constraints and team decision problems subjected to security constraints. Such a linear quadratic framework which incorporates security constraints is very general and can be applied to any physical system with linear dynamics, a quadratic cost, and which wants to secure itself from potential attacks from an adversary. Therefore, our results have practical significance for any physical system where the controller would like to hide its terminal operation from an adversary which could leverage information regarding the terminal state to undermine system operation.

In Team Decision Problems, there are two or more decision makers where each is tasked with making its own decision utilizing the information made available to it. It should be noted that the information available to the respective decision makers may or may not depend on the decisions made by other decision makers. We address team decision problems from a security perspective by incorporating security constraints and design optimal controllers subjected to such constraints. Our problem formulation and constraint structure has not previously been considered in problems of team decision theory and provides an important extension to this field of research. These decision making problems

have important practical applications in financial markets, corporate organizations, and military strategy.

For many control problems of interest, off-line computation is not available and problem need to be solved on-line. In addition, it is not possible to incorporate hard constraints in the optimization framework of these problems. Such problems are typically solved using a Receding Horizon Control (RHC) approach. Another advantage of RHC is the fact that it is able to anticipate future system behavior and apply appropriate control inputs accordingly. It should be noted that PID and LQR control techniques do not possess this ability to predict future system behavior. In RHC, at every time step a suitable control sequence is generated to solve a finite horizon optimal control problem by utilizing current and past measurements. The first element of this control sequence is applied to the plant and the procedure is repeated at the following time step.

Security constraints are generally hard constraints and for implementation purposes such problems typically require a suitable RHC approach. Therefore, a stochastic receding horizon control problem is presented and analyzed in subsequent chapters. We consider this problem under assumptions of limited computational capabilities which generally inhibit the controller's capability to perform complex on-line optimization. This inability to use any complex on-line optimization techniques is tackled by adopting an efficient randomized algorithm based scheme to randomly generate the required control inputs. The framework considered is general enough to be applied to any control problem which has hard constraints on the control inputs. This work finds significant applications in small devices and miniature robotics which is an area of high interest for both the government as well as the industry. The developed techniques provide bounds on sample

sizes, which guarantee several notions of probable near minimum to an optimal control problem. It should be noted that efficient and rapid sample generation can be done on any miniature device by utilizing analog electronics.

We also consider the aforementioned second line of security problems in the design of control systems. In these problems, the system is tasked to make measurements in order to detect the presence of an adversary in its environment which could potentially attack or undermine normal system operation. Due to the recent nature of cyber attacks on industrial and energy systems it is extremely important to determine potential attackers before they could launch a cyber attack. The problem formulations that we adopt to address these problems are quite general and can easily be utilized to design efficient algorithms and security protocols. Such problems find wide applications in the fields of optimal sampling, sensor networks, optimal agent placement, cyber espionage, optimal estimation, intruder detection, biological surveillance, electronic warfare, and military surveillance.

In the sequel, a security problem is considered where the system is tasked to detect the presence of an adversary which occurs on a specified set of points with a known distribution. The system has access to a team of identical sensors which can be deployed to make measurements regarding the presence of the adversary. The measurements made by the sensors are assumed to be noisy with well known probabilities of detection and false alarm which are provided by the manufacturer of these sensors. This problem can be classified as a centralized detection along with optimal sensor placement. The goal of this research is to come up with some general sensor placement principles which also provide jointly optimal intruder detection policies.

1.1 Main Contributions

The main research contributions and summaries of the upcoming chapters are provided below:

1. In Chapter 2, we consider a linear quadratic optimal control problem subject to security constraints. We consider the presence of an adversary which can make noisy partial measurements of the state and wants to estimate the terminal state of the system. The task is to generate control sequences such that the adversary is unable to estimate the terminal state of the system. This is done by minimizing a quadratic cost function while satisfying security constraints. Security metrics which provide different formulations for the security constraints are considered and analyzed. The optimization problems are shown to be convex and the optimal solution is computed by using Lagrangian based optimization techniques specifically duality. For the case when the terminal state has a discrete distribution the optimal solution is shown to be nonlinear in the terminal state.

   This is followed by considering the case when the terminal state has a continuous distribution. The security constraints are introduced by using a security metric based on the difference of conditional means. The resulting infinite dimensional optimization problems are shown to be convex. The generalized Kuhn Tucker Theorem is utilized to prove that the optimal solution is affine in the terminal state.

2. In Chapter 3, several team decision problems under security constraints are analyzed. Specifically, we consider problem formulations where there are two deci-

sion makers each possessing a different dynamical system. Each decision maker receives information regarding the respective terminal states that it is required to reach and applies a control sequence accordingly. An adversary makes partial noisy measurements of the states of both systems and tries to estimate their respective terminal states. The controllers of both systems minimize a common quadratic cost criterion. In addition, the terminal states of both systems are assumed to be either identical or correlated.

We first consider the case where the respective terminal states of both systems are assumed to be identical. This problem can be solved by utilizing the generalized Kuhn Tucker theorem along with some regularity conditions. The structure of this problem is similar to the security problems considered in Chapter 2 and the same proof techniques are utilized to obtain optimal solutions. We assume that the terminal state is reached by the controller with a continuous distribution. It is shown that the optimal solution is affine in the terminal state which is identical for both systems.

Next, we consider the general case where the terminal states of the decision makers are correlated in the sense that they are both reached with distributions which have the same mean but different variances. The information available to the decision makers is the respective terminal states of both systems and the problem has a partially nested information structure. We use a generalized security metric to introduce the security constraints. The resulting infinite dimensional optimization problems are convex. Utilizing the Kuhn Tucker Theorem in conjunction with some assumptions and regularity conditions we prove that the optimal solution is affine

in the information available to the respective decision makers.

3. In Chapter 4, a stochastic receding horizon control problem is presented and analyzed. We consider a linear, discrete, and time invariant system with bounded disturbance noise and hard bounds on the control input. We consider the case when the distribution of the noise is either unknown or is well known with a distribution function whose variance is difficult to compute. Utilizing a suboptimal disturbance feedback scheme, the optimization problem is shown to be convex. The problem of minimizing the empirical mean of the cost function instead of the expectation of the cost function is analyzed. Utilizing Pollard dimension theory we provide bounds on the disturbance sample size to compute the empirical minimum of the problem. This is done by first computing the Pollard dimension of the family of cost functions.

   Next, we consider the problem formulation where there are hard computational constraints and the controller is not capable to perform any complex on-line optimization. This problem is addressed by randomly generating both the control inputs and the disturbances from the space of admissible control inputs and the space of admissible disturbances respectively. Bounds on sample sizes are provided which guarantee several notions of probable near minimum to the problem. Finally, model uncertainty is incorporated into the problem framework and relevant bounds on sample sizes are provided which guarantee the existence of a probable near minimax value.

4. In Chapter 5, a centralized intruder detection problem with jointly optimal sensor

placement is considered. Specifically, we consider a team of sensors which is capable of making noisy measurements regarding the presence of an intruder at a particular point on which the sensor is placed. It is assumed that the intruder occurs on a specified set of placement points with a uniform distribution. Sensors make measurements regarding the presence of the intruder and report their observations to a centralized decision making authority. The decision maker solves a jointly optimal detection and sensor placement problem. It is assumed that the number of placement points is greater or equal to the number of sensors. This is a difficult optimization problem where the number of ways to place sensors on respective placement points increases exponentially with the number of sensors. We assume that the sensors are identical and make conditionally independent observations.

For the case when the number of sensors is equal to the number of placement points, we prove that uniform placement of sensors is not strictly optimal. This result holds regardless of the sensor local probability of detection and probability of false alarm. We introduce a majorization based partial order for the placement of sensors. For the case when the number of sensors is less than or equal to six, we show that for a fixed local probability of detection (probability of false alarm) increasing the probability of false alarm (probability of detection) results in optimal placements that are placed higher on a majorization based partial order. This result has many practical applications and can be used in the design of several sub-optimal schemes.

5. We provide conclusions and future research directions in Chapter 6.

Chapter 2: Linear Quadratic Control Under Security Constraints

In this chapter, we consider the problem of designing an optimal control system subjected to system security constraints. We consider a deterministic, linear, and time-invariant system for which the terminal state can either take a finite or an infinite number of values. It is assumed that the controller knows the value of the terminal state to reach and applies a control sequence accordingly. An adversary makes partial noisy measurements of the state trajectory and wants to estimate the terminal state of the system. It is assumed that the adversary has knowledge of the set of values taken by the terminal state.

The task of the controller is to develop a strategy to reach the terminal state while providing minimum information to the adversary thereby hindering its ability to estimate the terminal state. Different security metrics like the probability of error of the adversary, in estimating the terminal state, and some conditional mean based security metrics are considered and analyzed. In the sequel, these security metrics are used to introduce security constraints. We compute control sequences which minimize a given quadratic cost function while satisfying these security constraints. The resulting optimization problems are shown to be convex and techniques from Lagrangian duality and the generalized Kuhn Tucker theorem are employed to compute the optimal solutions. The cases of a Gaussian distribution and a more general finite mean distribution for the noise in the measurements

made by the adversary are considered and analyzed. This problem has important civilian and military applications. In addition, the problem formulation and the security constraints are general enough to be applied to most physical systems where security is a concern.

Control under cyber-physical security constraints (see [6], [7], [8], [9], [10], [11], [12], and [13]) is a very active area of research. Many interesting formulations and results have recently been presented in the literature. In [9], a security problem is considered where a jammer can block the communication link between the controller and the plant. The problem is formulated as a dynamic zero sum game and a saddle-point equilibrium between the controller and the jammer is shown to exist. The optimal jammer policy is proven to be of a threshold type. The effects of false data injection attacks in control systems are analyzed in [10]. Necessary and sufficient conditions are provided under which the attacker can destabilize the system through false data injections while evading detection. In [11], system stability and resilience under feedback schemes is characterized in the presence of attacks on sensors and actuators. A game theoretic analysis is provided in [12] where an attacker can physically capture sensor nodes in a wireless network, replicate the captured nodes, and eventually take over the network. Nash equilibrium solutions are provided for both the cases when the node capture rate is time invariant and when it is time varying. In [13], the problem of cyber-physical security is addressed by incorporating a geometric control approach. A mathematical framework for attacks and monitors is presented and fundamental monitoring limitations are characterized from both a system theoretic and a graph theoretic perspective.

We motivate the main research framework in this chapter by presenting some inter-

esting real life applications of such problems:

1. **Police Drug Bust:** Consider the situation where a convoy of police vehicles is assigned to inspect suspicious neighborhoods in a city. Once the police convoy reaches a neighborhood they completely seal all escape routes and do a complete house to house search for drugs, weapons, and other criminal activity. Also as soon as a neighborhood is sealed the criminals in other neighborhoods get tipped off and escape. The police convoy has several routes to reach each neighborhood respectively. The criminals have spies posted near the police station and can make some initial measurements regarding the route taken by the convoy. The task of the convoy is to optimize the route in such a way that the criminals get minimum information regarding the neighborhood that will actually be inspected by the police on any given day.

2. **Soccer Penalty kick:** Consider the situation where a striker in soccer takes a penalty kick. Now the striker has three options and can either hit the ball straight, left, or to the right side of the net. The goalkeeper can dive on either side of the net or stand in the middle in order to stop the penalty. The goalkeeper can make some measurements by observing how the striker runs in to strike the ball. The task of the striker is to choose an option and execute the kick such that the goalkeeper cannot predict the actual location of the ball and score a goal. If the striker adopts the perfect secrecy policy then the goal keeper will have no choice but to guess where the striker will strike the ball and make his dive accordingly. In that case the probability that the goal keeper dives in the right direction is $\frac{1}{3}$. However, there is also

a cost affiliated with using a high secrecy policy and the striker might not be able to strike the ball effectively, based on his limited striking capabilities, if he chooses a highly secure policy. Therefore, the striker faces a trade off between secrecy and performance and our mathematical framework in the sections to follow addresses this trade off.

3. **Bat Swarm Predation:** Consider a swarm of bats that is flying over to a specific part of a forest to eat fruits. The swarm is composed of both experienced adult bats and some juvenile bats. Using its experience an adult bat selects a certain tree to fly over to and eat some fruits. Now this bat knows that other young bats will follow it to the selected tree to steal some fruit from it. Therefore, its wants to hide its terminal tree location as much as possible from other bats until it is time to make a dive towards the selected tree. The more security it incorporates in its trajectory until the time to dive the more time it will have to eat fruit before other bats reach that tree. However, more secrecy which means hiding its strategy till the last moment before the dive also results in a higher cost as the bat has to put in a lot of effort to make a really good dive. Therefore, a similar trade off between security and performance is observed in this natural phenomenon as well.

4. **Cruise Missile Control:** Consider a cruise missile launching system that is tasked to strike a set of land based targets from a sea based location. It is assumed that the intended targets do not have the capabilities to bring down the missiles but given advance knowledge of the strikes will remove the high value targets from the targeted locations making the strikes useless. The adversaries have some allies located near

the missile launching site which can make some partial noisy measurements of the trajectories of the missiles. These allies have the ability to then inform the intended targets of the location of the strikes. The task of the missile launching system is to design the missile trajectories in such a way that the measurements made by the adversary cannot determine the intended location of the strikes.

The following notation is adopted:

- Random variables are represented using bold face capital letters, for example $\mathbf{X_T}$ is used to represent the terminal state. Realizations of these random variables are represented using small letters, like x_T.

- The probability of error is denoted by P_e, the prior probability distribution by π, the probability density of a random variable $\mathbf{X}$ if it exists by $p(x)$, the joint probability density of $\mathbf{X}$ and $\mathbf{Y}$ by $p(x,y)$, and the conditional probability density of $\mathbf{X}$ given $\mathbf{Y}$ by $p(x|y)$.

- Capital letter H denotes a hypothesis and M is used to denote the number of hypotheses.

- $I_{m\times m}$ represents the $m \times m$ identity matrix and $0_{m\times n}$ is used to represent the $m \times n$ matrix of zeros. Logarithm to the base 2 and natural logarithm are denoted by log and ln respectively.

- The standard ℓ_p norm is denoted by $\|.\|_p$.

- The set of real numbers is denoted by $\Re$, the n-dimensional space of real numbers by $\Re^n$, and the empty set is denoted by ϕ.

This chapter is organized into five main sections. In Section 1, we present a precise mathematical formulation of the problem. Section 2 is focused on designing secure control laws for the case when the terminal state can take two different values with specified probabilities. Under the assumption of a Gaussian distribution for measurement noise, we utilize the probability of error as a security constraint. The optimization problem is shown to be convex. We follow this by considering the case of a more general finite mean noise distribution. A security constraint based on the conditional mean is analyzed. In Section 3, we consider the case when the terminal state can take M different values where M is a natural number. A generalization of the conditional mean based security constraint is analyzed and the resulting optimization problem is shown to be convex. Section 4 considers the case where the terminal state takes values with a continuous distribution. A conditional mean based security constraint is analyzed and the optimal solution is shown to be affine in the terminal state. Simulation based results and related discussions are provided in detail in Section 5.

2.1 Problem Formulation

Consider the following linear and discrete time-invariant system given by:

$$x_{k+1} = Ax_k + Bu_k, \quad k = 0, ..., T-1 \tag{2.1}$$

where $x_k \in \Re^n$ is the state of the system, $u_k \in \Re^m$ is the control input, A is an $n \times n$ matrix, and B is an $n \times m$ matrix. Without loss of generality, the initial state x_0 is assumed to be zero. The cases of both finite and continuous distributions of the terminal state will

be analyzed. In Section 2, we assume that $x_T \in \{x^0, x^1\}$ and in Section 3 it is assumed that $x_T \in \{x^0, ..., x^{M-1}\}$. The framework for the terminal state with the continuous distribution case will be presented in Section 4. In the finite distribution case, the desired terminal state is drawn from $\{x^0, ..., x^{M-1}\}$ with prior distribution $\pi_0, ..., \pi_{M-1}$. The controller knows the value of the terminal state and accordingly applies the appropriate control sequence, $\{u_0, ..., u_{T-1}\}$, to reach it.

The adversary does not know the actual value of the terminal state, which is random, but knows its distribution. The adversary is restricted to make only the first $(k+1)$ measurements of the state with $k < T$. These measurements are noisy and are given as follows:

$$\mathbf{Y_i} = Cx_i + \mathbf{V_i}, \quad i = 0, ..., k \tag{2.2}$$

where C is a $p \times n$ matrix and $\mathbf{V_0}, ..., \mathbf{V_k}$ are $p \times 1$ independent and identically distributed random vectors. Using (2.1) we can write the measurement model in compact form as follows:

$$\mathbf{Y_{0,k}} = \bar{C}U_{0,k-1} + \mathbf{V_{0,k}} \tag{2.3}$$

where $\mathbf{Y_{0,k}}$, $\bar{C}$, $U_{0,k-1}$ and $\mathbf{V_{0,k}}$ are given as follows:

$$\mathbf{Y_{0,k}} = \begin{bmatrix} \mathbf{Y_0} \\ \vdots \\ \mathbf{Y_k} \end{bmatrix}, \ \mathbf{V_{0,k}} = \begin{bmatrix} \mathbf{V_0} \\ \vdots \\ \mathbf{V_k} \end{bmatrix}, \ U_{0,k-1} = \begin{bmatrix} u_0 \\ \vdots \\ u_{k-1} \end{bmatrix}, \ \bar{C} = \begin{bmatrix} 0_{p\times m} & 0_{p\times m} & \dots & 0_{p\times m} \\ CB & 0_{p\times m} & \dots & 0_{p\times m} \\ \vdots & \vdots & \ddots & \vdots \\ CA^{k-1}B & CA^{k-2}B & \dots & CB \end{bmatrix} \tag{2.4}$$

We first consider the case when the noise vectors $\mathbf{V_0}, ..., \mathbf{V_k}$ have a Gaussian distribution and then we consider the case when these noise vectors have a general finite mean distribution. We assume that $\pi_i > 0$, where $i = 0, ..., M-1$.

Main Assumption: The dynamical system is assumed to be controllable in the sense that starting from the origin any value of the terminal state can be reached at time T, by applying an appropriate control sequence. Therefore, we are assuming that the matrix:

$$\begin{bmatrix} A^{T-1}B & A^{T-2}B & \dots & B \end{bmatrix}$$

is of full rank.

The aforementioned controllability assumption implies that there are many control sequences which drive the state trajectory to the specified terminal state. We denote any control sequence which drives the system to the terminal state x^i by $U^i_{0,T-1}$. Using the measurement model, the adversary solves a hypothesis testing problem. Under hypothesis H_i, when the terminal state is x^i, the information available to the adversary is as follows:

$$\mathbf{Y_{0,k}} = \bar{C}U^i_{0,k-1} + \mathbf{V_{0,k}} \tag{2.5}$$

It should be noted that the security constraints are dependent on the information, $\bar{C}U^i_{0,k-1}$, which is provided by the controller to the adversary. The quadratic cost to be minimized is provided below:

$$\mathbb{U}'Q\mathbb{U} = \sum_{i=0}^{M-1} \pi_i {U^i_{0,T-1}}' \tilde{Q} U^i_{0,T-1} \tag{2.6}$$

where $\tilde{Q}$ is a $Tm \times Tm$ symmetric positive definite matrix. The symmetric positive definite matrix Q and the control vector $\mathbb{U}$ are given as follows:

$$\mathbb{U} = \begin{bmatrix} U^0_{0,T-1} \\ \vdots \\ U^{M-1}_{0,T-1} \end{bmatrix}, \; Q = \begin{bmatrix} \pi_0\tilde{Q} & 0_{Tm\times Tm} & \dots & 0_{Tm\times Tm} \\ 0_{Tm\times Tm} & \pi_1\tilde{Q} & \dots & 0_{Tm\times Tm} \\ \vdots & \vdots & \ddots & \vdots \\ 0_{Tm\times Tm} & 0_{Tm\times Tm} & \dots & \pi_{M-1}\tilde{Q} \end{bmatrix} \tag{2.7}$$

Since the control sequences $U^0_{0,T-1}, ..., U^{M-1}_{0,T-1}$ must drive the system to the terminal states $x^0, ..., x^{M-1}$ we need to introduce the following equality constraints:

$$B_T U^i_{0,T-1} = x^i, \; i = 0, ..., M-1 \tag{2.8}$$

which can be written in compact form as follows:

$$F\mathbb{U} = b \tag{2.9}$$

where F, b, and B_T are given as follows:

$$F = \begin{bmatrix} B_T & 0_{n\times Tm} & \dots & 0_{n\times Tm} \\ 0_{n\times Tm} & B_T & \dots & 0_{n\times Tm} \\ \vdots & \vdots & \ddots & \vdots \\ 0_{n\times Tm} & 0_{n\times Tm} & \dots & B_T \end{bmatrix}, b = \begin{bmatrix} x^0 \\ \vdots \\ x^{M-1} \end{bmatrix}, \; B_T = \begin{bmatrix} A^{T-1}B, & A^{T-2}B, & \dots, B \end{bmatrix} \tag{2.10}$$

The optimization problem that we will solve will involve minimization of the cost

function (2.6), subject to the equality constraint (2.9), and the security constraints that we will provide in the next two sections. The optimization will be performed with respect to the control variable $\mathbb{U}$. By utilizing an appropriate re-parametrization the equality constraints can be removed from this optimization problem . Let U_b be a suitable control vector which is provided to us and satisfies $FU_b = b$. Note that there always exists such a control vector because of the controllability assumptions. Let $\tilde{F}$ be the matrix whose columns form a basis for the Null space of F. Then we can write:

$$\mathbb{U} = U_b + \tilde{F}\eta, \quad \eta \in \Re^{dim(Null(F))} \tag{2.11}$$

It should be noted from the definition of $\tilde{F}$ that for any η, $F(\tilde{F}\eta) = 0$. Now η becomes our new optimization variable and we do not need to incorporate the equality constraint (2.9). The cost function can now be re-written as follows:

$$\mathbb{U}'Q\mathbb{U} = U_b'QU_b + 2U_b'Q\tilde{F}\eta + \eta'\tilde{F}'Q\tilde{F}\eta \tag{2.12}$$

2.2 Secure Control: A Binary Framework

In this section, we consider the framework where the terminal state can take two different values x^0 and x^1 with probabilities π_0 and π_1 respectively. We consider two different cases of measurement noise distribution.

2.2.1 Gaussian Noise Distribution:

Consider the case when $\mathbf{V_0}, ..., \mathbf{V_k}$ are iid and have a Gaussian $\mathcal{N}(0, \tilde{\Sigma})$ distribution. Then $\mathbf{V_{0,k}}$ is a $\mathcal{N}(0, \Sigma)$ random vector where the covariance matrix Σ is block diagonal and has matrices $\tilde{\Sigma}$ on its diagonal. The minimum probability of error, in the adversary's estimate of the terminal state, is introduced as a security constraint. Under hypotheses H_0 and H_1 the measurements have the following distributions:

$$H_0 : \mathbf{Y_{0,k}} = \bar{C}U^0_{0,k-1} + \mathbf{V_{0,k}} \sim \mathcal{N}(\bar{C}U^0_{0,k-1}, \Sigma) \tag{2.13}$$

$$H_1 : \mathbf{Y_{0,k}} = \bar{C}U^1_{0,k-1} + \mathbf{V_{0,k}} \sim \mathcal{N}(\bar{C}U^1_{0,k-1}, \Sigma) \tag{2.14}$$

We use a Bayesian formulation with a uniform cost and knowledge of the priors to compute the minimum probability of error. The optimal Bayes test is a likelihood ratio test [14]. The likelihood ratio is given as follows:

$$L(y_{0,k}) = \frac{p(y_{0,k}|H_1)}{p(y_{0,k}|H_0)}$$

$$= \exp\left\{ (U^1_{0,k-1} - U^0_{0,k-1})'\bar{C}'\Sigma^{-1}y_{0,k} - \frac{1}{2}(U^1_{0,k-1} - U^0_{0,k-1})'\bar{C}'\Sigma^{-1}\bar{C}(U^1_{0,k-1} + U^0_{0,k-1}) \right\} \tag{2.15}$$

The optimal Bayes test γ_B is given as follows:

$$\gamma_B(y_{0,k}) = \begin{Bmatrix} H_1 & \text{if} & L(y_{0,k}) \geq \frac{\pi_0}{\pi_1} \\ H_0 & \text{if} & L(y_{0,k}) < \frac{\pi_0}{\pi_1} \end{Bmatrix} \tag{2.16}$$

By taking ln on both sides we can write the inequality $L(y_{0,k}) \geq \frac{\pi_0}{\pi_1}$ as:

$$(U^1_{0,k-1} - U^0_{0,k-1})' \bar{C}' \Sigma^{-1} y_{0,k} \geq \tau$$

$$\tau = \frac{1}{2}(U^1_{0,k-1} - U^0_{0,k-1})' \bar{C}' \Sigma^{-1} \bar{C}(U^1_{0,k-1} + U^0_{0,k-1}) + \ln(\frac{\pi_0}{\pi_1})$$

Now $\mathbf{Y_{0,k}}$ is a Gaussian random vector whose linear transformation by definition also has a Gaussian distribution. By computing the mean and variance of $(U^1_{0,k-1} - U^0_{0,k-1})' \bar{C}' \Sigma^{-1} \mathbf{Y_{0,k}}$ under H_0 and H_1 we get:

$$H_0 : \ (U^1_{0,k-1} - U^0_{0,k-1})' \bar{C}' \Sigma^{-1} \mathbf{Y_{0,k}} \sim \mathcal{N}\big((U^1_{0,k-1} - U^0_{0,k-1})' \bar{C}' \Sigma^{-1} \bar{C} U^0_{0,k-1}, d^2\big) \quad (2.17)$$

$$H_1 : \ (U^1_{0,k-1} - U^0_{0,k-1})' \bar{C}' \Sigma^{-1} \mathbf{Y_{0,k}} \sim \mathcal{N}\big((U^1_{0,k-1} - U^0_{0,k-1})' \bar{C}' \Sigma^{-1} \bar{C} U^1_{0,k-1}, d^2\big) \quad (2.18)$$

$$d^2 = (U^1_{0,k-1} - U^0_{0,k-1})' \bar{C}' \Sigma^{-1} \bar{C}(U^1_{0,k-1} - U^0_{0,k-1})$$

The probability of error in estimating the true value of the terminal state is given by:

$$P_e = \pi_0 P\left(L\big(\mathbf{Y_{0,k}} \geq \frac{\pi_0}{\pi_1}\big) \middle| H_0\right) + \pi_1 P\left(L\big(\mathbf{Y_{0,k}} < \frac{\pi_0}{\pi_1}\big) \middle| H_1\right)$$

$$= \pi_0 - \pi_0 \Phi\left(\frac{1}{d} \ln \frac{\pi_0}{\pi_1} + \frac{d}{2}\right) + \pi_1 \Phi\left(\frac{1}{d} \ln \frac{\pi_0}{\pi_1} - \frac{d}{2}\right) \quad (2.19)$$

where Φ is the pdf of a standard normal $\mathcal{N}(0,1)$ distribution. For the special case of equi-probable priors, $\pi_0 = \pi_1 = \frac{1}{2}$, the above expression simplifies to give:

$$P_e = \rho\left(\frac{d}{2}\right) \quad (2.20)$$

Here ρ denotes the Q-function, the tail probability of the standard normal distribution. Consider the following optimization problem which introduces the probability of error as a security constraint:

Problem 2.2.1:

Minimize the cost function

$$U_b' Q U_b + 2U_b' Q \tilde{F} \eta + \eta' \tilde{F}' Q \tilde{F} \eta$$

subject to the constraint:

$$P_e \geq \alpha$$

where $\alpha \geq 0$ is a constraint parameter that we choose. This constraint basically tells how inaccurate the estimate of the adversary is in determining the actual value of the terminal state. The value of α provides a measure on the security level of the control sequences. The following result shows that this security constraint is convex in the optimization variable η.

Proposition 2.2.1.1:

The probability of error constraint is convex in η and Problem 2.2.1 is a convex program.

Proof:

From (2.19), we note that P_e is decreasing in d which is nonnegative. Therefore:

$$P_e \geq \alpha \quad \Leftrightarrow \quad d^2 \leq \alpha_1$$

where α_1 can be determined from the values of α, π_0, and π_1. For the special case where $\pi_0 = \pi_1$ we have $\alpha_1 = 4(\rho^{-1}(\alpha))^2$. Consider the following notation which enables us to write d^2 in terms of η.

$$U_{0,k-1}^i = GS_i(U_b + \tilde{F}\eta),\ G = [I_{km\times km}\ \ 0_{km\times(T-k)m}]$$

$$S_0 = [I_{Tm\times Tm}\ \ 0_{Tm\times Tm}],\ S_1 = [0_{Tm\times Tm}\ \ I_{Tm\times Tm}] \tag{2.21}$$

$$d^2 = (U_b + \tilde{F}\eta)'(S_1 - S_0)'G'\bar{C}'\Sigma^{-1}\bar{C}G(S_1 - S_0)(U_b + \tilde{F}\eta)$$

Clearly d^2 is convex in η, $d^2 \leq \alpha_1$ forms a convex set, and the cost is strictly convex in η. Therefore, Problem 2.2.1 is a convex program. □

Using Proposition 2.2.1.1 and (2.21) we solve the following convex program:

$$\min_{\eta}\ \ U_b'QU_b + 2U_b'Q\tilde{F}\eta + \eta'\tilde{F}'Q\tilde{F}\eta$$

subject to the constraint:

$$(U_b + \tilde{F}\eta)'(S_1 - S_0)'G'\bar{C}'\Sigma^{-1}\bar{C}G(S_1 - S_0)(U_b + \tilde{F}\eta) \leq \alpha_1 \tag{2.22}$$

We can practically solve this convex program by using standard convex optimization software like cvx [15]. By making some constraint qualification assumptions we characterize the optimal solution using Lagrangian duality.

Assumption 2.1: We assume that α is selected such that: $\left\{ \eta \in \Re^{dim(Null(F))} \mid (U_b + \tilde{F}\eta)'(S_1 - S_0)'G'\bar{C}'\Sigma^{-1}\bar{C}G(S_1 - S_0)(U_b + \tilde{F}\eta) < \alpha_1 \right\} \neq \phi$.

This assumption ensures that there exists a η such that the constraints in (2.22) are satisfied with strict inequality. This is precisely Slater's condition (see [16] for details) for this problem. Therefore, Assumption 2.1 implies that the duality gap is zero.

Proposition 2.2.1.2

The optimal solution to Problem 2.2.1, under Assumption 2.1, is non-linear in b and is given by:

$$\eta^* = -\left(\tilde{F}'Q\tilde{F} + \lambda^*\tilde{F}'\mathscr{L}'\mathscr{L}\tilde{F}\right)^{-1}\left(\tilde{F}'Q + \lambda^*\tilde{F}'\mathscr{L}'\mathscr{L}\right)U_b$$

where $\lambda^* \geq 0$ is the solution to the following equation:

$$\left\| \mathscr{L}U_b - \mathscr{L}\tilde{F}\left(\tilde{F}'Q\tilde{F} + \lambda\tilde{F}'\mathscr{L}'\mathscr{L}\tilde{F}\right)^{-1}\left(\tilde{F}'Q + \lambda\tilde{F}'\mathscr{L}'\mathscr{L}\right)U_b \right\|_2 = \sqrt{\alpha_1}$$

where $\mathscr{L} = W'\bar{C}G(S_1 - S_0)$, $\Sigma^{-1} = WW'$, and b is the vector of terminal states.

