ESTIMATION THEORETIC ANALYSES OF LOCATION SECRECY AND RIS-AIDED LOCALIZATION UNDER HARDWARE IMPAIRMENTS

A DISSERTATION SUBMITTED TO

THE GRADUATE SCHOOL OF ENGINEERING AND SCIENCE

OF BILKENT UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR

THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

ELECTRICAL AND ELECTRONICS ENGINEERING

By

Cüneyd Öztürk

June 2022

Estimation Theoretic Analyses of Location Secrecy and RIS-Aided Localization under Hardware Impairments

By Cüneyd Öztürk

June 2022

We certify that we have read this dissertation and that in our opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of Doctor of Philosophy.

Sinan Gezici (Advisor)

Orhan Arıkan

Tolga Mete Duman

Umut Orguner

Berkan Dülek

Approved for the Graduate School of Engineering and Science:

Ezhan Karaşan
Director of the Graduate School

ABSTRACT

ESTIMATION THEORETIC ANALYSES OF LOCATION SECRECY AND RIS-AIDED LOCALIZATION UNDER HARDWARE IMPAIRMENTS

Cüneyd Öztürk
Ph.D. in Electrical and Electronics Engineering
Advisor: Sinan Gezici
June 2022

In this thesis, we present estimation theoretic analyses of location secrecy and reconfigurable intelligent surface (RIS) aided localization under hardware impairments. First, we consider a wireless source localization network in which a target node emits localization signals that are used by anchor nodes to estimate the target node position. In addition to target and anchor nodes, there can also exist eavesdropper nodes and jammer nodes which aim to estimate the position of the target node and to degrade the accuracy of localization, respectively. We propose the problem of eavesdropper selection with the goal of optimally placing a given number of eavesdropper nodes to a subset of possible positions in the network to estimate the target node position as accurately as possible. As the performance metric, the Cramér-Rao lower bound (CRLB) related to the estimation of the target node position by eavesdropper nodes is derived, and its convexity and monotonicity properties are investigated. By relaxing the integer constraints, the eavesdropper selection problem is approximated by a convex optimization problem and algorithms are proposed for eavesdropper selection. Moreover, in the presence of parameter uncertainty, a robust version of the eavesdropper selection problem is developed. Then, the problem of jammer selection is proposed where the aim is to optimally place a given number of jammer nodes to a subset of possible positions for degrading the localization accuracy of the network as much as possible. A CRLB expression from the literature is used as the performance metric, and its concavity and monotonicity properties are derived. Also, a convex optimization problem and its robust version are derived after relaxation. Moreover, the joint eavesdropper and jammer selection problem is proposed with the goal of placing certain numbers of eavesdropper and jammer nodes to a subset of possible positions. Simulation results are presented to illustrate performance of the proposed algorithms.

Second, a wireless source localization network consisting of synchronized target and anchor nodes is considered. An anchor placement problem is formulated to minimize the CRLB on estimation of target node positions by anchor nodes. It is shown that the anchor placement

problem can be approximated as a minimization problem of the ratio of two supermodular functions. Due to the lack of a polynomial time algorithm for such problems, an *anchor selection* problem is proposed to solve the anchor placement problem. Via relaxation of integer constraints, the anchor selection problem is approximated by a convex optimization problem, which is used to propose two algorithms for anchor selection. Furthermore, extensions to quasi-synchronous wireless localization networks are discussed. To examine the performance of the proposed algorithms, various simulation results are presented.

Third, we investigate the problem of RIS-aided near-field localization of a user equipment (UE) served by a base station (BS) under phase-dependent amplitude variations at each RIS element. Through a misspecified Cramér-Rao bound (MCRB) analysis and a resulting lower bound (LB) on localization, we show that when the UE is unaware of amplitude variations (i.e., assumes unit-amplitude responses), severe performance penalties can arise, especially at high signal-to-noise ratios (SNRs). Leveraging Jacobi-Anger expansion to decouple range-azimuth-elevation dimensions, we develop a low-complexity approximated mismatched maximum likelihood (AMML) estimator, which is asymptotically tight to the LB. To mitigate performance loss due to model mismatch, we propose to jointly estimate the UE location and the RIS amplitude model parameters. The corresponding Cramér-Rao bound (CRB) is derived, as well as an iterative refinement algorithm, which employs the AMML method as a subroutine and alternatingly updates individual parameters of the RIS amplitude model. Simulation results indicate fast convergence and performance close to the CRB. The proposed method can successfully recover the performance loss of the AMML under a wide range of RIS parameters and effectively calibrate the RIS amplitude model online with the help of a user that has an a-priori unknown location.

Fourth, we consider RIS-aided localization scenarios with RIS pixel failures, where individual RIS elements can become faulty due to hardware imperfections. We explore the impact of such failures on the localization performance. To that aim, an MCRB analysis is conducted and numerical results indicate that performance loss for estimating the UE position can be significant in the presence of pixel failures. To remedy this issue, we develop two different diagnosis strategies to determine which pixels are failing, and design robust methods to perform localization in the presence of faulty elements. One strategy is based on the ℓ_1-regularization method, and the second one employs a successive approach. Both methods significantly reduce the performance loss due to pixel failures. The successive one performs very close to the theoretical bounds at high SNRs even though it has a higher computational cost than the ℓ_1-regularization based method.

In the final part of the dissertation, the optimal encoding strategy of a scalar parameter is performed in the presence of jamming based on an estimation theoretic criterion. Namely,

the aim is to obtain the optimal encoding function at the transmitter that minimizes the expectation of the conditional Cramér-Rao bound (ECRB) at the receiver when the jammer has access to the parameter and alters the received signal by sending an encoded version of the parameter. Via calculus of variations, the optimal encoding function at the transmitter is characterized explicitly, and an algorithm is proposed to calculate it. Numerical examples demonstrate benefits of the proposed optimal encoding approach.

Keywords: Anchor placement, calculus of variations, Cramér-Rao lower bound (CRLB), eavesdropping, hardware impairments, jamming, maximum likelihood estimator, misspecified Cramér-Rao bound (MCRB), localization, optimization, parameter estimation, reconfigurable intelligent surfaces (RIS), secrecy.

ÖZET

KONUM GİZLİLİĞİNİN VE DONANIMSAL HATALAR ALTINDA YYAY DESTEKLİ KONUMLANDIRMANIN KESTİRİM KURAMSAL ANALİZLERİ

Cüneyd Öztürk
Elektrik ve Elektronik Mühendisliği, Doktora
Tez Danışmanı: Sinan Gezici
Haziran 2022

Bu tezde, donanımsal hatalar altında yeniden yapılandırılabilir akıllı yüzey (YYAY) destekli konumlandırma ve konum gizliliğinin kestirim kuramsal analizleri sunulmaktadır. İlk olarak, hedef düğümlerinin çapa düğümlerine sinyaller gönderdiği ve çapa düğümlerinin bu sinyalleri kullanarak hedef düğümlerinin konumunu kestirdiği bir kablosuz kaynak konumlandırma ağı düşünülmektedir. Kablosuz kaynak konumlandırma ağlarında, hedef ve çapa düğümlerinin yanı sıra, hedef düğümlerinin konumunu kestirmeye çalışan gizli dinleyici düğümleri ve çapa düğümlerinin konumlandırma performansını düşürmeyi hedefleyen karıştırıcı düğümler de bulunabilir. Gizli dinleyici düğümlerin hedef düğümlerin konumunu olabildiğince doğru bir şekilde kestirmesi için, gizli dinleyici düğümü seçme problemi tanımlanmaktadır. Gizli dinleyici düğümlerinin hedef düğümlerinin konumunu kestirmesiyle alakalı olan Cramér-Rao alt sınırı (CRAS) performans metriği olarak seçilmekte ve bu CRAS'nin gizli dinleyici düğümü seçme vektörüne göre olan dışbükeyliği ve monotonluğu incelenmektedir. Tam sayı kısıtlamaları gevşetildiğinde, gizli dinleyici seçme problemine dışbükey optimizasyon problemi olarak yaklaşılmakta ve bu problemi çözmek için bazı algoritmalar önerilmektedir. Bunun yanı sıra, parametrelerin belirsizliği altında, gizli dinleyici seçme probleminin gürbüz versiyonu geliştirilmektedir. Daha sonra, karıştırıcı düğümlerinin çapa düğümlerinin konumlandırma performansını olabildiğince düşürmesi için karıştırıcı düğümlerini seçme problemi önerilmektedir. Literatürde bulunan bir CRAS ifadesi performans metriği olarak kullanılmakta ve bu ifadenin karıştırıcı düğümü seçme vektörüne göre içbükeyliği ve monotonluğu incelenmektedir. Tam sayı sınırlarının gevşetilmesinden sonra, dışbükey optimizasyon problemi elde edilmekte ve gürbüz versiyonu da çözülmektedir. Ayrıca, gizli dinleyici ve karıştırıcı düğümü seçme problemleri ortak olarak önerilmektedir. Önerilen algoritmaların performanslarını göstermek için benzetim sonuçları sunulmaktadır.

İkinci olarak, senkronize olmuş hedef ve çapa düğümlerini içeren bir kablosuz kaynak konumlandırma ağı düşünülmektedir. Çapa düğümleri tarafından kestirilen hedef düğümlerinin konumu ile alakalı olan CRAS'nin minimize edilmesi için çapa düğümlerinin

yerleştirilmesi problemi formüle edilmektedir. Çapa düğümlerinin yerleştirilmesi problemine iki süper modüler fonksiyonunun birbirine olan oranının minimize edilmesi problemi ile yaklaşılabileceği gösterilmektedir. Bu problemlerin çözümü için polinomsal zamanda algoritma eksikliğinden dolayı, çapa düğümü yerleştirme problemine çapa düğümü seçme problemi olarak yaklaşılmaktadır. Tam sayı kısıtlamaları gevşetildiğinde, çapa düğümü seçme problemine dışbükey optimizasyon problemi olarak yaklaşılmaktadır. Bu problemin çözümü için iki farklı algoritma önerilmektedir. Daha sonra, yarı senkronize olan kablosuz konumlandırma ağları için analizler genişletilmektedir. Önerilen algoritmaların performanslarını incelemek için, benzetim sonuçları sunulmaktadır.

Üçüncü olarak, baz istasyonu servisi ve faza bağlı genlik değişimleri altında, YYAY destekli yakın alanda konumlandırma problemi incelenmektedir. Yanlış tanımlanmış Cramér-Rao sınırı (YTCRS) analizi ve sonucunda konumlandırma ile ilgili çıkan alt sınır (AS) kullanılarak, özellikle yüksek sinyal gürültü oranlarında, genlik değişimlerinin bilinmediği ve genliklerin bire eşit olduğunu varsayıldığında, konumlandırma açısından ciddi performans kayıplarının oluşabileceği gösterilmektedir. Jacobi-Anger açılımı kullanılarak, asimptotik olarak AS ile sıkı olan, düşük karmaşıklığa sahip, yaklaşık yanlış tanımlanmış maksimum olabilirlik (YYTMO) kestiricisi geliştirilmektedir. Modeli yanlış bilmekten kaynaklanan performans kaybını önlemek için, kullanıcının konumu ve YYAY genlik modeli parametreleri beraber kestirilmeye çalışılmaktadır. Buna karşılık gelen Cramér-Rao sınırı (CRS) ve YYAY genlik model parametrelerini dönüşümlü bir biçimde güncelleyen YYTMO kestricisini alt program olarak kullanan yinelemeli bir algoritma elde edilmektedir. Benzetim sonuçlarına göre, bu algoritma hızlı bir şekilde yakınsamaktadır ve performansı CRS'ye yakın çıkmaktadır. Önerilen yöntem geniş bir aralıktaki YYAY parametreleri için YYTMO'nun performans kayıplarını başarılı bir şekilde azaltmaktadır.

Dördüncü olarak, YYAY pikselleri donanımsal kusurlar nedeniyle bozulmalar yaşadığında, YYAY destekli konumlandırma problemleri incelenmektedir. Bu kusurların konumlandırma performansı üzerine etkisi çalışılmaktadır. Bu amaçla, YTCRS analizi yürütülmekte ve benzetim sonuçlarına göre piksel bozulmalarının konumlandırma performansı üzerindeki etkisinin ciddi olabileceği gözlemlenmektedir. Buna çare olmak için, hangi piksellerin bozulduğunu anlamak ve piksel bozulmaları altında gürbüz konumlandırma yöntemleri geliştirmek anacıyla, iki farklı strateji önerilmektedir. İlk strateji ℓ_1-düzenleme metodu tabanlı iken, ikinci strateji ise ardışık bir yaklaşım kullanmaktadır. İki strateji de piksel arızalarından kaynaklanan performans kayıplarını önemli ölçüde düşürmektedir. İkinci strateji, ilk stratejiye göre daha yüksek hesaplama maliyetine sahip olsa da yüksek sinyal gürültü oranlarında kuramsal sınırlara çok yakın performans göstermektedir.

Tezin son kısmında, karıştırıcı varlığı altında, kestirim kuramsal kriter tabanlı skaler

bir parametrenin en iyi kodlama stratejisi incelenmektedir. Bir başka deyişle, karıştırıcı gönderilecek olan skaler parametreye ulaşabildiğinde ve bu parametreyi kodlayıp alıcıdaki sinyali bozabildiğinde, gönderici tarafından kullanılabilecek kodlama fonksiyonları arasından alıcıdaki koşullu CRS'nin ortalamasını minimize edilen kodlama fonksiyonu seçilmektedir. Varyasyonlar hesabı kullanılarak, göndericinin en iyi kodlama fonksiyonu tam olarak karakterize edilmekte ve bu kodlama fonksiyonunu elde etmek için bir algoritma önerilmektedir. Sayısal örnekler önerilen kodlama stratejisinin faydalarını göstermektedir.

Anahtar sözcükler: Çapa yerleşimi, varyasyonlar hesabı, Cramér-Rao alt sınırı (CRAS), gizli dinleyici, donanımsal hatalar, karıştırma, maksimum olabilirlik kestirimi, yanlış tanımlanmış Cramér-Rao sınırı (YTCRS), konumlandırma, optimizasyon, parametre kestirimi, yeniden yapılandıralbilir akıllı yüzeyler (YYAY), gizlilik.

Acknowledgement

I would like to first and foremost thank my advisor Prof. Sinan Gezici. His experience, knowledge and motivation for math was a great inspiration for me. His door was always open and he always gently responded to my spontaneous visits. I will miss those visits and conversations about research and life. It was a pleasure and honor for me to work with him.

Also, I would like to thank my thesis monitoring committee members Prof. Tolga Mete Duman and Prof. Umut Orguner for their support and advices. I am very thankful to Prof. Orhan Arıkan and Prof. Berkan Dülek for agreeing to serve on my dissertation examination committee.

In addition, I would like to thank Dr. Musa Furkan Keskin and Prof. Henk Wymeersch for introducing me reconfigurable intelligent surfaces and invaluable suggestions during our joint studies. I would also like to extend my thanks to Dr. Çağrı Göken as I learned a lot from him about 5G-New Radio.

I am sincerely grateful to all my friends and colleagues for motivating and enjoyable discussions. Finally, I owe my deepest gratitude to my family for their love, continuous support during my PhD studies.

I acknowledge the financial support of the Scientific and Technological Research Council of Turkey (TÜBİTAK) through 2211 Scholarship Program of BİDEB during my PhD studies.

Contents

List of Figures

Chapter 1

Introduction

In wireless localization networks, position information is commonly extracted based on signal exchanges between anchor nodes with known positions and target (source) nodes whose position are to be estimated [1, 2]. Based on the signaling procedure, wireless localization networks are classified into two groups as *self localization* and *source (network-centric) localization* networks [1]. In the self localization scenario, target nodes estimate their positions via signals transmitted from anchor nodes whereas in source localization networks, anchor nodes estimate positions of target nodes from signals emitted by target nodes.

Wireless localization networks can be vulnerable to various attacks such as eavesdropping, jamming, sybil, and wormhole attacks [3–6]. For example, eavesdropper nodes may listen to signals transmitted from target nodes and estimate their positions, which breaches location secrecy [4, 5]. In wireless localization networks, location secrecy cannot be guaranteed via encryption since location related information can be gathered by eavesdropper nodes by just listening to signal exchanges rather than intercepting packets [5]. As another type of attack, jammer nodes can degrade the localization accuracy of a network by transmitting jamming signals [6]. If jamming levels exceed certain limits, location information can be useless for specific applications due to its inaccuracy.

In Chapter 2, the focus is on eavesdropping and jamming attacks in wireless source localization networks. We investigate the optimal eavesdropper and jammer selection strategies

in wireless localization networks in order to quantify the adverserial capabilities of eavesdropper and jammer nodes. Where to locate anchor nodes for achieving high localization accuracy is another crucial issue in wireless localization networks. In Chapter 3, the problem of anchor placement for TOA based wireless localization networks is considered.

Moreover, among the envisioned technological enablers for 6G, three stand out as being truly disruptive: the transition from 30 GHz to beyond 100 GHz (the so-called higher mmWave and lower THz bands) [7–9], the convergence of communication, localization, and sensing (referred to as integrated sensing and communication (ISAC) or integrated sensing, localization, and communication (ISLAC)) [10–14], and the introduction of reconfigurable intelligent surfaces (RISs) [15–17]. RISs can enhance the localization performance. In Chapter 4, the problem of RIS-aided localization under imperfect knowledge of RIS amplitudes is considered. Furthermore, due to its hardware characteristics, RIS elements can fail [18, 19]. In Chapter 5, we examine how these failures can affect localization accuracy.

Furthermore, communication systems can be vulnerable to various types of malicious attacks such as eavesdropping and jamming [20] (and references therein). While eavesdroppers aim to infer messages between transmitters and receivers, jammers try to disrupt communications among devices in a given network. In Chapter 6, in the presence of a jammer, the optimal encoding of a scalar parameter is examined. In the following sections, we provide a literature review and summarize our main contributions.

1.1 Eavesdropper and Jammer Selection Strategies in Wireless Localization Networks

1.1.1 Literature Review

In the literature, there exist a few studies related to physical-layer location secrecy or eavesdropping in wireless localization networks [4, 5, 21]. In [4], a location secrecy metric (LSM) is proposed by considering only the position of a target node and the measurement model of an eavesdropper node. The aim of the eavesdropper node is to obtain an estimate of the

target node position based on its measurement model, where the estimate can be either a point or a set of points. The definition of the LSM is based on the escaping probability of the target node from the eavesdropper node, i.e., the probability that the position of the target node is not an element of the set of estimated positions by the eavesdropper node. In practice, the measurement model of an eavesdropper node depends on several parameters in addition to the position of the target node [21]. For example, an eavesdropper node can extract location information based on signal exchanges between target and anchor nodes by using time difference of arrival (TDOA) approaches. In that case, the time offset becomes another unknown parameter. Hence, the definition of the LSM is extended in [21] by also taking channel conditions and time offsets into account. For some specific scenarios, LSM is calculated and algorithms are proposed to protect location secrecy by diminishing the estimation capability of an eavesdropper node [21]. In [5], considering round-trip-measurements in a network, an eavesdropping model is presented by using TDOA approaches. Also, power allocation frameworks for anchor and target nodes are presented to degrade the estimation performance of an eavesdropper node while maintaining the localization accuracy of the network [5].

Related to jamming and anti-jamming techniques in wireless localization networks, a great amount of research has been conducted in the literature [6, 22–35]. Placement of jammer nodes in wireless localization networks can serve for different purposes [23]. Namely, the aim of placing jammer nodes can be either to reduce the localization accuracy of the network (i.e., adversarial) [6, 24, 25, 35, 36], or to protect the network from eavesdropper attacks [22, 26–31, 33]. In [6], optimal power allocation schemes are developed for jammer nodes under peak and total power limits by maximizing the average or minimum Cramér-Rao lower bounds (CRLBs) in self localization networks. The same problem is considered in [25] for source localization networks. In [35], the average CRLB of target nodes is maximized while keeping their minimum CRLB above a certain threshold for self-localization networks. In [6, 25, 35], it is assumed that positions and the number of jammer nodes are fixed. When positions of jammer nodes can be changed, their optimal placement can be considered for achieving the best jamming performance. In [24], the optimal jammer placement problem is investigated for wireless self-localization networks in the presence of constraints on possible locations of jammer nodes. On the other hand, in [33], jammer nodes are placed to reduce the received signal quality of eavesdropper nodes while not preventing the operation of the

actual network.

Game theoretic approaches are also utilized for determining jamming strategies [23,34]. In [23], an attacker tries to maximize the damage on network activity while the aim of a defender is to secure a multi-hop multi-channel network. The action of the attacker is determined by the selection of jammer node positions and a channel hopping strategy whereas the action of the defender is based on the channel hopping strategy. In [34], two different power control games between anchor nodes and jammer nodes are formulated for self-localization networks based on the average CRLB and the worst-case CRLB criteria. Nash equilibria of the proposed games are analyzed and it is shown that both games have at least one pure-strategy Nash equilibrium.

In the literature, eavesdropping and jamming attacks have not been considered jointly for wireless localization networks. However, for communications networks, [37–39] investigate effects of jamming and eavesdropping together. In [37], a secure transmission scheme is proposed for a wiretap channel when a source communicates with a legitimate unmanned aerial vehicle (UAV) in the presence of eavesdroppers. Full duplex active eavesdropping is assumed, i.e., wiretappers can perform eavesdropping and jamming simultaneously. In [38], a multiple-input multiple-output communication system with a transmitter, a receiver and an adversarial wiretapper is considered. The wiretapper is able to act as either an eavesdropper or a jammer. The transmitter makes a decision between allocating all the power to information signals or broadcasting some artificial interference signals to jam the wiretapper. A game theoretic formulation of this problem is also given in [38], and its Nash equilibria are analyzed. In [39], the considered wireless network contains wireless users, relay stations, base station (BS), and an attacker who has the ability to act as an eavesdropper and as a jammer. The aim of the attacker is to degrade the secrecy rate of the network and the transmission rate of the users. Each user connects to one of the relay stations so that the amount of potential interference from other users is reduced and the expected level of security for the transmission is increased. This problem is formulated as an $(N+1)$ person noncooperative game where N is the number of users and existence of mixed-strategy Nash equilibria is shown.