Proof:

Let $\Sigma^{-1} = WW'$ be the Cholesky decomposition of the inverse of the covariance matrix. The Lagrangian can be written as follows:

$$L(\eta, \lambda) = U_b'QU_b + 2U_b'Q\tilde{F}\eta + \eta'\tilde{F}'Q\tilde{F}\eta + \lambda\left(U_b'\mathscr{L}'\mathscr{L}U_b + 2\eta'\tilde{F}'\mathscr{L}'\mathscr{L}U_b\right.$$

$$+\eta'\tilde{F}'\mathscr{L}'\mathscr{L}\tilde{F}\eta-\alpha_1\Big) \tag{2.23}$$

It should be noted that the Lagrangian, $L(\eta,\lambda)$, is strictly convex in η. This is due to the columns of $\tilde{F}$ being linearly independent. Strong duality holds from Slater's conditions and we can solve the dual problem to get the optimal cost. Strict convexity, strong duality, and the fact that the optimal cost is finite ensure that we can obtain the solution of the primal problem through the dual problem [16] (See Ch. 5). The Lagrange dual function is given by:

$$g(\lambda)=\min_{\eta}\Big\{U_b'QU_b+2U_b'Q\tilde{F}\eta+\eta'\tilde{F}'Q\tilde{F}\eta+\lambda\Big(U_b'\mathscr{L}'\mathscr{L}U_b+2\eta'\tilde{F}'\mathscr{L}'\mathscr{L}U_b$$

$$+\eta'\tilde{F}'\mathscr{L}'\mathscr{L}\tilde{F}\eta-\alpha_1\Big)\Big\} \tag{2.24}$$

Computing the gradient of the Lagrangian with respect to η and setting it equal to zero we get:

$$\eta=-\Big(\tilde{F}'Q\tilde{F}+\lambda\tilde{F}'\mathscr{L}'\mathscr{L}\tilde{F}\Big)^{-1}\Big(\tilde{F}'Q+\lambda\tilde{F}'\mathscr{L}'\mathscr{L}\Big)U_b \tag{2.25}$$

Plugging (2.25) into (2.24) we get:

$$g(\lambda)=U_b'QU_b-2U_b'Q\tilde{F}\Big(\tilde{F}'Q\tilde{F}+\lambda\tilde{F}'\mathscr{L}'\mathscr{L}\tilde{F}\Big)^{-1}\Big(\tilde{F}'Q+\lambda\tilde{F}'\mathscr{L}'\mathscr{L}\Big)U_b+$$

$$U_b'\big(\tilde{F}'Q+\lambda\tilde{F}'\mathscr{L}'\mathscr{L}\big)'\big(\tilde{F}'Q\tilde{F}+\lambda\tilde{F}'\mathscr{L}'\mathscr{L}\tilde{F}\big)^{-1}\big(\tilde{F}'Q+\lambda\tilde{F}'\mathscr{L}'\mathscr{L}\big)U_b+\lambda U_b'\mathscr{L}'\mathscr{L}U_b$$

$$-2\lambda U_b'\big(\tilde{F}'Q+\lambda\tilde{F}'\mathscr{L}'\mathscr{L}\big)'\big(\tilde{F}'Q\tilde{F}+\lambda\tilde{F}'\mathscr{L}'\mathscr{L}\tilde{F}\big)^{-1}\tilde{F}'\mathscr{L}'\mathscr{L}U_b-\lambda\alpha$$

The optimal cost can be obtained by maximizing the Lagrange dual function with

respect to λ, which is assumed to be non-negative. Differentiating g with respect to λ and setting the derivative equal to zero we get:

$$\Big(U_b'\big(\tilde{F}'Q+\lambda\tilde{F}'\mathscr{L}'\mathscr{L}\big)'\big(\tilde{F}'Q\tilde{F}+\lambda\tilde{F}'\mathscr{L}'\mathscr{L}\tilde{F}\big)^{-1}\tilde{F}'\mathscr{L}'\mathscr{L}\tilde{F}\big(\tilde{F}'Q\tilde{F}+\lambda\tilde{F}'\mathscr{L}'\mathscr{L}\tilde{F}\big)^{-1}\times$$

$$\big(\tilde{F}'Q+\lambda\tilde{F}'\mathscr{L}'\mathscr{L}\big)U_b\Big)+U_b'\mathscr{L}'\mathscr{L}U_b-\Big(2U_b'\big(\tilde{F}'Q+\lambda\tilde{F}'\mathscr{L}'\mathscr{L}\big)'\big(\tilde{F}'Q\tilde{F}+\lambda\tilde{F}'\mathscr{L}'\mathscr{L}\tilde{F}\big)^{-1}$$

$$\times\tilde{F}'\mathscr{L}'\mathscr{L}U_b\Big)=\alpha$$

Simplifying this equation we get:

$$\left\|\mathscr{L}U_b-\mathscr{L}\tilde{F}\left(\tilde{F}'Q\tilde{F}+\lambda\tilde{F}'\mathscr{L}'\mathscr{L}\tilde{F}\right)^{-1}\left(\tilde{F}'Q+\lambda\tilde{F}'\mathscr{L}'\mathscr{L}\right)U_b\right\|_2=\sqrt{\alpha_1} \qquad (2.26)$$

Plugging the optimal value of $\lambda\geq 0$, denoted by λ^*, which solves the above equation into (2.25) provides an optimal solution to the problem, proving the claim of the proposition. It should be noted from (2.26) that λ^* is non-linear in U_b, which is linear in b. Therefore, the optimal solution of the problem is non-linear in b. □

Proposition 2.2.1.2 gives us a form of the optimal control sequences which will satisfy the probability of error security constraint. The convexity of this problem makes it very easy to practically implement these results using commercial optimization solvers.

2.2.2 Finite Mean Noise Distribution

In this section, we consider the case where the noise vectors $\mathbf{V_0},...,\mathbf{V_k}$ are iid and have a general distribution with a finite mean. Computing a closed form expression for the

probability of error is a very difficult problem with this framework even for the specific case of the exponential family of distributions [17].

We consider a new security framework based on the conditional mean which leads to a constraint very similar in structure to (2.22). Let μ be the mean of the noise vector $\mathbf{V_{0,k}}$, defined in (2.3). Under the hypotheses H_0 and H_1 the measurement model is given by:

$$\begin{aligned} H_0 &: \mathbf{Y_{0,k}} = \bar{C}GS_0(U_b + \tilde{F}\eta) + \mathbf{V_{0,k}} \\ H_1 &: \mathbf{Y_{0,k}} = \bar{C}GS_1(U_b + \tilde{F}\eta) + \mathbf{V_{0,k}} \end{aligned} \tag{2.27}$$

Problem 2.2.2:

Minimize the cost function:

$$U_b' Q U_b + 2U_b' Q \tilde{F}\eta + \eta' \tilde{F}' Q \tilde{F}\eta$$

subject to the constraint:

$$\Big(E(\mathbf{Y_{0,k}} \,|H_1) - E(\mathbf{Y_{0,k}} \,|H_0)\Big)' \Big(E(\mathbf{Y_{0,k}} \,|H_1) - E(\mathbf{Y_{0,k}} \,|H_0)\Big) \leq \alpha_2 \ , \quad \alpha_2 \geq 0 \tag{2.28}$$

The security constraint in (2.28) has a nice operational interpretation. It basically measures how far apart the means of the observations are under the two hypotheses. The further apart the means the easier it will be for the adversary to estimate the terminal state. It has the same intuitive interpretation as the probability of error constraint utilized in the

previous section. It should be noted that when α_2 is equal to zero the adversary does not get any useful information from the partial noisy state measurements.

Proposition 2.2.2.1:

The security metric in Problem 2.2.2 is convex in η and Problem 2.2.2 is a convex program.

Proof:

Now the difference between the conditional means can be computed to get:

$$E(\mathbf{Y}_{\mathbf{0},\mathbf{k}} \,|H_1) - E(\mathbf{Y}_{\mathbf{0},\mathbf{k}} \,|H_0) = \bar{C}G(S_1 - S_0)(U_b + \tilde{F}\eta) \tag{2.29}$$

Using (2.29) the constraint in (2.28) can be written as:

$$U_b' \mathscr{Z}' \mathscr{Z} U_b + 2\eta' \tilde{F}' \mathscr{Z}' \mathscr{Z} U_b + \eta' \tilde{F}' \mathscr{Z}' \mathscr{Z} \tilde{F} \eta \leq \alpha_2 \tag{2.30}$$

where $\mathscr{Z} = \bar{C}G(S_1 - S_0)$. Clearly this security constraint is convex and Problem 2.2.2 is a convex program. □

The security constraint (2.30) is very similar to (2.22), as $\mathscr{L}'\mathscr{L} = \mathscr{Z}'\Sigma^{-1}\mathscr{Z}$, and hence this section generalizes the work in section 2.2.1. In order to be able to use Lagrangian duality techniques we make the following assumption.

Assumption 2.2: We assume that α_2 is selected such that: $\left\{ \eta \in \Re^{dim(Null(F))} \mid U_b' \mathscr{Z}' \mathscr{Z} U_b + 2\eta' \tilde{F}' \mathscr{Z}' \mathscr{Z} U_b + \eta' \tilde{F}' \mathscr{Z}' \mathscr{Z} \tilde{F} \eta < \alpha_2 \right\} \neq \phi$.

This assumption ensures that Slater's conditions are satisfied for this problem.

Proposition 2.2.2.2:

The optimal solution of Problem 2.2.2, under Assumption 2.2, is non-linear in b and is given by:

$$\eta^* = -\left(\tilde{F}'Q\tilde{F} + \lambda^*\tilde{F}'\mathscr{Z}'\mathscr{Z}\tilde{F}\right)^{-1}\left(\tilde{F}'Q + \lambda^*\tilde{F}'\mathscr{Z}'\mathscr{Z}\right)U_b$$

where $\lambda^* \geq 0$ is the solution to the following equation:

$$\left\|\mathscr{Z}U_b - \mathscr{Z}\tilde{F}\left(\tilde{F}'Q\tilde{F} + \lambda\tilde{F}'\mathscr{Z}'\mathscr{Z}\tilde{F}\right)^{-1}\left(\tilde{F}'Q + \lambda\tilde{F}'\mathscr{Z}'\mathscr{Z}\right)U_b\right\|_2 = \sqrt{\alpha_2}$$

Proof:

The proof follows exactly along the same lines as the proof of Proposition 2.2.1.2 to which the reader is referred. □

Using these results we can design a secure controller for any system for which the adversary makes observations where the additive noise is drawn from a general finite mean distribution. The aforementioned security constraint can also be extended to the M-ary framework. We explore and develop one such extension in the following section.

2.3 Secure Control: A M-ary Framework

In this section, we consider the framework where the terminal state can take M different values $x^0, ..., x^{M-1}$ with probabilities $\pi_0, ..., \pi_{M-1}$, respectively. It is assumed that the measurement noise vector $\mathbf{V_{0,k}}$ has a general distribution with a finite mean.

We now present a new security metric which is also defined using the concept of

the difference of conditional means. Under the hypothesis $H_i,\ i = 0,...,M-1$, the measurement model is given by:

$$H_i : \mathbf{Y}_{\mathbf{0},\mathbf{k}} = \bar{C}GS_i(U_b + \tilde{F}\eta) + \mathbf{V}_{\mathbf{0},\mathbf{k}},\ \ i = 0,...,M-1 \tag{2.31}$$

Consider the following security metric:

$$\sum_{i=0}^{M-1} \pi_i \left(E\left(\mathbf{Y}_{\mathbf{0},\mathbf{k}} \middle| H_i\right) - \sum_{j=0}^{M-1} \pi_j E\left(\mathbf{Y}_{\mathbf{0},\mathbf{k}} \middle| H_j\right) \right)' \left(E\left(\mathbf{Y}_{\mathbf{0},\mathbf{k}} \middle| H_i\right) - \sum_{j=0}^{M-1} \pi_j E\left(\mathbf{Y}_{\mathbf{0},\mathbf{k}} \middle| H_j\right) \right) \tag{2.32}$$

This security metric can be considered to be a generalization to the concept of the difference of conditional means which was employed in the binary framework. The distribution π_i is used to assign weights to each quadratic quantity in (2.32), which provides a difference of the conditional mean given one hypothesis with the weighted sum of the conditional means given other hypotheses. A smaller value of this metric makes it more difficult for the adversary to predict the terminal state and indicates a higher level of security of the control sequences. Using this security metric, we can state the following optimization problem:

Problem 2.3: Minimize the cost function

$$U_b' Q U_b + 2U_b' Q \tilde{F} \eta + \eta' \tilde{F}' Q \tilde{F} \eta$$

subject to the security constraint:

$$\sum_{i=0}^{M-1} \pi_i \left(E\left(\mathbf{Y}_{\mathbf{0},\mathbf{k}} \middle| H_i\right) - \sum_{j=0}^{M-1} \pi_j E\left(\mathbf{Y}_{\mathbf{0},\mathbf{k}} \middle| H_j\right) \right)' \left(E\left(\mathbf{Y}_{\mathbf{0},\mathbf{k}} \middle| H_i\right) - \sum_{j=0}^{M-1} \pi_j E\left(\mathbf{Y}_{\mathbf{0},\mathbf{k}} \middle| H_j\right) \right) \leq \alpha_3 \tag{2.33}$$

The parameter α_3 is selected to be non-negative. A small α_3 indicates that a lower level of useful information can be transmitted to the adversary. For the case of α_3 equal to zero, the controller will be restricted to those control sequences which generate the same state trajectory for the first k+1 time steps. Using the measurement model we get:

$$E\left(\mathbf{Y}_{\mathbf{0},\mathbf{k}} \middle| H_i\right) - \sum_{j=0}^{M-1} \pi_j E\left(\mathbf{Y}_{\mathbf{0},\mathbf{k}} \middle| H_j\right) = \bar{C}G\left(S_i - \sum_{j=0}^{M-1} \pi_j S_j\right)\left(U_b + \tilde{F}\eta\right) \tag{2.34}$$

Using (2.34), and $\mathscr{Z}_i = \bar{C}G\left(S_i - \sum_{j=0}^{M-1} \pi_j S_j\right)$, we can write (2.33) as:

$$\sum_{i=0}^{M-1} \pi_i \left(U_b' \mathscr{Z}_i' \mathscr{Z}_i U_b + 2\eta' \tilde{F}' \mathscr{Z}_i' \mathscr{Z}_i U_b + \eta' \tilde{F}' \mathscr{Z}_i' \mathscr{Z}_i \tilde{F} \eta \right) \leq \alpha_3 \tag{2.35}$$

Clearly (2.35) is convex in η and hence we conclude that Problem 2.3 is a convex program. By making similar assumptions we can extend the results stated in section 2.2.2 to the M-ary framework.

Assumption 2.3: We assume that α_3 is selected such that: $\left\{ \eta \in \Re^{dim(Null(F))} \mid \sum_{i=0}^{M-1} \pi_i \left(U_b' \mathscr{Z}_i' \mathscr{Z}_i U_b + 2\eta' \tilde{F}' \mathscr{Z}_i' \mathscr{Z}_i U_b + \eta' \tilde{F}' \mathscr{Z}_i' \mathscr{Z}_i \tilde{F} \eta \right) < \alpha_3 \right\} \neq \phi$.

This assumption ensures that Slater's conditions are satisfied for this problem and hence the duality gap is zero.

Proposition 2.3.1: The optimal solution of Problem 2.3, under Assumption 2.3, is non-linear in b and is given by:

$$\eta^* = -\left(\tilde{F}'Q\tilde{F} + \lambda^* \sum_{i=0}^{M-1} \pi_i \tilde{F}' \mathscr{Z}_i' \mathscr{Z}_i \tilde{F}\right)^{-1} \left(\tilde{F}'Q + \lambda^* \sum_{i=0}^{M-1} \pi_i \tilde{F}' \mathscr{Z}_i' \mathscr{Z}_i\right) U_b$$

where $\lambda^* \geq 0$ is the solution to the following equation:

$$\sum_{k=0}^{M-1} \pi_k \left\| \mathscr{Z}_k U_b - \mathscr{Z}_k \tilde{F} \left(\tilde{F}'Q\tilde{F} + \lambda \sum_{i=0}^{M-1} \pi_i \tilde{F}' \mathscr{Z}_i' \mathscr{Z}_i \tilde{F}\right)^{-1} \left(\tilde{F}'Q + \lambda \sum_{i=0}^{M-1} \pi_i \tilde{F}' \mathscr{Z}_i' \mathscr{Z}_i \tilde{F}\right) U_b \right\|_2 = \sqrt{\alpha_3}$$

Proof:

The proof follows exactly like the proof of Proposition 2.2.2.2 to which the reader is referred. □

The results stated in Proposition 2.3.1 are very similar to the results presented in Propositions 2.2.1.2 and 2.2.2.2. These results imply that the optimal solution is non-linear in the vector of terminal states. In order to find the optimal solution in these problems we need to solve for the equality of a norm to a design parameter. In Proposition 2.3.1, we have the weighted sum of such norms equaling $\sqrt{\alpha_3}$.

2.4 Secure Control: Terminal State with a Continuous Distribution

In this section, we consider the situation where the terminal state has a continuous finite mean distribution with given density function $p(x_T)$. In addition, the components of the terminal state are assumed to have a finite variance. It is assumed that the adversary knows the distribution of the terminal state. We first provide a definition of the Gateaux

differential which will be used repeatedly in this section and also in Chapter 3.

Definition 2.4: **(Gateaux Differential [18])**

Let X be a vector space and let T be a transformation defined on a domain $D \subset X$. Let $x \in D$, $\gamma \in \Re$, and let h be arbitrary in X. If the limit

$$\delta T(x;h) = \lim_{\gamma \to 0} \frac{1}{\gamma}[T(x+\gamma h) - T(x)]$$

exists, it is called the Gateaux differential of T at x with increment h. If the limit exists for each $h \in X$, then T is said to be Gateaux differentiable at x.

Let $U(x_T)$ be the control sequence which drives the system to the terminal state x_T, which mathematically implies that $B_T U(x_T) = x_T$. It should be noted that such a control sequence exists because of the main controllability assumption. Also in this case the control input vector, $U(.)$, is a function of the terminal state. Consider the following cost functional:

$$\mathbb{J}\big(U(.)\big) = \int_{\Re^n} U(x_T)' \tilde{Q} U(x_T) p(x_T)\, dx_T \tag{2.36}$$

The functions $U(.)$ are $\mathbb{L}^2$ integrable and belong to the space $\mathbb{L}^2(\Re^n, \mathscr{B}(\Re^n), \mu_p)$. Note that $\mathscr{B}(\Re^n)$ is the Borel σ-algebra on $\Re^n$ and μ_p is the probability measure corresponding to the probability distribution of the terminal state. We use the same technique which we employed in the previous sections to remove the equality constraint, $B_T U(x_T) = x_T$. Let $\tilde{U}(x_T)$ be a given control function such that $B_T \tilde{U}(x_T) = x_T, \forall x_T \in \Re^n$. We assume that $\tilde{U}(x_T)$ is linear in x_T. This is possible due to the controllability assumption and one possible choice for this control function is $\tilde{U}(x_T) = B_T^{\dagger} x_T$, where $B_T^{\dagger}$ is the

Moore-Penrose pseudoinverse of B_T. Let $\tilde{B}$ be a basis for the null space of B_T. Then we can write:

$$U(x_T) = \tilde{U}(x_T) + \tilde{B}\eta(x_T),\ \eta(x_T) \in \Re^q,\ q = dim(Null(B_T)) \tag{2.37}$$

Using (2.37), $\eta(.)$ becomes our new optimization variable and the cost functional can be re-written as follows:

$$\mathbb{J}\big(\eta(.)\big) = \int_{\Re^n} \Big(\tilde{U}(x_T) + \tilde{B}\eta(x_T)\Big)' \tilde{Q} \Big(\tilde{U}(x_T) + \tilde{B}\eta(x_T)\Big) p(x_T)\, dx_T \tag{2.38}$$

We assume that the observation noise has a general distribution with a finite mean. Under the hypothesis H_{x_T}, the measurements made by the adversary are given by:

$$H_{x_T}: \quad \mathbf{Y}_{0,k} = \bar{G}U(x_T) + \mathbf{V}_{0,k}, \quad \bar{G} = \bar{C}G \tag{2.39}$$

where $\bar{C}$ is given by (2.4) and $G = [I_{km\times km}\ \ 0_{km\times(T-k)m}]$. We now introduce the following general security metric based on the difference of conditional means:

$$\int_{\Re^n}\int_{\Re^n} p(x_T)p(y_T)\Big(E\big(Y_{0,k}\big|H_{x_T}\big) - E\big(Y_{0,k}\big|H_{y_T}\big)\Big)' \times \Big(E\big(Y_{0,k}\big|H_{x_T}\big) - E\big(Y_{0,k}\big|H_{y_T}\big)\Big) dy_T dx_T \tag{2.40}$$

where y_T is another realization of the terminal state. This security metric basically provides a measure on the difference of the conditional means. The higher the value of this metric the easier it will be for the adversary to estimate the terminal state. Using the

measurement model this metric can be simplified as follows:

$$\int_{\Re^n}\int_{\Re^n} p(x_T)p(y_T)\Big(U(x_T)-U(y_T)\Big)'\bar{G}'\bar{G}\Big(U(x_T)-U(y_T)\Big)dy_T dx_T \tag{2.41}$$

Using the cost functional (2.38), and the security constraint (2.41), we can state the following optimization problem:

Problem 2.4:

$$\min_{\eta(.)} \int_{\Re^n}\Big(\tilde{U}(x_T)+\tilde{B}\eta(x_T)\Big)'\tilde{Q}\Big(\tilde{U}(x_T)+\tilde{B}\eta(x_T)\Big)p(x_T)\,dx_T$$

subject to the security constraint:

$$\int_{\Re^n}\int_{\Re^n} p(x_T)p(y_T)\Big(\tilde{U}(x_T)-\tilde{U}(y_T)+\tilde{B}\big(\eta(x_T)-\eta(y_T)\big)\Big)'\bar{G}'\bar{G} \times\Big(\tilde{U}(x_T)-\tilde{U}(y_T)+\tilde{B}\big(\eta(x_T)-\eta(y_T)\big)\Big)\,dy_T dx_T \;\le\; \alpha_4$$

where α_4 is assumed to be nonnegative. A small value of α_4 indicates that a lower level of useful information is provided to the adversary. If α_4 is equal to zero, then the first k control inputs of all admissible control sequences will be the same. It should be noted that if α_4 is very small and if k is very large then there can be instances when the problem might be infeasible. However, this can be overcome by assuming much stronger controllability assumptions. One such assumption could be to require B to be of full rank to ensure that the problem is feasible for some extreme cases. It should be noted that Problem 2.4 is an infinite dimensional convex optimization problem. We provide a

solution to this problem by utilizing the Generalized Kuhn Tucker Theorem [18] (See Ch. 9).

Assumption 2.4: Consider only those values of α_4 for which the appropriate Lagrange multiplier to the problem, λ^*, is such that $\left[I_{q\times q} - 2\lambda^* \tilde{B}'\bar{G}'\bar{G}\tilde{B}\left(\tilde{B}'\left(\tilde{Q}+2\lambda^*\bar{G}'\bar{G}\right)\tilde{B}\right)^{-1}\right]$ is nonsingular.

Assumption 2.5: We assume that the constraint parameter, α_4, and the system dynamics are selected such that the optimal solution $\eta^*(.)$ to Problem 2.4 satisfies the security constraint and that there exists a $h(.) \in \mathbb{L}^2(\Re^n, \mathscr{B}(\Re^n), \mu_p)$ such that:

$$\int_{\Re^n}\int_{\Re^n} p(x_T)p(y_T)\left(\tilde{U}(x_T)-\tilde{U}(y_T)+\tilde{B}\left(\eta^*(x_T)-\eta^*(y_T)\right)\right)'\bar{G}'\bar{G}\left(\tilde{U}(x_T)-\tilde{U}(y_T)+\tilde{B}\left(\eta^*(x_T)-\eta^*(y_T)\right)\right)dy_T dx_T + 4\int_{\Re^n}\left(\tilde{U}(x_T)+\tilde{B}\eta^*(x_T)\right)'\bar{G}'\bar{G}\tilde{B}h(x_T)p(x_T)dx_T - 4\int_{\Re^n}\int_{\Re^n}\left(\tilde{U}(x_T)+\tilde{B}\eta^*(x_T)\right)'\bar{G}'\bar{G}\tilde{B}h(y_T)p(y_T)p(x_T)dy_T dx_T < \alpha_4$$

It should be noted that Assumption 2.5 is the standard regularity assumption required to apply the Generalized Kuhn Tucker Theorem. This regularity condition is a natural analog to the interior point condition employed for inequality constraints in the global theory of convex optimization (see [18]). Note that this condition excludes the possibility of incorporating an equality constraint by reducing the cone to a point or by including a constraint and its negative counterpart. Using the concept of Gateaux differentials, Assumption 2.4, Assumption 2.5, and the generalized Kuhn Tucker Theorem we obtain the following result.

Proposition 2.4.1: The optimal solution to Problem 2.4, under Assumption 2.4 and Assumption 2.5, is affine in x_T and is given by:

$$\eta^*(x_T) = -\left(\tilde{B}'\tilde{Q}\tilde{B} + 2\lambda^*\tilde{B}'\bar{G}'\bar{G}\tilde{B}\right)^{-1}\left(\tilde{B}'\tilde{Q} + 2\lambda^*\tilde{B}'\bar{G}'\bar{G}\right)\tilde{U}(x_T) \; +$$
$$2\lambda^*\left(\tilde{B}'\tilde{Q}\tilde{B} + 2\lambda^*\tilde{B}'\bar{G}'\bar{G}\tilde{B}\right)^{-1}\left(\tilde{B}'\bar{G}'\bar{G} - \left(I_{q\times q} - 2\lambda^*\Gamma_{\lambda^*}\right)^{-1}\Gamma_{\lambda^*}\tilde{B}'\tilde{Q}\right)\int p(y_T)\tilde{U}(y_T)dy_T$$

where $\Gamma_{\lambda^*} = \tilde{B}'\bar{G}'\bar{G}\tilde{B}\left(\tilde{B}'\left(\tilde{Q} + 2\lambda^*\bar{G}'\bar{G}\right)\tilde{B}\right)^{-1}$ and $\lambda^* \geq 0$ is the solution to the following equation:

$$\lambda^*\Bigg[-2\int_{\Re^n}\int_{\Re^n} p(x_T)p(y_T)\left(\tilde{U}(x_T) + \tilde{B}\eta^*(x_T)\right)'\bar{G}'\bar{G}\left(\tilde{U}(y_T) + \tilde{B}\eta^*(y_T)\right)dy_T dx_T +$$
$$2\int_{\Re^n} p(x_T)\left(\tilde{U}(x_T) + \tilde{B}\eta^*(x_T)\right)'\bar{G}'\bar{G}\left(\tilde{U}(x_T) + \tilde{B}\eta^*(x_T)\right)dx_T - \alpha_4\Bigg] = 0$$

Proof:

We will first compute the Gateaux differential of the Lagrangian and then use the generalized Kuhn Tucker theorem conditions to compute the optimal solution. Now the Lagrangian can be written as follows:

$$J_\lambda(\eta(.)) = \int_{\Re^n} p(x_T)\left(\tilde{U}(x_T) + \tilde{B}\eta(x_T)\right)'\left(\tilde{Q} + 2\lambda\bar{G}'\bar{G}\right)\left(\tilde{U}(x_T) + \tilde{B}\eta(x_T)\right)dx_T$$
$$-2\lambda\int_{\Re^n}\int_{\Re^n} p(x_T)p(y_T)\left(\tilde{U}(x_T) + \tilde{B}\eta(x_T)\right)'\bar{G}'\bar{G}\left(\tilde{U}(y_T) + \tilde{B}\eta(y_T)\right)dy_T dx_T \quad (2.42)$$

For any admissible variation $h(.) \in \mathbb{L}^2(\Re^n, \mathscr{F}, \mu_p)$ the Gateaux differential of the La-

grangian is given by:

$$\delta J_\lambda(\eta(.),h(.)) = 2\int_{\Re^n} p(x_T)\tilde{U}(x_T)'\left(\tilde{Q}+2\lambda\bar{G}'\bar{G}\right)\tilde{B}h(x_T)dx_T + 2\int_{\Re^n} p(x_T)\times$$
$$\eta(x_T)'\tilde{B}'\left(\tilde{Q}+2\lambda\bar{G}'\bar{G}\right)\tilde{B}h(x_T)dx_T - 4\lambda\int_{\Re^n}\int_{\Re^n} p(x_T)p(y_T)\tilde{U}(x_T)'\bar{G}'\bar{G}\tilde{B}h(y_T)dy_T dx_T$$
$$-4\lambda\int_{\Re^n}\int_{\Re^n} p(x_T)p(y_T)\eta(x_T)'\tilde{B}'\bar{G}'\bar{G}h(y_T)\ dy_T dx_T \quad (2.43)$$

Using the Kuhn Tucker conditions and setting the Gateaux differential equal to zero we get:

$$\int_{\Re^n} p(x_T)h(x_T)'\Bigg(\tilde{B}'\tilde{Q}\tilde{U}(x_T)+2\lambda\tilde{B}'\bar{G}'\bar{G}\tilde{U}(x_T)+\tilde{B}'\tilde{Q}\tilde{B}\eta(x_T)+2\lambda\tilde{B}'\bar{G}'\bar{G}\tilde{B}\eta(x_T)$$
$$-2\lambda\int_{\Re^n} p(y_T)\tilde{B}'\bar{G}'\bar{G}\tilde{U}(y_T)dy_T - 2\lambda\int_{\Re^n} p(y_T)\tilde{B}'\bar{G}'\bar{G}\tilde{B}\eta(y_T)dy_T\Bigg)dx_T = 0,\ \forall\ h(.) \quad (2.44)$$

Now (2.44) holds if and only if:

$$\tilde{B}'\left(\tilde{Q}+2\lambda\bar{G}'\bar{G}\right)\tilde{U}(x_T)+\tilde{B}'\left(\tilde{Q}+2\lambda\bar{G}'\bar{G}\right)\tilde{B}\eta(x_T) - 2\lambda\int_{\Re^n} p(y_T)\tilde{B}'\bar{G}'\bar{G}\tilde{U}(y_T)dy_T$$
$$-2\lambda\int_{\Re^n} p(y_T)\tilde{B}'\bar{G}'\bar{G}\tilde{B}\eta(y_T)dy_T = 0, \quad \forall x_T\in\Re^n \quad (2.45)$$

Now multiplying (2.45) throughout by $p(x_T)\Gamma_\lambda$ and integrating over x_T we get:

$$\left(I_{q\times q}-2\lambda\Gamma_\lambda\right)\int_{\Re^n} p(x_T)\tilde{B}'\bar{G}'\bar{G}\tilde{B}\eta(x_T)dx_T = -\int_{\Re^n} p(x_T)\Gamma_\lambda\tilde{B}'\tilde{Q}\tilde{U}(x_T)dx_T$$

Using Assumption 2.4 we get:

$$\int_{\Re^n} p(x_T)\tilde{B}'\bar{G}'\bar{G}\tilde{B}\eta(x_T)dx_T = -\left(I_{q\times q} - 2\lambda\Gamma_\lambda\right)^{-1}\int_{\Re^n} p(x_T)\Gamma_\lambda\tilde{B}'\tilde{Q}\tilde{U}(x_T)dx_T \quad (2.46)$$

Now plugging (2.46) into (2.45) we get:

$$\eta^*(x_T) = -\left(\tilde{B}'\tilde{Q}\tilde{B} + 2\lambda^*\tilde{B}'\bar{G}'\bar{G}\tilde{B}\right)^{-1}\left(\tilde{B}'\tilde{Q} + 2\lambda^*\tilde{B}'\bar{G}'\bar{G}\right)\tilde{U}(x_T) +$$
$$2\lambda^*\left(\tilde{B}'\tilde{Q}\tilde{B} + 2\lambda^*\tilde{B}'\bar{G}'\bar{G}\tilde{B}\right)^{-1}\left(\tilde{B}'\bar{G}'\bar{G} - \left(I_{q\times q} - 2\lambda^*\Gamma_{\lambda^*}\right)^{-1}\Gamma_{\lambda^*}\tilde{B}'\tilde{Q}\right)\int_{\Re^n} p(y_T)\tilde{U}(y_T)dy_T \quad (2.47)$$

which from the Kuhn Tucker conditions is the optimal solution. Also from the Kuhn Tucker conditions λ^* is given by the solution of the following equation:

$$\lambda^*\Bigg[-2\int_{\Re^n}\int_{\Re^n} p(x_T)p(y_T)\left(\tilde{U}(x_T) + \tilde{B}\eta^*(x_T)\right)'\bar{G}'\bar{G}\left(\tilde{U}(y_T) + \tilde{B}\eta^*(y_T)\right)dy_T dx_T +$$
$$2\int_{\Re^n} p(x_T)\left(\tilde{U}(x_T) + \tilde{B}\eta^*(x_T)\right)'\bar{G}'\bar{G}\left(\tilde{U}(x_T) + \tilde{B}\eta^*(x_T)\right)dx_T - \alpha_4\Bigg] = 0 \quad (2.48)$$

It should be noted that λ^* depends upon $\tilde{U}(.), p(.)$, and α_4 but not on the terminal state, x_T. Also $\tilde{U}(x_T)$ is selected to be linear in x_T. Therefore, we conclude from (2.47) that the optimal solution to Problem 2.4 is affine in x_T. □

Proposition 2.4.1 is an interesting result as it shows that the optimal solution is affine in the terminal state. Contrary to the results in the previous sections we obtain an affine solution for the case when the terminal state has a continuous distribution. Since the cost function is strictly convex so the optimal solution is unique. Assumption 2.4 and

Assumption 2.5 can be checked by first solving the problem and then using the optimal solution to check if the assumptions are satisfied. It should be noted that Assumption 2.4 allows us to operate only over particular regimes of the parameter, α_4. However, it is not very restrictive and we can still work with a wide range of parameter values as the assumption fails for only a finite number of values. Such an assumption can be removed if we consider the following simpler security constraint which also results in a solution which is affine in the terminal state.

$$\int_{\Re^n} p(x_T)U(x_T)'\bar{G}'\bar{G}U(x_T)\,dx_T \leq \alpha_5, \;\; \alpha_5 \geq 0 \tag{2.49}$$

The main difference between these constraints is that in (2.49) we compare the first k components of a control sequence, which drive the system to a particular terminal state, with the zero control sequence. For the security constraint employed in Problem 2.4, we compare the first k components of two control sequences which drive the system to different terminal state values. Both constraints are then constructed by multiplying with relevant probability densities, integrating over $\Re^n$, and using some appropriate security parameters.