Although a location secrecy metric is developed in [4, 21] and the problem of protecting location secrecy is investigated in [5], there exist no studies that consider the problem of

eavesdropper selection. In Chapter 2, we propose the eavesdropper selection problem, in which the aim is to optimally place a given number of eavesdropper nodes to a subset of possible positions such that the location secrecy of target nodes is reduced as much as possible. The optimal eavesdropper selection problem is studied from the perspective of eavesdropper nodes for determining performance limits of eavesdropping. The CRLB for estimation of target node positions by eavesdroppers is employed as the performance metric. The eavesdropper selection problem also carries similarities to the anchor placement problem (e.g., [40–43]), in which the aim is to determine the optimal positions of anchor (reference) nodes for optimizing accuracy of target localization. While the optimization is performed over positions of anchor nodes in the anchor placement problem, the aim is to choose the best positions from a finite set of possible positions in the eavesdropper selection problem. (Hence, different theoretical approaches are utilized in Chapter 2.)

In addition, even though jamming and anti-jamming strategies are investigated extensively under various scenarios in [6,22–35], there has been no consideration about *jammer selection*. In Chapter 2, we propose the jammer selection problem. The goal is to place a given number of jammer nodes to a subset of possible positions to degrade the localization accuracy of a wireless network where the CRLB related to estimation of target node positions by anchor nodes is used as the performance metric.

Moreover, despite the work in [37–39], which consider both jamming and eavesdropping for wireless communication networks based on performance metrics such as outage probability, transmission rate and secrecy rate, the presence of jammer and eavesdropper nodes together has not been investigated for wireless localization networks. In Chapter 2, we focus on a wireless localization network with multiple eavesdropper and jammer nodes, and formulate the *joint eavesdropper and jammer selection* problem by employing the CRLB as an estimation theoretic performance metric. The goal is to place certain numbers of eavesdropper and jammer nodes to a subset of possible positions in order to degrade the accuracy of the localization network while keeping the eavesdropping capability above a threshold. In particular, eavesdropper nodes aim to minimize the average CRLB related to their estimation of target node positions whereas jammer nodes seek to maximize the average CRLB for estimating target node positions by anchor nodes via emitting noise signals.

1.1.2 Contributions

In Chapter 2, eavesdropper and jammer selection strategies in wireless localization networks are investigated [44, 45]. The main contributions of this chapter can be specified as follows:

- We formulate the eavesdropper selection, jammer selection, and joint eavesdropper and jammer selection problems in a wireless source localization network for the first time in the literature.
- For the eavesdropper selection problem, a novel CRLB expression (used as a performance metric for location secrecy) is derived related to the estimation of target node positions by eavesdropper nodes.
- We prove that the CRLB expression derived for the eavesdropper selection problem is convex and non-increasing with respect to the selection vector, which specifies the selection of positions for placing eavesdropper nodes.
- For the jammer selection problem, we utilize a CRLB expression from the literature and prove that it is concave and non-decreasing with respect to the selection vector.
- We express the eavesdropper selection, jammer selection, and joint eavesdropper and jammer selection problems as convex optimization problems after relaxation.
- We propose algorithms to solve the proposed problems by considering both perfect and imperfect knowledge of system parameters, and develop robust approaches in the presence of imperfect knowledge.

1.2 Anchor Placement in TOA based Wireless Localization Networks via Convex Relaxation

1.2.1 Literature Review

For both self localization and source localization networks, the main goal is to maintain high localization accuracy [1]. Determining where to place anchor nodes and how to allocate power among them are crucial issues to address for achieving high localization accuracy. There exist a vast amount of studies on these issues such as [40, 42, 46–53]. For example, in [49], anchor positions are assumed to be known, and optimization problems for optimal power allocation among anchor nodes, anchor selection, and anchor deployment are proposed to minimize the estimation error for target position considering a time-of-arrival (TOA) based approach. The problem of anchor placement is also investigated in [42], and a near-optimal node placement algorithm is proposed. In addition to anchor and target nodes, assisting nodes are placed in the network to improve localization accuracy, and an upper bound on the gap between the near-optimal node placement algorithm and the optimal placement strategy is provided [42]. Apart from the TOA based approach, there also exist some studies that consider the optimal anchor placement problem for time-difference-of-arrival (TDOA) and angle-of-arrival (AOA) based wireless localization networks [40, 53].

1.2.2 Contributions

In Chapter 3, we consider a wireless source localization network consisting of anchor and target nodes, and propose an *anchor selection* problem to solve the anchor placement problem [43]. The main contributions of this chapter can be summarized as follows:

- We formulate the anchor placement problem for TOA based source localization networks by considering the Cramér-Rao lower bound (CRLB) as a performance metric, and we discretize the problem due to its non-convexity.

- After discretization, we prove the equivalence of this problem to the problem of minimizing the ratio of two supermodular functions. Due to the lack of a polynomial time algorithm for such problems [54], we express the resulting problem as an anchor selection problem.

- Even though the problem of anchor selection is considered in [49], its convexity properties are not investigated and specific algorithms are not proposed to solve it. We prove that the objective function of this problem is convex with respect to the anchor selection vector. After relaxing the integer constraints, we come up with a convex optimization problem, which is related to the solution of the anchor selection problem.

- We propose two algorithms to solve the proposed anchor selection problem and present simulation results for both two and three dimensional wireless localization networks.

- We also show that this analysis can easily be extended to TDOA and received signal strength (RSS) based wireless localization networks.

1.3 RIS-aided Near-Field Localization under Phase-Dependent Amplitude Variations

1.3.1 Literature Review

RISs are large passive metasurfaces, comprising arrays of programmable reflective unit cells, and have the ability to shape the propagation environment by judiciously adjusting the phase shifts at each reflecting element, thus locally boosting the signal-to-noise ratio (SNR) to improve communication quality [55–58]. This is especially relevant in beyond 100 GHz to overcome sudden drops in rate caused by temporary blockage of the line-of-sight (LoS) path [57, 59]. In order to provide enhanced performance in downlink single- and multi-user systems, passive reflect beamforming at the RIS can be optimized, potentially together with active beamforming at the base station (BS), to maximize energy efficiency [58, 60], sum-rate [61–63] and mutual information [64], as well as to minimize total transmit power at the BS [65, 66].

In parallel with the benefits for communications, RISs can similarly improve localization performance [67]. Stronger even, RISs with known position and orientation enjoy the ability to enable localization in scenarios where it would otherwise be impossible [68]. In this respect, the large aperture of the RIS has several interesting properties. First of all, the SNR-boosting provides accurate delay measurements when wideband signals are used [8, 69]. Secondly, the large number of elements provides high resolution in angle-of-arrival (AoA) (for uplink localization) or angle-of-departure (AoD) (for downlink localization) [8]. Third, when the user equipment (UE) is close to the RIS (in the sense that the distance to the RIS is of similar order as the physical size of the RIS), wavefront curvature effects (so-called geometric near-field) can be harnessed to localize the user [59, 67, 70–74], even when the LoS path between the BS and UE is blocked, irrespective of whether wideband or narrowband signals are used. Moreover, closed-form RIS phase profile designs taking into account the spherical wavefront can be employed to improve localization accuracy under near-field conditions [69, 75]. As a step further, joint benefits in ISLAC applications can be reaped via RIS phase profile adjustment by simultaneous optimization of localization and communications metrics [76].

In ISLAC scenarios, critical to the effective utilization of RIS is the control of individual RIS elements, commonly through phase shifters, which provide element-by-element control with a certain resolution and allow coherent combination of paths to/from the RIS [56, 63]. For localization, in contrast to communication, the receiver should be equipped with the knowledge of the RIS phase profiles to apply suitable high-accuracy processing methods [17]. The ability to modulate the RIS phase profiles brings additional benefits, such as separating the controlled and uncontrolled multipath through temporal coding [77]. Hence, the ability to control the RIS in a precise and known manner is essential for ISLAC applications, which necessitates the availability of accurate and simple RIS phase control models. Such models should ideally account for the per-element response [78], the finite quantization of the control [56, 79], mutual coupling [80], calibration effects, and power losses. Most studies on RIS localization have considered ideal phase shifters (e.g. [59, 68–71, 73, 81]), omitting the listed impairments. How these proposed localization approaches fare under these impairments is both unknown and important.

1.3.2 Contributions

In Chapter 4, a RIS-aided near-field localization problem is analyzed when the amplitude information of the RIS elements is imperfect [82, 83]. The main contributions and novelty of this chapter can be summarized as follows:

- MCRB Analysis of Near-Field Localization under RIS Non-Idealities: Employing the misspecified Cramér-Rao bound (MCRB) [84, 85] as a tool to assess the accuracy loss under model mismatch, we provide a simple expression to find the *pseudo-true parameter* for the considered scenario and derive the MCRB of the pseudo-true parameter and the lower bound (LB) of the true parameter. The MCRB analysis over a wide range of RIS model parameters reveals an order-of-magnitude localization performance degradation due to model misspecification at high SNRs, both in terms of the LB and the mismatched maximum-likelihood (MML) estimator [85]. In contrast, when the true phase control model is available, localization performance is relatively stable, for all considered model parameter settings.

- Low-Complexity Near-Field Localization via Jacobi-Anger Expansion: Building upon the ideas in [70, 82], we develop a novel low-complexity near-field localization algorithm using Jacobi-Anger expansion, which enables decoupling of range, azimuth and elevation dimensions. The resulting algorithm, named approximated MML (AMML), avoids the costly 3-D search over the UE position by performing three 1-D searches and attains the corresponding theoretical limits.

- Joint Localization and Online RIS Calibration: Under the assumption of known RIS amplitude model with unknown parameters, we propose an efficient approximate maximum-likelihood (ML) (AML) algorithm for joint localization and online RIS calibration. The proposed approach iteratively updates the RIS model parameters based on an initial UE location estimate from the output of the model-unaware AMML method, and refines the UE location using the updated RIS model. The AML algorithm is shown to significantly outperform the AMML estimator at high SNRs (where degradation due to model mismatch is most evident), closing the performance gap with respect to the case with known model parameters, and converges quickly to the corresponding model-aware CRB in few iterations.

1.4 RIS-aided Localization under Pixel Failures

1.4.1 Literature Review

In [86], antenna array diagnosis is studied in a standard mmWave setup without a RIS and several compressive sensing based techniques are proposed to identify the faulty antenna elements and the resulting amplitude and phase distortions. The AoA estimation problem under element failures is considered in [87], where the diagnosis of faulty elements is formulated as a Toeplitz matrix reconstruction problem. Recently, several papers investigate RIS element failures in mmWave communications [18, 19]. In [18], the authors present different types of pixel errors (e.g., stuck at state, out of state) and their spatial distribution (independent, clustered, etc.). The paper also explores the effect of pixel errors on the radiation pattern through simulations.

The study in [19] establishes a failure model to specify the amplitude and phase shift of faulty elements and proposes diagnostic methods by exploiting the sparsity property of failures. In addition to element failures resulting from internal hardware imperfections, RIS element blockages due to external environmental effects such as dust, rain and ice are studied in recent works [88, 89]. In [88], blockages at both the BS and RIS are considered and an iterative algorithm is proposed to jointly estimate the blockage coefficients of the BS and RIS. In [89], the authors propose a two-stage algorithm for joint RIS diagnosis and channel estimation in a RIS-aided mmWave MIMO system.

1.4.2 Contributions

In Chapter 5, the problem of RIS-aided localization under pixel failures is studided. The main contributions can be listed as follows:

- We analyze how detrimental RIS pixel failures can be for RIS-aided localization. To quantify the effect of these failures, we present some fundamental limits based on the theoretical bounds provided in Chapter 4.

- We propose an ℓ_1-regularization based algorithm to jointly estimate pixel failures and the UE position.
- In addition to the ℓ_1-regularization based algorithm, we propose a successive joint localization and failure diagnosis algorithm.
- Via simulations, it is shown that the successive joint localization and failure diagnosis algorithm achieves the theoretical performance bounds in the high SNR regime.

1.5 Parameter Encoding for ECRB Minimization in the Presence of Jamming

1.5.1 Literature Review

In the presence of eavesdropping, secure transmission of scalar and vector parameters is investigated in an estimation theoretic framework in [90–92]. In particular, the optimal encoding strategy for a scalar parameter is investigated in [90] by minimizing the expectation of the conditional Cramér-Rao bound (ECRB) at the intended receiver under a constraint on the mean-squared error (MSE) at the eavesdropper. In [92], the optimal encoding strategy for estimation theoretic security is analyzed, where the transmitter is allowed to perform randomization between two one-to-one and continuous encoding functions and the eavesdropper is fully aware of the encoding strategy at the transmitter. In addition, the work in [90] is extended to the case of vector parameters in [91].

Among various studies on jamming of communication systems, [93–97] formulate the problem of transmitting a parameter to a receiver under jamming attacks as a zero-sum game, and analyze optimal policies of the transmitter, receiver and jammer under various scenarios. Specifically, [93] investigates the problem of transmitting a sequence of independent and identically distributed Gaussian random variables through a Gaussian memoryless channel in the presence of an intelligent jammer. The optimal policies of the receiver and the jammer are determined, and the uniqueness of the solution is proved. In [94], by relaxing the Gaussian source and channel assumptions, optimal policies of the transmitter, jammer and receiver

are obtained. The work in [94] is extended to the zero-delay jamming setting in [95].

1.5.2 Contributions

In Chapter 6, an optimal parameter encoding problem is proposed for ECRB minimization in the presence of a jammer. A scalar parameter is transmitted over a noisy and flat-fading channel to a receiver, and the jammer, which has access to the parameter as in [97], sends an encoded version of the parameter to the receiver for degrading estimation performance. Our contributions can be listed as follows:

- Considering a generic prior distribution for the parameter, we formulate the problem of determining the optimal encoding strategy at the transmitter that minimizes the ECRB at the receiver in the presence of jamming for the first time in the literature.
- The optimal encoding function of the transmitter is determined among the class of differentiable and monotone increasing functions based on variational analyses, which leads to nonlinear encoding functions in general (cf. [94]).
- To determine the optimal encoding function based on the theoretical results, an algorithm is proposed. (This approach can also be used when the encoding function of the transmitter is restricted to be monotone decreasing.)
- In addition, the problem is analyzed for the general case by removing the monotonicity assumption over the encoding function of the transmitter. Numerical examples are presented to illustrate the benefits of the proposed optimal encoding approach in the presence of jamming.

1.6 Organization of the Dissertation

The organization of the thesis is as follows. In Chapter 2, we investigate the eavesdropper and jammer selection strategies in wireless localization networks. In Chapter 3, anchor placement

in TOA based wireless localization networks is studied. In Chapter 4, the problem of RIS-aided localization under hardware impairments is examined. Then, in Chapter 5, when some of the pixels of the RIS fail, the problem of joint localization and diagnosis of pixel failures is studied. Then, in Chapter 6, we investigate the optimal scalar parameter encoding strategy of the transmitter in the presence of jamming attacks.

Chapter 2

Eavesdropper and Jammer Selection Strategies in Wireless Localization Networks

In this chapter, we formulate and study the eavesdropper selection, jammer selection and joint eavesdropper and jammer selection problems. For the eavesdropper selection problem, the CRLB for estimating the positions of the target nodes by the eavesdropper nodes is derived. For both the eavesdropper and the jammer selection problems, analytical properties of the corresponding CRLB expressions are presented. By relaxing the integer constraints in the proposed selection problems, we are able to express all the problems as convex optimization problems. By using convex optimization techniques, we propose algorithms for solving the considered problems.

2.1 Motivation

The investigation of the eavesdropper selection, jammer selection, and joint eavesdropper and jammer selection problems is important to identify the adversarial capabilities of eavesdropper and/or jammer nodes.

As a motivating example of an application scenario for the eavesdropper selection problem, consider a restricted environment such as a military facility or a factory (e.g., imagine an area in Figure 2.1 covering blue squares and cross signs). In this environment, target nodes can represent the personnel or important equipment, which send signals to anchors nodes so that their locations can be tracked by the wireless localization network. A fixed number of eavesdropper nodes can be placed at some of feasible locations outside the restricted environment (red triangles in Figure 2.1), e.g., under some camouflage. The aim of eavesdropper nodes is to gather accurate location information about target nodes (i.e., personnel or equipment) for leaking critical information. To this aim, they need to be placed at optimal locations among the feasible locations, leading to the proposed eavesdropper selection problem.

Considering the same setting, jammer nodes can be placed at some of feasible locations for the purpose of reducing the accuracy of the localization network so that the network will not be able to track critical equipment or personnel with sufficient localization accuracy. This scenario can also be encountered in a battle-field in order to disrupt the localization capability of an enemy network. Similarly, the joint eavesdropper and jammer selection problem can be considered for both gathering location information about target nodes and reducing the accuracy of the localization network.

2.2 Notation

Throughout this chapter, $\mathbf{X} \succeq \mathbf{Y}$ denotes that $\mathbf{X}-\mathbf{Y}$ is a positive semi-definite matrix, $\mathbf{x} \succeq \mathbf{y}$ means that $x_i \geq y_i$ for all $i = 1, 2, \ldots, n$, where $\mathbf{x} = [x_1 \; x_2 \ldots x_n]^\intercal$ and $\mathbf{y} = [y_1 \; y_2 \ldots y_n]^\intercal$, and $\mathrm{tr}\{\cdot\}$ represents the trace of a square matrix. Also, the following definitions are used: (i) Let $f(\cdot)$ be a real-valued function of $\mathbf{z} \in \mathbb{R}^n$. $f(\mathbf{z})$ being non-increasing in $\mathbf{z}$ means that if $\mathbf{z}$ and $\mathbf{w}$ satisfy $\mathbf{z} \succeq \mathbf{w}$, $f(\mathbf{z}) \leq f(\mathbf{w})$ holds. (ii) Let $g(\cdot)$ be a real-valued of function of $\mathbf{X} \in S_+^n$, where S_+^n is the set of positive semi-definite matrices in $\mathbb{R}^{n \times n}$. Then, $g(\mathbf{X})$ being non-increasing in $\mathbf{X}$ means that if $\mathbf{X}$ and $\mathbf{Y}$ satisfy $\mathbf{X} \succeq \mathbf{Y}$, $g(\mathbf{X}) \leq g(\mathbf{Y})$ holds.

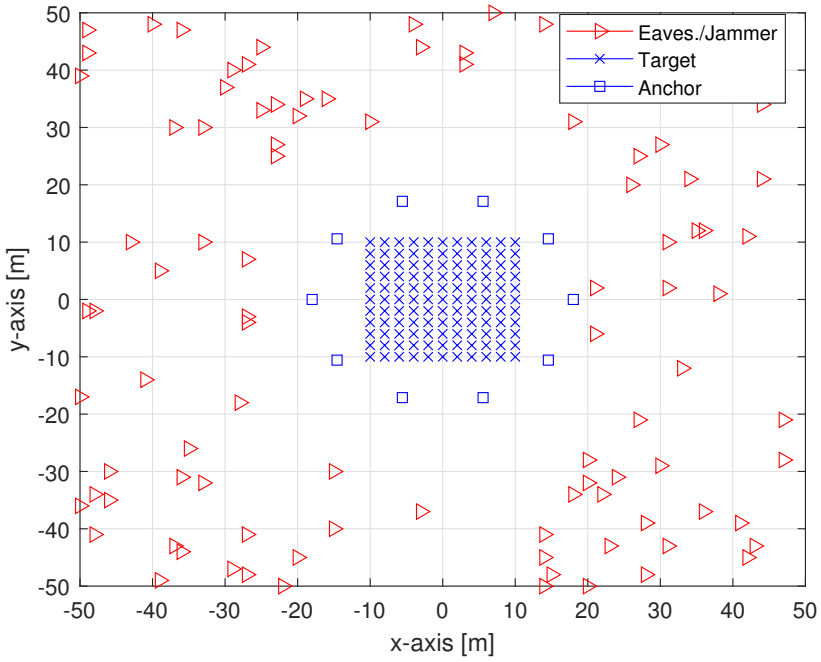


Figure 2.1: Illustration of the wireless source localization network.

2.3 System Model

Consider a two-dimensional wireless source localization network in which a target node (source) transmits signals that are used by anchor nodes to estimate its location. The number of anchor nodes is denoted by N_A and they are located at $\mathbf{y}_j \in \mathbb{R}^2$ for $j = 1, 2, \ldots, N_A$. Also, there exists some prior information about the location of the target node such that it is located at $\mathbf{x}_i \in \mathbb{R}^2$ with probability $w_i \geq 0$ for $i = 1, 2, \ldots, N_T$, where N_T is the number of possible locations for the target node, and $\sum_{i=1}^{N_T} w_i = 1$. Let $\mathcal{A}_i$ represent the set of locations of anchor nodes that are connected to the ith target position (i.e., location $\mathbf{x}_i$) for $i = 1, 2, \ldots, N_T$. Moreover, let $\mathcal{A}_L^{(i)}$ and $\mathcal{A}_{NL}^{(i)}$ denote, respectively, the locations of anchor nodes having line-of-sight (LOS) and non-line-of-sight (NLOS) connections to the target node located at $\mathbf{x}_i$.