2.5 Simulations

In this section, we provide an analysis of the behavior of the cost function as the security constraint parameter is varied. In addition, we utilize simulations to analyze the behavior of the optimal solution. We consider the framework of Problem 2.2.1 and further make the assumption that the priors are equi-probable. Consider the system dynamics:

$$A = \begin{bmatrix} 1 & 23 & 4 \\ 5 & 7 & 12 \\ 1 & 23 & 16 \end{bmatrix}, B = \begin{bmatrix} 1 & 4 & 4.3 \\ 6 & 2.3 & 8 \\ 12 & 7 & 1.8 \end{bmatrix}, b_1 = \begin{bmatrix} 53 \\ 75 \\ 100 \\ 32 \\ 37 \\ -8 \end{bmatrix}$$

Let $\Sigma = 2 \times I_{12\times 12}$, $Q = 5 \times I_{30\times 30}$, and $\alpha = 0.45$. We assume that $T = 5$ and $k = 2$. Using these values α_1 is calculated to be $4\left(\rho^{-1}(0.45)\right)^2$. We use the standard optimization software cvx to compute the optimal control sequences. The optimal solution, $\mathbb{U}$, is

given in (2.50).

$$\mathbb{U}(1:15) = \begin{bmatrix} -0.0118 \\ 0.0128 \\ 0.0076 \\ -0.0048 \\ -0.0023 \\ 0.0099 \\ \hline 0.0032 \\ 0.0052 \\ -0.0221 \\ 0.5366 \\ 0.0016 \\ -0.3726 \\ 0.1369 \\ 0.0453 \\ -0.1924 \end{bmatrix}, \quad \mathbb{U}(16:30) = \begin{bmatrix} -0.0118 \\ 0.0127 \\ 0.0076 \\ -0.0051 \\ -0.0020 \\ 0.0093 \\ \hline -0.0063 \\ -0.0058 \\ 0.0251 \\ -0.5374 \\ -0.0018 \\ 0.3736 \\ -0.1371 \\ -0.0454 \\ 0.1927 \end{bmatrix} \tag{2.50}$$

It should be noted that $\mathbb{U}(1:15)$ correspond to the first 15 elements of the control vector $\mathbb{U}$ which drive the system to the terminal state $\begin{bmatrix} 53 & 75 & 100 \end{bmatrix}'$. Similarly $\mathbb{U}(16:30)$ correspond to the control inputs which drive the system to the terminal state $\begin{bmatrix} 32 & 37 & -8 \end{bmatrix}'$, respectively. It should be noted that $k = 2,\ m = 3$, and hence the ad-

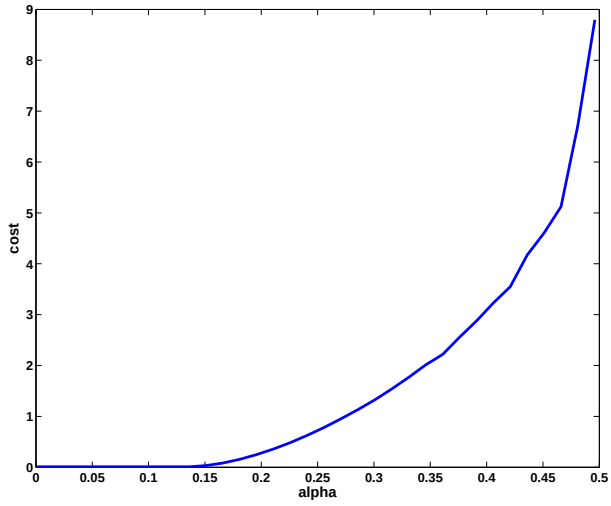

Figure 2.1: Optimal Cost vs α for the system with terminal state vector b_1

versary can only make noisy measurements of the first 2 control inputs, which are colored red, of these control vectors. Note that the control inputs which the adversary measures in both cases are very similar to one another thereby providing minimum useful information to the adversary. This is what we expected and this further signifies the importance of incorporating security constraints in control problems.

The simulation in Fig. 2.1 utilizes the system described above. We plot the optimal cost against the constraint parameter α, where $P_e \geq \alpha$. As discussed in Section 2.2 if $\alpha > 0.5$ then the security constraint becomes infeasible. Clearly as α is increased the problem becomes more constrained and cost increases respectively. An exponential increase in the cost is observed by an increase in the value of α, for $\alpha \geq 0.14$. In Fig. 2.1, $\begin{bmatrix} 53 & 75 & 100 & 32 & 37 & -8 \end{bmatrix}'$ was utilized as the vector of terminal states. In order to avoid any confusion we clarify that the value of the optimal cost, for $0 \leq \alpha \leq 0.15$, is approximately 0.01 and not zero.

We now consider a different dynamical system and a different vector of terminal

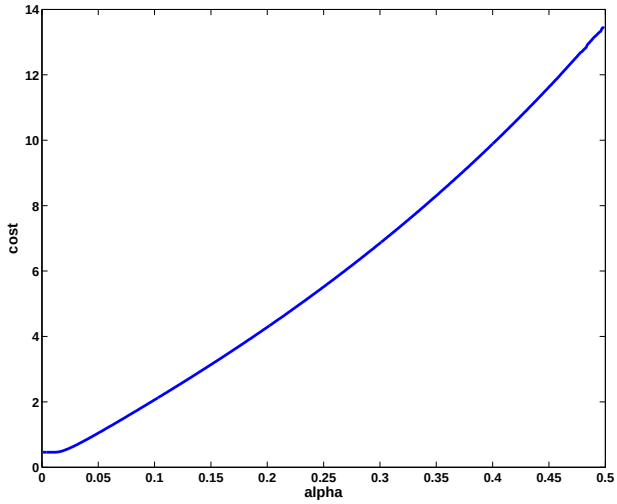

Figure 2.2: Optimal Cost vs α for the system with terminal state vector b_2

states to analyze the increase in the optimal cost with the value of α. Let:

$$A = \begin{bmatrix} 1 & 3 & 4 \\ 3.1 & 7 & 2 \\ 5 & 3 & 6 \end{bmatrix}, \; B = \begin{bmatrix} 1 & 4 & 0.3 \\ 6 & 3 & 2 \\ 2 & 7 & 9 \end{bmatrix}, b_2 = \begin{bmatrix} 10 \\ 12 \\ -8 \\ 4 \\ 7 \\ 5 \end{bmatrix}$$

We take $\Sigma = 0.5 \times I_{12\times 12}$, $Q = 10 \times I_{30\times 30}$, $T = 5$ and $k = 3$. Fig. 2.2 shows the increase in the optimal cost with the value of α for this system. Clearly in this case the optimal cost increases less rapidly than in the case of Fig. 2.1. Unlike the previous system, the optimal cost does not stay constant over a large range of values of α. Therefore, we can conclude that for this system the probability of error constraint is more tightly enforced as compared to the previous system. Also the rate of change in the optimal

cost is approximately constant. These simulations further show the importance of the constraint parameters in the optimal solution. Similar results can be obtained when we employ constraints based on the conditional mean.

Chapter 3: Team Decision Theory under Security Constraints

In this chapter, we extend the research ideas presented in Chapter 2 to problems in Team Decision Theory. We incorporate various security constraints which lead to different formulations under the framework of team decision theory. In a team decision problem, there are two or more decision makers each responsible for making a local decision by utilizing the information made available to it. The decisions made by the individual decision makers generally optimize a common cost or payoff criterion. The motivation for team decision problems initially came from decision making within organizations ([19], [20], [21]).

The first team decision problem was formulated by Marshak [19], in 1956. The adopted approach came from game theory and decision theory. The fundamental result for verifying the global optimality of a team decision rule was first provided by Radner in [20]. In the literature, this result is commonly referred to as Radner's Theorem. Under some assumptions it provides sufficient conditions under which a person by person optimal decision rule is globally optimal and is proved using a Hilbert space approach. However, this result is difficult to verify due to the requirement of a local finiteness condition. Using this result Radner showed that for the case of a quadratic cost and jointly Gaussian information variables the optimal solution is affine in the information available

to the decision makers. The difficulty in verifying the local finiteness condition is overcome in [22], which provides a generalized version of Radner's Theorem. This is done by requiring the existence of certain integrals. This generalized result is then used to establish the optimality of affine control laws for the exponential of a quadratic performance index with jointly Gaussian state and observations.

The results presented in ([19], [20], [21], [22]) deal with the static version of team decision problems. In static team problems, the information available to any decision maker is independent of the actions of other decision makers. In contrast, in dynamic team problems the information available to any decision maker varies with the actions of other decision makers. In dynamic team problems the dependence of a decision maker's rule on the policy of another decision maker converts the problem, with a cost originally quadratic in the decision rules, into a non convex optimization problem. Similarly this interdependence converts a Gaussian information structure to be non-Gaussian at the individual decision maker. The non-convex nature of the cost and the non-Gaussian form of the information variables make problems in dynamic team decision theory very difficult to solve.

Under the assumptions of a specialized information structure it is possible to convert a dynamic team problem into a static team problem. This information structure is called the "Partially Nested Information Structure" and was first introduced in [23]. In this case the information of a decision maker, whose decision rule depends on the decisions made by other decision makers, also contains the information available to those decision makers and hence can infer their decisions from the available information. It should be noted that team decision problems with quadratic constraints have been previously considered

in [24]. However, we consider a different problem formulation and incorporate a new security constraint framework.

The team decision problems considered in the sequel are subjected to security constraints. We consider a team of decision makers each possessing a different dynamical system and tasked with computing control sequences which generate a specified terminal state. The initial state of each dynamical system is assumed to be zero. An adversary makes partial measurements of the state trajectory of each decision maker and tries to estimate the terminal state. The terminal states are assumed to be either identical or correlated. The task of the controllers is to design control sequences such that the respective state trajectories reach the specified terminal state while minimizing a quadratic cost criterion and satisfying security constraints. The cost function, to be defined in the next section, is quadratic in the control sequences of the decision makers. Note that the cost is coupled among the decision makers and is obtained by integrating over the terminal states with respect to their probability density function.

Utilizing the aforementioned framework our aim is to prove that the optimal control policies of the decision makers, which provide the globally optimal solution, are affine in the terminal state. The optimal solution can be obtained from the Generalized Kuhn Tucker Theorem, which was also utilized in Section 2.4. This requires certain standard regularity conditions along with assumptions similar in structure to Assumption 2.4.

3.1 Problem Formulation

In order to simplify the presentation we consider the case when we have two decision makers. This formulation and the corresponding results can easily be extended to the case when we have more decision makers. Consider the following linear and time invariant dynamical systems each assigned to a specific decision maker:

$$(I): \quad \begin{pmatrix} x^1_{j+1} = A_1 x^1_j + B_1 u^1_j, \ j = 0, ..., T-1 \\ \mathbf{Y}^1_j = C_1 x^1_j + \mathbf{V}^1_j, \ j = 0, ..., k \end{pmatrix} \tag{3.1}$$

$$(II): \quad \begin{pmatrix} x^2_{j+1} = A_2 x^2_j + B_2 u^2_j, \ j = 0, ..., T-1 \\ \mathbf{Y}^2_j = C_2 x^2_j + \mathbf{V}^2_j, \ j = 0, ..., k \end{pmatrix} \tag{3.2}$$

where $x^i_j \in \Re^n, \ i = 1, 2$, are the states of system (I) and system (II) respectively, $u^i_j \in \Re^m, i = 1, 2$, are the control inputs, $A_i, \ i = 1, 2$, are $n \times n$ matrices and $B_i, \ i = 1, 2$, are the $n \times m$ matrices respectively. $\mathbf{Y}^1_0, ..., \mathbf{Y}^1_k$ are the measurements corresponding to system (I) that are available to the adversary and similarly $\mathbf{Y}^2_0, ..., \mathbf{Y}^2_k$ are the measurements of system (II) that are available to the adversary. C_1 and C_2 are $p \times n$ matrices, respectively. $\mathbf{V^1_0}, ..., \mathbf{V^1_k}$ are $p \times 1$ independent and identically distributed random vectors and the same assumption holds for $\mathbf{V^2_0}, ..., \mathbf{V^2_k}$. We assume that both system (I) and system (II) are completely controllable. We assume that the noise vectors have a general distribution with a finite mean. Now we can write the observation and noise vectors in compact form

as follows:

$$\mathbf{V^1_{0,k}} = \begin{bmatrix} \mathbf{V^1_0} \\ \vdots \\ \mathbf{V^1_k} \end{bmatrix}, \mathbf{V^2_{0,k}} = \begin{bmatrix} \mathbf{V^2_0} \\ \vdots \\ \mathbf{V^2_k} \end{bmatrix}, \mathbf{Y^1_{0,k}} = \begin{bmatrix} \mathbf{Y^1_0} \\ \vdots \\ \mathbf{Y^1_k} \end{bmatrix}, \mathbf{Y^2_{0,k}} = \begin{bmatrix} \mathbf{Y^2_0} \\ \vdots \\ \mathbf{Y^2_k} \end{bmatrix} \tag{3.3}$$

We present two different cases in this chapter. First, we consider the case when both systems are tasked to drive their state trajectories to an identical terminal state. This is followed by considering the case when both systems drive their state trajectories to correlated terminal states.

3.2 Team Decision Theory: Identical Terminal State

In this section, we consider the team problem where the controllers of both systems are tasked to drive their trajectories to the same terminal state, x_T. We assume that the terminal state, x_T, is reached with a continuous distribution. In addition, it is assumed that this distribution has a finite mean and a finite covariance. We assume that we are given the probability density function, $p(.)$, of this distribution.

Let $U_1(x_T)$ be the sequence of control inputs that drive the state trajectory of system (I) to the terminal state x_T and similarly let $U_2(x_T)$ be the sequence of control inputs which drives the state trajectory of system (II) to the terminal state x_T.

$$U_1(.) = \begin{bmatrix} u^1_0 \\ \vdots \\ u^1_{T-1} \end{bmatrix}, U_2(.) = \begin{bmatrix} u^2_0 \\ \vdots \\ u^2_{T-1} \end{bmatrix} \tag{3.4}$$

The measurements made by the adversary are assumed to have a general noise distribution with a finite mean. Under the hypothesis H_{x_T}, for which the terminal state is x_T, the measurements made by the adversary from each system can be written in compact form as follows:

$$H_{x_T} : \mathbf{Y^1_{0,k}} = \bar{G}_1 U_1(x_T) + \mathbf{V^1_{0,k}}, \;\; \mathbf{Y^2_{0,k}} = \bar{G}_2 U_2(x_T) + \mathbf{V^2_{0,k}} \tag{3.5}$$

where $\bar{G}_1$ and $\bar{G}_2$ are given by:

$$\bar{G}_i = \bar{C}_i G_i, \; G_i U_i(.) = \begin{bmatrix} u_0^i \\ \vdots \\ u_{k-1}^i \end{bmatrix}, \; \bar{C}_i = \begin{bmatrix} 0_{p\times m} & 0_{p\times m} & \cdots & 0_{p\times m} \\ C_i B_i & 0_{p\times m} & \cdots & 0_{p\times m} \\ \vdots & \vdots & \ddots & \vdots \\ C_i A_i^{k-1} B_i & C_i A_i^{k-2} B_i & \cdots & C_i B_i \end{bmatrix}, \; i = 1,2 \tag{3.6}$$

Since the control sequence $U_i(x_T), \; i = 1,2$, drives the state trajectories of the respective dynamical systems to the terminal state, x_T, the following equality constraints are required:

$$F_i U_i(x_T) = x_T, \; i = 1,2$$

$$F_i = \begin{bmatrix} A_i^{T-1} B_i & A_i^{T-2} B_i & \cdots & B_i \end{bmatrix}, \; i = 1,2 \tag{3.7}$$

Now utilizing the structure of the security metric presented in Section 2.4, we introduce the following security metric which can be used to introduce the security constraints

for this problem:

$$\int_{x_T}\int_{y_T} p(x_T)p(y_T)\Big(E\big(\mathbf{Y^1_{0,k}}|x_T\big)-E\big(\mathbf{Y^1_{0,k}}|y_T\big)\Big)'\Big(E\big(\mathbf{Y^1_{0,k}}|x_T\big)-E\big(\mathbf{Y^1_{0,k}}|y_T\big)\Big)dy_T dx_T$$
$$+\int_{x_T}\int_{y_T} p(x_T)p(y_T)\Big(E\big(\mathbf{Y^2_{0,k}}|x_T\big)-E\big(\mathbf{Y^2_{0,k}}|y_T\big)\Big)'\Big(E\big(\mathbf{Y^2_{0,k}}|x_T\big)-E\big(\mathbf{Y^2_{0,k}}|y_T\big)\Big)dy_T dx_T \tag{3.8}$$

where y_T is another realization for the terminal state. This security metric measures the difference of the conditional means for the two systems for different terminal state values and then adds their sum. Using equation (3.5) we get that the difference of conditional means is given by:

$$E\big(\mathbf{Y^i_{0,k}}|x_T\big)-E\big(\mathbf{Y^i_{0,k}}|y_T\big)=\bar{G}_iU_i(x_T)-\bar{G}_iU_i(y_T),\ i=1,2 \tag{3.9}$$

Using (3.9), the security metric can be simplified to get:

$$\int_{x_T}\int_{y_T} p(x_T)p(y_T)\Big(U_1(x_T)-U_1(x_T)\Big)'\bar{G}_1'\bar{G}_1\Big(U_1(x_T)-U_1(x_T\Big)dy_T dx_T$$
$$+\int_{x_T}\int_{y_T} p(x_T)p(y_T)\Big(U_2(x_T)-U_2(x_T)\Big)'\bar{G}_2'\bar{G}_2\Big(U_2(x_T)-U_2(x_T\Big)dy_T dx_T$$

From the above expression we note that this security metric provides a measure on the difference of the state trajectories whose noisy counterpart is accessible to the adversary. A lower value of this metric indicates a more secure policy for both systems. In this metric the integral of the differences of state trajectories for different terminal states of both systems are weighted equally. We can also assign other weights without changing

the problem structure significantly and the solution methodology outlined below will also be applicable to that case. Consider the following optimization problem:

Problem 3.1:

$$\min_{U_1(.),U_2(.)} \quad \int_{x_T} U_1(x_T)' Q_1 U_1(x_T) + U_2(x_T)' Q_2 U_2(x_T)\, dx_T$$

subject to the constraints:

$$\int_{x_T}\int_{y_T} p(x_T)p(y_T)\Big(U_1(x_T)-U_1(x_T)\Big)' \bar{G}_1' \bar{G}_1 \Big(U_1(x_T)-U_1(x_T)\Big) dy_T dx_T$$
$$+ \int_{x_T}\int_{y_T} p(x_T)p(y_T)\Big(U_2(x_T)-U_2(x_T)\Big)' \bar{G}_2' \bar{G}_2 \Big(U_2(x_T)-U_2(x_T)\Big) dy_T dx_T \leq \gamma_1$$

$$F_1 U_1(x_T) = x_T, \;\; F_2 U_2(x_T) = x_T$$

where Q_1 and Q_1 are symmetric positive definite matrices of appropriate dimensions. It should be noted that the security parameter γ_1 is taken to be nonnegative. The security constraint provides a level of security offered by the respective controllers. The functions $U_1(.)$ and U_2 are $\mathbb{L}^2$ integrable and belong to the space $\mathbb{L}^2(\Re^n, \mathscr{B}(\Re^n), \mu_p)$. Note that $\mathscr{B}(\Re^n)$ is the Borel σ-algebra on $\Re^n$ and μ_p is the probability measure corresponding to the distribution of the terminal state.

It should be noted that in Problem 3.1 both the cost and security constraints of both systems are coupled. Therefore, the optimal solution of a decision maker will depend on the optimal policy employed by the other decision maker. Also the same information, which is the terminal state, is available to both decision makers and hence the problem has a partially nested information structure.

Now using the same technique that was utilized in Chapter 2 we can remove the equality constraints in (3.7) and also write the aforementioned problem in a more compact form. Let $U(.)$, F, and $\bar{G}$ be defined such that:

$$U(.) = \begin{bmatrix} U_1(.) \\ \\ U_2(.) \end{bmatrix}, \; F = \begin{bmatrix} F_1 & 0 \\ \\ 0 & F_2 \end{bmatrix}, \; \bar{G} = \begin{bmatrix} \bar{G}_1 & 0 \\ \\ 0 & \bar{G}_2 \end{bmatrix}, \; Q = \begin{bmatrix} Q_1 & 0 \\ \\ 0 & Q_2 \end{bmatrix} \tag{3.10}$$

Using equation (3.10) we can write the equality constraints as follows:

$$FU(x_T) = \begin{bmatrix} x_T \\ \\ x_T \end{bmatrix}, \; x_T \in \Re^n \tag{3.11}$$

Let $\tilde{F}$ be a basis for the Null space of F and $\tilde{U}(x_T)$ be a given control function such that:

$$F\tilde{U}(x_T) = \begin{bmatrix} x_T \\ \\ x_T \end{bmatrix}, \; F\tilde{F}\eta(x_T) = 0, \; x_T \in \Re^n$$

where $\eta(.)$ is a $q \times 1$ dimensional function which will serve as our new optimization parameter. Note that q is the dimension of the Null space of F. Also $\tilde{U}(.)$ is selected to be linear in the terminal state. This is possible due to the controllability assumption of the dynamical systems. Using this notation the control input function can be expressed as follows:

$$U(x_T) = \tilde{U}(x_T) + \tilde{F}\eta(x_T)$$

Similarly we can write:

$$\sum_{i=1}^{2}\Big(U_i(x_T)-U_i(y_T)\Big)'\bar{G}_i'\bar{G}_i\Big(U_i(x_T)-U_i(y_T)\Big)=$$
$$\Big(\tilde{U}(x_T)-\tilde{U}(y_T)+\tilde{F}\eta(x_T)-\tilde{F}\eta(y_T)\Big)'\bar{G}'\bar{G}\Big(\tilde{U}(x_T)-\tilde{U}(y_T)+\tilde{F}\eta(x_T)-\tilde{F}\eta(y_T)\Big)$$

Using the aforementioned notation we can re-write Problem 3.1 as follows:

$$\min_{\eta(.)}\ \int_{\Re^n}\Big(\tilde{U}(x_T)+\tilde{F}\eta(x_T)\Big)'Q\Big(\tilde{U}(x_T)+\tilde{F}\eta(x_T)\Big)dx_t$$

subject to the constraint:

$$\int_{x_T}\int_{y_T}\Big(\tilde{U}(x_T)-\tilde{U}(y_T)+\tilde{F}\big(\eta(x_T)-\eta(y_T)\big)\Big)\bar{G}'\bar{G}\Big(\tilde{U}(x_T)-\tilde{U}(y_T)+$$
$$\tilde{F}\big(\eta(x_T)-\eta(y_T)\big)\Big)p(x_T)p(y_T)dx_Tdy_T\ \leq\ \gamma_1$$

We will solve Problem 3.1 by utilizing the Generalized Kuhn Tucker Theorem. In order to do that we make the following assumptions.

Assumption 3.1: It is assumed that we consider only those values of γ_1 for which the appropriate Lagrange multiplier to the problem, λ^*, is such that the matrix $\Big[I_{q\times q}-2\lambda^*\tilde{F}'\bar{G}'\bar{G}\tilde{F}\Big(\tilde{F}'\big(\tilde{Q}+2\lambda^*\bar{G}'\bar{G}\big)\tilde{F}\Big)^{-1}\Big]$ is nonsingular.

Assumption 3.2: We assume that the constraint parameter, γ_1, and the system dynamics are selected such that the optimal solution $\eta^*(.)$ to Problem 3.1 satisfies the aforemen-

tioned security constraint and that there exists a $h(.) \in \mathbb{L}^2(\Re^n, \mathscr{B}(\Re^n), \mu_p)$ such that:

$$\int_{\Re^n}\int_{\Re^n} p(x_T)p(y_T)\left(\tilde{U}(x_T)-\tilde{U}(y_T)+\tilde{F}\left(\eta^*(x_T)-\eta^*(y_T)\right)\right)'\bar{G}'\bar{G}\left(\tilde{U}(x_T)-\tilde{U}(y_T)+\tilde{F}\left(\eta^*(x_T)-\eta^*(y_T)\right)\right)dy_T dx_T \; + \; 4\int_{\Re^n}\left(\tilde{U}(x_T)+\tilde{F}\eta^*(x_T)\right)'\bar{G}'\bar{G}\tilde{F}h(x_T)p(x_T)dx_T - \; 4\int_{\Re^n}\int_{\Re^n}\left(\tilde{U}(x_T)+\tilde{F}\eta^*(x_T)\right)'\bar{G}'\bar{G}\tilde{F}h(y_T)p(y_T)p(x_T)dy_T dx_T \; < \; \gamma_1$$

It should be noted that Assumption 3.2 is the standard regularity assumption required to apply the Generalized Kuhn Tucker Theorem. Note that this assumption excludes the possibility of incorporating an equality constraint. Using the concept of Gateaux differentials, Assumption 3.1, Assumption 3.2, and the generalized Kuhn Tucker Theorem we obtain the following result.

Proposition 3.1: The optimal solution of Problem 3.1 under Assumption 3.1 and Assumption 3.2 is affine in the terminal state, x_T, and is given as follows:

$$\eta^*(x_T) = -\left(\tilde{F}'Q\tilde{F}+2\lambda^*\tilde{F}'\bar{G}'\bar{G}\tilde{F}\right)^{-1}\left(\tilde{F}'Q+2\lambda^*\tilde{F}'\bar{G}'\bar{G}\right)\tilde{U}(x_T)+2\lambda^*\left(\tilde{F}'Q\tilde{F}+2\lambda^*\tilde{F}'\bar{G}'\bar{G}\tilde{F}\right)^{-1}\left(\tilde{F}'\bar{G}'\bar{G}-\left(I-2\lambda^*\Gamma_{\lambda^*}\right)^{-1}\Gamma_{\lambda^*}\tilde{F}'Q\right)\int p(y_T)\tilde{U}(y_T)dy_T$$

where $\Gamma_{\lambda^*} = \tilde{F}'\bar{G}'\bar{G}\tilde{F}\left(\tilde{F}'\left(Q+2\lambda^*\bar{G}'\bar{G}\right)\tilde{F}\right)^{-1}$ and $\lambda^* \geq 0$ is the solution to the following equation:

$$\lambda^*\Bigg[-2\int_{x_T}\int_{y_T} p(x_T)p(y_T)\left(\tilde{U}(x_T)+\tilde{F}\eta^*(x_T)\right)'\bar{G}'\bar{G}\left(\tilde{U}(y_T)+\tilde{F}\eta^*(y_T)\right)dy_T dx_T + \; 2\int_{x_T} p(x_T)\left(\tilde{U}(x_T)+\tilde{F}\eta^*(x_T)\right)'\bar{G}'\bar{G}\left(\tilde{U}(x_T)+\tilde{F}\eta^*(x_T)\right)-\gamma_1\Bigg] = 0$$

Proof. The proof of Proposition 3.1 follows along the same lines as the proof of Proposition 2.4.1 to which the reader is reffered. □

Since the cost function is strictly convex so it should be noted that the optimal solution is unique. Assumption 3.1 and Assumption 3.2 can be checked by first solving the problem and then using the optimal solution to check if the assumptions are satisfied. It should be noted that Assumption 3.1 allows us to operate only over particular regimes of the parameter, γ_1. However, it is not very restrictive and we can still work with a wide range of parameter values as the assumption fails for only a finite number of values.