In the wireless localization network, there also exist N different locations specified by the set $\mathcal{N} = \{\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_N\}$, at which either jammer or eavesdropper nodes can be placed. Eavesdropper nodes listen to the signals transmitted from the target node to the anchor

nodes and aim to estimate the location of the target node. On the other hand, jammer nodes degrade the localization performance of the anchor nodes by transmitting zero-mean white Gaussian noise [6, 98]. It is assumed that at any given time, at most N_E locations in $\mathcal{N}$ can be used for eavesdropping purposes, whereas at most N_J of them can be used for jamming purposes, where $N_E+N_J \leq N$. In other words, there exist at most N_E eavesdropper nodes and N_J jammer nodes that can be placed at some of the N possible locations. Let $\mathcal{N}_E$ and $\mathcal{N}_J$ denote the set of locations in $\mathcal{N}$ at which eavesdropper nodes and jammer nodes are placed, respectively.

Considering a wideband wireless localization network as in [99], the signal transmitted from the ith target position (i.e., $\mathbf{x}_i$) that is intended for the anchor node located at $\mathbf{y}_j$ is denoted by $s_{ij}(t)$. If an eavesdropper node is placed at $\mathbf{p}_k$ (i.e., if $\mathbf{p}_k \in \mathcal{N}_E$), the received signal at that eavesdropper node due to the transmission of $s_{ij}(t)$ is represented by $r^E_{ijk}(t)$. This signal is expressed as

$$r^E_{ijk}(t) = \sum_{l=1}^{L^E_{ijk}} \alpha^{(E,l)}_{ijk} s_{ij}\big(t - \tau^{(E,l)}_{ijk}\big) + n_{ijk}(t) \tag{2.1}$$

for $t \in [T_1^{(E,k)}, T_2^{(E,k)})$ and $(i,j) \in \mathcal{S}_k$, where $T_1^{(E,k)}$ and $T_2^{(E,k)}$ specify the observation interval for the eavesdropper node located at $\mathbf{p}_k$, $\mathcal{S}_k = \{(i,j) \mid \mathbf{p}_k \in \mathcal{N}_E,\, \mathbf{y}_j \in \mathcal{A}_i\}$, L^E_{ijk} represents the number of paths between the target node located at $\mathbf{x}_i$ and the eavesdropper node located at $\mathbf{p}_k$ (due to the transmission of $s_{ij}(t)$), $\alpha^{(E,l)}_{ijk}$ and $\tau^{(E,l)}_{ijk}$ denote, respectively, the amplitude and the delay of the lth multipath component, and $n_{ijk}(t)$ is zero-mean white Gaussian noise with a power spectral density level of σ_k^2. Considering orthogonal channels between target and anchor nodes, $n_{ijk}(t)$ is modeled as independent for all i, j, k [24, 25, 100]. The delays of the paths are characterized by the following expression:

$$\tau^{(E,l)}_{ijk} = \frac{1}{c}\left(\|\mathbf{x}_i - \mathbf{p}_k\| + b^{(E,l)}_{ijk} + \Delta_i\right) \tag{2.2}$$

where c is the propagation speed, $b^{(E,l)}_{ijk} \geq 0$ is the range bias ($b^{(E,1)}_{ijk} = 0$ for LOS propagation and $b^{(E,1)}_{ijk} > 0$ for NLOS), and Δ_i characterizes the time offset between the clocks of the target node located at $\mathbf{x}_i$ and the eavesdropper nodes. It is assumed that the eavesdropper nodes are perfectly synchronized among themselves and there exist no clock drifts. (Please see [101, 102] for clock drift mitigation mechanisms.) However, there is no synchronization between the target node and the eavesdropper nodes. Furthermore, for any $i = 1, 2, \ldots, N_T$,

we define $\mathcal{N}_L^{(i)} \triangleq \{(j,k) \mid \ b_{ijk}^{(E,1)} = 0\}$ and $\mathcal{N}_{NL}^{(i)} \triangleq \{(j,k) \mid \ b_{ijk}^{(E,1)} \neq 0\}$, which are the set of anchor and eavesdropper node indices corresponding, respectively, to LOS and NLOS connections between the eavesdropper nodes and the target node located at $\mathbf{x}_i$. (For example, if $b_{i32}^{(E,1)} = 0$, it means that the eavesdropper node at position $\mathbf{p}_2$ and the target node at position $\mathbf{x}_i$ are in LOS during the transmission of the signal from that target node to the anchor node at position $\mathbf{y}_3$ (i.e., during the transmission of $s_{i3}(t)$).)

On the other hand, due to the existence of jammer nodes, the signal received at the anchor node located at $\mathbf{y}_j$ coming from the target node located at $\mathbf{x}_i$ can be expressed as

$$r_{ij}^A(t) = \sum_{l=1}^{L_{ij}^A} \alpha_{ij}^{(A,l)} s_{ij}\big(t - \tau_{ij}^{(A,l)}\big) + \sum_{\{l:\mathbf{p}_l \in \mathcal{N}_J\}} \gamma_{lj}\sqrt{P_l^J} v_{lij}(t) + \eta_{ij}(t) \tag{2.3}$$

for the observation interval $[T_1^{(A,j)}, T_2^{(A,j)})$ and for $\mathbf{y}_j \in \mathcal{A}_i$, where $\alpha_{ij}^{(A,l)}$ and $\tau_{ij}^{(A,l)}$ denote, respectively, the amplitude and the delay of the lth multipath component between the target node at location $\mathbf{x}_i$ and the anchor node at location $\mathbf{y}_j$, L_{ij}^A represents the number of multipaths between the target node at location $\mathbf{x}_i$ and anchor node at location $\mathbf{y}_j$, γ_{lj} is the channel coefficient between the anchor node at location $\mathbf{y}_j$ and the jammer node located at $\mathbf{p}_l$, and P_l^J is the transmit power of the jammer node at position $\mathbf{p}_l$. Moreover, $\sqrt{P_l^J} v_{lij}(t)$ and $\eta_{ij}(t)$ are the jammer noise and the measurement noise, respectively. It is assumed that both of them are independent zero-mean white Gaussian random processes, where the average power of $v_{lij}(t)$ is equal to one and that of $\eta_{ij}(t)$ is equal to ${\tilde{\sigma}_j}^2$. It is modeled that $v_{lij}(t)$ is independent for all l, i, j and $\eta_{ij}(t)$ is independent for all i, j due to the presence of orthogonal channels between target and anchor nodes [25]. Furthermore, the delays of the paths are characterized by

$$\tau_{ij}^{(A,l)} = \frac{1}{c}\left(\|\mathbf{y}_j - \mathbf{x}_i\|_2 + b_{ij}^{(A,l)}\right) \tag{2.4}$$

where $b_{ij}^{(A,l)} \geq 0$ is the range bias of the lth path between the target node located at $\mathbf{x}_i$ and the anchor node located at $\mathbf{y}_j$. ($b_{ij}^{(A,1)} = 0$ for LOS propagation and $b_{ij}^{(A,1)} > 0$ for NLOS.) Unlike the expression in (2.2), no clock offsets are considered in (2.4) since target and anchor nodes are assumed to be synchronized.

2.4 Eavesdropper Selection Problem

In this section, we assume that there exist only eavesdropper nodes in the environment, i.e., $N_J = 0$, and focus on the eavesdropper selection problem. In this case, the aim is to choose at most N_E locations from set $\mathcal{N}$ for eavesdropping purposes so that the location of the target node is estimated as accurately as possible in the mean-square sense.

For quantifying the location estimation accuracy, the CRLB is used as a performance metric since the mean-squared error of the maximum likelihood (ML) estimator is asymptotically tight to the CRLB in the high SNR regime [103]. Based on the CRLB metric, the eavesdropper selection problem is investigated in the presence of perfect and imperfect knowledge of system parameters in the following sections.

2.4.1 Problem Formulation

To formulate the eavesdropper selection problem, we introduce a selection vector $\mathbf{z}^E = [z_1^E \; z_2^E \ldots z_N^E]^\intercal$, specified as

$$z_k^E = \begin{cases} 1, & \text{if } \mathbf{p}_k \in \mathcal{N}_E \\ 0, & \text{otherwise} \end{cases} \tag{2.5}$$

where $\sum_{k=1}^{N} z_k^E \leq N_E$. In addition, for the target position i, $\boldsymbol{\theta}_i$ is defined as follows:

$$\boldsymbol{\theta}_i \triangleq [\mathbf{x}_i^\intercal \; \Delta_i \; \boldsymbol{\kappa}_{i1}^\intercal \; \boldsymbol{\kappa}_{i2}^\intercal \ldots \boldsymbol{\kappa}_{iN}^\intercal]^\intercal \tag{2.6}$$

where $\boldsymbol{\kappa}_{ik}$ is the vector obtained by concatenating the elements of $\tilde{\boldsymbol{\kappa}}_{ijk}$ vertically, $\boldsymbol{\kappa}_{ik} = [\tilde{\boldsymbol{\kappa}}_{ijk}^\intercal]_{j\in\mathcal{A}_i}^\intercal$, with

$$\tilde{\boldsymbol{\kappa}}_{ijk} = \begin{cases} \begin{bmatrix} \alpha_{ijk}^{(E,1)} & b_{ijk}^{(E,2)} & \ldots b_{ijk}^{(E,L_{ijk}^E)} & \alpha_{ijk}^{(E,L_{ijk}^E)} \end{bmatrix}^\intercal, & \text{if } b_{ijk}^{(E,1)} = 0, \\ \begin{bmatrix} b_{ijk}^{(E,2)} & \alpha_{ijk}^{(E,2)} & \ldots b_{ijk}^{(E,L_{ijk}^E)} & \alpha_{ijk}^{(E,L_{ijk}^E)} \end{bmatrix}^\intercal, & \text{otherwise.} \end{cases}$$

for any i, j, k.