3.3 Team Decision Theory: Correlated Terminal State

The problem formulation presented in Section 3.1 is for the case when the terminal state is identical for both decision makers. A more general problem formulation is when the terminal states are not identical but correlated in the sense that they both have the same mean but different variance. Consider the same system dynamics for both decision makers which was provided in Section 3.1. We assume that both systems are completely controllable. Consider the following terminal states corresponding to system (I) and system (II):

$$x_T^1 = w_1 + w_3, \qquad x_T^2 = w_2 + w_3 \tag{3.12}$$

where w_1, w_2, and w_3 are independent Gaussian random vectors. Furthermore, it is assumed that the mean vector of both w_1 and w_2 is zero and w_3 is not zero. Therefore, the terminal states have the same mean but different variance. The information variable which contains information regarding both terminal states is available to both decision

makers and is given by:

$$z = \begin{bmatrix} x_T^1 \\ \\ x_T^2 \end{bmatrix} \tag{3.13}$$

This assumption ensures that this team decision problem has a partially nested information structure. It should be noted that the information variable z has a Gaussian distribution with density function $q(.)$. Using a similar notation to the problem formulation in Section 3.2, let $U_1(z)$ be the control sequence that drives system (I) to the terminal state x_T^1 and let $U_2(z)$ be the control sequence that drives system (II) to the terminal state x_T^2.

$$U_1(.) = \begin{bmatrix} u_0^1 \\ \vdots \\ u_{T-1}^1 \end{bmatrix}, \quad U_2(.) = \begin{bmatrix} u_0^2 \\ \vdots \\ u_{T-1}^2 \end{bmatrix}$$

We require the following equality constraints:

$$F_1 U_1(z) = x_T^1, \qquad F_2 U_2(z) = x_T^2 \tag{3.14}$$

where F_1 and F_2 are given as follows:

$$F_i = \begin{bmatrix} A_i^{T-1} B_i & A_i^{T-2} B_i & \cdots & B_i \end{bmatrix}, \; i = 1,2$$

We assume that the adversary makes partial noisy measurements of both systems and wants to estimate their respective terminal states. Under Hypothesis H_z the following

measurement model is available to the adversary:

$$H_z : \mathbf{Y^1_{0,k}} = \bar{G}_1 U_1(z) + \mathbf{V^1_{0,k}},\ \mathbf{Y^2_{0,k}} = \bar{G}_2 U_2(z) + \mathbf{V^2_{0,k}} \tag{3.15}$$

where $\bar{G}_1$ and $\bar{G}_2$ are given by:

$$\bar{G}_i = \bar{C}_i G_i,\ G_i U_i(.) = \begin{bmatrix} u_0^i \\ \vdots \\ u_{k-1}^i \end{bmatrix},\ \bar{C}_i = \begin{bmatrix} 0_{p\times m} & 0_{p\times m} & \cdots & 0_{p\times m} \\ C_i B_i & 0_{p\times m} & \cdots & 0_{p\times m} \\ \vdots & \vdots & \ddots & \vdots \\ C_i A_i^{k-1} B_i & C_i A_i^{k-2} B_i & \cdots & C_i B_i \end{bmatrix},\ i = 1,2$$

As mentioned in Section 3.1, the noise vectors $\mathbf{V^1_{0,k}}$ and $\mathbf{V^2_{0,k}}$ are assumed to have a general distribution with a finite mean. Now we introduce a more general security metric which will be utilized in the sequel to introduce the security constraints:

$$\begin{aligned} &\int_{z_1}\int_{z_2} q(z_1)q(z_2)\Big(E(\mathbf{Y^1_{0,k}}|z_1) - E(\mathbf{Y^1_{0,k}}|z_2)\Big)'\Big(E(\mathbf{Y^1_{0,k}}|z_1) - E(\mathbf{Y^1_{0,k}}|z_2)\Big)dz_1 dz_2 + \\ &\int_{z_1}\int_{z_2} q(z_1)q(z_2)\Big(E(\mathbf{Y^2_{0,k}}|z_1) - E(\mathbf{Y^2_{0,k}}|z_2)\Big)'\Big(E(\mathbf{Y^2_{0,k}}|z_1) - E(\mathbf{Y^2_{0,k}}|z_2)\Big)dz_1 dz_2 + \\ &\int_z q(z)\Big(E(\mathbf{Y^1_{0,k}}|z) - E(\mathbf{Y^2_{0,k}}|z)\Big)'\Big(E(\mathbf{Y^1_{0,k}}|z) - E(\mathbf{Y^2_{0,k}}|z)\Big)dz \end{aligned} \tag{3.16}$$

where z_1 and z_2 are realizations of the information variable which is available to the decision makers. It should be noted that this security metric measures the difference of the conditional means of each system with respect to different hypotheses and also provides a measure on the difference of conditional means of both systems with respect to one another. The last term of this security metric enables us to secure the system

from an adversary which would like to take advantage due to the correlated nature of the terminal states of both systems. Now using the measurement model this security metric can be simplified to get:

$$\int_{z_1}\int_{z_2} q(z_1)q(z_2)\Big(U_1(z_1)-U_1(z_2)\Big)'\bar{G}_1'\bar{G}_1\Big(U_1(z_1)-U_1(z_2)\Big)dz_1dz_2 + \int_{z_1}\int_{z_2} q(z_1)q(z_2)\Big(U_2(z_1)-U_2(z_2)\Big)'\bar{G}_2'\bar{G}_2\Big(U_2(z_1)-U_2(z_2)\Big)dz_1dz_2 + \int_{z} q(z)\Big(\bar{G}_1U_1(z)-\bar{G}_2U_2(z)\Big)'\Big(\bar{G}_1U_1(z)-\bar{G}_2U_2(z)\Big)dz \tag{3.17}$$

We are familiar with the first two terms of the security metric as they were introduced in the previous section. The last term measures the difference, for a given information variable, between the first $(k+1)$ values of the state trajectories of system (I) and system (II) respectively. A small value of this last term ensures that the adversary cannot exploit information regarding the terminal states, due to their correlation, by separately observing the trajectories of both systems. Utilizing this security metric we can state the following team decision problem:

Problem 3.2:

$$\min_{U_1(.),U_2(.)} \int_{\Re^{2n}} q(z)\Big(U_1(z)'Q_1U_1(z)+U_2(z)'Q_2U_2(z)\Big)dz$$

subject to the constraints:

$$F_1U_1(z)=x_T^1, \quad F_2U_2(z)=x_T^2$$

$$\int_{z_1}\int_{z_2} q(z_1)q(z_2)\Big(U_1(z_1)-U_1(z_2)\Big)'\bar{G}_1'\bar{G}_1\Big(U_1(z_1)-U_1(z_2)\Big)dz_1dz_2+\int_{z_1}\int_{z_2} q(z_1)q(z_2)$$
$$\times\Big(U_2(z_1)-U_2(z_2)\Big)'\bar{G}_2'\bar{G}_2\Big(U_2(z_1)-U_2(z_2)\Big)dz_1dz_2+\int_z q(z)\Big(\bar{G}_1U_1(z)-\bar{G}_2(z)\Big)'\times$$
$$\Big(\bar{G}_1U_1(z)-\bar{G}_2U_2(z)\Big)\ \leq\ \gamma_2$$

where $\gamma \geq 0$ is the constraint parameter. The functions $U_1(.)$ and U_2 are $\mathbb{L}^2$ integrable and belong to the space $\mathbb{L}^2(\Re^{2n}, \mathscr{B}(\Re^{2n}), \mu_q)$. Note that $\mathscr{B}(\Re^{2n})$ is the Borel σ-algebra on $\Re^{2n}$ and μ_q is the probability measure corresponding to the distribution of the information variable, z.

It should be noted that Problem 3.3 is an infinite dimensional convex optimization problem. Also note that each decision maker has access to the information variable, z. Therefore, this problem has a partially nested information structure. Our framework and constraints are unique and offer an important extension to the field of team decision theory. Now we can write the input dynamics in compact form as follows:

$$U(z)=\begin{bmatrix}U_1(z)\\ \\ U_2(z)\end{bmatrix},\ F=\begin{bmatrix}F_1 & 0\\ \\ 0 & F_2\end{bmatrix}$$

Using this notation the equality constraints can be re-written as: $FU(z)=z,\ z\in\Re^{2n}$

Similarly, let $\bar{G},\ H$, and Q be defined as follows:

$$Q=\begin{bmatrix}Q_1 & 0\\ \\ 0 & Q_2\end{bmatrix},\ \bar{G}=\begin{bmatrix}\bar{G}_1 & 0\\ \\ 0 & \bar{G}_2\end{bmatrix},\ H=\begin{bmatrix}\bar{G}_1'\\ \\ -\bar{G}_2'\end{bmatrix}\begin{bmatrix}\bar{G}_1 & -\bar{G}_2\end{bmatrix}$$

Using this notation we can simplify the security metric as follows:

$$\int_{z_1}\int_{z_2} q(z_1)q(z_2)\Big(U_1(z_1)-U_1(z_2)\Big)'\bar{G}_1'\bar{G}_1\Big(U_1(z_1)-U_1(z_2)\Big)dz_1dz_2+\int_{z_1}\int_{z_2} q(z_1)q(z_2)$$
$$\Big(U_2(z_1)-U_2(z_2)\Big)'\bar{G}_2'\bar{G}_2\Big(U_2(z_1)-U_2(z_2)\Big)dz_1dz_2+\int_z q(z)\Big(\bar{G}_1U_1(z)-\bar{G}_2U_2(z)\Big)'$$
$$\Big(\bar{G}_1U_1(z)-\bar{G}_2U_2(z)\Big)dz=\int_{z_1}\int_{z_2} q(z_1)q(z_2)\Big(U(z_1-U(z_2)\Big)'\bar{G}'\bar{G}\Big(U(z_1-U(z_2)\Big)dz_1dz_2$$
$$+\int_z q(z)U(z)'HU(z)dz$$

Similarly the cost function can be simplified to get:

$$\int_z q(z)\Big(U_1(z)'Q_1U_1(z)+U_2(z)'Q_2U_2(z)\Big)dz=\int_z q(z)U(z)'QU(z)dz$$

Now we will use the same technique that has been utilized previously to remove the equality constraints. Let $\tilde{U}(z)$ be a given control function such that:

$$F\tilde{U}(z)=z,\ \ z\in\Re^{2n}$$

Let $\tilde{F}$ be a basis for the Null space of F such that:

$$F\tilde{F}\eta(z)=0,\ \ \eta(z)\in\Re^q,\ \ q=dim(Null(F))$$

Using this we can re-write the control function $U(z)$ as follows:

$$U(z)=\tilde{U}(z)+\tilde{F}\eta(z)$$

Using the aforementioned notation we can simplify Problem 3.2 as follows:

$$\min_{\eta(.)} \int_z q(z)\Big(\tilde{U}(z)+\tilde{F}\eta(z)\Big)' Q\Big(\tilde{U}(z)+\tilde{F}\eta(z)\Big)dz$$

subject to the constraints:

$$\int_{z_1}\int_{z_2} q(z_1)q(z_2)\Big(\tilde{U}(z_1)-\tilde{U}(z_2)+\tilde{F}\eta(z_1)-\tilde{F}\eta(z_2)\Big)'\bar{G}'\bar{G}\Big(\tilde{U}(z_1)-\tilde{U}(z_2)+$$
$$\tilde{F}\eta(z_1)-\tilde{F}\eta(z_2)\Big)dz_1dz_2+\int_z q(z)\Big(\tilde{U}(z)+\tilde{F}\eta(z)\Big)'H\Big(\tilde{U}(z)+\tilde{F}\eta(z)\Big)dz \;\le\; \gamma_2$$

We will solve Problem 3.2 by utilizing the generalized Kuhn Tucker Theorem. In order to do that we need to make the following assumptions:

Assumption 3.3: We consider only those values of γ_2 for which the appropriate Lagrange multiplier, λ^*, to the problem is small enough such that the matrix $\Big[I_{q\times q}-2\lambda^*\tilde{F}'\bar{G}'\bar{G}\tilde{F}\times$
$\times\Big(\tilde{F}'\big(\tilde{Q}+2\lambda^*\bar{G}'\bar{G}+\lambda^*H\big)\tilde{F}\Big)^{-1}\Big]$ is nonsingular.

Assumption 3.4: We assume that the constraint parameter, γ_2, and the system dynamics are selected such that the optimal solution $\eta^*(.)$ to Problem 3.2 satisfies the aforementioned security constraint and that there exists a $h(.)\in\mathbb{L}^2(\Re^{2n},\mathscr{B}(\Re^{2n}),\mu_q)$ such that:

$$\int_{z_1}\int_{z_2}\Big(\tilde{U}(z_1)-\tilde{U}(z_2)+\tilde{F}\eta^*(z_1)-\tilde{F}\eta^*(z_2)\Big)'\bar{G}'\bar{G}\Big(\tilde{U}(z_1)-\tilde{U}(z_2)+\tilde{F}\eta^*(z_1)$$
$$-\tilde{F}\eta^*(z_2)\Big)q(z_1)q(z_2)dz_1dz_2+\int_z\Big(\tilde{U}(z)+\tilde{F}\eta^*(z)\Big)'H\Big(\tilde{U}(z)+\tilde{F}\eta^*(z)\Big)dz$$
$$+\;4\int_z\Big(\tilde{U}(z)+\tilde{F}\eta^*(z)\Big)'\bar{G}'\bar{G}\tilde{F}h(z)dz+2\int_z\Big(\tilde{U}(z)+\tilde{F}\eta^*(z)\Big)'H\tilde{F}h(z)dz$$
$$-\;4\int_{z_1}\int_{z_2}\eta^*(z_1)'\tilde{F}'\bar{G}'\bar{G}\tilde{F}h(z_2)q(z_1)q(z_2)dz_1dz_2\;<\;\gamma_2$$

It should be noted that Assumption 3.4 is a standard regularity condition that is required in order to apply the generalized Kuhn Tucker Theorem. Using Assumption 3.3 and Assumption 3.4 we can state the following result:

Proposition 3.2: The optimal solution to Problem 3.2 under Assumption 3.3 and Assumption 3.4 is affine in the information variable, z, and is given as follows:

$$\eta^*(z) = -\left(\tilde{F}'\left(Q+2\lambda^*\bar{G}'\bar{G}+\lambda^*H\right)\tilde{F}\right)^{-1}\tilde{F}'\left(Q+2\lambda^*\bar{G}'\bar{G}+\lambda^*H\right)\tilde{U}(z)+2\lambda^*\left(\tilde{F}'\left(Q\right.\right.$$
$$\left.\left.+2\lambda^*\bar{G}'\bar{G}+\lambda^*H\right)\tilde{F}\right)^{-1}\left(\tilde{F}'\bar{G}'\bar{G}-\left(I-2\lambda^*\Gamma(\lambda^*)\right)^{-1}\Gamma(\lambda^*)\tilde{F}'\left(Q+\lambda^*H\right)\right)\int_z q(z)\tilde{U}(z)dz$$

where $\Gamma(\lambda^*) = \tilde{F}'\bar{G}'\bar{G}\tilde{F}\left(\tilde{F}'\left(Q+2\lambda^*\bar{G}'\bar{G}+\lambda^*H\right)\tilde{F}\right)^{-1}$ and the appropriate Lagrange multiplier, $\lambda^* \geq 0$, is the solution to the following equation:

$$\lambda^*\left[\int_{z_1}\int_{z_2}\left(\tilde{U}(z_1)-\tilde{U}(z_2)+\tilde{F}\eta^*(z_1)-\tilde{F}\eta^*(z_2)\right)'\bar{G}'\bar{G}\left(\tilde{U}(z_1)-\tilde{U}(z_2)+\tilde{F}\eta^*(z_1)-\right.\right.$$
$$\left.\left.\tilde{F}\eta^*(z_2)\right)q(z_1)q(z_2)dz_1dz_2+\int_z q(z)\left(\tilde{U}(z)+\tilde{F}\eta^*(z)\right)'H\left(\tilde{U}(z)+\tilde{F}\eta^*(z)\right)dz-\gamma_2\right]=0$$

Proof. Now using the cost function, the security constraint, and a Lagrange multiplier, λ, we can write the augmented Lagrangian as follows:

$$J(\eta(.)) = \int_z\left(\tilde{U}(z)+\tilde{F}\eta(z)\right)'\left(Q+2\lambda\bar{G}'\bar{G}+\lambda H\right)\left(\tilde{U}(z)+\tilde{F}\eta(z)\right)q(z)dz$$
$$-2\lambda\int_{z_1}\int_{z_2}q(z_1)q(z_2)\left(\tilde{U}(z_1)+\tilde{F}\eta(z_1)\right)'\bar{G}'\bar{G}\left(\tilde{U}(z_2)+\tilde{F}\eta(z_2)\right)dz_1dz_2 \quad (3.18)$$

Now for any admissible variation, $h(.) \in \mathbb{L}^2(\Re^{2n}, \mathscr{B}(\Re^{2n}), \mu_q)$, we can compute the Gateaux

differential as follows:

$$\delta J(\eta(.),h(.)) = 2\int_z \tilde{U}(z)'\Big(Q+2\lambda\bar{G}'\bar{G}+\lambda H\Big)\tilde{F}h(z)dz+2\int_z h(z)'\tilde{F}'\Big(Q+2\lambda\bar{G}'\bar{G}+\lambda H\Big)$$
$$\times\tilde{F}\eta(z)dz-4\lambda\int_{z_1}\int_{z_2}\tilde{U}(z_1)'\bar{G}'\bar{G}\tilde{F}h(z_2)q(z_1)q(z_2)dz_1dz_2-4\lambda\int_{z_1}\int_{z_2}\eta(z_1)'\tilde{F}'\bar{G}'\bar{G}$$
$$\times h(z_2)q(z_1)q(z_2)dz_1dz_2 \tag{3.19}$$

Now setting the Gateaux differential equal to zero for arbitrary admissible $h(.)$ we get that:

$$\tilde{F}'\Big(Q+2\lambda\bar{G}'\bar{G}+\lambda H\Big)\Big(\tilde{U}(z)+\tilde{F}\eta(z)\Big)-2\lambda\int_z\tilde{F}'\bar{G}'\bar{G}\Big(\tilde{U}(z)+\tilde{F}\eta(z)\Big)q(z)dz=0 \tag{3.20}$$

Using Assumption 3.3 we multiply throughout by $q(z)\Gamma(\lambda) = q(z)\tilde{F}'\bar{G}'\bar{G}\tilde{F}\Big(\tilde{F}'\big(Q+2\lambda\bar{G}'\bar{G}+\lambda H\big)\tilde{F}\Big)^{-1}$ followed by integrating the resulting expression over z to get:

$$\int_z\tilde{F}'\bar{G}'\bar{G}\tilde{F}q(z)\eta(z)dz=-\Big(I-2\lambda\Gamma(\lambda)\Big)^{-1}\int_z q(z)\Gamma(\lambda)\tilde{F}'\big(Q+\lambda H\big)\tilde{U}(z)dz \tag{3.21}$$

It should be noted $\big(I-2\lambda\Gamma(\lambda)\big)$ is invertible due to Assumption 3.3. Now plugging (3.21) into (3.20) we get that:

$$\tilde{F}'\big(Q+2\lambda\bar{G}'\bar{G}+\lambda H\big)\tilde{F}\eta(z)=-\tilde{F}'\big(Q+2\lambda\bar{G}'\bar{G}+\lambda H\big)\tilde{U}(z)+2\lambda\int_z\tilde{F}'\bar{G}'\bar{G}\tilde{U}(z)q(z)dz$$

Using this expression and the generalized Kuhn Tucker Theorem the optimal solution is

given by:

$$\eta^*(z) = -\left(\tilde{F}'\left(Q+2\lambda^*\bar{G}'\bar{G}+\lambda^*H\right)\tilde{F}\right)^{-1}\tilde{F}'\left(Q+2\lambda^*\bar{G}'\bar{G}+\lambda^*H\right)\tilde{U}(z)+2\lambda^*\left(\tilde{F}'\left(Q\right.\right.$$
$$\left.\left.+2\lambda^*\bar{G}'\bar{G}+\lambda^*H\right)\tilde{F}\right)^{-1}\left(\tilde{F}'\bar{G}'\bar{G}-\left(I-2\lambda^*\Gamma(\lambda^*)\right)^{-1}\Gamma(\lambda^*)\tilde{F}'\left(Q+\lambda^*H\right)\right)\int_z q(z)\tilde{U}(z)dz \tag{3.22}$$

Since $\tilde{U}(z)$ is selected to be linear in z so the optimal solution is affine in z. Also from the generalized Kuhn Tucker Theorem the appropriate Lagrange multiplier λ^* is given by the following equation:

$$\lambda^*\left[\int_{z_1}\int_{z_2}\left(\tilde{U}(z_1)-\tilde{U}(z_2)+\tilde{F}\eta^*(z_1)-\tilde{F}\eta^*(z_2)\right)'\bar{G}'\bar{G}\left(\tilde{U}(z_1)-\tilde{U}(z_2)+\tilde{F}\eta^*(z_1)-\right.\right.$$
$$\left.\left.\tilde{F}\eta^*(z_2)\right)q(z_1)q(z_2)dz_1dz_2+\int_z q(z)\left(\tilde{U}(z)+\tilde{F}\eta^*(z)\right)'H\left(\tilde{U}(z)+\tilde{F}\eta^*(z)\right)dz-\gamma_2\right]=0 \tag{3.23}$$

This completes the proof. □

It should be noted that the Lagrange multiplier is a function of $\tilde{U}(.)$, the probability density $q(.)$, and the system dynamics but does not depend on the information variable z. The controller of each system uses the terminal state information of the other system to derive its inputs. This is due to the structure of our security metric which aims to minimize the benefit that an adversary can gain by utilizing the correlative nature of the terminal states. Therefore, we can claim that not only are the individual control systems secure from an adversary but the overall team decision system is secure from an adversary which aims to make measurements regarding system operation to potentially undermine

system operation.

Since the cost function is strictly convex so it should be noted that the optimal solution is unique. Assumption 3.3 and Assumption 3.4 can be checked by first solving the problem and then using the optimal solution to check if the assumptions are satisfied. It should be noted that these assumptions are not really restrictive and are valid for a large set of problems. Our results are along the same lines as that of Radner [20] which state that the optimal solution of the team decision problem under some assumptions is affine in the information variables. The important difference is that we have incorporated security constraints in this problem formulation and have utilized the Kuhn Tucker Theorem to prove our results.

Chapter 4: Stochastic Receding Horizon Control using Randomized Algorithms

Receding horizon control (RHC) or Model predictive control (MPC) is a pervasive control technique, typically employed to solve constrained problems where off-line computation is impractical and the problem needs to be solved on-line. In the deterministic setting, a suitable finite horizon control sequence is generated at each time step by using current and past measurements. The first element of this control sequence is applied to the plant and the procedure is repeated at the following time step. Most formulations of robust RHC minimize a cost evaluated at the maximizing disturbance. It is well known that such min-max formulations may lead to conservative designs. Using appropriate noise assumptions, recent results focus on either extending the deterministic framework or optimization in the feedback policy space.

In stochastic receding horizon control (SRHC) the disturbances are modeled as stochastic processes, whose statistical descriptions are known, and the expectation of the cost function is minimized. Such an alternative framework leads to results that may be less conservative than min-max formulations. In order to account for the presence of disturbances the optimization is performed with respect to control policies rather than control sequences. This is an active area of research and some exciting related work has appeared

in ([27], [28], [29], and [30]). A SRHC problem with multiplicative noise is given in [27], where hard state and control constraints are converted to soft probabilistic ones and the resulting optimization problem is formulated as a semi-definite program. In [28], a SRHC problem formulation is provided by employing a stochastic programming approach and efficient solution techniques are presented. In [29], the case of unbounded noise is considered along with hard bounds on the control inputs. A sub-optimal feedback scheme utilizing the available noise measurements is used to convert the optimization problem into a convex program. Constraints and noise assumptions similar to [29] are used in [30], along with selecting the controller on some suitable function spaces. The resulting optimization problems in [30], are shown to be convex.

An interesting research area where SRHC can have important applications is small scale devices like miniature robotics, small sensors, and other small platforms which require on-line computation. Such devices have low power and limited payload capabilities and cannot accommodate the infrastructure required to perform complex on-line computation. The main contribution of this chapter is to provide a finite horizon optimal control problem, inspired by SRHC, and to present bounds on disturbance and control sample sizes using results from randomized algorithms. Such randomization based techniques require limited computations and can be implemented on many small devices. It should be noted that randomized algorithms (see [31]) have previously been implemented in robust control (see [32], [33]) and utilized in [34] and [35] in the context of RHC. In [34], a random convex programming technique is used to solve a min-max formulation of the robust RHC problem while [35] uses a dynamic programming (DP) technique to minimize the empirical mean of the cost function in a SRHC setting. Such DP based schemes

are computationally complex, suffer from the curse of dimensionality, and are generally inapplicable towards small devices.

We consider a finite horizon optimal control problem with hard bounds on the control inputs and bounded noise. The bounded noise assumption enables us to incorporate statistical learning techniques. In addition to considering the case when the system is affected by additive disturbances we also present an analysis for the case when the system is affected by both additive disturbances and model uncertainty. The computational complexity is reduced by seeking sub-optimal solutions. This is done by using a specialized disturbance feedback scheme when only additive disturbances are present and a specialized state feedback scheme when both additive disturbances and model uncertainty are present. These sub-optimal feedback schemes allow us to significantly reduce the computational complexity of these problems.

The following notation is adopted:

- Let $\Re$ denote the set of real numbers and let $\mathbb{Z}^+$ denote the set of nonnegative integers.

- The probability measure associated with a random variable X is denoted by P_X. If $X^1,...,X^k$ are independent and identically distributed (iid) samples of X then the product probability measure $P_{X_1} \times .... \times P_{X_k}$ is denoted by P_X^k. If Ω is the sample space of X then the product sample space for the iid samples is denoted by Ω^k.

- $I_{m\times m}$ represents the $m \times m$ identity matrix and $0_{m\times n}$ represents the $m \times n$ matrix of zeros. For a $n \times 1$ vector x, x_i denotes the ith element where $i = 1,...,n$.

- $E_{x_i}[.]$ denotes the conditional expectation of $[.]$ given x_i.

- Logarithm to the base 2 and natural logarithm are denoted by log and ln respectively.

- $\lceil . \rceil$ denotes the ceiling function and $\|.\|_p$ denotes the standard ℓ_p norm.

This chapter is organized in five main sections. In Section 1, we provide the problem formulation for the case where noise enters the system in the form of additive disturbances. Randomized algorithms for minimizing the empirical mean of the cost function using Pollard dimension theory are provided in Section 2. In Section 3, both the additive disturbances and the control parameters are randomly generated, according to specific probability measures. Bounds on control and disturbance sample sizes, which guarantee certain performance specifications, are provided. The case incorporating model uncertainty along with additive disturbances is considered in Section 4. Finally, simulations and a performance based analysis is presented in Section 5.

4.1 Problem Formulation

Consider the following linear time-invariant system in discrete time:

$$x_{i+1} = Ax_i + Bu_i + Dw_i \ , \qquad i \in \mathbb{Z}^+ \tag{4.1}$$

where $x_i \in \Re^n$ is the state, $u_i \in \Re^m$ is the control input, and $w_i \in \Re^n$ is the additive disturbance. A is an $n \times n$ matrix, B is an $n \times m$ matrix, and we assume that D is an $n \times n$

non-singular matrix. The disturbances form an iid process and are bounded as follows:

$$w_i \in \mathscr{W} = \{w \in \Re^n \mid \|w\|_\infty \leq W_{max}\}, \quad i \in \mathbb{Z}^+ \tag{4.2}$$

We assume hard bounds on the control inputs which are given by:

$$u_i \in \mathscr{U} = \{u \in \Re^m \mid \|u\|_\infty \leq U_{max}\}, \quad i \in \mathbb{Z}^+ \tag{4.3}$$

The input bound U_{max} and the disturbance bound W_{max} are assumed to be known. The following cost function is to be minimized at each time step k:

$$E_{x_k}\left[\sum_{i=k}^{k+N-1} x_i' Q_i x_i + u_i' R_i u_i + x_{k+N}' Q_{k+N} x_{k+N}\right] \tag{4.4}$$

subject to the aforementioned dynamics and constraints. We assume knowledge of the initial state x_k. $Q_k, ..., Q_{k+N}$ and $R_k, ..., R_{k+N}$ are $n \times n$ and $m \times m$ matrices which are assumed symmetric and positive definite. Given the initial state x_k, we want to minimize the cost over causal state feedback policies of the following form:

$$\begin{bmatrix} u_k \\ u_{k+1} \\ \vdots \\ u_{k+N-1} \end{bmatrix} = \begin{bmatrix} \pi_k(x_k) \\ \pi_{k+1}(x_k, x_{k+1}) \\ \vdots \\ \pi_{k+N-1}(x_k, x_{k+1}, \ldots, x_{k+N-1}) \end{bmatrix} \tag{4.5}$$

where $\pi_k, ..., \pi_{k+N-1}$ are control policies that satisfy (4.3). It should be noted that

only the initial state x_k is known to us. The states $x_{k+1}, ..., x_{k+N-1}$ are random and dependent upon the additive disturbances $w_k, ..., w_{k+N-2}$ and the stochastic control inputs. Control policies are designed to account for the presence of disturbances in the system. If control sequences were used instead of control policies, as is done in the case of the classical RHC problem, then the effect of disturbances would be unaccounted for and would lead to stability issues and poor performance. The SRHC approach can be described as follows:

1. Given the initial state x_k, determine an optimal control policy sequence $\{\pi_k^*, ..., \pi_{k+N-1}^*\}$ that minimizes the cost function subject to the constraints.

2. Apply the first element of the control vector (resulting from the optimal policy), u_k^*, to the dynamical system.

3. update k to k+1 and repeat step 1.

It should be noted that the system dynamics and the cost are time invariant. Therefore, it suffices to only consider the case $k = 0$. Consider the following problem:

Problem 4.1: Minimize the cost function

$$E_{x_0}\left[\sum_{i=0}^{N-1} x_i' Q_i x_i + u_i' R_i u_i + x_N' Q_N x_N\right] \tag{4.6}$$

over causal state feedback policies, subject to the system dynamics (4.1), (4.2), and control constraints (4.3).

In order to obtain an optimal solution to the aforementioned problem we need to solve the associated dynamic programming equations. Instead, in this work we focus on

the following sub-optimal disturbance feedback scheme, previously employed by ([29], [30], [37], [38], [39], [40], and [41]), which leads to a tractable convex approach:

$$u_i = \sum_{j=0}^{i-1} M_{i,j} w_j + v_i, \;\; i \in \{0, ..., N-1\} \tag{4.7}$$

where $M_{i,j}$ is an $m \times n$ matrix and v_i is an $n \times 1$ vector. Given $x_0, ..., x_N$ the disturbances $w_0, ..., w_{N-1}$ can be calculated from the equation:

$$w_i = D^{-1}\{x_{i+1} - Ax_i - Bu_i\}, \;\; i \in \{0, ..., N-1\} \tag{4.8}$$

The disturbance feedback scheme (4.7) can be shown to be equivalent (see [36]) to the following standard sub-optimal state feedback scheme:

$$u_i = \sum_{j=0}^{i} K_{i,j} x_j + \tilde{v}_i, \;\; i \in \{0, ..., N-1\} \tag{4.9}$$

The feedback gain matrices $\bar{K}$, $\bar{M}$ and the vectors V, $\tilde{V}$ are given by:

$$\bar{M} = \begin{bmatrix} 0_{m\times n} & 0_{m\times n} & 0_{m\times n} & \dots & 0_{m\times n} \\ M_{1,0} & 0_{m\times n} & 0_{m\times n} & \dots & 0_{m\times n} \\ M_{2,0} & M_{2,1} & 0_{m\times n} & \dots & 0_{m\times n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ M_{N-1,0} & \dots & \dots & M_{N-1,N-2} & 0_{m\times n} \end{bmatrix}, V = \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_{N-1} \end{bmatrix}, \tilde{V} = \begin{bmatrix} \tilde{v}_0 \\ \tilde{v}_1 \\ \vdots \\ \tilde{v}_{N-1} \end{bmatrix}$$

$$\bar{K} = \begin{bmatrix} K_{0,0} & 0_{m\times n} & 0_{m\times n} & \dots & 0_{m\times n} \\ K_{1,0} & K_{1,1} & 0_{m\times n} & \dots & 0_{m\times n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ K_{N-1,0} & \dots & \dots & K_{N-1,N-1} & 0_{m\times n} \end{bmatrix}, U = \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_{N-1} \end{bmatrix}, W = \begin{bmatrix} w_0 \\ w_1 \\ \vdots \\ w_{N-1} \end{bmatrix}$$

Now we can write the cost in compact notation as follows:

$$\sum_{i=0}^{N-1} x_i' Q_i x_i + u_i' R_i u_i + x_N' Q_N x_N = X' \bar{Q} X + U' \bar{R} U \tag{4.10}$$

where $\bar{A}$, $\bar{B}$, $\bar{D}$, $\bar{Q}$, $\bar{R}$, and X are given as follows:

$$U = \bar{M} W + V, \;\; X = \bar{A} x_0 + \bar{B} U + \bar{D} W \tag{4.11}$$

$$\bar{Q} = \begin{bmatrix} Q_0 & 0_{n\times n} & \dots & 0_{n\times n} \\ 0_{n\times n} & Q_1 & \dots & 0_{n\times n} \\ \vdots & \vdots & \ddots & \vdots \\ 0_{n\times n} & \dots & \dots & Q_N \end{bmatrix}, \bar{R} = \begin{bmatrix} R_0 & 0_{m\times m} & \dots & 0_{m\times m} \\ 0_{m\times m} & R_1 & \dots & 0_{m\times m} \\ \vdots & \vdots & \ddots & \vdots \\ 0_{m\times m} & \dots & \dots & R_N \end{bmatrix}, \bar{A} = \begin{bmatrix} I_{n\times n} \\ A \\ \vdots \\ A^N \end{bmatrix}, X = \begin{bmatrix} x_0 \\ \vdots \\ x_N \end{bmatrix}$$

$$\bar{B} = \begin{bmatrix} 0_{n\times m} & 0_{n\times m} & 0_{n\times m} & \dots & 0_{n\times m} \\ B & 0_{n\times m} & 0_{n\times m} & \dots & 0_{n\times m} \\ AB & B & 0_{n\times m} & \dots & 0_{n\times m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A^{N-1}B & A^{N-2}B & \dots & \dots & B \end{bmatrix}, \bar{D} = \begin{bmatrix} 0_{n\times n} & 0_{n\times n} & 0_{n\times n} & \dots & 0_{n\times n} \\ D & 0_{n\times n} & 0_{n\times n} & \dots & 0_{n\times n} \\ AD & D & 0_{n\times n} & \dots & 0_{n\times n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A^{N-1}D & A^{N-2}D & \dots & \dots & D \end{bmatrix}$$

The equivalence of (4.7) and (4.9) is in the sense that for any admissible $(\bar{K}, \tilde{V})$ an ad-

missible $(\bar{M}, V)$ can be found that yields the same state and input for all disturbances. Utilizing the disturbance feedback scheme we show that the minimization of the expectation of (4.10), subject to (4.1), (4.2), and (4.3) is convex.

Proposition 4.1: Consider the dynamical system (4.1) affected by the additive disturbances (4.2) and subject to the control constraints (4.3). Then Problem 4.1 under the disturbance feedback scheme (4.7) is a convex program with respect to the decision variables $(\bar{M}, V)$ and can be written as follows:

$$\min_{\bar{M},V} E_{x_0}\Big[x_0'\bar{A}'\bar{Q}\bar{A}x_0 + 2x_0'\bar{A}'\bar{Q}\bar{B}(\bar{M}W+V) + 2x_0'\bar{A}'\bar{Q}\bar{D}W + 2W'\bar{D}'\bar{Q}\bar{B}(\bar{M}W+V) +$$

$$W'\bar{D}'\bar{Q}\bar{D}W + (\bar{M}W+V)'(\bar{B}'\bar{Q}\bar{B}+\bar{R})(\bar{M}W+V)\Big]$$

subject to:

$$\|\bar{M}W+V\|_\infty \leq U_{max},\ W \in \mathscr{W}^N \tag{4.12}$$

Proof. Now X and U are affine functions of the decision variables $(\bar{M}, V)$, the cost $X'\bar{Q}X + U'\bar{R}U$ is quadratic, and $\bar{Q}$ and $\bar{R}$ are positive definite. Therefore $X'\bar{Q}X + U'\bar{R}U$ is convex in the decision variables $(\bar{M}, V)$. Now taking expectation retains convexity (see [16], section 3.2) so we can conclude that the cost function is convex. Also $\bar{M}W + V$ is convex in the decision variables and the infinity norm is component wise nondecreasing hence the constraints form a convex set (see [16] pp. 87-88) in the decision variables. Therefore, we conclude that the optimization problem is a convex program.

Now plugging (4.11) into (4.10) we get:

$$X'\bar{Q}X + U'\bar{R}U = x_0'\bar{A}'\bar{Q}\bar{A}x_0 + 2x_0'\bar{A}'\bar{Q}\bar{B}(\bar{M}W + V) + 2x_0'\bar{A}'\bar{Q}\bar{D}W + 2W'\bar{D}'\bar{Q}\bar{B}(\bar{M}W + V)$$

$$+(\bar{M}W + V)'\bar{B}'\bar{Q}\bar{B}(\bar{M}W + V) + W'\bar{D}'\bar{Q}\bar{D}W + W'\bar{M}'\bar{R}\bar{M}W + 2V'\bar{R}\bar{M}W + V'\bar{R}V$$

By taking the expectation and further simplifying the above expression we get the cost function:

$$E_{x_0}\Big[\, x_0'\bar{A}'\bar{Q}\bar{A}x_0 + 2x_0'\bar{A}'\bar{Q}\bar{B}(\bar{M}W + V) + 2W'\bar{D}'\bar{Q}\bar{B}(\bar{M}W + V) + 2x_0'\bar{A}'\bar{Q}\bar{D}W + W'\bar{D}'\bar{Q}\bar{D}W$$

$$+ (\bar{M}W + V)'(\bar{B}'\bar{Q}\bar{B} + \bar{R})(\bar{M}W + V)\,\Big]$$

This completes the proof. □

Remark 4.1: Using Hölder's inequality [42], the constraints in Proposition 4.1 can be simplified as:

$$\max_{i=1,\ldots,Nm}\{|V_i| + \|\bar{M}_i\|_1 W_{max}\} \leq U_{max}$$

where $\bar{M}_i$ corresponds to the ith row of the matrix $\bar{M}$ and V_i is the ith element of the vector V.

4.2 Randomized Algorithms: Utilizing the Pollard Dimension

It is assumed that either the distribution of the disturbance is unknown or is known with a probability density function whose variance is difficult to compute. Therefore,

instead of minimizing the expectation of the cost function in Problem 4.1, we will reformulate the problem by minimizing the empirical mean of the cost function. It should be noted that we need the iid samples of the disturbances to compute the empirical mean of the cost function. We utilize some results from statistical learning theory to compute the required disturbance sample size. To simplify our notation we define:

$$C(\bar{M},V,W) = x_0'\bar{A}'\bar{Q}\bar{A}x_0 + 2x_0'\bar{A}'\bar{Q}\bar{B}(\bar{M}W+V) + 2x_0'\bar{A}'\bar{Q}\bar{D}W + 2W'\bar{D}'\bar{Q}\bar{B}(\bar{M}W+V)$$
$$+ W'\bar{D}'\bar{Q}\bar{D}W + (\bar{M}W+V)'(\bar{B}'\bar{Q}\bar{B}+\bar{R})(\bar{M}W+V) \quad (4.13)$$

Using Hölder's inequality we get:

$$C(\bar{M},V,W) \leq \|x_0\|_\infty \|\bar{A}'\bar{Q}\bar{A}x_0\|_1 + 2\|\bar{B}'\bar{Q}\bar{A}x_0\|_1 U_{max} + 2\|\bar{D}'\bar{Q}\bar{A}x_0\|_1 W_{max} +$$
$$2\|\bar{B}'\bar{Q}\bar{D}W\|_1 U_{max} + \|(\bar{B}'\bar{Q}\bar{B}+\bar{R})(\bar{M}W+V)\|_1 U_{max} + \|\bar{D}'\bar{Q}\bar{D}W\|_1 W_{max} \leq C_{max} \quad (4.14)$$

where C_{max} is a finite upper bound to the cost function and holds for all $(\bar{M},V,W)$ satisfying:

$$\max_{i=1,\ldots,Nm} \{|V_i| + \|\bar{M}_i\|_1 W_{max}\} \leq U_{max}\ , \quad \|W\|_\infty \leq W_{max}$$

Next, we define the normalized cost function $\underline{C}(\bar{M},V,W)$ as follows:

$$\underline{C}(\bar{M},V,W) = \frac{C(\bar{M},V,W)}{C_{max}} \quad (4.15)$$

So the normalized cost takes values in the bounded interval $[0,1]$. Next, we generate iid samples $(W^1,\ldots,W^\gamma)$ of the disturbance vector W according to the probability measure

P_W and define the empirical mean of the normalized cost as follows:

$$\hat{\underline{C}}(\bar{M},V,W^1,...,W^\gamma) = \frac{1}{\gamma}\sum_{i=1}^{\gamma}\frac{C(\bar{M},V,W^i)}{C_{max}} \tag{4.16}$$

Problem 4.2: Consider the following optimization problem:

$$\min_{\bar{M},V} \ \hat{\underline{C}}(\bar{M},V,W^1,...,W^\gamma)$$

subject to the constraint:

$$\max_{i=1,...,Nm} |V_i| + \|\bar{M}_i\|_1 W_{max} \leq U_{max}$$

Problem 4.2 is a relaxation of Problem 4.1 that retains convexity and is computationally more tractable because it does not require any integration. The sample size in (4.16) must be selected so that the solution of Problem 4.2 is guaranteed to perform well when compared to the solution in Problem 4.1. A useful sample selection policy is given by the Chernoff bound combined with Hoeffding's inequality [43]:

$$P_W^\gamma\left\{(W^1,...,W^\gamma)\in \mathscr{W}^\gamma : \left|\hat{\underline{C}}(\bar{M},V,W^1,...,W^\gamma) - E_{x_0}\{\underline{C}(\bar{M},V,W)\}\right| \geq \varepsilon\right\} \leq 2e^{-2\gamma\varepsilon^2} \tag{4.17}$$

We can use the Chernoff bound to find the appropriate disturbance sample size. However, this has a limitation in the sense that (4.17) is for a given $(\bar{M},V)$ and does not provide a criterion for comparing the optimal solutions of both problems. Using bounds

from statistical learning theory (see [33], [44]) and Pollard dimension theory (see [43], [45]) we can compare the performance of empirical minima of the cost function, provided by the solution of Problem 4.2, to the optimal minima that is provided by the solution of Problem 4.1. The upcoming results and the affiliated discussions in the sequel will further clarify this comparison criterion.

Definition 4.2: (Pollard Dimension [43]) Consider a measurable space $(\Omega, \mathscr{F})$ and a family of real valued, bounded, non-negative, measurable functions $\mathscr{G}$ on this space with an upper bound κ. A set $S = \{x_1, ..., x_n\} \subseteq \Omega$ is said to be P-shattered by $\mathscr{G}$ if there exists a real vector $c \in [0, \kappa]^n$ such that for every binary vector $e \in \{0,1\}^n$, there exists a corresponding function $g_e \in \mathscr{G}$ such that:

$$\left\{ \begin{array}{ll} g_e(x_i) \geq c_i & if\ e_i = 1 \\ g_e(x_i) < c_i & if\ e_i = 0 \end{array} \right\}$$

The Pollard dimension, denoted P-dimension, is the largest integer n such that there exists a set of cardinality n that is P-shattered by $\mathscr{G}$.

Define the decision variable $y = (\bar{M}, V)$ and the admissible control space $\mathscr{Y}$ as follows:

$$\mathscr{Y} = \{y \in \Re^{Nm \times Nn} \times \Re^{Nm} : \max_{i=1,...,Nm} |V_i| + \|\bar{M}_i\|_1 W_{max} \leq U_{max}\}$$

Denote $\underline{C}(y,.)$ as $\underline{C}_y$ where $\underline{C}_y : \mathscr{W} \rightarrow [0,1]$. We will compute the P-dimension of

the function family Ψ. The family of functions Ψ is defined by:

$$\Psi = \{\underline{C}_y : y \in \mathscr{Y}\}$$

Lemma 4.2: The P-dimension of Ψ is upper bounded by $2(Nn+1)(Nm)\log(8e)$.

Proof. We will use a result from [46] to compute the P-dimension, which is also stated according to our settings in [43]. However, in order to use this result we have to reformulate the admissible control space $\mathscr{Y}$ as a vector space. In its current form, $\mathscr{Y}$ is a product of a matrix space with a vector space. This is done by vectorizing the matrix $\bar{M}$ and forming a new vector Z which contains $\bar{M}$ and V. It should be noted that this change of variables does not change the structure of the optimization problem.

Let $\bar{M}_{(:,1)}, \bar{M}_{(:,2)}, ..., \bar{M}_{(:,Nn)}$ denote the columns of the matrix $\bar{M}$. Next, we define the $(N^2nm+Nm)\times 1$ dimensional vector Z as follows:

$$Z = \begin{bmatrix} \bar{M}_{(:,1)} \\ \vdots \\ \bar{M}_{(:,Nn)} \\ V \end{bmatrix} \tag{4.18}$$

Define the matrices $\mathscr{H}_j,\ j = 1, ..., Nn+1$ as follows:

$$\mathscr{H}_1 = [I_{Nm\times Nm},\ 0_{Nm\times NnNm}]\ ,\ \mathscr{H}_{Nn+1} = [0_{Nm\times NnNm},\ I_{Nm\times Nm}]$$

$$\mathscr{H}_i = [0_{Nm\times(i-1)Nm},\ I_{Nm\times Nm},\ 0_{Nm\times(Nn-i+1)Nm}],\ i = 2, ..., Nn \tag{4.19}$$

Using (4.18) and (4.19) we can write $\bar{M}W + V$ as follows:

$$\bar{M}W + V = \sum_{i=1}^{Nn} W_i \mathscr{H}_i Z + \mathscr{H}_{Nn+1} Z \tag{4.20}$$

By plugging (4.20) into (4.13) we can write $\underline{C}(y,W) < c$ as the following polynomial inequality in Z, W, and c:

$$x_0' \bar{A}' \bar{Q} \bar{A} x_0 + 2x_0' \bar{A}' \bar{Q} \bar{B} \left(\sum_{i=1}^{Nn} W_i \mathscr{H}_i Z + \mathscr{H}_{Nn+1} Z \right) + 2x_0' \bar{A}' \bar{Q} \bar{D} W + W' \bar{D}' \bar{Q} \bar{D} W +$$

$$2W' \bar{D}' \bar{Q} \bar{B} \left(\sum_{i=1}^{Nn} W_i \mathscr{H}_i Z + \mathscr{H}_{Nn+1} Z \right) + \left\{ \left(\sum_{i=1}^{Nn} W_i \mathscr{H}_i Z + \mathscr{H}_{Nn+1} Z \right)' \left(\bar{B}' \bar{Q} \bar{B} + \bar{R} \right) \right.$$

$$\left. \times \left(\sum_{i=1}^{Nn} W_i \mathscr{H}_i Z + \mathscr{H}_{Nn+1} Z \right) \right\} \tag{4.21}$$

The degree of this polynomial inequality with respect to the vector Z is 2. Therefore, by utilizing Theorem 11.1 of [43] we conclude that the P-dimension of Ψ is upper bounded by, $\Psi \leq 2(Nn+1)(Nm)\log(8e)$. □

Next, we state Pollard's Theorem, see [33] for more details, which will be used to prove a result in this chapter:

Theorem 4.2.1: **(Pollard)** Let $\mathscr{J}$ be a family of measurable functions mapping a set $B \subseteq \Re^{Nm}$ into $[0,1]$. Assume that the Pollard dimension of this function family is $d < \infty$. Then for any $\varepsilon > 0$:

$$P_W^{\gamma}\left\{(W^1,...,W^{\gamma})\in \mathscr{W}^{N\gamma}: \sup_{J\in\mathscr{J}}\left|E(J(W))-\frac{1}{\gamma}\sum_{j=1}^{\gamma}J(W^j)\right|>\varepsilon\right\}$$
$$\leq 8\left(\frac{16e}{\varepsilon}\log(\frac{16e}{\varepsilon})\right)^{d}e^{-\gamma\varepsilon^2/32}$$

Note that Pollard's Theorem is a result on the Uniform Convergence of Empirical Means (UCEM). It is now applied in conjunction with Lemma 4.2, to outline a performance criterion for the efficiency of the solution of Problem 4.2. This is done by providing an appropriate lower bound on the disturbance sample size.

Theorem 4.2.2: Let $W^1,...,W^{\gamma}$ be iid samples of the disturbance vector W generated according to the probability measure P_W and let $\hat{y}^* = \arg\min_{y\in\mathscr{Y}} \hat{\underline{C}}(y,W^1,...,W^{\gamma})$. Given $\varepsilon,\delta>0$, If:

$$\gamma \geq \frac{128}{\varepsilon^2}\left[\log(\frac{8}{\delta})+2(Nn+1)(Nm)\log(8e)\left(\log(\frac{32e}{\varepsilon})+\log\log(\frac{32e}{\varepsilon})\right)\right]$$

then:

$$P_W^{\gamma}\left\{(W^1,...,W^{\gamma})\in\mathscr{W}^{N\gamma}: E\underline{C}(\hat{y}^*,W)-\min_{y\in\mathscr{Y}}E\underline{C}(y,W)\leq\varepsilon\right\}\geq 1-\delta$$

Proof. By applying Pollard's theorem and Lemma 3.1 we get that:

$$P_W^{\gamma}\left\{(W^1,...,W^{\gamma})\in\mathscr{W}^{N\gamma}: \sup_{\underline{C}_y\in\Psi}\left|E\underline{C}(y,W)-\frac{1}{\gamma}\sum_{i=1}^{\gamma}\underline{C}(y,W^i)\right|\leq\frac{\varepsilon}{2}\right\}$$

$$\geq 1-8\left(\frac{32e}{\varepsilon}\log(\frac{32e}{\varepsilon})\right)^{2(Nn+1)(Nm)\log(8e)}e^{-\gamma\varepsilon^2/128} \tag{4.22}$$

Let $y^* = \arg\min_{y \in \mathscr{Y}} E\underline{C}(y,W)$. Then by using (4.22) we can write:

$$P_W^{\gamma}\left\{(W^1,...,W^{\gamma}) \in \mathscr{W}^{N\gamma} : \left|E\underline{C}(y^*,W) - \frac{1}{\gamma}\sum_{i=1}^{\gamma}\underline{C}(y^*,W^i)\right| \leq \frac{\varepsilon}{2}, \left|E\underline{C}(\hat{y}^*,W) - \right.\right.$$

$$\left.\left.\frac{1}{\gamma}\sum_{i=1}^{\gamma}\underline{C}(\hat{y}^*,W^i)\right| \leq \frac{\varepsilon}{2}\right\} \geq 1 - 8\left(\frac{32e}{\varepsilon}\log(\frac{32e}{\varepsilon})\right)^{2(Nn+1)(Nm)\log(8e)} e^{-\gamma\varepsilon^2/128} \qquad (4.23)$$

So we have that:

$$\frac{1}{\gamma}\sum_{i=1}^{\gamma}\underline{C}(\hat{y}^*,W^i) - \frac{\varepsilon}{2} \;\leq\; E\underline{C}(\hat{y}^*,W) \;\leq\; \frac{1}{\gamma}\sum_{i=1}^{\gamma}\underline{C}(\hat{y}^*,W^i) + \frac{\varepsilon}{2}$$

$$\frac{1}{\gamma}\sum_{i=1}^{\gamma}\underline{C}(y^*,W^i) - \frac{\varepsilon}{2} \;\leq\; E\underline{C}(y^*,W) \;\leq\; \frac{1}{\gamma}\sum_{i=1}^{\gamma}\underline{C}(y^*,W^i) + \frac{\varepsilon}{2}$$

$$\Rightarrow\; E\underline{C}(y^*,W) \;\geq\; -\frac{\varepsilon}{2} + \frac{1}{\gamma}\sum_{i=1}^{\gamma}\underline{C}(y^*,W^i) \;\geq\; -\frac{\varepsilon}{2} + \frac{1}{\gamma}\sum_{i=1}^{\gamma}\underline{C}(\hat{y}^*,W^i)$$

$$\geq\; -\frac{\varepsilon}{2} - \frac{\varepsilon}{2} + E\underline{C}(\hat{y}^*,W) \;\geq\; -\varepsilon + E\underline{C}(\hat{y}^*,W) \qquad (4.24)$$

Now using (4.23), (4.24), and the value of γ we get:

$$P_W^{\gamma}\left\{(W^1,...,W^{\gamma}) \in \mathscr{W}^{N\gamma} : E\underline{C}(\hat{y}^*,W) - E\underline{C}(y^*,W) \leq \varepsilon\right\} \geq$$

$$1 - 8\left(\frac{32e}{\varepsilon}\log(\frac{32e}{\varepsilon})\right)^{2(Nn+1)(Nm)\log(8e)} e^{-\gamma\varepsilon^2/128} \;\geq\; 1-\delta$$

This completes the proof of the theorem. □

It should be noted that the results outlined in Theorem 4.2.2 require us to solve a convex program. This might not be practically possible for some important resource-

constrained applications. The results developed in the next section address such situations where we have severe computational constraints.

4.3 Randomized Algorithms: Randomly Generated Control Inputs

In many control problems, that involve constrained large scale dynamical systems, the minimization of the empirical cost could be computationally intensive. We mitigate this problem by randomly generating both the control parameters and the additive disturbances and solve for a *probable near minimum* to Problem 4.1. First, we define several notions of probable near minimum to a cost function.

Definition 4.3.1: (Probably Approximate Near Minimum to Level α [43]) Let $(X, \mathscr{F}, P_X)$ be a probability space, $f : X \to \Re$ be a measurable function, and $\alpha > 0$ be some given real number. A number $f_0 \in \Re$ is said to be a probably approximate near minimum of $f(.)$ to level α, also called Type II near minimum, provided that:

$$f_0 \geq \min_{x \in X} f(x), \;\; P_X\{x \in X : f(x) < f_0\} \leq \alpha$$

Definition 4.3.2: (Probably Approximate Near Minimum to Accuracy ε and Level α [43]) Let $(X, \mathscr{F}, P_X)$ be a probability space, $f : X \to \Re$ be a measurable function, and $\varepsilon, \alpha > 0$ be some given real numbers. Then $\hat{f}_0$ is said to be a probably approximate near minimum of $f(.)$ to accuracy ε and level α, also called Type III near minimum, if:

$$\hat{f}_0 \geq \min_{x \in X} f(x) - \varepsilon, \; P_X\{x \in X : f(x) < \hat{f}_0 - \varepsilon\} \leq \alpha \tag{4.25}$$

Next, we present a result that provides a probably approximate near minimum of Problem 4.1 to accuracy ε and level α. Appropriate lower bounds on control and disturbance sample sizes are provided which enable us to compute the aforementioned notion of probable near minimum.

Theorem 4.3: Given $\varepsilon, \alpha, \delta > 0$, generate iid disturbance samples $W^1, ..., W^\gamma$ from $\mathscr{W}^N$ according to the probability measure P_W and iid control samples $y^1, ..., y^q$ from $\mathscr{Y}$ according to the probability measure P_y where:

$$q \geq \left\lceil \frac{\log(\frac{2}{\delta})}{\log(\frac{1}{1-\alpha})} \right\rceil, \ \gamma \geq \left\lceil \frac{1}{2\varepsilon^2} \ln \frac{4q}{\delta} \right\rceil$$

Define $\hat{\underline{C}}_0 = \min\limits_{i=1,...,q} \hat{\underline{C}}(y^i, W^1, ..., W^\gamma)$. Then:

$$P_{(y,W)}^{(q,\gamma)} \Bigg\{ (y^1, ..., y^q) \in \mathscr{Y}^q, (W^1, ..., W^\gamma) \in \mathscr{W}^\gamma : \ \hat{\underline{C}}_0 \geq \min_{y \in \mathscr{Y}} E\{\underline{C}(y, W)\} - \varepsilon, \\ P_y^q(y \in \mathscr{Y} : E\{\underline{C}(y, W)\} < \hat{\underline{C}}_0 - \varepsilon) \leq \alpha \Bigg\} \geq 1 - \delta$$

where $P_{(y,W)}^{(q,\gamma)}$ is the product probability measure on the space $(\mathscr{Y}^q \times \mathscr{W}^\gamma)$. In other words with confidence $1 - \delta$, we can say that $\hat{\underline{C}}_0$ is a probably approximate near minimum of Problem 4.1 to accuracy ε and level α.

Proof. The proof follows directly from Lemma 11.1, Algorithm 11.5, and Section 11.3.5 in [43]. We also provide the full proof for the sake of completeness.

First we generate $y^1, \ldots, y^q$ iid samples from $\mathscr{Y}$ where $q \geq \dfrac{\log(\frac{2}{\delta})}{\log(\frac{1}{1-\alpha})}$. Define $\tilde{\underline{C}} = \min_{i=1,...,q} E\{\underline{C}(\bar{M}^i, V^i, W)\}$. We will prove that $\tilde{\underline{C}}$ is a probably approximate near minimum of Problem 4.1 to level α. Let us define $\underline{C}^*$ to be the optimal minimum to

Problem 4.1. Clearly we observe that $\tilde{\underline{C}} \geq \underline{C}^*$. We need to show that:

$$P_Y^q \left\{ (y^1, ..., y^q) : P_Y \left\{ y \in \mathscr{Y} : E\{\underline{C}(y, W)\} < \tilde{\underline{C}} \right\} \leq \alpha \right\} \geq 1 - \frac{\delta}{2}$$

Let $g(y) = -E\{\underline{C}(y,W)\}, y \in \mathscr{Y}$. Then $g(y)$ is a random variable if y is generated randomly from $\mathscr{Y}$. Let the distribution function of this random variable be given by:

$$F(b) = P_Y\{y \in \mathscr{Y} : g(y) \leq b\}$$

Also it should be noted that we can write:

$$-\tilde{\underline{C}} = -\min_{i=1,...,q} E\{\underline{C}(y^i, W)\} = \max_{i=1,...,q} -E\{\underline{C}(y^i, W)\}$$

By definition a distribution function is right continuous. We define $b_\alpha = \inf\{b : F(b) \geq 1 - \alpha\}$. By right continuity we get that $F(b_\alpha) \geq 1 - \alpha$. From the definition of b_α we have that if $b < b_\alpha$ then $F(b) < 1 - \alpha$. Suppose that $-\tilde{\underline{C}} \geq b_\alpha$. This implies that:

$$P_Y\{y \in \mathscr{Y} : g(y) > -\tilde{\underline{C}}\} \; = \; 1 - F(-\tilde{\underline{C}}) \; \leq \; \alpha$$

Taking the contrapositive of the above statement we get that:

$$P_Y\{y \in \mathscr{Y} : g(y) > -\tilde{\underline{C}}\} > \alpha \; \Rightarrow \; -\tilde{\underline{C}} < b_\alpha$$

Now $-\tilde{\underline{C}} < b_\alpha$ if and only if $-E\{\underline{C}(y^i, W)\} < b_\alpha, i = 1, ..., q$. Now these are independent

events each with probability no larger than $1-\alpha$.

$$\Rightarrow \;\; P_Y^q\left\{(y^1,...,y^q)\in \mathscr{Y}^q : P_Y\{y\in\mathscr{Y} : g(y) > -\underline{\tilde{C}}\} > \alpha\right\} \leq (1-\alpha)^q$$

$$\Rightarrow \;\; P_Y^q\left\{(y^1,...,y^q)\in \mathscr{Y}^q : P_Y\{y\in\mathscr{Y} : E\{\underline{C}(y,W)\} < \underline{\tilde{C}}\} > \alpha\right\} \leq (1-\alpha)^q$$

By utilizing the sample selection criterion $q \geq \dfrac{\log(\frac{2}{\delta})}{\log(\frac{1}{1-\alpha})}$ we get that:

$$P_Y^q\left\{(y^1,...,y^q)\in \mathscr{Y}^q : P_Y\{y\in\mathscr{Y} : E\{\underline{C}(y,W)\} < \underline{\tilde{C}}\} \leq \alpha\right\} \geq 1-\frac{\delta}{2}$$

From this we conclude that $\underline{\tilde{C}}$ is a probably approximate (Type II) near minimum of Problem 4.1 to level α. Next we generate $W^1,...,W^\gamma$ iid noise samples where $\gamma \geq \dfrac{1}{2\varepsilon^2}\ln(\dfrac{4q}{\delta})$. From the Chernoff bound combined with Hoeffding's inequality we get that:

$$P_W^\gamma\left\{(W^1,...,W^\gamma)\in \mathscr{W}^\gamma : \left|\frac{1}{\gamma}\sum_{j=1}^{\gamma}\underline{C}(y,W^j) - E\{\underline{C}(y,W)\}\right| > \varepsilon\right\} \leq 2e^{-2\gamma\varepsilon^2}$$

Consider $\underline{C}(y^i,W)$ and define $S(\gamma,\varepsilon),\ S_i(\gamma,\varepsilon),\ i=1,...,q$ as follows:

$$S_i(\gamma,\varepsilon) = \left\{(W^1,...,W^\gamma)\in \mathscr{W}^\gamma : \left|\frac{1}{\gamma}\sum_{j=1}^{\gamma}\underline{C}(y^i,W^j) - E\{\underline{C}(y^i,W)\}\right| > \varepsilon\right\}$$

$$\Rightarrow \;\; (S_i(\gamma,\varepsilon))^c = \left\{(W^1,...,W^\gamma)\in \mathscr{W}^\gamma : \left|\frac{1}{\gamma}\sum_{j=1}^{\gamma}\underline{C}(y^i,W^j) - E\{\underline{C}(y^i,W)\}\right| \leq \varepsilon\right\}$$

$$(S(\gamma,\varepsilon))^c = \left\{(W^1,...,W^\gamma)\in \mathscr{W}^\gamma : \max_{i=1,...,q}\left|\frac{1}{\gamma}\sum_{j=1}^{\gamma}\underline{C}(y^i,W^j) - E\{\underline{C}(y^i,W)\}\right| \leq \varepsilon\right\}$$

Clearly $(S(\gamma,\varepsilon))^c = \bigcap_{i=1}^{q}(S_i(\gamma,\varepsilon))^c \Rightarrow S(\gamma,\varepsilon) = \bigcup_{i=1}^{q} S_i(\gamma,\varepsilon)$. By sub-additivity we get that:

$$P_W^{\gamma}(S(\gamma,\varepsilon)) \leq \sum_{i=1}^{q} P_W^{\gamma}(S_i(\gamma,\varepsilon)) \leq 2qe^{-2\gamma\varepsilon^2} \leq \frac{\delta}{2}$$

$$P_W^{\gamma}\left\{(W^1,...,W^{\gamma}) \in \mathscr{W}^{\gamma} : \max_{i=1,...,q}\left|\frac{1}{\gamma}\sum_{j=1}^{\gamma}\underline{C}(y^i,W^j) - E\{\underline{C}(y^i,W)\}\right| \leq \varepsilon\right\} \geq 1-\frac{\delta}{2}$$

So we have with confidence $1-\frac{\delta}{2}$ that:

$$\left|\frac{1}{\gamma}\sum_{j=1}^{\gamma}\underline{C}(y^i,W^j) - E\{\underline{C}(y^i,W)\}\right| \leq \varepsilon, \quad i=1,...,q \tag{4.26}$$

Using (4.26) we will show that:

$$\left|\min_{i=1,...,q}\frac{1}{\gamma}\sum_{j=1}^{\gamma}\underline{C}(y^i,W^j) - \min_{i=1,...,q}E\{\underline{C}(y^i,W)\}\right| \leq \varepsilon$$

or in other words using the aforementioned notation we will show with confidence $1-\frac{\delta}{2}$ that $|\,\hat{\underline{C}}_0 - \tilde{\underline{C}}\,| \leq \varepsilon$. Let $i^* = \arg\min_{i=1,...,q}\frac{1}{\gamma}\sum_{j=1}^{\gamma}\underline{C}(y^i,W^j)$. Using (4.26) we get that:

$$\left|E\{\underline{C}(y^{i^*},W)\} - \frac{1}{\gamma}\sum_{j=1}^{\gamma}\underline{C}(y^{i^*},W^j)\right| \leq \varepsilon \Rightarrow \left|E\{\underline{C}(y^{i^*},W)\} - \hat{\underline{C}}_0\right| \leq \varepsilon$$

So we have $-\varepsilon + E\{\underline{C}(y^{i^*},W)\} \leq \hat{\underline{C}}_0$. Since $\tilde{\underline{C}} \leq E\{\underline{C}(y^{i^*},W)\}$ this implies that:

$$-\varepsilon \leq \hat{\underline{C}}_0 - \tilde{\underline{C}}$$

Let $i^{**} = \arg\min_{i=1,...,q} E\{\underline{C}(y^i, W)\}$. From (4.26) we get that:

$$\left| \frac{1}{\gamma} \sum_{j=1}^{\gamma} \underline{C}(y^{i^{**}}, W^j) - \tilde{\underline{C}} \right| \leq \varepsilon$$

$$\hat{\underline{C}}_0 \leq \frac{1}{\gamma} \sum_{j=1}^{\gamma} \underline{C}(y^{i^{**}}, W^j) \leq \tilde{\underline{C}} + \varepsilon \Rightarrow \hat{\underline{C}}_0 - \tilde{\underline{C}} \leq \varepsilon$$

Combining these two results we get that with confidence $1 - \frac{\delta}{2}$ we have that:

$$\left| \min_{i=1,...,q} \frac{1}{\gamma} \sum_{j=1}^{\gamma} \underline{C}(y^i, W^j) - \min_{i=1,...,q} E\{\underline{C}(y^i, W)\} \right| \leq \varepsilon$$

So far we have proved two statements:

$$P_Y^q \left\{ (y^1, ..., y^q) \in \mathscr{Y}^q : P\{y \in \mathscr{Y} : E\{\underline{C}(y, W)\} < \tilde{\underline{C}}\} \leq \alpha \right\} \geq 1 - \frac{\delta}{2}$$

$$P_W^{\gamma} \left\{ (W^1, ..., W^{\gamma}) \in \mathscr{W}^{\gamma} : \left| \hat{\underline{C}}_0 - \tilde{\underline{C}} \right| \leq \varepsilon \right\} \geq 1 - \frac{\delta}{2}$$

Now we combine both these statements to prove the claim of the Theorem. Since the samples $(y^1, ..., y^q)$ and $(W^1, ..., W^{\gamma})$ are independent of one another:

$$P_{y,W}^{(q,\gamma)} \left\{ (W^1, ..., W^{\gamma}) \in \mathscr{W}^{\gamma}, (y^1, ..., y^q) \in \mathscr{Y}^q : P_Y(y \in \mathscr{Y} : E\{\underline{C}(y, W)\} \leq \tilde{\underline{C}}) \leq \alpha, \left| \tilde{\underline{C}} - \hat{\underline{C}}_0 \right| \leq \alpha \right\}$$
$$\geq (1 - \frac{\delta}{2})^2 > 1 - \delta$$

Now $\left| \tilde{\underline{C}} - \hat{\underline{C}}_0 \right| \leq \varepsilon$ implies that $\tilde{\underline{C}} \geq \hat{\underline{C}}_0 - \varepsilon$ and $\hat{\underline{C}} \geq \underline{C}^* - \varepsilon$. Also we have that:

$$P_Y\left(y \in Y : E\{\underline{C}(y, W)\} < \hat{\underline{C}}_0 - \varepsilon\right) \leq P_Y\left(y \in Y : E\{\underline{C}(y, W)\} < \tilde{\underline{C}}_0\right) \leq \alpha$$

$$P_{y,W}^{(q,\gamma)}\Bigg\{(W^1,...,W^\gamma)\in\mathscr{W}^\gamma,(y^1,...,y^q)\in\mathscr{Y}^q:\ P_Y\big(y\in Y:E\{\underline{C}(y,W)\}<\hat{\underline{C}}_0-\varepsilon\big)\leq\alpha,\\ \hat{\underline{C}}_0\geq\underline{C}^*-\varepsilon\Bigg\}\geq 1-\delta$$

which proves that $\hat{\underline{C}}_0$ is a Type III near minimum of Problem 4.1 to accuracy ε and level α. □

Theorem 4.3 provides an appropriate criterion for sample size selection thereby enabling us to compute, with a certain confidence level, a probable near minimum of Problem 4.1. In contrast to the aforementioned results in Section 4.1 and Section 4.2, computation of a probable near minimum does not require us to solve a convex program. Therefore, if random samples could be rapidly generated, from the disturbance and admissible control spaces, then we can practically implement these results to solve SRHC problems on many small devices.