It is known that the estimation error vector satisfies [103]:

$$\mathbb{E}_{\boldsymbol{\theta}_i}\left\{(\boldsymbol{\theta}_i - \hat{\boldsymbol{\theta}}_i)(\boldsymbol{\theta}_i - \hat{\boldsymbol{\theta}}_i)^\intercal\right\} \succeq \mathbf{J}_{\boldsymbol{\theta}_i}^{-1} \tag{2.7}$$

where $\hat{\boldsymbol{\theta}}_i$ is any unbiased estimate of $\boldsymbol{\theta}_i$, and $\mathbf{J}_{\boldsymbol{\theta}_i}$ is the Fisher information matrix (FIM) for the parameter vector $\boldsymbol{\theta}_i$. From (2.7), the CRLB for estimating the position of the target node located at $\mathbf{x}_i$ is obtained as

$$\mathbb{E}_{\boldsymbol{\theta}_i}\left\{\|\hat{\mathbf{x}}_i - \mathbf{x}_i\|_2^2\right\} \geq \mathrm{tr}\{[\mathbf{J}_{\boldsymbol{\theta}_i}^{-1}]_{2\times 2}\} \tag{2.8}$$

where $\hat{\mathbf{x}}_i$ is any unbiased estimate of $\mathbf{x}_i$. It is noted from (2.8) that, for the CRLB calculation, we should focus on the equivalent Fisher information matrix (EFIM) for $\mathbf{x}_i$, which is a 2×2 matrix denoted by $\mathbf{J}_e^{(i)}(\mathbf{x}_i)$ such that $[\mathbf{J}_{\boldsymbol{\theta}_i}^{-1}]_{2\times 2} = \left(\mathbf{J}_e^{(i)}(\mathbf{x}_i)\right)^{-1}$ [99]. Since $[\mathbf{J}_{\boldsymbol{\theta}_i}]_{2\times 2}$ is a function of both $\mathbf{x}_i$ and $\mathbf{z}^E$, it is convenient to write $[\mathbf{J}_{\boldsymbol{\theta}_i}]_{2\times 2} \triangleq \mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^E)$. Hence, we formulate the proposed eavesdropper selection problem as follows:

$$\min_{\mathbf{z}^E} \quad \sum_{i=1}^{N_T} w_i \,\mathrm{tr}\left\{\left(\mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^E)\right)^{-1}\right\} \tag{2.9a}$$

$$\text{subject to} \quad \sum_{k=1}^{N} z_k^E \leq N_E, \tag{2.9b}$$

$$z_k^E \in \{0,1\} \text{ for } k = 1, 2, \ldots, N. \tag{2.9c}$$

Namely, the aim is to select the best locations for eavesdropper nodes for achieving the minimum average CRLB by considering possible target node positions ($\mathbf{x}_i$) and their probabilities (w_i).

2.4.2 Theoretical Results and Algorithms

To simplify the notation, let $f(\mathbf{z}^E)$ represent the objective function in (2.9); that is,

$$f(\mathbf{z}^E) \triangleq \sum_{i=1}^{N_T} w_i \,\mathrm{tr}\left\{\left(\mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^E)\right)^{-1}\right\}. \tag{2.10}$$

In the rest of this section, we first obtain a closed form expression of $\mathrm{tr}\left\{\left(\mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^E)\right)^{-1}\right\}$ for any target location i, and then analyze monotonicity and convexity properties of $f(\mathbf{z}^E)$ with respect to $\mathbf{z}^E$.

Proposition 2.1: For a given eavesdropper selection vector $\mathbf{z}^E$, the CRLB for estimating

the position of the target node located at $\mathbf{x}_i$ is given by

$$\mathrm{tr}\left\{\left(\mathbf{J}_e^{(i)}(\mathbf{x}_i,\mathbf{z}^E)\right)^{-1}\right\}=\frac{\tilde{p}_i(\mathbf{z}^E)}{\tilde{r}_i(\mathbf{z}^E)} \tag{2.11}$$

where

$$\tilde{p}_i(\mathbf{z}^E)=3\sum_{(u,k)\in\mathcal{N}_L^{(i)}}\sum_{(v,l)\in\mathcal{N}_L^{(i)}} z_k^E z_l^E \lambda_{uk}^{(i)}\lambda_{vl}^{(i)} p_{k,l}^{(i)}, \tag{2.12}$$

$$\tilde{r}_i(\mathbf{z}^E)=4\sum_{(u,k)\in\mathcal{N}_L^{(i)}}\sum_{(v,l)\in\mathcal{N}_L^{(i)}}\sum_{(s,m)\in\mathcal{N}_L^{(i)}} z_k^E z_l^E z_m^E \lambda_{uk}^{(i)}\lambda_{vl}^{(i)}\lambda_{sm}^{(i)} p_{k,l}^{(i)} p_{l,m}^{(i)} p_{m,k}^{(i)}, \tag{2.13}$$

$$\lambda_{jk}^{(i)}=\frac{8\pi\beta_{ij}^2}{c^2}(1-\chi_{jk}^{(i)})\mathrm{SNR}_{ijk}^{(1)}, \tag{2.14}$$

$$\beta_{ij}^2=\frac{\int_{-\infty}^{\infty} f^2|S_{ij}(f)|^2\,df}{\int_{-\infty}^{\infty}|S_{ij}(f)|^2\,df}, \tag{2.15}$$

$$\mathrm{SNR}_{ijk}^{(1)}=\frac{|\alpha_{ijk}^{(E,1)}|^2\int_{-\infty}^{\infty}|S_{ij}(f)|^2\,df}{2\sigma_k^2}, \tag{2.16}$$

$$p_{k,l}^{(i)}=\sin^2\left(\frac{\phi_{ik}-\phi_{il}}{2}\right) \tag{2.17}$$

with $S_{ij}(f)$ denoting the Fourier transform of $s_{ij}(t)$, $\chi_{jk}^{(i)}$ being the path overlap coefficient with $0\le\chi_{jk}^{(i)}\le 1$ [99], and ϕ_{ik} representing the angle from the ith target location to $\mathbf{p}_k$, i.e., $\phi_{ik}=\arctan\frac{x_{i2}-p_{k2}}{x_{i1}-p_{k1}}$ ($\mathbf{x}_i=[x_{i1}\ x_{i2}]^\intercal$, $\mathbf{p}_k=[p_{k1}\ p_{k2}]^\intercal$).

Proof: In [99, Thm. 1], the EFIM for estimating the location of a single target node is obtained for synchronized target and anchor nodes. Even though our network model is quite different from the system model described in Section II of [99], we benefit from the proof of [99, Thm. 1] in the first part of this proof.

In the proof of [99, Thm.1], vector $\boldsymbol{q}_k$ is defined as $\boldsymbol{q}_k=[\cos\phi_k\ \ \sin\phi_k]^\intercal$. We follow the same steps as in that proof by replacing vector $\boldsymbol{q}_k$ with vector $\boldsymbol{q}_{ik}$, which is defined as $\boldsymbol{q}_{ik}=[\cos\phi_{ik}\ \ \sin\phi_{ik}\ \ 1]^\intercal$.[1] Then, we can obtain the EFIM for $[\mathbf{x}_i\ \ \Delta_i]^\intercal$, denoted by

[1]The reason for using $\boldsymbol{q}_{ik}$ instead of $\boldsymbol{q}_k$ stems from the fact that in our system model, the number of the possible target locations is more than one. Also, the additional term 1 in $\boldsymbol{q}_{ik}$ compared to $\boldsymbol{q}_k$ is due to the time offset between the target node and the eavesdropper nodes; i.e., due to the Δ_i term.

$\mathbf{J}_e^{(i)}(\mathbf{x}_i, \Delta_i, \mathbf{z}^E)$, as follows:

$$\mathbf{J}_e^{(i)}(\mathbf{x}_i, \Delta_i, \mathbf{z}^E) = \begin{bmatrix} K_i(\mathbf{z}^E) & D_i(\mathbf{z}^E) & C_i(\mathbf{z}^E) \\ D_i(\mathbf{z}^E) & E_i(\mathbf{z}^E) & S_i(\mathbf{z}^E) \\ C_i(\mathbf{z}^E) & S_i(\mathbf{z}^E) & T_i(\mathbf{z}^E) \end{bmatrix} \tag{2.18}$$

where

$$K_i(\mathbf{z}^E) \triangleq \sum_{(j,k)\in\mathcal{N}_L^{(i)}} z_k^E \lambda_{jk}^{(i)} \cos^2\phi_{ik}, \tag{2.19}$$

$$E_i(\mathbf{z}^E) \triangleq \sum_{(j,k)\in\mathcal{N}_L^{(i)}} z_k^E \lambda_{jk}^{(i)} \sin^2\phi_{ik}, \tag{2.20}$$

$$C_i(\mathbf{z}^E) \triangleq \sum_{(j,k)\in\mathcal{N}_L^{(i)}} z_k^E \lambda_{jk}^{(i)} \cos\phi_{ik}, \tag{2.21}$$

$$S_i(\mathbf{z}^E) \triangleq \sum_{(j,k)\in\mathcal{N}_L^{(i)}} z_k^E \lambda_{jk}^{(i)} \sin\phi_{ik}, \tag{2.22}$$

$$D_i(\mathbf{z}^E) \triangleq \sum_{(j,k)\in\mathcal{N}_L^{(i)}} z_k^E \lambda_{jk}^{(i)} \sin\phi_{ik}\cos\phi_{ik}, \tag{2.23}$$

$$T_i(\mathbf{z}^E) \triangleq \sum_{(j,k)\in\mathcal{N}_L^{(i)}} z_k^E \lambda_{jk}^{(i)}. \tag{2.24}$$

By applying the Schur complement formula to (2.18), the following expression is obtained:

$$\begin{aligned} \mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^E) = &\begin{bmatrix} K_i(\mathbf{z}^E) & D_i(\mathbf{z}^E) \\ D_i(\mathbf{z}^E) & E_i(\mathbf{z}^E) \end{bmatrix} \\ &- \frac{\begin{bmatrix} C_i^2(\mathbf{z}^E) & C_i(\mathbf{z}^E)S_i(\mathbf{z}^E) \\ C_i(\mathbf{z}^E)S_i(\mathbf{z}^E) & S_i^2(\mathbf{z}^E) \end{bmatrix}}{T_i(\mathbf{z}^E)} \end{aligned} \tag{2.25}$$

Let $\mathbf{J}_1^{(i)}(\mathbf{x}_i, \mathbf{z}^E)$ and $\mathbf{J}_2^{(i)}(\mathbf{x}_i, \mathbf{z}^E)$ be defined as the first and second terms in (2.25), i.e.,

$$\mathbf{J}_1^{(i)}(\mathbf{x}_i, \mathbf{z}^E) \triangleq \begin{bmatrix} K_i(\mathbf{z}^E) & D_i(\mathbf{z}^E) \\ D_i(\mathbf{z}^E) & E_i(\mathbf{z}^E) \end{bmatrix} \tag{2.26}$$

$$\mathbf{J}_2^{(i)}(\mathbf{x}_i, \mathbf{z}^E) \triangleq \frac{\begin{bmatrix} C_i^2(\mathbf{z}^E) & C_i(\mathbf{z}^E)S_i(\mathbf{z}^E) \\ C_i(\mathbf{z}^E)S_i(\mathbf{z}^E) & S_i^2(\mathbf{z}^E) \end{bmatrix}}{T_i(\mathbf{z}^E)} \tag{2.27}$$

After some algebra, we derive the following expression from (2.25):

$$\mathrm{tr}\left\{\left(\mathbf{J}_e^{(i)}(\mathbf{x}_i,\mathbf{z}^E)\right)^{-1}\right\}=\frac{2\sum_{(u,k)\in\mathcal{N}_L^{(i)}}\sum_{(v,l)\in\mathcal{N}_L^{(i)}}p_{k,l}^{(i)}z_k^E z_l^E\lambda_{uk}^{(i)}\lambda_{vl}^{(i)}}{\sum\limits_{(u,k)\in\mathcal{N}_L^{(i)}}\sum\limits_{(v,l)\in\mathcal{N}_L^{(i)}}\sum\limits_{(s,m)\in\mathcal{N}_L^{(i)}}q_{k,l,m}^{(i)}z_k^E z_l^E z_m^E\lambda_{uk}^{(i)}\lambda_{vl}^{(i)}\lambda_{sm}^{(i)}} \tag{2.28}$$

where

$$\begin{aligned}q_{k,l,m}^{(i)}&=\cos\phi_{ik}\sin\phi_{il}\sin(\phi_{il}-\phi_{ik})-\cos\phi_{ik}\sin\phi_{im}\sin(\phi_{il}-\phi_{ik})\\&\quad-\cos\phi_{ik}\cos\phi_{il}\sin\phi_{im}(\sin\phi_{im}-\sin\phi_{ik}).\end{aligned} \tag{2.29}$$

Based on the trigonometric identity,

$$\sin a+\sin b-\sin(a+b)=4\sin\left(\frac{a}{2}\right)\sin\left(\frac{b}{2}\right)\sin\left(\frac{a+b}{2}\right)$$

we obtain the following relation:

$$q_{k,l,m}^{(i)}+q_{k,m,l}^{(i)}+q_{l,k,m}^{(i)}+q_{l,m,k}^{(i)}+q_{m,l,k}^{(i)}+q_{m,k,l}^{(i)}=16p_{k,l}^{(i)}p_{l,m}^{(i)}p_{m,k}^{(i)}\,. \tag{2.30}$$

Then, we can rearrange the denominator of (2.28) as follows:

$$\begin{aligned}&\sum_{(u,k)\in\mathcal{N}_L^{(i)}}\sum_{(v,l)\in\mathcal{N}_L^{(i)}}\sum_{(s,m)\in\mathcal{N}_L^{(i)}}q_{k,l,m}^{(i)}z_k^E z_l^E z_m^E\lambda_{uk}^{(i)}\lambda_{vl}^{(i)}\lambda_{sm}^{(i)}\overset{(a)}{=}\\&16\sum_{(u,k)\in\mathcal{N}_L^{(i)}}\sum_{\substack{(v,l)\in\mathcal{N}_L^{(i)}\\ l>k}}\sum_{\substack{(s,m)\in\mathcal{N}_L^{(i)}\\ m>l}}p_{k,l}^{(i)}p_{l,m}^{(i)}p_{m,k}^{(i)}z_k^E z_l^E z_m^E\lambda_{uk}^{(i)}\lambda_{vl}^{(i)}\lambda_{sm}^{(i)}\\&\overset{(b)}{=}\frac{8}{3}\sum_{(u,k)\in\mathcal{N}_L^{(i)}}\sum_{(v,l)\in\mathcal{N}_L^{(i)}}\sum_{(s,m)\in\mathcal{N}_L^{(i)}}p_{k,l}^{(i)}p_{l,m}^{(i)}p_{m,k}^{(i)}z_k^E z_l^E z_m^E\lambda_{uk}^{(i)}\lambda_{vl}^{(i)}\lambda_{sm}^{(i)}\end{aligned} \tag{2.31}$$

where (a) follows from (2.30), and (b) is due to the symmetry in the summand term, $p_{k,l}^{(i)}p_{l,m}^{(i)}p_{m,k}^{(i)}z_k^E z_l^E z_m^E\lambda_{uk}^{(i)}\lambda_{vl}^{(i)}\lambda_{sm}^{(i)}$. By replacing the denominator of (2.28) with the final expression in (2.31), the CRLB expression in (2.11)–(2.13) is obtained. ■

In Proposition 2.1, the CRLB is expressed in closed-form as a ratio of two polynomials in terms of the eavesdropper selection vector, which brings benefits in terms of computational cost. For example, it facilitates the calculation of the solution of (2.9) via an exhaustive search over all possible $\mathbf{z}^E$ vectors when N is sufficiently small. Also, it is noted that the proposed CRLB expression in Proposition 2.1 depends only on the LOS signals (see (2.11)–(2.13)), which is in accordance with the results in the literature (e.g., [99, Prop. 1] and [104]).

Remark 2.1: It is observed from the CRLB expression in (2.11)–(2.13) that if all $\lambda_{jk}^{(i)}$'s are scaled by the same nonnegative real number ξ, $\text{tr}\left\{\left(\mathbf{J}_e^{(i)}(\mathbf{x}_i,\mathbf{z}^E)\right)^{-1}\right\}$ is scaled by $1/\xi$ for all $i=1,2,\ldots,N_T$. Therefore, the optimal eavesdropper selection strategy (i.e., the solution of (2.9)) remains the same in such cases.

Remark 2.2: For the eavesdropper selection problem, the *probability distribution* of the target node positions is assumed to be known. Also, it is assumed that LOS/NLOS conditions for possible target-eavesdropper positions and $\lambda_{jk}^{(i)}$'s are known. Although these assumptions may not hold in some practical scenarios, they facilitate calculation of theoretical limits on the best achievable performance of eavesdropper nodes [6]. If eavesdropper nodes are smart and can learn all the environmental parameters, the localization accuracy derived in this work can be achieved; otherwise, the localization accuracy (hence the eavesdropping capability) is bounded by the obtained results.[2] In addition, when the $\lambda_{jk}^{(i)}$ terms and LOS/NLOS conditions are not known perfectly, the robust formulation of the eavesdropper selection problem in Section 2.4.3 can be employed to provide a more practical formulation (please also see Remark 2.6).

The following lemma characterizes the monotonicity of $f(\mathbf{z}^E)$ in (2.10) (i.e., the objective function in (2.9)) with respect to $\mathbf{z}^E$, which is also utilized in the analysis in Section 2.4.3 (Lemma 2.2).

Lemma 2.1: $f(\mathbf{z}^E)$ is non-increasing in $\mathbf{z}^E$.

Proof: As $w_i \geq 0$ in (2.10), the aim is to show that $\text{tr}\left\{\left(\mathbf{J}_e^{(i)}(\mathbf{x}_i,\mathbf{z}^E)\right)^{-1}\right\}$ is non-increasing in $\mathbf{z}^E$. Since $\text{tr}\left\{\left(\mathbf{J}_e^{(i)}(\mathbf{x}_i,\mathbf{z}^E)\right)^{-1}\right\}$ is non-increasing with respect to $\mathbf{J}_e^{(i)}(\mathbf{x}_i,\mathbf{z}^E)$, it is sufficient to prove the following implication:

$$\mathbf{z}^E \succeq \mathbf{w} \implies \mathbf{J}_e^{(i)}(\mathbf{x}_i,\mathbf{z}^E) \succeq \mathbf{J}_e^{(i)}(\mathbf{x}_i,\mathbf{w}) \tag{2.32}$$

In other words, from (2.25), we must prove that

$$\mathbf{J}_1^{(i)}(\mathbf{x}_i,\mathbf{z}^E) - \mathbf{J}_1^{(i)}(\mathbf{x}_i,\mathbf{w}) - \mathbf{J}_2^{(i)}(\mathbf{x}_i,\mathbf{z}^E) + \mathbf{J}_2^{(i)}(\mathbf{x}_i,\mathbf{w}) \succeq 0$$

[2]The tightness of the provided bounds in the presence of imperfect information about the distribution of the target node location is evaluated in Section 2.7.2.

It is noted that for any $\mathbf{y} = [y_1 \ y_2]^\intercal \in \mathbb{R}^2$, the following equalities hold:

$$\mathbf{y}^\intercal \mathbf{J}_1^{(i)}(\mathbf{x}_i, \mathbf{z}^E)\mathbf{y} = y_1^2 K_i(\mathbf{z}^E) + 2y_1 y_2 D_i(\mathbf{z}^E) + y_2^2 E_i(\mathbf{z}^E), \tag{2.33}$$

$$\mathbf{y}^\intercal \mathbf{J}_2^{(i)}(\mathbf{x}_i, \mathbf{z}^E)\mathbf{y} = \frac{\big(y_1 C_i(\mathbf{z}^E) + y_2 S_i(\mathbf{z}^E)\big)^2}{T_i(\mathbf{z}^E)}\,. \tag{2.34}$$

Therefore, by combining (2.33) and (2.34), the following relation can be obtained:

$$\mathbf{y}^\intercal (\mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^E) - \mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{w}))\mathbf{y} = h_i(\mathbf{z}^E) - h_i(\mathbf{w}) \tag{2.35}$$

where

$$h_i(\mathbf{z}^E) \triangleq y_1^2 K_i(\mathbf{z}^E) + 2y_1 y_2 D_i(\mathbf{z}^E) + y_2^2 E_i(\mathbf{z}^E) - \frac{\big(y_1 C_i(\mathbf{z}^E) + y_2 S_i(\mathbf{z}^E)\big)^2}{T_i(\mathbf{z}^E)}\,. \tag{2.36}$$

Hence, it is sufficient to show that $h_i(\mathbf{z}^E)$ is a non-decreasing function of $\mathbf{z}^E$. It is noted that

$$\begin{aligned}\frac{\partial h_i(\mathbf{z}^E)}{\partial z_k^E} &= \bar{\lambda}_k^{(i)}(y_1 \cos\phi_{ik} + y_2 \sin\phi_{ik})^2 - \bar{\lambda}_k^{(i)} \frac{2(y_1 C_i(\mathbf{z}^E) + y_2 S_i(\mathbf{z}^E))(y_1 \cos\phi_{ik} + y_2 \sin\phi_{ik})}{T_i(\mathbf{z}^E)} \\ &\quad + \bar{\lambda}_k^{(i)} \frac{(y_1 C_i(\mathbf{z}^E) + y_2 S_i(\mathbf{z}^E))^2}{T_i(\mathbf{z}^E)^2}\end{aligned} \tag{2.37}$$

where $\bar{\lambda}_k^{(i)}$ is given by $\bar{\lambda}_k^{(i)} = \sum_{j:(j,k)\in\mathcal{N}_L^{(i)}} \lambda_{jk}^{(i)} \geq 0$. Then, via the arithmetic mean-geometric mean inequality, it is seen that

$$\frac{\partial h_i(\mathbf{z}^E)}{\partial z_k^E} \geq 0 \tag{2.38}$$

for any $k = 1, 2, \ldots, N$. Therefore, we have the desired conclusion that $f(\mathbf{z}^E)$ is non-increasing in $\mathbf{z}^E$. ■

This result is actually quite intuitive as one expects improved performance for estimating the location of a target node as the number of eavesdropper nodes increases. Next, we prove the convexity of the objective function in (2.9) with respect to $\mathbf{z}^E$.

Proposition 2.2: $f(\mathbf{z}^E)$ in (2.10) is a convex function of $\mathbf{z}^E$.