It is also possible to prove a result analogous to Theorem 4.3 by utilizing Pollard dimension theory instead of the Chernoff bound. However, this leads to very large sample sizes for the disturbances which makes this methodology impractical (see section 11.3.5 in [43] for more details and examples).

4.4 Incorporating Model Uncertainty

In this section, we incorporate model uncertainty into the problem formulation and extend the results presented in Section 4.3. Consider the following linear time-invariant

system in discrete time:

$$x_{i+1} = A_\Delta x_i + B_\Delta u_i + D_\Delta w_i,\ i \in \mathbb{Z}^+ \tag{4.27}$$

where $\Delta \in \mathscr{O}$ which is assumed to be a compact and a convex set. The resulting matrices $A_\Delta,\ B_\Delta$, and D_Δ are assumed to have finite components for every Δ in $\mathscr{O}$. Due to the presence of model uncertainty in the system dynamics, we cannot use equation (4.8) to backtrack the disturbances from the states. Therefore, we will utilize the sub-optimal state feedback scheme specified in equation (4.9). Using a compact notation we obtain:

$$X = \bar{A}_\Delta x_0 + \bar{B}_\Delta U + \bar{D}_\Delta W \tag{4.28}$$

where $\bar{A}_\Delta, \bar{B}_\Delta, \bar{D}_\Delta$ are the same as in Section 4.1 except for the presence of model uncertainty in the system dynamics. Plugging the feedback scheme:

$$U = \bar{K}X + \tilde{V} \tag{4.29}$$

into equation (4.28) we get:

$$X = (I_{(Nn+n)\times(Nn+n)} - \bar{B}_\Delta \bar{K})^{-1} \left(\bar{A}_\Delta x_0 + \bar{B}_\Delta \tilde{V} + \bar{D}_\Delta W \right) \tag{4.30}$$

Note that $\bar{B}_\Delta \bar{K}$ is a strictly lower triangular matrix, therefore $(I_{(Nn+n)\times(Nn+n)} - \bar{B}_\Delta \bar{K})$ is non-singular. Let $\mathscr{L} = (I_{(Nn+n)\times(Nn+n)} - \bar{B}_\Delta \bar{K})^{-1}$. Using this notation the cost function

can be written as follows:

$$C(\bar{K},\tilde{V},W,\Delta) = X'\bar{Q}X + U'\bar{R}U = 2x_0'\bar{A}_\Delta'\mathscr{L}'\left(\bar{Q}\mathscr{L}\bar{B}_\Delta + \bar{K}'\bar{R} + \bar{K}'\bar{R}\bar{K}\mathscr{L}\bar{B}_\Delta\right)\tilde{V} +$$

$$x_0'\bar{A}_\Delta'\mathscr{L}'\left(\bar{Q} + \bar{K}'\bar{R}\bar{K}\right)\mathscr{L}\bar{A}_\Delta x_0 + 2W'\bar{D}_\Delta'\mathscr{L}'\left(\bar{Q}\mathscr{L}\bar{B}_\Delta + \bar{K}'\bar{R}\bar{K}\mathscr{L}\bar{B}_\Delta + \bar{K}'\bar{R}\right)\tilde{V} +$$

$$2x_0'\bar{A}_\Delta'\mathscr{L}'\left(\bar{K}'\bar{R}\bar{K} + \bar{Q}\right)\mathscr{L}\bar{D}_\Delta W + W'\bar{D}_\Delta'\mathscr{L}'\left(\bar{K}'\bar{R}\bar{K} + \bar{Q}\right)\mathscr{L}\bar{D}_\Delta W +$$

$$\tilde{V}'\left(\bar{B}_\Delta'\mathscr{L}'\bar{Q}\mathscr{L}\bar{B}_\Delta + 2\bar{R}\bar{K}\mathscr{L}\bar{B}_\Delta + \bar{R}\right)\tilde{V} \tag{4.31}$$

Let Cm_{max} be an upper bound to the cost $C(\bar{K},\tilde{V},W,\Delta)$. Define the normalized cost $\underline{C}(\bar{K},\tilde{V},W,\Delta)$ which takes values in $[0,1]$ as follows:

$$\underline{C}(\bar{K},\tilde{V},W,\Delta) = \frac{C(\bar{K},\tilde{V},W,\Delta)}{Cm_{max}}$$

Problem 4.4.1: Consider the following problem:

$$\min_{\bar{K},\tilde{V}} \; E_{x_0}\{\underline{C}(\bar{K},\tilde{V},W,\Delta)\}$$

subject to the constraint:

$$\|\bar{K}\mathscr{L}(\bar{A}_\Delta x_0 + \bar{B}_\Delta\tilde{V} + \bar{D}_\Delta W) + \tilde{V}\|_\infty \leq U_{max},\; W \in \mathscr{W}^N, \Delta \in \mathscr{O}$$

where the expectation is with respect to W and Δ.

Remark 4.4: Using Hölder's inequality the constraints in Problem 4.4.1 can be simplified

as follows:

$$\max_{i=1,...,Nm}\{|(\bar{K}\mathscr{L}\bar{A}_\Delta x_0+\bar{K}\mathscr{L}\bar{B}_\Delta\tilde{V}+\tilde{V})_i|+\|(\bar{K}\mathscr{L}\bar{D}_\Delta)_i\|_1 W_{max}\}\leq U_{max},\ \Delta\in\mathscr{O}$$

It should be noted that Problem 4.4.1 is in general a non-convex optimization problem. We employ the randomized algorithm techniques outlined in Section 4.3, to avoid the computational complexity resulting from this non-convexity. Generate iid samples $((W^1,\Delta^1),...,(W^\gamma,\Delta^\gamma))$ of the noise, according to the product measure $P_{W\times\Delta}$, from the space $\mathscr{W}^N\times\mathscr{O}$. First, we define the empirical mean of the cost function as follows:

$$\underline{\hat{C}}(\bar{K},\tilde{V},(W^1,\Delta^1),...,(W^\gamma,\Delta^\gamma))=\frac{1}{\gamma}\sum_{i=1}^{\gamma}\underline{C}(\bar{K},\tilde{V},W^i,\Delta^i) \tag{4.32}$$

We randomly generate the control parameters $(\bar{K},\tilde{V})$ from the space $\mathscr{Z}$, which is specified below, and compute a probable near minimum to Problem 4.4.1.

Let $z=(\bar{K},\tilde{V})$ and the admissible space $\mathscr{Z}$ be given by:

$$\mathscr{Z}=\Bigg\{z\in\Re^{Nm\times(Nn+n)}\times\Re^{Nm}:\max_{i=1,...,Nm}\{\ |(\bar{K}\mathscr{L}\bar{A}_\Delta x_0+\bar{K}\mathscr{L}\bar{B}_\Delta\tilde{V}+\tilde{V})_i| \\ +\ \|(\bar{K}\mathscr{L}\bar{D}_\Delta)_i\|_1 W_{max}\ \}\leq U_{max},\ \Delta\in\mathscr{O}\Bigg\}$$

Next, we state a result which is a generalization of Theorem 4.3 to the model uncertainty case.

Theorem 4.4.1: Given iid noise samples $(W^1,\Delta^1),....,(W^\gamma,\Delta^\gamma)$ generated from $\mathscr{W}^N\times\mathscr{O}$ according to the measure $P_{W\times\Delta}$ and iid control samples $z^1,...,z^r$ generated from $\mathscr{Z}$

according to the measure P_z. $\varepsilon, \alpha, \delta > 0$ are provided and integers r, γ are given by:

$$r \geq \left\lceil \frac{\log(\frac{2}{\delta})}{\log(\frac{1}{1-\alpha})} \right\rceil, \ \gamma \geq \left\lceil \frac{1}{2\varepsilon^2} \ln \frac{4q}{\delta} \right\rceil$$

Define $\widehat{\underline{Cm}}_0 = \min_{i=1,\ldots,r} \underline{C}(z^i, (W^1, \Delta^1), \ldots, (W^\gamma, \Delta^\gamma))$. Then with confidence $1-\delta$ we can say that $\widehat{\underline{Cm}}_0$ is a probably approximate near minimum of Problem 4.4.1 to accuracy ε and level α.

Proof. The proof follows along the same lines as the proof of Theorem 4.3. □

It should be noted that the techniques outlined in this theorem do not specifically require us to solve a non-convex optimization problem. Therefore, this result can be applied to efficiently compute a probable near minimum to Problem 4.4.1. Ultrafast random sample generation can be done on many small devices, utilizing analog circuits, making such results practically applicable.

Next, we present an alternative problem formulation addressing the model uncertainty case. We consider a problem formulation where the cost is maximized with respect to both the additive disturbance as well as the model uncertainty and minimized with respect to the control parameters. Such a formulation provides the control system designer more flexibility and allows us to introduce alternative randomization based techniques.

Problem 4.4.2: Consider the following optimization problem:

$$\min_{\bar{K}, \tilde{V}} \ \max_{\Delta, W} \ \underline{C}(\bar{K}, \tilde{V}, W, \Delta)$$

subject to:

$$\|\bar{K}\mathscr{L}(\bar{A}_{\Delta}x_0+\bar{B}_{\Delta}\tilde{V}+\bar{D}_{\Delta}W)+\tilde{V}\|_{\infty}\leq U_{max},\ \forall W\in\mathscr{W}^N,\forall\Delta\in\mathscr{O}$$

We now present a notion of a probable near minimax value which was first developed in [47] (which also provides a detailed interpretation) and which will be used to state a result.

Definition 4.4: **(Probable Near Minimax Value to Minimum level α and Maximum level β)** Let $(X,\mathscr{F},P_X)$ and $(Y,\mathscr{G},P_Y)$ be given probability spaces, and $\alpha,\beta>0$ be given real numbers, $f:X\times Y\rightarrow\Re$ be a measurable function, and $f^*=\inf\limits_{y\in Y}\sup\limits_{x\in X}f(x,y)$ be the exact minimax value. A number $f_0\in\Re$ is said to be a probable near minimax value of $f(.)$ to minimum level α and maximum level β if there exists a measurable function $f_L:Y\rightarrow\Re$ and a number $f_U\in\Re$ such that:

$$\inf_{y\in Y}f_L(y)\leq f_0\leq f_U,\ \ \inf_{y\in Y}f_L(y)\leq f^*\leq f_U$$

$$P_X\{x\in X:f(x,y)>f_L(y)\}\leq\beta,\forall y\in Y$$

$$P_Y\{y\in Y:\sup_{x\in X}f(x,y)<f_U\}\leq\alpha$$

Next, we randomly generate the controller parameters $z=(\bar{K},\tilde{V})$, the disturbance samples, and provide required bounds on respective sample sizes in order to compute a probable near minimax value of Problem 4.4.2, with minimum level α and maximum level β.

Theorem 4.4.2: Generate iid model uncertainty samples $(W^1, \Delta^1), ..., (W^\rho, \Delta^\rho)$ from the sample space $\mathscr{W} \times \mathscr{O}$ according to the probability measure $P_{W \times \Delta}$ and iid control samples $z^1, ..., z^s$ from the sample space $\mathscr{Z}$ according to the probability measure P_z where:

$$\rho \geq \left\lceil \frac{\ln(\frac{N}{\delta_\beta})}{\ln(\frac{1}{1-\beta})} \right\rceil, \quad s \geq \left\lceil \frac{\ln(\frac{1}{\delta_\alpha})}{\ln(\frac{1}{1-\alpha})} \right\rceil$$

where the level parameters $\alpha, \beta > 0$ and the confidence parameters $\delta_\alpha, \delta_\beta > 0$ are given. Define:

$$\underline{C}_{hyb} = \min_{i=1,...,s} \max_{j=1,...,\rho} \underline{C}(z^i, W^j, \Delta^j)$$

Then we can say with confidence $1 - (\delta_\alpha + \delta_\beta)$ that $\underline{C}_{hyb}$ is a probable near minimax value of Problem 4.4.2 to minimum level α and maximum level β.

Proof. The proof follows directly from Theorem 1 in [47] which relies on Lemma 11.1 in [43]. □

Theorem 4.4.2 provides a criterion for constructing a probable near minimax value of Problem 4.4.2. A different version of Theorem 4.4.2 can also be provided for the case when the exact minimax value forms a saddle point.

4.5 Simulations

Consider the following Schur stable A matrix and other system dynamics:

$$A = \begin{bmatrix} 0.19 & 0.33 & 0.24 \\ 0.39 & 0.28 & 0.30 \\ 0.25 & 0.37 & 0.50 \end{bmatrix}, B = \begin{bmatrix} 1 & 0.5 \\ 0.33 & 2 \\ 1.8 & 1.4 \end{bmatrix}, D = I_{3\times 3} \tag{4.33}$$

We take $U_{max} = 6$, $W_{max} = 2$, and horizon size $N = 10$. The symmetric positive definite matrices Q_i, R_i in the cost are selected as $Q_i = 5I_{3\times 3}$ and $R_i = 3I_{2\times 2}$.Therefore, $\bar{Q} = 5I_{33\times 33}$ and $\bar{R} = 3I_{20\times 20}$. Let the ith additive disturbance w_i be given by:

$$w_i = \begin{bmatrix} w_{i,1} \\ w_{i,2} \\ w_{i,3} \end{bmatrix}, \quad i \in \mathbb{Z}^+$$

We assume that the components $w_{i,1}, w_{i,2}, w_{i,3}$ of the additive disturbance w_i, are independent and uniformly distributed on the interval $[-2, 2]$. Therefore:

$$E(w_i) = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, Var(w_i) = \begin{bmatrix} \frac{4}{3} & 0 & 0 \\ 0 & \frac{4}{3} & 0 \\ 0 & 0 & \frac{4}{3} \end{bmatrix}$$

We consider the formulation of Problem 4.1. The resulting optimization problem is convex and we use the optimization software cvx [15] to compute the optimal solution. The accuracy, confidence, and level parameters are taken as $\varepsilon = 0.1, \delta = 0.01, \alpha = 0.05$.

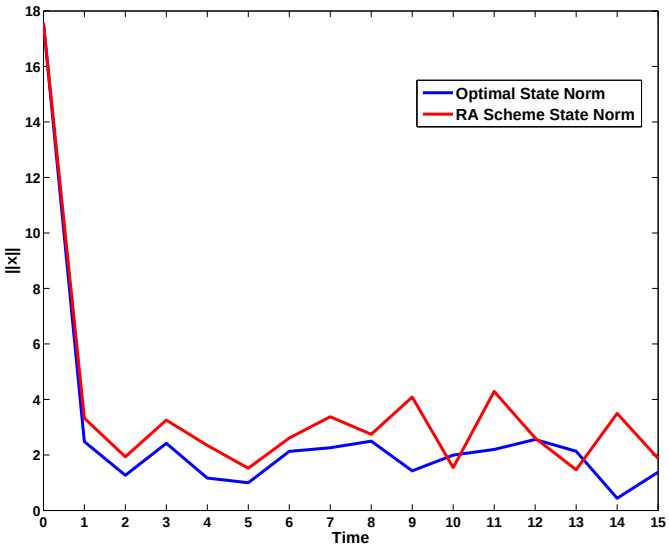

Figure 4.1: Randomized Algorithm Generated State vs Optimal State of Problem 2.1 using initial state $[8,12,10]'$

Using the sample size bounds specified by Theorem 4.3, greater than 530 iid control samples and 614 iid disturbance samples are respectively generated to compute a probable near minimum of Problem 4.1. We generate the control parameters by restricting the components of the gain matrix $\bar{M}$ to be less than $|0.17|$ and the components of the vector V to be less than $|3.82|$, while satisfying the control constraints. This assumption enables us to generate high quality iid control samples rapidly from the admissible control space.

The initial state is assumed to be $[8,12,10]'$ and $[9,-18,25]'$ for the results presented in Fig. 4.1 and Fig. 4.2, respectively. Only the first element of the control sample which provides the probable near minimum value is selected and applied to the actual dynamical system, as is typically done in RHC. Using this randomized scheme, the actual state of the system is generated and compared to the actual state generated by the optimal solution to Problem 4.1.

In Fig. 4.1 and Fig. 4.2, the Euclidean norm of the state is used to compare the

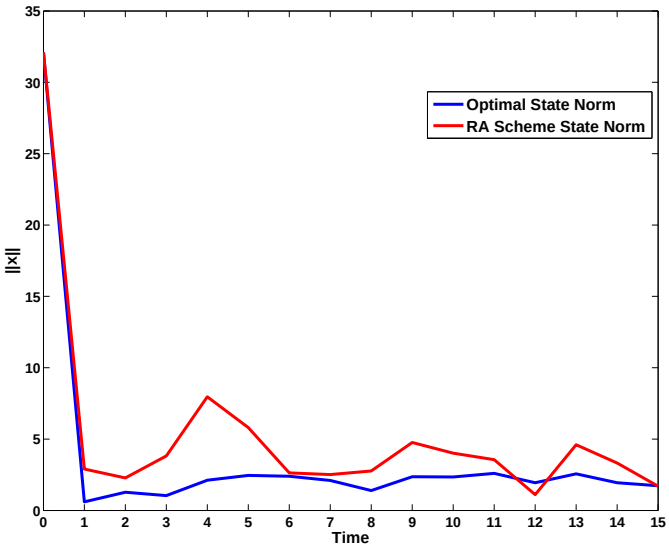

Figure 4.2: Randomized Algorithm Generated State vs Optimal State of Problem 2.1 using initial state $[9, -18, 25]'$

performance of the optimal and probable near minimum solutions of Problem 4.1, the later of which is computed by the randomized scheme specified in Theorem 4.3. Simulation results show that the randomized scheme performs pretty well though at the expense of incurring some extra cost, which is as expected. From the simulations, we conclude that such relaxed reformulations of the SRHC problem utilizing randomized algorithms are computationally efficient, provide good performance, and can have important implications for any device which is unable to perform complex on-line optimization.

Chapter 5: Optimal Sensor Placement for Intruder Detection

The fields of detection, resource allocation, and security have seen a lot of research activity in the past few decades. Different frameworks have been designed to tackle various problems using a host of techniques from statistics, engineering, and economics. The fields of centralized and decentralized detection, see [48] for a review, have been a major research focus in the communications, controls, and statistics communities and are now considered mature. Our main focus in this chapter is to develop and pursue research ideas in the intersection of these fields. In this chapter, we operate within the centralized detection framework under which complete observations are available to the decision makers. This preference for a relatively simple and more developed framework enables us to fully extract the benefits offered by the multi-disciplinary nature of these research ideas. In contrast to the work in Chapter 2, where we designed control policies which revealed partial state information to an adversary which was trying to estimate the terminal state of the system, in this chapter we consider the problem of detecting an intruder present in the environment of a system using a team of sensors.

Centralized detection of an intruder is considered, whose location is modeled as uniform across a specified set of points. A team of sensors is tasked to make observations which are then completely reported to a centralized decision making authority. The chal-

lenge is to optimally place the sensors, before measurements are made, and to compute an optimal decision rule for detecting the location of the intruder. Simplifying assumptions like a uniform prior distribution and conditional independence of observations are assumed. It should be noted that sensor observations are noisy as a result of their inability to make perfect observations. This limited capability of the sensors makes the conditional independence assumption practically reasonable [49].

We exploit majorization theory, see [50] and [51] for a review, within the framework of this chapter to establish general laws governing the jointly optimal detection and placement policies. Majorization is an important mathematical technique for partial ordering of vectors of real numbers. It is widely used in mathematical statistics and has recently been applied to solve challenging problems in controls [52] and communications [53].

The following notation is adopted:

- Capital letters N and M are used to denote the number of sensors and the number of placement points respectively.

- Vectors are represented as $\bar{x} = (x_1, ..., x_k)$, where the vector length would be obvious from the context.

- The observation vector received by the fusion center is denoted by $\bar{y} = (y_1, ..., y_N)$, the position vector of the sensors is denoted by $\bar{u} = (u_1, ..., u_N)$, and the placement vector for the sensors is denoted by $\bar{v} = (v_1, ..., v_M)$.

- Random variables are represented by bold face capital letters, such as $\mathbf{X}$ is used to represent the position of the intruder. Realizations are represented using small letters.

- The probability of error is denoted by P_e, the prior distribution by π, the probability density of a random variable **A** if it exists by $p(a)$, the joint probability density of **A** and **B** by $p(a,b)$, and the conditional probability density of **A** given **B** by $p(a|b)$. Here a and b are the realizations of the random variables **A** and **B**.

- The observation space is denoted by Ω.

This chapter is organized in four main sections. In Section 5.1 we provide the problem formulation. The main results of this chapter are presented in Section 5.2 and Section 5.3, respectively. In Section 5.2, we use mathematical induction to establish general principles under which uniform placement of sensors is never strictly optimal. In Section 5.3, majorization theory is exploited to formalize important properties of the optimal placement. Simulation based results are discussed in Section 5.4.

5.1 Problem Formulation

In this section, we present a precise statement and a mathematical formulation for this problem. We first present a main assumption that will be utilized throughout this chapter.

Assumption 5.1: We assume that the observations of the sensors are conditionally independent given the actual location of the intruder. In other words if $\bar{y} = (y_1, ..., y_N)$ are the observations reported by the sensors and if the actual location of the intruder is $j,\ j = 1, ..., M$, then:

$$p(\bar{y}\,|\mathbf{X} = j) = \prod_{i=1}^{N} p(y_i\,|\mathbf{X} = j)$$

5.1.1 Sensor Placement, Data Collection, and Performance Criterion

Consider a team of N identical sensors tasked with detecting the location of an intruder $\mathbf{X}$ which can occur on a specified set of points $\{1,....,M\}$, with a uniform distribution. It is assumed that $N \leq M$. The sensors are placed using a specific sensor position vector (or sensor placement vector), sensors make observations, and report them directly to a fusion center. The observations made by the sensors are assumed to be conditionally independent, given the true position of the intruder. The fusion center collects these observations and computes an estimate of the position of the intruder. It should be noted that the sensors report complete observations to the fusion center. The performance criterion minimized at the fusion center is the probability of error in detecting the actual location of the intruder. The main problem is to design jointly optimal location detection and sensor placement policies.

5.1.2 Observation Model

The sensor position vector $\bar{u}$, of length N, indicates the points at which each sensor is placed whereas the sensor placement vector $\bar{v}$, of length M, indicates how many sensors are placed at each point. It should be noted that:

$$1 \leq u_j \leq M,\ j = 1,...,N$$

$$0 \leq v_k \leq N,\ k = 1,...,M$$

Let $\mathbf{Y}_k$ be the measurement obtained by sensor k, $k = 1,...,N$. The random variable

$\mathbf{Y}_k$ either takes the value 1 (Intruder present at the position of sensor k) or the value 0 (Intruder not present at the position of sensor k). The observation model is presented below:

$$Pr(\mathbf{Y}_k = 1|\mathbf{X} = u_k) = P_D$$

$$Pr(\mathbf{Y}_k = 1|\mathbf{X} \neq u_k) = P_F$$

where P_D and P_F are the local probability of detection and the local probability of false alarm of the sensors respectively. We assume that these values are well known to us and have been provided by the manufacturer of these sensors. It should be noted that the sensors can only make measurements at the points on which they are placed and cannot infer any information regarding the presence of the intruder at other points.

5.1.3 M-ary Hypothesis Testing

The problem is modeled as an M-ary hypothesis testing problem [7, pp. 46-52] under the Bayesian formulation. Under a uniform prior distribution, $\pi_i = \frac{1}{M}$, the probability of error at the fusion center for a specific sensor position vector $(u_1, ..., u_N)$ is given by [8, pp. 7-9]:

$$P_e(\bar{u}, P_F, P_D) = \min_{\delta} \frac{1}{M} \sum_{i=1}^{M} \sum_{\bar{y} \in \Gamma_i} \sum_{j=1, j \neq i}^{M} p_{\bar{u}}(\bar{y} \,|\mathbf{X} = j)$$

where $\Gamma_i, i = 1, ..., M$, defines a partition of the observation space Ω such that $\Omega = \bigcup_{i=1}^{M} \Gamma_i$ and $\Gamma_i = \{\bar{y} \in \Omega \mid \delta(\bar{y}) = H_i\}$. Here $p_{\bar{u}}(\bar{y} \,|\mathbf{X} = j)$ is the conditional joint probability mass function (pmf) for the random variables ($\mathbf{Y}_1$,...,$\mathbf{Y}_N$) given that $\mathbf{X}$= j and when the sensor position vector, $\bar{u}$, is utilized for sensor placement. It should be noted that the

joint pmf depends on the sensor position vector (or sensor placement vector). Since we consider identical sensors using the same observation model it is sufficient to consider the number of sensors which are placed at each point. In the calculation of the joint pmf, the sensor placement vector is more convenient to use than the sensor position vector. In the sequel, we will utilize the sensor placement vector $\bar{v} = (v_1, ..., v_M)$ instead of the sensor position vector $\bar{u} = (u_1, ..., u_N)$ to calculate the probabilities of error. It should be noted that we use the notation $p_{\bar{v}}(\bar{y} \,|\mathbf{X} = j)$ for the conditional joint pmf for the random variables ($\mathbf{Y}_1$,...,$\mathbf{Y}_N$), given that $\mathbf{X}$= j, and when $\bar{v}$ is utilized as the sensor placement vector.

5.1.4 Calculation of Conditional Probabilities

Since the observations are conditionally independent:

$$p_{\bar{v}}(\bar{y} \,|\mathbf{X} = j) = \prod_{i=1}^{N} p_{\bar{v}}(y_i \,|\mathbf{X} = j), \quad j = 1, ..., M$$

It should be noted that the probability of error is invariant to permutations of the sensor placement vector, hence without loss of generality, we will only consider placements of the form $v_1 \geq v_2 \geq .... \geq v_M$. For notational convenience we assume that during deployment the sensors are placed in an ascending order, i-e first v_1 sensors are deployed on point 1 followed by v_2 sensors on point 2 and, so on. We hasten to add that this deployment policy is really not restrictive; it merely amounts to a relabeling of the observation areas or locations: location 1 is the one with the most number of sensors, and so on. Thus location j need not be 'adjacent' to location $j-1$ or $j+1$. This deployment policy en-

sures that observations $(y_1,...,y_{v_1})$ are made by sensors operating at point 1 and similarly we can interpret the observations $(y_{v_1+1},...,y_N)$. With $N \leq M$ and the aforementioned assumptions in place, it is clear that $(v_{N+1},...,v_M) = (0,...,0)$. Note that depending on the values of the v_i's it is possible that $v_k = 0$, for $k = k_0,...,N$ where $2 \leq k_0 \leq N$, as well. The conditional probability is calculated as follows:

$$p_{\bar{v}}(\bar{y}\,|\mathbf{X}=j) = \left\{(P_F)^{z(1,N)}(1-P_F)^{N-z(1,N)}\chi_{(v_j=0)}\right\} + \left\{(P_D)^{a_j}(1-P_D)^{v_j-a_j}(P_F)^{z(1,N)-a_j} \times \right.$$

$$\left.(1-P_F)^{N-z(1,N)-(v_j-a_j)}\chi_{(v_j\neq 0)}\right\} \tag{5.1}$$

where a_j is the number of accurate 'alarmed' sensors at location j and is given by:

$$a_j = y_1 + ... + y_{v_j}, \;\; j = 1$$

$$a_j = y_{(v_1+...+v_{j-1})+1} + ... + \; y_{(v_1+...+v_{j-1})+v_j}, \;\; j = 2,...,M$$

and $z(1,N)$ for any integer N is given by:

$$z(1,N) = y_1 + ... + y_N$$

5.1.5 Problem Statement

Given N sensors and M placement points we want to solve the following optimization problem:

$$P_e^*(P_F,P_D) = \min_{\delta,\bar{v}} \frac{1}{M}\sum_{i=1}^{M}\sum_{\bar{y}\in\Gamma_i}\sum_{j=1,j\neq i}^{M} p_{\bar{v}}(\bar{y}\,|\mathbf{X}=j)$$

subject to the constraints:

$$(v_1, ..., v_N) \in \Lambda^N$$

where the set Λ^N is given by the integer partition of N. For example $\Lambda^4 = \{(4,0,0,0),$ $(3,1,0,0),\ (2,2,0,0),\ (2,1,1,0),\ (1,1,1,1)\}$

Definition 5.1: **(Partition Function)** The partition function $f(N)$ of a positive integer N is defined as the number of ways in which N can be written as a sum of positive integers. For example, the integer 4 can be written as $4,\ 3+1,\ 2+2,\ 2+1+1$, and $1+1+1+1$ giving the partition function value, $f(4) = 5$.

Using this definition, the size of the constraint set Λ^N is given by:

$$|\Lambda^N| = f(N)$$

The partition function $f(N)$ of an integer N can be expressed asymptotically as [55]:

$$f(N) \approx \frac{1}{4N\sqrt{3}} \times e^{\pi\sqrt{\frac{2N}{3}}}\ as\ N \to \infty$$

This expression was first proved by S. Ramanujan and G. Hardy in 1918. The form of the cost function and the exponential complexity of the constraint set make this problem difficult to solve for a general (N,M). We prove important solution properties for this problem in Section 4.2 and Section 4.3.

For any placement $\bar{v}$ the probability of error is given by:

$$P_e(\bar{v}, P_F, P_D) = \min_{\delta} \frac{1}{M} \sum_{i=1}^{M} \sum_{\bar{y} \in \Gamma_i} \sum_{j=1, j \neq i}^{M} p_{\bar{v}}(\bar{y}\,|\mathbf{X} = j)$$

Minimization is carried out by optimally selecting Γ_i, where $i = 1, ..., M$:

$$\Gamma_i^* = \left\{ \bar{y} \in \Omega \;\middle|\; \sum_{j=1, j\neq i}^{M} p_{\bar{v}}(\bar{y} \,|\mathbf{X} = j) \leq \sum_{j=1, j\neq k}^{M} p_{\bar{v}}(\bar{y} \,|\mathbf{X} = j), i \neq k \right\}$$

which can be simplified to give:

$$\Gamma_i^* = \left\{ \bar{y} \in \Omega \;\middle|\; p_{\bar{v}}(\bar{y} \,|\mathbf{X} = i) \;=\; \max_{k=1,...,M} p_{\bar{v}}(\bar{y} \,|\mathbf{X} = k) \right\} \tag{5.2}$$

Using (5.2) and the uniform distribution of the priors the optimal decision rule is given by:

$$\delta^*(\bar{y}) = \left\{ H_i \;\middle|\; \pi(H_i|\bar{y}) = \max_{k=1,..,M} \pi(H_k|\bar{y}) \right\}, \bar{y} \in \Omega \tag{5.3}$$

where $\pi(H|\bar{y})$ is the posterior distribution given the observation vector $\bar{y}$. Note that the optimal decision rule in (5.3) is the Maximum A Posteriori Probability (MAP) rule. It should be noted that the δ^* presented above is optimal for any arbitrary placement $\bar{v}$ and therefore the optimization problem can be rewritten as follows:

$$P_e^*(P_F, P_D) = \min_{\bar{v}} \frac{1}{M} \sum_{i=1}^{M} \sum_{\bar{y} \in \Gamma_i^*} \sum_{j=1, j\neq i}^{M} p_{\bar{v}}(\bar{y} \,|\mathbf{X} = j) \tag{5.4}$$

subject to the constraint:

$$(v_1, ..., v_N) \in \Lambda^N$$

For notational convenience we will use the following form of $P_e(\bar{v}, P_F, P_D)$ in the sequel:

$$P_e(\bar{v}, P_F, P_D) = \frac{1}{M} \sum_{\bar{y} \in \{0,1\}^N} \min_{i=1,..,M} \{ \sum_{j=1, j \neq i}^{M} p_{\bar{v}}(\bar{y} \,|\mathbf{X} = j) \tag{5.5}$$

where $\{0,1\}^N$ is used to denote the observation space Ω and $P_e(\bar{v}, P_F, P_D)$ is a function of $(\bar{v}, P_F, P_D)$.

5.2 Characterization of the Optimal Solution

We first provide a definition of the strict optimality of a sensor placement and then present the main results of this section.

Definition 5.2: **(Strict Optimality of Placement)** We call a placement $\bar{v}'$ strictly optimal if there exists a point (P_F', P_D') on the (P_F, P_D) plane such that:

$$P_e(\bar{v}', P_F', P_D') < P_e(\bar{v}, P_F', P_D')$$

for any placement $\bar{v} \neq \bar{v}'$ where $(v_1, ..., v_N) \in \Lambda^N$, $(v_{N+1}, ..., v_M) = (0, ..., 0)$.

It should be noted that an optimal placement for (5.4) gives an optimal solution to the aforementioned problem. Utilizing Definition 5.2, the main result of this section is presented as follows:

Theorem 5.2: For the case $(M = N)$, the uniform sensor placement $(v_1, ..., v_N) = (1, ..., 1)$ is not strictly optimal.

Proof. We will prove this result by utilizing mathematical induction. For notational con-

venience we will use the following form of $P_e(v_1,...,v_M)$ in the proof:

$$P_e(v_1,...,v_M) = \frac{1}{N}\sum_{\bar{y}\in\{0,1\}^M}\min_{i=1,..,N}\{\sum_{j=1,j\neq i}^{N} p_{\bar{v}}(\bar{y}\,|\mathbf{X}=j)\} \tag{5.6}$$

For M sensors we have 2^M observations so $\{0,1\}^M$ is used to denote the observation space Ω.

First consider the case M=N=2. In this case (5.6) can be simplified to give:

$$P_e(v_1,v_2) = \frac{1}{2}\Big[\sum_{i=0}^{1}\sum_{j=0}^{1}\min\Big\{p_{(v_1,v_2)}\big((i,j)\,|\mathbf{X}=1\big), p_{(v_1,v_2)}\big((i,j)\,|\mathbf{X}=2\big)\Big\}\Big] \tag{5.7}$$

Using equation (5.1) the conditional probabilities for the $(v_1,v_2)=(1,1)$ and $(v_1,v_2)=(2,0)$ placements are given as follows:

$$\begin{aligned}
p_{(1,1)}\big((y_1,y_2)|\,\mathbf{X}=1\big) &= (P_D)^{y_1}(1-P_D)^{1-y_1}(P_F)^{y_2}(1-P_F)^{1-y_2}\\
p_{(1,1)}\big((y_1,y_2)|\,\mathbf{X}=2\big) &= (P_D)^{y_2}(1-P_D)^{1-y_2}(P_F)^{y_1}(1-P_F)^{1-y_1}\\
p_{(2,0)}\big((y_1,y_2)|\,\mathbf{X}=1\big) &= (P_D)^{y_1+y_2}(1-P_D)^{2-y_1-y_2}\\
p_{(2,0)}\big((y_1,y_2)|\,\mathbf{X}=2\big) &= (P_F)^{y_1+y_2}(1-P_F)^{2-y_1-y_2}
\end{aligned} \tag{5.8}$$

Plugging (5.8) into (5.7) we get:

$$\begin{aligned}
P_e\big(1,1\big) &= \frac{1}{2}\Big[(1-P_D)(1-P_F)+P_DP_F+2\min\{P_F-P_DP_F,P_D-P_DP_F\}\Big]\\
P_e\big(2,0\big) &= \frac{1}{2}\Big[\min\{(1-P_D)^2,(1-P_F)^2\}+\min\{P_D^2,P_F^2\}+2\min\{P_D(1-P_D),P_F(1-P_F)\}\Big]
\end{aligned} \tag{5.9}$$

First consider the case $\mathbf{P_D} > \mathbf{P_F}$:

For $P_D > P_F, P_D(1-P_D) > P_F(1-P_F)$:

$$P_e(1,1) = \frac{1}{2}\left[1 + P_F - P_D\right]$$
$$P_e(2,0) = \left[\frac{1}{2} + (P_F - P_D) + \frac{(P_D^2 - P_F^2)}{2}\right]$$

where $(P_D^2 - P_F^2) - (P_D - P_F) < 0 \Rightarrow P_e(2,0) < P_e(1,1)$

For $P_D > P_F, P_D(1-P_D) = P_F(1-P_F)$:

$$P_e(1,1) = P_e(2,0) = \frac{1}{2}\left[1 + P_F - P_D\right]$$

For $P_D > P_F, P_D(1-P_D) < P_F(1-P_F)$:

$$P_e(1,1) = \frac{1}{2}\left[1 + (P_F - P_D)\right], P_e(2,0) = \frac{1}{2}\left[1 + (P_F^2 - P_D^2)\right]$$

where $(P_F^2 - P_D^2) < (P_F - P_D) \Rightarrow P_e(2,0) < P_e(1,1)$

For the case $\mathbf{P_D} = \mathbf{P_F}$ we have:

$$P_e(2,0) = P_e(1,1) = \frac{1}{2}$$

For the purposes of this proof it is sufficient to only consider the case $P_D \geq P_F$. Further details regarding this sufficiency are provided at the end of the proof. This proves that uniform placement is not strictly optimal for *M*=*N*=2.

Assume that the result holds for M=N=k:

$$P_e\big(\underbrace{1,...,1}_{k}\big) \geq P_e\big(\underbrace{2,1,...,1,0}_{k}\big) \tag{5.10}$$

Calculation of $\mathbf{P_e}\big(\underbrace{1,...,1}_{\mathbf{k}}\big)$:

Using equations (5.1) and (5.6) we get the following expression:

$$P_e\big(\underbrace{1,...,1}_{k}\big) = \frac{1}{k}\Bigg[\sum_{\bar{y}\in\{0,1\}^k} \min_{i=1,..,k}\big\{A_i(\bar{y})\big\}\Bigg]$$

$$A_i(\bar{y}) = \sum_{j=1,j\neq i}^{k}\Big\{(P_D)^{y_j}(1-P_D)^{1-y_j}(P_F)^{(y_1+...+y_k)-y_j}(1-P_F)^{k-1-(y_1+...+y_k)+y_j}\Big\} \tag{5.11}$$

Calculation of $\mathbf{P_e}\big(\underbrace{2,1,...,1,0}_{\mathbf{k}}\big)$:

Using equations (5.1) and (5.6) we get the following expression:

$$P_e\big(\underbrace{2,1,...,1,0}_{k}\big) = \frac{1}{k}\Bigg[\sum_{\bar{y}\in\{0,1\}^k} \min_{i=1,..,k}\big\{B_i(\bar{y})\big\}\Bigg] \tag{5.12}$$

where $B_i(\bar{y}), i = 1,..,k$ is given by:

$$B_1(\bar{y}) = \Bigg[\sum_{j=2}^{k-1}(P_D)^{y_{j+1}}(1-P_D)^{1-y_{j+1}}(P_F)^{(y_1+...+y_k)-y_{j+1}}(1-P_F)^{k-1-(y_1+...+y_k)+y_{j+1}}\Bigg]$$

$$+(P_F)^{(y_1+..+y_k)}(1-P_F)^{k-(y_1+..+y_k)}$$

$$B_i(\bar{y}) = \Bigg[\sum_{j=2, j\neq i}^{k-1} (P_D)^{y_{j+1}} (1-P_D)^{1-y_{j+1}} (P_F)^{(y_1+\ldots+y_k)-y_{j+1}} (1-P_F)^{k-1-(y_1+\ldots+y_k)+y_{j+1}} \Bigg]$$
$$+ (P_F)^{(y_1+..+y_k)} (1-P_F)^{k-(y_1+..+y_k)} + (P_D)^{y_1+y_2} (1-P_D)^{2-y_1-y_2} (P_F)^{(y_3+\ldots+y_k)}$$
$$\times (1-P_F)^{k-2-(y_3+\ldots+y_k)} \ , \ \ i = 2, \ldots, k-1$$

$$B_k(\bar{y}) = \Bigg[\sum_{j=2}^{k-1} (P_D)^{y_{j+1}} (1-P_D)^{1-y_{j+1}} (P_F)^{(y_1+\ldots+y_k)-y_{j+1}} (1-P_F)^{k-1-(y_1+\ldots+y_k)+y_{j+1}} \Bigg]$$
$$+ (P_D)^{y_1+y_2} (1-P_D)^{2-y_1-y_2} (P_F)^{(y_3+\ldots+y_k)} (1-P_F)^{k-2-(y_3+\ldots+y_k)} \tag{5.13}$$

Using equation (5.10) we can conclude that:

$$\Bigg[\sum_{\bar{y}\in\{0,1\}^k} \min_{i=1,\ldots,k} \{A_i(\bar{y})\} - \sum_{\bar{y}\in\{0,1\}^k} \min_{i=1,\ldots,k} \{B_i(\bar{y})\} \Bigg] \geq 0$$

In order to prove the Theorem we need to show that:

$$P_e\big(\underbrace{1,\ldots,1}_{k+1}\big) \geq P_e\big(\underbrace{2,1,\ldots,1,0}_{k+1}\big)$$

Calculation of $\mathbf{P_e}\big(\underbrace{1,\ldots,1}_{\mathbf{k+1}}\big)$:

Using equations (5.1), (5.6) and (5.11) we get the following expression:

$$P_e\big(\underbrace{1,...,1}_{k+1}\big) = \frac{1}{k+1}\Bigg[\sum_{\bar{y}\in\{0,1\}^k}\Bigg\{\min\big\{(1-P_F)A_1(\bar{y})+c(\bar{y}),.....,(1-P_F)A_k(\bar{y})+c(\bar{y}),$$
$$(1-P_F)A_k(\bar{y})+c^*(\bar{y})\big\} \;+\; \min\big\{(P_F)A_1(\bar{y})+d(\bar{y}),.....,$$
$$(P_F)A_k(\bar{y})+d(\bar{y}),(P_F)A_k(\bar{y})+d^*(\bar{y})\big\}\Bigg\}\Bigg] \tag{5.14}$$

where $c(\bar{y}), c^*(\bar{y}), d(\bar{y}), d^*(\bar{y})$ are provided below:

$$c(\bar{y}) = (1-P_D)(P_F)^{(y_1+...+y_k)}(1-P_F)^{k-(y_1+...+y_k)}$$
$$c^*(\bar{y}) = (P_D)^{y_k}(1-P_D)^{1-y_k}(P_F)^{(y_1+...+y_{k-1})}(1-P_F)^{k-(y_1+...+y_{k-1})}$$
$$d(\bar{y}) = P_D(P_F)^{(y_1+...+y_k)}(1-P_F)^{k-(y_1+...+y_k)}$$
$$d^*(\bar{y}) = (P_D)^{y_k}(1-P_D)^{1-y_k}(P_F)^{y_1+..+y_{k-1}+1}(1-P_F)^{k-1-(y_1+..+y_{k-1})} \tag{5.15}$$

Calculation of $\mathbf{P_e}\big(\underbrace{2,1,...,1,0}_{\mathbf{k+1}}\big)$:

Using equations (5.1), (5.6) and (5.12) we get the following expression:

$$P_e\big(\underbrace{2,1,...,1,0}_{k+1}\big) = \frac{1}{k+1}\Bigg[\sum_{\bar{y}\in\{0,1\}^k}\Bigg\{\min\big\{(1-P_F)B_1(\bar{y})+c(\bar{y}),.....,(1-P_F)B_{k-1}(\bar{y})+c(\bar{y}),$$
$$(1-P_F)B_{k-1}(\bar{y})+c^*(\bar{y}),(1-P_F)B_k(\bar{y})+c(\bar{y})\big\}+\min\big\{(P_F)B_1(\bar{y})+d(\bar{y}),$$
$$\ldots,(P_F)B_{k-1}(\bar{y})+d(\bar{y}),(P_F)B_{k-1}(\bar{y})+d^*(\bar{y}),(P_F)B_k(\bar{y})+d(\bar{y})\big\}\Bigg\}\Bigg] \tag{5.16}$$

If $P_D = 1$ or $P_F = 0$ then $c^*(\bar{y}) \geq c(\bar{y})$. If $P_D < 1$ and $P_F > 0$ then $c^*(\bar{y})$ can be expressed in terms of $c(\bar{y})$ as follows:

$$c^*(\bar{y}) = c(\bar{y}) \left(\frac{P_D(1-P_F)}{P_F(1-P_D)} \right)^{y_k} \tag{5.17}$$

First consider the case where we have good sensors i-e sensors for which $\mathbf{P_D} \geq \mathbf{P_F}$. From equation (5.17) we have that $c^*(\bar{y}) \geq c(\bar{y})$. Therefore, we can eliminate the terms involving $c^*(\bar{y})$ from equations (5.14) and (5.16). We will first consider the situations where we can eliminate the terms involving $d^*(\bar{y})$ from equation (5.14) and then proceed by doing a similar analysis for equation (5.16). If $y_k = 1$, then $d^*(\bar{y}) = d(\bar{y})$. Using equations (5.11), (5.15), and $(y_{k-1}, y_k) = (0,0)$ we obtain:

$$\begin{aligned} \big(P_F A_k(\bar{y}) + d^*(y)\big) - \big(P_F A_{k-1}(\bar{y}) - d(\bar{y})\big) = \\ (P_F)^{(y_1+\ldots+y_{k-2})}(1-P_F)^{k-1-(y_1+\ldots+y_{k-2})}(P_F - P_D) \leq 0 \end{aligned} \tag{5.18}$$

From equations (5.11), (5.15), and $(y_{k-1}, y_k) = (1,0)$ we obtain:

$$(P_F)A_k(\bar{y}) + d^*(\bar{y}) = (P_F)A_{k-1}(\bar{y}) + d(\bar{y}) \tag{5.19}$$

Similarly it can be shown for $(y_{j-1}, y_k) = (1,0)$:

$$(P_F)A_k(\bar{y}) + d^*(\bar{y}) = (P_F)A_{j-1}(\bar{y}) + d(\bar{y}), j = 2, \ldots, k \tag{5.20}$$

So for $\bar{y} \in \{0,1\}^k/(0,\ldots,0)$ we can eliminate the term $(P_F)A_k(\bar{y}) + d^*(\bar{y})$ from equa-

tion (5.14).

For the observation $\bar{y} = (0, ..., 0)$:

$$\min\left\{(P_F)A_1(\bar{y}) + d(\bar{y}), ..., (P_F)A_k(\bar{y}) + d(\bar{y}), (P_F)A_k(\bar{y}) + d^*(\bar{y})\right\} = (P_F)A_k(\bar{y}) + d^*(\bar{y})$$

Let $a_1, ..., a_{2^k}$ be given as follows:

$$\sum_{u=1}^{2^k} a_u = \sum_{\bar{y}\in\{0,1\}^k} \min_{i=1,..,k} \{P_F A_i(\bar{y}) + d(\bar{y})\} \tag{5.21}$$

$$a_u = \min_{i=1,...,k} \{P_F A_i(y_1, ..., y_k) + d(y_1, ..., y_k)\}, \;\; u = dec(y_1 ... y_k) + 1$$

Here $dec(y_1 ... y_k)$ is the decimal value of the binary number $y_1 ... y_k$. Equations (5.18), (5.19), and (5.20) imply that:

$$\sum_{\bar{y}\in\{0,1\}^k} \min\{P_F A_1(\bar{y}) + d(\bar{y}), ..., P_F A_k(\bar{y}) + d(\bar{y}), P_F A_k(\bar{y}) + d^*(\bar{y})\} = (a_1^{'} - a_1) + \sum_{u=1}^{2^k} a_u$$

$$a_1 = (k-1)(1-P_D)(1-P_F)^{k-1} + P_D(1-P_F)^k$$

$$a_1^{'} = (k-1)(1-P_D)(1-P_F)^{k-1} + P_F(1-P_D)(1-P_F)^{k-1}$$

Using the same notation as in (5.21), $b_1, ..., b_{2^k}$ can be given as follows:

$$\sum_{u=1}^{2^k} b_u = \sum_{\bar{y}\in\{0,1\}^k} \min_{i=1,..,k} \{P_F B_i(\bar{y}) + d(\bar{y})\}$$

Using equation (5.13) for $\bar{y} = (0,...,0)$ we get that:

$$B_k(\bar{y}) \leq B_i(\bar{y}) \leq B_1(\bar{y}), \quad i = 2,..,k-1$$

$$\Rightarrow \quad b_1 = P_F B_k(0,...,0) + d(0,...,0)$$

Let $b_1^{'} = P_F B_{k-1}(0,...,0) + d^*(0,...,0)$. Using the expressions for $a_1, a_1^{'}, b_1, b_1^{'}$ we get that:

$$(a_1^{'} - a_1) - (b_1^{'} - b_1) = -(P_F)(P_D - P_F)(1 - P_F)^{k-1} \tag{5.22}$$

We have two cases here $P_D \geq P_F, P_D(1-P_D) \geq P_F(1-P_F)$ and $P_D \geq P_F, P_D(1-P_D) < P_F(1-P_F)$. First we consider the case:

Case A: $\mathbf{P_D \geq P_F, P_D(1-P_D) < P_F(1-P_F)}$

Using equation (5.13) and $P_D(1-P_D) < P_F(1-P_F)$ we get:

$$B_k(\bar{y}) < B_1(\bar{y}) \leq B_i(\bar{y}), \quad \bar{y} = (1,0,...,0)$$

$$\Rightarrow \quad b_{2^{k-1}+1} = P_F B_k(1,0,...,0) + d(1,0,...,0)$$

Let $b^{'}_{2^{k-1}+1} = P_F B_{k-1}(1,0,...,0) + d^*(1,0,...,0)$. Then using $b_{2^{k-1}+1}, b^{'}_{2^{k-1}+1}$ we get:

$$b_{2^{k-1}+1} - b^{'}_{2^{k-1}+1} = P_F(P_D - P_F)(1-P_F)^{k-1} \tag{5.23}$$

Using (5.22) and (5.23) we get:

$$(a_1^{'} - a_1) - (b_1^{'} - b_1) - (b_{2^{k-1}+1}^{'} - b_{2^{k-1}+1}) = 0$$

These equations imply that:

$$\sum_{\bar{y}\in\{0,1\}^k} \min\left\{P_F B_1(\bar{y}) + d(\bar{y}), ..., P_F B_{k-1}(\bar{y}) + d(\bar{y}), P_F B_{k-1}(\bar{y}) + d^*(\bar{y}), P_F B_k(\bar{y}) + d(\bar{y})\right\}$$
$$\leq\ b_1' \ +\ b'_{2^{k-1}+1} \ +\ \sum_{i=2, i\neq 2^{k-1}+1}^{2^k} b_i$$

Therefore we can conclude that:

$$\sum_{\bar{y}\in\{0,1\}^k} \min\left\{P_F A_1(\bar{y}) + d(\bar{y}), ..., P_F A_k(\bar{y}) + d(\bar{y}), P_F A_k(\bar{y}) + d^*(\bar{y})\right\} - \sum_{\bar{y}\in\{0,1\}^k} \min\Big\{$$
$$P_F B_1(\bar{y}) + d(\bar{y}), ..., P_F B_{k-1}(\bar{y}) + d(\bar{y}), P_F B_{k-1}(\bar{y}) + d^*(\bar{y}), P_F B_k(\bar{y}) + d(\bar{y})\Big\}$$
$$\geq\ (a_1' - a_1) - (b_1' - b_1) - (b'_{2^{k-1}+1} - b_{2^{k-1}+1}) + \sum_{i=1}^{2^k} a_i - \sum_{i=1}^{2^k} b_i\ \geq\ 0$$

which implies that:

$$\Rightarrow (\mathbf{k}+\mathbf{1})\left[P_e(\underbrace{1,...,1}_{k+1}) - P_e(\underbrace{2,1,..,1,0}_{k+1})\right] \geq \left[(1-P_F)\left\{\sum_{\bar{y}\in\{0,1\}^k} \min_{i=1,..,k} A_i(\bar{y}) - \right.\right.$$
$$\left.\left.\sum_{\bar{y}\in\{0,1\}^k} \min_{i=1,..,k} B_i(\bar{y})\right\} + P_F\left\{\sum_{\bar{y}\in\{0,1\}^k} \min_{i=1,..,k} A_i(\bar{y}) - \sum_{\bar{y}\in\{0,1\}^k} \min_{i=1,..,k} B_i(\bar{y})\right\}\right] \geq 0$$

This proves the result for Case A. Next, we prove the result for Case B.

Case B: $\mathbf{P_D \geq P_F, P_D(1-P_D) \geq P_F(1-P_F)}$

For this case we will modify the induction steps slightly and use the above results and discussions to complete the proof. We will show that:

$$(k+1)\left[P_e(\underbrace{1,...,1}_{k+1}) - P_e(\underbrace{2,1,...,1,0}_{k+1})\right] \geq (P_D - P_F)(1-P_D-P_F)(1-P_F)^{k-1}$$

From (5.9) it is clear that this results holds for M=N=2:

$$2\big(P_e(1,1) - P_e(2,0)\big) = (P_D - P_F)(1-P_D-P_F)$$

Assume that it holds for M=N=k:

$$(k)\left[P_e(\underbrace{1,...,1}_{k}) - P_e(\underbrace{2,1,...,1,0}_{k})\right] \geq (P_D - P_F)(1-P_D-P_F)(1-P_F)^{k-2} \tag{5.24}$$

Using equation (5.13) and $P_D(1-P_D) \geq P_F(1-P_F)$:

$$B_1(\bar{y}) \leq B_k(\bar{y}) \leq B_i(\bar{y}), \bar{y} = (1,0,...,0)$$

$$\Rightarrow b_{2^{k-1}+1} = P_F B_1(1,0,...,0) + d(1,0,...,0)$$

Let $b'_{2^{k-1}+1} = P_F B_{k-1}(1,0,...,0) + d^*(1,0,...,0)$. Using the values of $b_{2^{k-1}+1}, b'_{2^{k-1}+1}$ we get:

$$b_{2^{k-1}+1} - b'_{2^{k-1}+1} = P_D P_F (P_D - P_F)(1-P_F)^{k-2}$$

$$\Rightarrow (a_1^{'} - a_1) - (b_1^{'} - b_1) - (b_{2^{k-1}+1}^{'} - b_{2^{k-1}+1}) = P_F(P_D - P_F)(P_D + P_F - 1)(1 - P_F)^{k-2} \tag{5.25}$$

Consider the observation $(y_1, ..., y_k) = (0, 1, 0, .., 0)$:

$$B_1(\bar{y}) \leq B_k(\bar{y}) \leq B_i(\bar{y}), \bar{y} = (0, 1, 0, ..., 0)$$

$$\Rightarrow b_{2^{k-2}+1} = P_F B_1(0, 1, 0, ..., 0) + d(0, 1, 0, ..., 0) \tag{5.26}$$

Let $b_{2^{k-2}+1}^{'} = P_F B_{k-1}(0, 1, 0, ..., 0) + d^*(0, 1, 0, ..., 0)$.

Using (5.25 and (5.26) we get:

$$(a_1^{'} - a_1) - (b_1^{'} - b_1) - (b_{2^{k-1}+1}^{'} - b_{2^{k-1}+1}) - (b_{2^{k-2}+1}^{'} - b_{2^{k-2}+1}) =$$
$$P_F(P_D - P_F)(P_D + P_F - 1)(1 - P_F)^{k-2} + P_D P_F(P_D - P_F)(1 - P_F)^{k-2}$$

This implies that:

$$(k+1)\left[P_e(\underbrace{1, ..., 1}_{k+1}) - P_e(\underbrace{2, 1, ..., 1, 0}_{k+1})\right] \geq$$
$$(1 - P_F)\left\{ \sum_{\bar{y} \in \{0,1\}^k} \left(\min_{i=1,..,k} (A_i(\bar{y}) + c(\bar{y})) - \min_{i=1,..,k} (B_i(\bar{y}) + c(\bar{y})) \right) \right\} + (P_F)\left\{ \sum_{\bar{y} \in \{0,1\}^k} \right.$$
$$\left. \left(\min_{i=1,..,k} (A_i(\bar{y}) + d(\bar{y})) - \min_{i=1,..,k} (B_i(\bar{y}) + d(\bar{y})) \right) \right\} + P_D P_F(P_D - P_F)(1 - P_F)^{k-2}$$
$$- P_F(P_D - P_F)(1 - P_D - P_F)(1 - P_F)^{k-2} \tag{5.27}$$

Using (5.24), (5.27), and the fact that $P_D P_F(P_D - P_F)(1 - P_F)^{k-2} \geq 0$, we can conclude

that:

$$(k+1)\left[P_e(\underbrace{1,...,1}_{k+1}) - P_e(\underbrace{2,1,...,1,0}_{k+1})\right] \geq (P_D - P_F)(1-P_D-P_F)(1-P_F)^{k-1} \geq 0$$

This proves the claim for the case $\mathbf{P_D} \geq \mathbf{P_F}$.

A proof for the aforementioned case is sufficient to conclude that the result holds for all values of P_D, P_F. This is due to the fact that for the case $P_D < P_F$ the detector will simply flip the observation bits and the same optimal strategy, which was employed for the case $P_D > P_F$, will be employed by the fusion center. □

Theorem 5.2 is somewhat counterintuitive and holds regardless of the values of P_D and P_F. It is quite natural to assume that uniform placement of sensors should be strictly optimal for sensors that possess a high detection probability and a low probability of false alarm. This results proves that this natural assumption fails for the case when the number of sensors equal the number of placement points. A system employing a sensor placement policy utilizing the the results of this theorem can significantly outperform any policy which does not take these results into consideration. These observations help in preserving computational resources for systems which have limited computational and optimization capabilities.

Next we present some important properties of the optimal placement, on the (P_F, P_D) plane, by varying the number of placement points. We prove that the optimal placement structure on the (P_F, P_D) plane, for the specific case of $N < M$, is invariant to an increase in the value of M.

Proposition 5.2: The sensor-placement point pairs (N, M_1) and (N, M_2), where $N < M_1 < M_2$, have the same optimal placement structure on the (P_F, P_D) plane.

Proof. We will use the notation $P_e(\bar{v}, P_F, P_D)\big|_{M_1}$ and $P_e(\bar{v}, P_F, P_D)\big|_{M_2}$ to distinguish between these two cases. It should be noted that the length of the placement vector $\bar{v} = (v_1, ..., v_{M_i})$ is indicated by $M_i, i = 1, 2$.

First consider the case (N, M_1) where we have N agents and M_1 placement points. For a specific placement vector $\bar{v}$ the probability of error, $P_e(\bar{v}, P_F, P_D)\big|_{M_1}$, is given by:

$$P_e(\bar{v}, P_F, P_D)\big|_{M_1} = \frac{1}{M_1} \sum_{\bar{y} \in \{0,1\}^N} \min_{i=1,..,M_1} \{ \sum_{j=1, j \neq i}^{M_1} p_{\bar{v}}(\bar{y} \,|\mathbf{X} = j)\} \tag{5.28}$$

where $p_{\bar{v}}(\bar{y} \,|\mathbf{X} = j)$ is given by equation (5.1). Now $v_j = 0$ for $j = (N+1), ..., M_1$. Therefore, we can take $p_{\bar{v}}(\bar{y} \,|\mathbf{X} = j) = p(\bar{y} \,|\mathbf{X} = N+1)$ for $j = (N+1), ..., M_1$. Note that $p(\bar{y} \,|\mathbf{X} = N+1)$ does not depend on the placement vector $\bar{v}$. This is due to the fact that no sensor is placed at the point $N+1$. An application of this fact allows (5.28) to be updated as follows:

$$P_e(\bar{v}, P_F, P_D)\big|_{M_1} = \frac{1}{M_1} \sum_{\bar{y} \in \{0,1\}^N} \min_{i=1,..,N+1} \Bigg[\sum_{j=1, j \neq i}^{N} p_{\bar{v}}(\bar{y} \,|\mathbf{X} = j) + (M_1 - N) p(\bar{y} \,|\mathbf{X} = N+1)$$

$$\times \chi_{(i \neq N+1)} + \, (M_1 - N - 1) p(\bar{y} \,|\mathbf{X} = N+1) \chi_{(i = N+1)} \Bigg] \tag{5.29}$$

Consider another placement vector $\hat{\bar{v}}$, where $(\hat{v}_1, ..., \hat{v}_N) \in \Lambda^N$

$$P_e(\hat{\bar{v}}, P_F, P_D)\big|_{M_1} = \frac{1}{M_1} \sum_{\bar{y} \in \{0,1\}^N} \min_{i=1,..,N+1} \Bigg[\sum_{j=1, j \neq i}^{N} p_{\hat{\bar{v}}}(\bar{y} \,|\mathbf{X} = j) + (M_1 - N) p(\bar{y} \,|\mathbf{X} = N+1)$$

$$\times \chi_{(i\neq N+1)} + \ (M_1 - N - 1)p(\bar{y}\,|\mathbf{X} = N+1)\chi_{(i=N+1)}\Big] \tag{5.30}$$

Both (N, M_1) and (N, M_2) have the same set of admissible placements, determined by Λ^N. Similarly, $P_e(\bar{v})\big|_{M_2}$ and $P_e(\hat{\bar{v}})\big|_{M_2}$ can be written as follows:

$$P_e(\bar{v}, P_F, P_D)\big|_{M_2} = \frac{1}{M_2} \sum_{\bar{y}\in\{0,1\}^N} \min_{i=1,..,N+1} \Bigg[\sum_{j=1, j\neq i}^{N} p_{\bar{v}}(\bar{y}\,|\mathbf{X} = j) + (M_1 - N)p(\bar{y}\,|\mathbf{X} = N+1)$$

$$\times \chi_{(i\neq N+1)} + (M_1 - N - 1)p(\bar{y}\,|\mathbf{X} = N+1)\chi_{(i=N+1)} + (M_2 - M_1)p(\bar{y}\,|\mathbf{X} = N+1)\chi_{(i\neq N+1)} +$$

$$(M_2 - M_1)p(\bar{y}\,|\mathbf{X} = N+1)\chi_{(i=N+1)}\Bigg] \tag{5.31}$$

$$P_e(\hat{\bar{v}}, P_F, P_D)\big|_{M_2} = \frac{1}{M_2} \sum_{\bar{y}\in\{0,1\}^N} \min_{i=1,..,N+1} \Bigg[\sum_{j=1, j\neq i}^{N} p_{\hat{\bar{v}}}(\bar{y}\,|\mathbf{X} = j) + (M_1 - N)p(\bar{y}\,|\mathbf{X} = N+1)$$

$$\times \chi_{(i\neq N+1)} + (M_1 - N - 1)p(\bar{y}\,|\mathbf{X} = N+1)\chi_{(i=N+1)} + (M_2 - M_1)p(\bar{y}\,|\mathbf{X} = N+1)\chi_{(i\neq N+1)} +$$

$$(M_2 - M_1)p(\bar{y}\,|\mathbf{X} = N+1)\chi_{(i=N+1)}\Bigg] \tag{5.32}$$

Equations (5.29), (5.30), (5.31), and (5.32) imply that:

$$M_2 \times P_e(\bar{v}, P_F, P_D)\big|_{M_2} - M_2 \times P_e(\hat{\bar{v}}, P_F, P_D)\big|_{M_2} =$$

$$M_1 \times P_e(\bar{v}, P_F, P_D)\big|_{M_1} - M_1 \times P_e(\hat{\bar{v}}, P_F, P_D)\big|_{M_1} \tag{5.33}$$

Since $\bar{v}$ and $\hat{\bar{v}}$ are two arbitrarily chosen placements whose first N elements belong to the set Λ^N, (5.33) implies that as we transition from (N, M_1) to (N, M_2) the comparison equations determining the optimal placements remain unchanged. Therefore, we conclude that the sensor-placement point pairs (N, M_1) and (N, M_2) have the same optimal placement

structure on the (P_F, P_D) plane. This completes the proof. □

Proposition 5.2 has important practical implications. It implies that if we are given a sensor-placement pair (N,M), where $N < M$, we only need to analyze the sensor-placement pair $(N,N+1)$ and the optimal placement structure will be hold for all $M > N$. This results in a significant reduction in computational complexity. Theorem 5.2 and Proposition 5.2 can be utilized in the design of efficient algorithms for systems that have limited computational capabilities for performing numerical optimization.

Corollary 5.2: Let $\mathscr{V}(N,M_1)$ be the set of strictly optimal placements for the sensor-placement pair $(N,M_1), M_1 = N$. Then $\mathscr{V}(N,M_2) = \mathscr{V}(N,M_1) \cup \{(v_1,...,v_N) = (1,...,1), (v_{N+1},...,v_{M_2}) = (0,...,0)\}$ is the set of strictly optimal placements for the sensor-placement pair (N,M_2), $M_2 > N$.

Corollary 5.2 follows directly from Theorem 5.2, Proposition 5.2, and some basic facts regarding the uniform placement of sensors. One can easily recognize the fact that uniform placement of sensors will always belong to the set of strictly optimal placements $\mathscr{V}(N,M)$, for a sensor-placement pair (N,M), $N < M$. This fact can be established by considering extremely high values of P_D along with extremely low values of P_F.

5.3 A Majorization Approach

In this section, we will utilize some concepts from Majorization Theory to characterize several important properties regarding the optimal placement of sensors. First, we define some terms that will be used throughout the sequel.

Definition 5.3.1: **(Majorization** [51], pp. 6-7) For $\bar{x}, \bar{y} \in \Re^n$, $\bar{x}$ is said to be majorized by $\bar{y}$, $\bar{y} \succ \bar{x}$, provided that:

$$\sum_{j=1}^{k} x_{[j]} \leq \sum_{j=1}^{k} y_{[j]} \ , \quad \sum_{j=1}^{n} x_{[j]} = \sum_{j=1}^{n} y_{[j]}$$

where $k = 1, ..., n-1$ and $x_{[j]}$ represents the elements of $\bar{x}$ in non-increasing order, $x_{[1]} \geq .... \geq x_{[n]}$.

Definition 5.3.2: **(Majorization-Based Partial Order)** Sensor placements $\bar{\alpha}, \bar{\beta}$, and $\bar{\gamma}$ can be placed on a majorization-based partial order $(\bar{\alpha}, \bar{\beta}, \bar{\gamma})$ if the following ordering exists: $\bar{\alpha} \succ \bar{\beta} \succ \bar{\gamma}$. The placement $\bar{\alpha}$ is said to be at the highest level on this partial order followed by $\bar{\beta}$ and then $\bar{\gamma}$.

Using the aforementioned definitions the main result of this section can be stated as follows:

Proposition 5.3: For $N \leq 6$ and for fixed P_D (or fixed P_F), increasing P_F (or increasing P_D) leads to optimal placements that are higher in the majorization-based partial order.

Proof. We will only consider the sensor-placement pair $(N, M) = (4, 4)$. Other cases where $N \leq 6$ can be proved similarly.

The admissible placement set is given by $\Lambda^N = \{(1,1,1,1), (2,1,1,0), (2,2,0,0), (3,1,0,0), (4,0,0,0)\}$. Since $N = M$ we do not need to consider the placement $(1,1,1,1)$. Using majorization theory the following majorization-based partial order can be defined:

$$(4,0,0,0) \succ (3,1,0,0) \succ (2,2,0,0) \succ (2,1,1,0) \tag{5.34}$$

Using (5.6) we obtain the following optimality regions on the (P_F, P_D) plane on which these placements are respectively optimal. Detailed derivations which provide these regions can be found in [56]. It should be noted that at points on which more than one placement is optimal we choose the placement which preserves this result. For $P_D > P_F$, these regions are given as follows:

$(4,0,0,0)$ is the optimal placement if (P_F, P_D) belongs to the set:

$$\left\{(P_F,P_D)\in[0,1]^2 \;\middle|\; (P_D-P_F)\big[-(P_D+P_F)(P_D^2+P_F^2)+(P_D^2+P_DP_F+P_F^2)+(1-P_F^3)\big]<0\right\} \tag{5.35}$$

$(3,1,0,0)$ is the optimal placement if (P_F, P_D) belongs to the set:

$$\left\{(P_F,P_D)\in[0,1]^2 \;\middle|\; \left((P_D-P_F)\big[-(P_D+P_F)(P_D^2+P_F^2)+(P_D^2+P_DP_F+P_F^2)+(1-P_F^3)\big]\geq 0\right)\right.$$

$$\left.,\left(2(P_D^2-P_F^2)-(P_D-P_F)-(P_D^3-P_F^3)-P_DP_F^2(P_D-P_F)<0\right),\left(P_D^3(1-P_D)<P_F^3(1-P_F)\right)\right\}$$

$$\bigcup\left\{(P_F,P_D)\in[0,1]^2 \;\middle|\; \left((P_D+P_F-1)^2>P_DP_F(1-P_F)\right),\left(P_D^3(1-P_D)\geq P_F^3(1-P_F)\right),\right.$$

$$\left.\left(P_D^2(1-P_D)<P_F^2(1-P_F)\right)\right\} \tag{5.36}$$

$(2,2,0,0)$ is the optimal placement if (P_F, P_D) belongs to the set:

$$\left\{(P_F,P_D)\in[0,1]^2 \;\middle|\; \left((P_D^2-P_F^2)(2-P_D^2-2P_F^2)\geq 0\right),\left(2(P_D^2-P_F^2)-(P_D-P_F)-\right.\right.$$

$$\left.\left.(P_D^3-P_F^3)-P_DP_F^2(P_D-P_F)\geq 0\right),\left(2(P_D-P_F)+2P_F^3(1-P_F)-P_DP_F^2(1-P_F)-\right.\right.$$

$$P_D P_F^2(1-P_D) - (P_D^2 - P_F^2) - P_F(P_D - P_F) \leq 0\Bigg), \Bigg(P_D^3(1-P_D) < P_F^3(1-P_F)\Bigg)\Bigg\}$$

$$\bigcup \Bigg\{(P_F, P_D) \in [0,1]^2 \;\Bigg|\; \Bigg(2(1-P_F) < P_D\Bigg), \Bigg((P_D + P_F - 1)^2 \leq P_D P_F(1-P_F)\Bigg),$$

$$\Bigg(P_D^3(1-P_D) \geq P_F^3(1-P_F)\Bigg)\Bigg\} \tag{5.37}$$

$(2,1,1,0)$ is the optimal placement if (P_F, P_D) belongs to the set:

$$\Bigg\{(P_F, P_D) \in [0,1]^2 \;\Bigg|\; 2(1-P_F) \geq P_D\Bigg\} \tag{5.38}$$

For $P_D = P_F$, all the placements have the same probability of error and therefore we choose either the highest placement in the majorization-based partial order to be the optimal placement or select other higher placements which preserve the statement of this proposition.

Using (5.35), (5.36), (5.37), and (5.38), for $P_D > P_F$, and the aforementioned placement policy at the boundary, $P_D = P_F$, we observe that by fixing P_D in the interval $[0, \frac{2}{3}]$ and by increasing P_F, from 0 to P_D, the optimal placement will be $(2,1,1,0)$. For P_D fixed in the interval $(\frac{2}{3}, \frac{373}{539}]$ and by increasing P_F from 0 to P_D, the optimal placement will start as the $(2,1,1,0)$ placement and will then switch over to the $(2,2,0,0)$ placement. For P_D fixed in the interval $(\frac{373}{539}, \frac{947}{1093}]$ and by increasing P_F from 0 to P_D, the optimal placement will start as the $(2,1,1,0)$ placement, switch over to the $(2,2,0,0)$ placement, and will end up as the $(3,1,0,0)$ placement. Finally for P_D fixed in the interval $(\frac{947}{1093}, 1]$ and for P_F increased from 0 to P_D, the optimal placement will start as the $(2,1,1,0)$ placement, then switch over to the $(2,2,0,0)$ placement first and then to the $(3,1,0,0)$ placement,

and finally end up as the $(4,0,0,0)$ placement. This implies that for the sensor-placement point pair $(N,M) = (4,4)$ for fixed P_D, increasing P_F leads to optimal placements that are higher in the majorization-based partial order.

Similarly, from equations (5.35), (5.36), (5.37), and (5.38) it can be shown that for fixed P_F, increasing P_D leads to placements that are higher in the majorization-based partial order.

We present a plot of (5.35), (5.36), (5.37), and (5.38) on the (P_F, P_D) plane in Section 5.4 which further validates the statement of this proposition for the case $M = N = 4$. Other cases where $N \leq 6$ can be proved similarly by using equation (5.6). □

For $N > 6$ the aforementioned result does not necessarily hold. Consider the case where $(N,M) = (7,8)$. Clearly $(3,2,1,1,0,0,0) \succ (2,2,2,1,0,0,0)$, so $(3,2,1,1,0,0,0)$ is at a higher level than $(2,2,2,1,0,0,0)$ on the majorization-based partial order for this problem. Using equation (5.6) we get $(3,2,1,1,0,0,0)$ as the optimal placement for $(P_F, P_D) = (0.46, 0.6)$ whereas $(2,2,2,1,0,0,0)$ is the optimal placement for $(P_F, P_D) = (0.48, 0.6)$. Therefore for fixed P_D and $N > 6$, increasing P_F does not necessarily result in the optimal placement being higher on the majorization-based partial order. Also for $(P_F, P_D) = (0.48, 0.5)$ the placement $(3,2,1,1,0,0,0)$ is strictly optimal whereas $(2,2,2,1,0,0,0)$ is the strictly optimal placement for $(P_F, P_D) = (0.48, 0.6)$. Therefore, we can conclude that for fixed P_F and $N > 6$, increasing P_D does not necessarily result in the optimal placement being higher on the majorization-based partial order and vice versa for fixed P_D and increasing P_F. This counterexample clearly shows that this result does not necessarily hold for $N > 6$.

It should be noted that we are considering a partial ordering and therefore not all elements of Λ^N can be placed on a majorization-based partial order. There can be many sets of optimal placements dependent on what we choose as the optimal placement at points where no placement is strictly optimal. For a given (N,M), an important question is the existence of a set of optimal placements which can be placed on a majorization-based partial order. The following conjecture addresses this question:

Conjecture 5.3: For any (N,M) there exists a set of optimal placements, $\mathscr{O}^N = \{(v_1,....,v_M)|(v_1,....,v_N) \subseteq \Lambda^N, (v_{N+1},...,v_M) = (0,...,0)\}$, on the (P_F,P_D) plane which can be placed on a majorization-based partial order.

We explain the intuition behind this conjecture by considering the sensor-placement pair, $(N,M) = (6,6)$, which has Λ^N of size $|\Lambda^N| = 11$. Note that the placements $(4,1,1)$ and $(3,3)$ are not comparable with respect to a majorization ordering. Similarly $(3,1,1,1)$ and $(2,2,2)$ are not comparable. The conjecture would be false if every set of optimal placements contained both $(4,1,1)$ and $(3,3)$ or contained both $(3,1,1,1)$ and $(2,2,2)$. $\{(6,0),(5,1),(4,2),(3,2,1),(2,2,1,1),(2,1,1,1,1)\}$ is a set of optimal placements for this case. It should be noted that for high values of P_F, $P_D \geq P_F$, the optimal placements tend to have a large number of sensors placed at a small number of points (concentrated placement) and for low values of P_F the optimal placements tend to have a small number of sensors placed at a large number of points (spread out placement). In this case the placements $(4,2),(3,2,1)$, and $(2,2,1,1)$ are optimal in the regions where one would have naturally expected the placements $(3,1,1,1),(2,2,2),(4,1,1)$, and $(3,3)$ to be optimal. The aforementioned example indicates existence of the following properties of non-comparable placements which form the basis of this conjecture:

- Placements containing sensors concentrated at few points but not enough to outperform other placements, for higher values of P_F, which are highly concentrated and can be placed on a majorization-based partial order.

- Placements containing sensors that are relatively spread out but not enough to outperform other placements, for lower values of P_F, which have a higher spread of sensors and can be placed on a majorization-based partial order.

- Placements not possessing a fine balance between concentration and spread of sensors to be optimal for values of P_F that are neither high nor low.

5.4 Simulations

We present two examples in this section that further illustrate the statements of the theorems and propositions of Section 5.2 and Section 5.3.

Example 5.4.1: $\mathbf{N = 4}$

Let $(N,M) = (4,4)$, $P_D > P_F$. A (P_F, P_D) plane using a set of optimal placements is given in Fig. 5.1. The arrows are used to represent the regions, on the (P_F, P_D) plane, in which a particular placement is optimal. In Fig. 5.1 we observe that uniform placement is not strictly optimal. Fig. 5.1 clearly shows that for fixed P_D, increasing P_F leads to optimal placements that are higher on the majorization-based partial order which is given by (5.34). Similarly for fixed P_F, increasing P_D leads to optimal placements that are higher on the majorization-based partial order given by (5.34).

Now consider $(N,M) = (4,5)$, $P_D > P_F$. A (P_F, P_D) plane using a set of optimal placements is given in Fig. 5.2. In Fig. 5.2, we observe that uniform placement is strictly

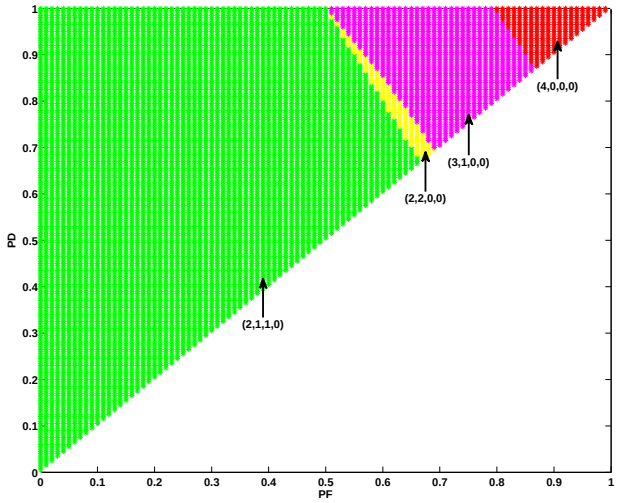

Figure 5.1: Optimal Placement Structure over (P_F, P_D) for $(N,M) = (4,4)$

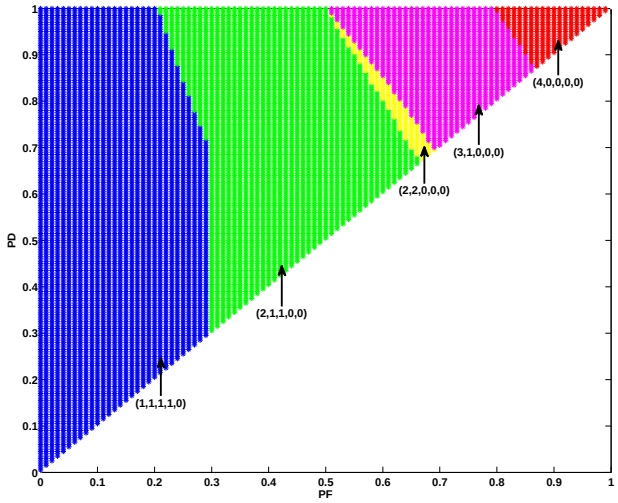

Figure 5.2: Optimal Placement Structure over (P_F, P_D) for $(N,M) = (4,5)$

optimal along with the set of optimal placements for the case $(N,M) = (4,4)$. This was previously prescribed by Corollary 5.2 and this example provide a practical validation.

Example 5.4.2: **N = 5**

Consider the case $(N,M) = (5,6)$, $P_D > P_F$. A (P_F, P_D) plane using a set of optimal placements for this case is given in Fig. 5.3. It is observed that by fixing either P_D or P_F, increasing the other parameter leads to optimal placements that are higher on the majorization based partial order: $(5,0) \succ (4,1) \succ (3,2) \succ (2,2,1) \succ (2,1,1,1) \succ (1,1,1,1,1)$. It

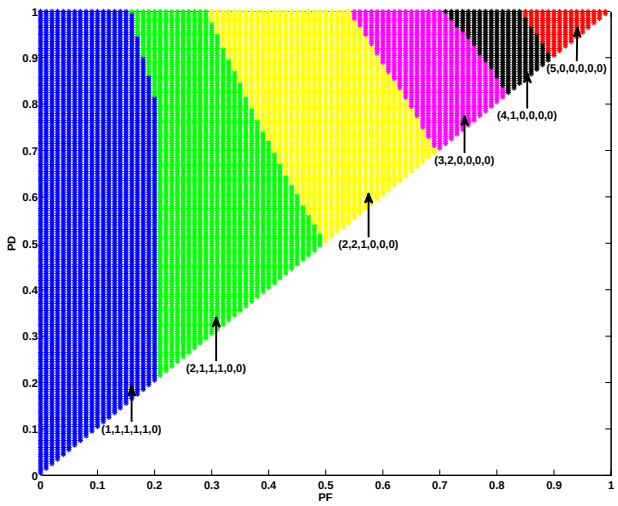

Figure 5.3: Optimal Placement Structure over (P_F, P_D) for $(N, M) = (5, 6)$

should also be noted that uniform placement is strictly optimal in this case. These simulations verify the statements of the results and signify their practical importance as outlined in Section 5.2 and Section 5.3.

Chapter 6: Conclusions and Future Research Directions

6.1 Conclusions

In Chapter 2, several security constraints have been incorporated in the control synthesis of a linear quadratic optimal control problem. The resulting optimization problems have been shown to be convex. Lagrangian duality techniques have been used to compute and characterize the optimal solutions and their properties. The optimal solution is shown to be affine for the case when the terminal state has a continuous distribution. Utilizing the standard optimization software cvx, we have computed the optimal control sequences and have also validated the results via numerical simulations.

In Chapter 3, several team decision problems under security constraints have been considered. We have analyzed the case where the respective terminal states of both systems are assumed to be identical. This problem is solved by utilizing the generalized Kuhn Tucker theorem along with some regularity conditions. The structure of this problem is similar to the security problems considered in Chapter 2 and the similar techniques are utilized to compute the optimal solutions. We have also considered the general case where the terminal states of the decision makers are correlated. A generalized security metric is utilized to introduce the security constraints. The resulting infinite dimensional optimization problems have been shown to be convex. Utilizing the Kuhn Tucker Theo-

rem in conjunction with some standard assumptions and regularity conditions the unique optimal solution is shown to be affine in the information available to the respective decision makers.

In Chapter 4, We have introduced techniques from classical statistical learning theory to develop several formulations of the SRHC problem. Pollard dimension for the quadratic cost functions affiliated with the SRHC problem has been computed. Sample size bounds are provided which enable us to compute several notions of near minimum to the optimal solution. The problem framework has also been extended to incorporate model uncertainity and related notions of near minimax values and affiliated performance bounds have also been provided. These results have important applications due to their efficiency and ease of implementation. Given mechanisms for random generation of control and noise samples, the randomized algorithm based solution methodology presented in this chapter efficiently handles both convex and non-convex problems.

In Chapter 5, the problem has been formulated using a Bayesian M-ary hypothesis testing framework. We have characterized several placement principles for sensors tasked with detecting the location of a randomly placed intruder. In particular, notions from Majorization Theory, such as majorization-based partial orders, have been used to formalize important sensor placement properties. The uniform placement of sensors has been thoroughly analyzed, resulting in conditions under which uniform placement is not strictly optimal. In addition, changes in the optimal placement structure due to a variation in the number of placement points and local sensor parameters have been analyzed and related design principles have been presented.

6.2 Future Research Directions

6.2.1 Linear Quadratic Control Under Security Constraints

For optimal control problems, subjected to security constraints, one future research direction is to incorporate additive disturbances in the problem framework. This results in a more general formulation of these problems and is considerably harder to tackle. It shouled be noted that when the dynamical system is subjected to additive disturbances then convergence of the state trajectories to a particular point cannot be guaranteed. However, the problem can be reformulated by requiring convergence to a norm ball around a particular terminal state value. The cost function can also be reformulated by penalizing the difference between the actual terminal state that the system attains as compared to the required terminal state. It should be noted that with the incorporation of additive disturbance the optimization needs to be performed over a space of control policies rather then control sequences. If control sequences are to be used instead of control policies then the effects of disturbances would be unaccounted for and would lead to stability issues and poor performance. New security metrics can also be designed and a performance analysis can be done for different metrics within this framework. Computing the optimal solutions for this extended framework are interesting future research problems. Dynamic programming, the Maximum Principle, and other optimization techniques could be utilized to compute a solution for these problems.

Another future research direction is to consider different measurement frameworks for the adversary. One suggestion is to consider the case when the adversary gets a fixed

number of random measurements of the state trajectory rather than the first k measurements. If the adversary is allowed to incorporate different measurement frameworks then the problem can also be formulated by utilizing techniques from non cooperative game theory.

6.2.2 Team Decision Theory Under Security Constraints

For team problems one interesting extension is to consider the case when both decision makers only have access to their own terminal states but do not have knowledge of the terminal state of the other decision maker. The terminal states can be assumed to be correlated in the sense that they have the same mean but different variances. A similar security metric to the one utilized in Chapter 3 can also be used to enforce the security constraints in this case. However, this is a challenging problem and requires a different problem formulation. It would be interesting to compare the solution of this problem to the team problems solved in Chapter 3. Techniques like the generalized Kuhn Tucker Theorem and results from team decision theory like Radner's theorem could be utilized to compute a solution to this problem.

6.2.3 Optimal Sensor Placement for Intruder Detection

One research direction to pursue in problems of optimal sensor placement is to consider the dynamic version of the problem stated in Chapter 5. Instead of just placing the sensors once we can consider the case of redeploying the sensors at each time step and using their reported measurements to track the intruder. The sensor placements and

reported measurements in the previous time steps can be utilized to update the optimal sensor placements. The intruder can be assumed to be either static, as was done in Chapter 5, or dynamic in the sense that it changes its position at each step. Techniques from dynamic programming can be utilized to obtain a solution to these problems. We also assumed a uniform prior distribution for the problem framework in Chapter 5. An interesting extension is to consider other prior distributions for the location of the intruder. It would be interesting to pursue these extensions and to develop some generalized sensor placement and detection principles for these problems.

Bibliography

[1] Dept of Homeland Security, "Industrial control systems subject to 200 attacks in 2012", *Homeland Security News Wire*, Jan 14, 2013.
http://www.homelandsecuritynewswire.com/dr20130114-dhs-industrial-control-systems-subject-to-200-attacks-in-2012

[2] R. Lemos, "Industrial Control Systems Faced Nearly 200 Attacks: DHS", *Eweek*, Jan 3, 2013.
http://www.eweek.com/security/industrial-control-systems-faced-nearly-200-attacks-dhs/

[3] K. Dilanian, "Cyber-attacks a bigger threat than Al Qaeda, officials say", *Los Angeles Times*, March 12, 2013.
http://www.latimes.com/news/nationworld/world/la-fg-worldwide-threats-20130313,0,3374690.story

[4] D. Klobucher, "U.S. Prepares Counterstrike Against Cyber-Attack", *Forbes*, March 15, 2013.
http://www.forbes.com/sites/sap/2013/03/15/u-s-prepares-counterstrike-against-cyber-attack/

[5] R. Beheti, H. Gill, "Cyber Physical Systems", *The Impact of Control Technology*, IEECSS, 2011.

[6] A. Cardenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," *Proceedings of the 3rd Conference on Hot Topics in Security*, 2008.

[7] A. Cardenas, S. Amin, and S. Sastry, "Secure Control: Towards survivable cyber-physical systems," *28th International Conference Distributed Computing Systems Workshops*, 2008, pp. 495-500.

[8] Y. Mo, T. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-Physical Security of a Smart Grid Infrastructure", *Proceedings of the IEEE Special Issue on Cyber-Physical Systems*, Vol. 100, 2012, pp. 195-209.

[9] A. Gupta, C. Langbort, and T. Basar, "Optimal Control in the presence of an intelligent jammer with limited actions," *49th IEEE Conference on Decision and Control*, 2010, pp. 1096-1101.

[10] Y. Mo, and B. Sinopli, "False Data Injection Attacks in Control Systems", *1st Workshop on Secure Control Systems*, 2010.

[11] H. Fawzi, P. Tabuada, and S. Diggavi, "Security of control systems under sensors and actuator attacks", *51st IEEE Conference on Decision and Control*, 2012, pp. 3412-3417.

[12] Q. Zhu, L. Bushnell, and T. Basar, "Game Theoretic Analysis of Node Capture and Cloning Attack with Multiple Attackers in Wireless Sensor Networks", *51st IEEE Conference on Decision and Control*, 2012, pp. 3404-3411.

[13] F. Pasqualetti, F. Dorfler, and F. Bullo, "Cyber-Physical Security via Geomtric Control: Distributed Monitoring and Mailicious Attacks", *51st IEEE Conference on Decision and Control*, 2012.

[14] V. Poor, *An Introduction to Signal Detection and Estimation*, Springer, 2nd ed, 1994.

[15] M. Grant and S. Boyd, *"CVX: Matlab software for disciplined convex programming"*, http://stanford.edu/boyd/cvx, 2000.

[16] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, New York, 2004.

[17] P. Bickel and K. Doksum, *Mathematical Statistics: Basic Ideas and Selected Topics*, Vol 1, Pearson Prentice Hall, 2nd ed, 2007.

[18] D. Luenberger, *Optimization by Vector Space Methods*, Wiley, 1969.

[19] J. Marshak, "Elements for a theory of teams", *Management Science*, Vol. 1, pp. 127-137, 1955.

[20] R. Radner, "Team Decision Theory", *Annals of Mathematical Statistics*, Vol. 33, pp. 857-881, 1962.

[21] R. Radner and J. Marshak, *Economic Theory of Teams*, University Press, New Haven CT, 1972.

[22] J. C. Krainak, J. L. Speyer, and S. I. Marcus, "Static Team Problems - Part I: Sufficient Conditions and the Exponential Cost Criterion", *IEEE Transactions on Automatic Control*, Vol. 27, No. 4, pp. 839-848, 1982.

[23] Y. C. Ho and K. Chu, "Team Decision Theory and Information Structures in Optimal Control Problems-Part I", *IEEE Transactions of Automatic Control*, Vol. 17, No. 1, pp. 15-22, 1972.

[24] A. Gattami, "Multi-Objective Linear Quadratic Team Optimization", Arxiv Technical Report, 2012, http://arxiv.org/abs/1209.2551

[25] D. Q. Mayne, J. B. Rwalings, C. V. Rao, and P. O. M. Scokaert, "Constrained Model Predictive Control: Stability and optimality", *Automatica*, vol. 36, pp. 789-814, 2000.

[26] W. H. Kwon, S. Han, *"Receding Horizon Control: Model Predictive Control for State Space Models"*, Springer, London, 2005.

[27] J. A. Primbs, C. H. Sung, "Stochastic Receding Horizon Control of Constrained Linear Systems with State and Control Multiplicative Noise", *IEEE Trans. Autom. Control*, vol. 44, no. 2, pp. 221-230, Feb. 2009.

[28] D. M. Pena, A. Bemporad, and T. Alamo, "Stochastic Programming Applied to Model Predictive Control", *in Proc. Conf. Decision Control*, 2005, pp. 1361-1366.

[29] P. Hokayem, D. Chatterjee, and J. Lygeros, "On Stochastic Receding Horizon Control with Bounded Control Inputs", *in Proc. Conf. Decision Control*, 2009, pp. 6359-6364.

[30] D. Chatterjee, P. Hokayem, and J. Lygeros, "Stochastic Receding Horizon Control With Bounded Control Inputs: A Vector Space Approach", *IEEE Trans. Autom. Control*, vol. 56, no. 11, pp. 2704-2710, 2011.

[31] R. Motwani, P. Raghavan, *"Randomized Algorithms"*, Cambridge University Press, New York, 1995.

[32] M. Vidyasagar, "Randomized Algorithms for robust controller synthesis using statistical learning theory", *Automatica*, vol. 37, pp. 1515-1528, 2001.

[33] R. Tempo, G. Calafiore, and F. Dabbene, *"Randomized Algorithms for Analysis and Control of Uncertain Systems"*, Springer, London, 2010.

[34] G. C. Calafiore, L. Fagiano, "Robust Model Predictive Control via Random Convex Programming", *in Proc. Conf. Decision Control*, pp. 1910-1915, 2011.

[35] I. Batina, "Model Predictive Control for stochastic systems by randomized algorithms", *PhD dissertation*, Technische Universiteit Eindhoven, 2004.

[36] P. J. Goulart, E. C. Kerrigan, and J. M. Maciejowski, "Optimization over state feedback policies for robust control with constraints", *Automatica*, vol. 42, pp. 523-533, 2006.

[37] A. Ben-Tal, A. Goryashko, E. Guslitzer, and A. Nemirovski, "Adjustable robust solutions of uncertain linear programs", *Mathematical Programming*, vol. 99, no. 2, pp. 351-376, 2004.

[38] S. J. Gartska, R. J. Wets, "On decision rules in stochastic programming", *Mathematical Programming*, vol. 7, pp. 117-143, 1974.

[39] E. Guslister, "Uncertainty-immunized solutions in linear programming", *Master's Thesis*, Technion, Israeli Institute of Technoloy, 2002.

[40] J. Löfberg, "Approximations of closed-loop MPC", *In Proc. Conf. Decision Control*, pp. 1438-1442, 2003.

[41] D. H. van Hessem, O. H. Bosgra, "A conic reformulation of model predictive control including bounded and stochastic disturbances under state and input constraints", *in Proc. Conf. Decision Control*, pp. 4643-4648, 2011.

[42] H. L. Royden, P. M. Fitzpatrick, *"Real Analysis"*, Prentice Hall, Boston, 2010.

[43] M. Vidyasagar, *"Learning and Generalization: With Applications to Neural Networks"*, Springer, London, 2003.

[44] V. N. Vapnik, *"Statistical Learning Theory"*, Wiley-Interscience, New York, 1998.

[45] D. Pollard, *"Convergence of Stochastic Processes"*, Springer-Verlag, New York, 1984.

[46] M. Karpinski, A. J. Macintyre, "Polynomial bounds for VC dimension of sigmoidal and general Pfaffian neural networks", *J. Comput. Syst. Sci.* vol. 54, pp. 169-176, 1997.

[47] Y. Fujisaki, Y. Kozawa, "Probabilistic Robust Controller Design: Probable Near Minimax Value and Randomized Algorithms", *in Proc. Conf. Decision Control*, pp. 1938-1943, 2003.

[48] J. Tsitsiklis, *"Decentralized Detection,"* in Advances in Signal Processing, vol. 2, H. V. Poor and J. B. Thomas, editors, JAI Press, 1993, pp. 297-344.

[49] J. Chamberland, V. V. Veeravalli, *"Wireless Sensors in Distributed Detection Applications,"* IEEE Signal Processing Magazine, vol. 24, no. 3, May 2007, pp. 16-25.

[50] B. Arnold, *"Majorization: Here, There, and Everywhere,"* Statistical Science, vol. 22, no. 3, 2007, pp. 407-413.

[51] A. Marshall, I. Olkin, *"Inequalities: Theory of Majorization and Its Applications,"* Academic Press, New York, 1979.

[52] G. Lipsa, N. Martins, *"Remote State Estimation with Communication Costs for First-Order LTI Systems,"* IEEE Transactions on Automatic Control, vol. 56, no. 9, Sept 2011.

[53] B. Hajek, K. Mitzel, and S. Yang, *"Paging and Registration in Cellular Networks: Jointly Optimal Policies and an Iterative Algorithm,"* IEEE Transactions on Information Theory, vol. 54, no. 2, Feb 2008, pp. 608-622.

[54] H. Van Trees, *"Detection, Estimation, and Modulation Theory: Part I,"* Wiley-Interscience, New York, 2001.

[55] G. H. Hardy, S. Ramanujan,*"Asymptotic Formulae in Combinatory Analysis,"* Proc. London Math Soc. vol. 17, 1918, pp. 75-115.

[56] W. Malik, N. Martins, and A. Swami, *"Optimal Sensor Placement for Intruder Detection,"* Arxiv Technical Report, Sept 2011, http://arxiv.org/abs/1109.5466