*Proof:*As $w_i \geq 0$ for $i = 1, 2, \ldots, N_T$ in (2.10), it is sufficient to prove that $\mathrm{tr}\left\{\left(\mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^E)\right)^{-1}\right\}$ is a convex function of $\mathbf{z}^E$. It is known that $\mathrm{tr}\{\mathbf{X}^{-1}\}$ is a convex function of $\mathbf{X}$ for any positive semi-definite $\mathbf{X}$ [105]. Also, $\mathrm{tr}\{\mathbf{X}^{-1}\}$ is non-increasing in $\mathbf{X}$. Therefore, it is sufficient to prove that $\mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^E)$ is a concave function of $\mathbf{z}^E$.

To explain why this is sufficient, we define function g as $g(\mathbf{X}) \triangleq \mathrm{tr}\{\mathbf{X}^{-1}\}$. Then, we are interested in the convexity of $g(\mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^E))$ with respect to $\mathbf{z}^E$. In other words, we should prove that for any $\nu \in [0,1]$, and $\mathbf{z}^E, \mathbf{w} \in \mathbb{R}^N$,

$$g(\mathbf{J}_e^{(i)}(\mathbf{x}_i, \nu\mathbf{z}^E + (1-\nu)\mathbf{w})) \leq \nu g(\mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^E)) + (1-\nu) g(\mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{w})). \tag{2.39}$$

If $\mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^E)$ is a concave function of $\mathbf{z}^E$, then $\mathbf{J}_e^{(i)}(\mathbf{x}_i, \nu\mathbf{z}^E + (1-\nu)\mathbf{w}) \geq \nu\mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^E) + (1-\nu)\mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{w})$ holds. Since $g(\cdot)$ is non-increasing and convex in its argument, it then leads to (2.39).

In order to prove that $\mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^E)$ is a concave function of $\mathbf{z}^E$, we should show that for any $\gamma \in [0,1]$ and $\mathbf{z}^E, \mathbf{w} \in \mathbb{R}^N$, the following relation is true:

$$\mathbf{J}_e^{(i)}(\mathbf{x}_i, \gamma\mathbf{z}^E + (1-\gamma)\mathbf{w}) \succeq \gamma\mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^E) + (1-\gamma)\mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{w}). \tag{2.40}$$

Based on the relations in (2.25)–(2.27), the inequality in (2.40) can be reduced to the following:

$$\gamma\mathbf{J}_2^{(i)}(\mathbf{x}_i, \mathbf{z}^E) + (1-\gamma)\mathbf{J}_2^{(i)}(\mathbf{x}_i, \mathbf{w}) \succeq \mathbf{J}_2^{(i)}(\mathbf{x}_i, \gamma\mathbf{z}^E + (1-\gamma)\mathbf{w}) \tag{2.41}$$

since $\mathbf{J}_1^{(i)}(\mathbf{x}_i, \mathbf{z}^E)$ is linear in $\mathbf{z}^E$.

It is deduced from (2.34) that for proving (2.40), it is sufficient to show that

$$\begin{aligned} &\gamma\frac{\big(y_1 C_i(\mathbf{z}^E) + y_2 S_i(\mathbf{z}^E)\big)^2}{T_i(\mathbf{z}^E)} + (1-\gamma)\frac{\big(y_1 C_i(\mathbf{w}) + y_2 S_i(\mathbf{w})\big)^2}{T_i(\mathbf{w})} \\ &\geq \frac{\big(y_1 C_i(\mathbf{s}) + y_2 S_i(\mathbf{s})\big)^2}{T_i(\mathbf{s})} \end{aligned} \tag{2.42}$$

where $\mathbf{s} = \gamma\mathbf{z}^E + (1-\gamma)\mathbf{w}$. By applying the Cauchy-Schwarz inequality to the left-hand-side of (2.42), the following inequality is obtained:

$$\begin{aligned} &\gamma\frac{\big(y_1 C_i(\mathbf{z}^E) + y_2 S_i(\mathbf{z}^E)\big)^2}{T_i(\mathbf{z}^E)} + (1-\gamma)\frac{\big(y_1 C_i(\mathbf{w}) + y_2 S_i(\mathbf{w})\big)^2}{T_i(\mathbf{w})} \geq \\ &\frac{\Big(\gamma\big(y_1 C_i(\mathbf{z}^E) + y_2 S_i(\mathbf{z}^E)\big) + (1-\gamma)\big(y_1 C_i(\mathbf{w}) + y_2 S_i(\mathbf{w})\big)\Big)^2}{\Big(\gamma T_i(\mathbf{z}^E) + (1-\gamma)T_i(\mathbf{w})\Big)} \end{aligned} \tag{2.43}$$

As $C_i(\cdot)$, $S_i(\cdot)$, and $T_i(\cdot)$ are linear in their arguments, (2.43) is actually the same as (2.42), which was to be proved. Hence, the desired conclusion in reached. ■

As a consequence of Proposition 2.2, the optimization problem in (2.9) becomes a convex optimization problem by relaxing the last constraint in (2.9c). Furthermore, it is deduced from Lemma 2.1 that if $\mathbf{z}^* = [z_1^* \; z_2^* \ldots z_N^*]^\intercal$ is a solution of (2.9), then (2.9b) must be satisfied with equality, i.e., $\sum_{j=1}^{N} z_j^* = N_E$ must hold. Therefore, the relaxed version of (2.9) can be formulated as follows:

$$\min_{\mathbf{z}^E} \quad \sum_{i=1}^{N_T} w_i \mathrm{tr}\left\{\left(\mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^E)\right)^{-1}\right\} \tag{2.44a}$$

$$\text{subject to} \quad \sum_{k=1}^{N} z_k^E = N_E, \tag{2.44b}$$

$$0 \leq z_k^E \leq 1 \text{ for } k = 1, 2, \ldots, N. \tag{2.44c}$$

As (2.44) is a convex problem, its solution can be obtained via convex optimization tools [105] (called the *relaxed algorithm* in Section 2.7). After finding the solution of (2.44), we propose the following two algorithms to obtain a solution of the original problem in (2.9). First, we can simply set the largest N_E components of the solution of (2.44) to one, and the others to zero (called the *largest-N_E algorithm* in Section 2.7). Second, starting from this solution, we can use a modified version of the Local Optimization algorithm discussed in [106] and obtain the solution of (2.9) (called *the proposed swap algorithm* in Section 2.7). The details of the proposed swap algorithm is provided in Algorithm 1, where $\mathbf{z}^*$ and $\mathbf{z}^*_{\text{largest-}N_E}$ denote the optimal selection vectors obtained by the relaxed algorithm and the largest-N_E algorithm, respectively, $N_{\text{swap}}^{\max}$ is the upper limit for the number of swap operations, and μ determines the stopping criterion. While performing one swap operation, one checks whether there is a decrease in the objective function by simply swapping one of the N_E selected positions with one of the $N - N_E$ positions that are not selected.

Algorithm 1 Proposed Swap Algorithm

Input: $\mathbf{z}^*, \mathbf{z}^*_{\text{largest-}N_E}, \mu, N^{\max}_{\text{swap}}$

Output: $\mathbf{z}^*_{\text{swap}}$.

Set **boolean** b $\leftarrow$ true, c$\leftarrow$0
if $|f(\mathbf{z}^*) - f(\mathbf{z}^*_{\text{largest-}N_E})| \leq \mu f(\mathbf{z}^*)$ **then**
    b $\leftarrow$ false, $\mathbf{z}^*_{\text{swap}} \leftarrow \mathbf{z}^*_{\text{largest-}N_E}$
else
    $\mathbf{z}_{\text{temp}} \leftarrow \mathbf{z}^*_{\text{largest-}N_E}$
end if
while b is true **do**
    c $\leftarrow$ c + 1
    Obtain all $N_E(N - N_E)$ possible selection vectors by applying one swap operation to $\mathbf{z}_{\text{temp}}$, and compute the corresponding objectives. Let $\mathbf{z}_{\text{temp-2}}$ be the selection vector among those vectors which yields the minimum objective.
    if $|f(\mathbf{z}_{\text{temp}}) - f(\mathbf{z}_{\text{temp-2}})| \leq \mu f(\mathbf{z}_{\text{temp}})$ & c $< N^{\max}_{\text{swap}}$ **then**
        b $\leftarrow$ false, $\mathbf{z}^*_{\text{swap}} \leftarrow \mathbf{z}_{\text{temp-2}}$.
    else if $c = N^{\max}_{\text{swap}}$ **then**
        b $\leftarrow$ false, $\mathbf{z}^*_{\text{swap}} \leftarrow \mathbf{z}_{\text{temp-2}}$.
    else
        $\mathbf{z}_{\text{temp}} \leftarrow \mathbf{z}_{\text{temp-2}}$
    end if
end while

Remark 2.3: It should be noted that the proposed swap algorithm presented in Algorithm 1 reduces to the proposed largest-N_E algorithm if (i) the objective value achieved by the largest-N_E algorithm is sufficiently close to the bound specified by the relaxed algorithm, or (ii) the objective value achieved by the proposed swap algorithm after the first swap operation is the same as that achieved by the largest-N_E algorithm.

2.4.3 Robust Eavesdropper Selection Problem

In the previous section, it is assumed that the eavesdropper nodes have the perfect knowledge of $\{\lambda_{jk}^{(i)}\}$ (see (2.11) and (2.14)). In this section, we propose a robust eavesdropper selection problem in the presence of imperfect knowledge about the system parameters by introducing some uncertainty in $\{\lambda_{jk}^{(i)}\}$. For simplicity of notation, we assume that $\mathcal{A}_i = \{\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_{N_A}\}$, i.e., all the anchor nodes are connected to the ith target position for any i. (The proposed approach can easily be extended to scenarios in which this assumption does not hold.)

To formulate a robust version of the eavesdropper selection problem, we first define $\mathbf{\Lambda}_E$ as follows:

$$\mathbf{\Lambda}_E \triangleq \left[\boldsymbol{\lambda}_E^{(1)}\ \boldsymbol{\lambda}_E^{(2)} \ldots \boldsymbol{\lambda}_E^{(N_T)}\right],$$

where

$$\boldsymbol{\lambda}_E^{(i)} \triangleq \left[\lambda_{11}^{(i)}\ \ldots\ \lambda_{1N}^{(i)}\ \lambda_{21}^{(i)}\ \ldots\ \lambda_{2N}^{(i)} \ldots \lambda_{N_A1}^{(i)}\ \ldots\ \lambda_{N_AN}^{(i)}\right]^\intercal.$$

We also introduce the estimated versions of $\boldsymbol{\lambda}_E^{(i)}$ as $\hat{\boldsymbol{\lambda}}_E^{(i)}$ for $i = 1, 2, \ldots, N_T$, which are given by

$$\hat{\boldsymbol{\lambda}}_E^{(i)} \triangleq \left[\hat{\lambda}_{11}^{(i)}\ \ldots\ \hat{\lambda}_{1N}^{(i)}\ \hat{\lambda}_{21}^{(i)}\ \ldots\ \hat{\lambda}_{2N}^{(i)} \ldots \hat{\lambda}_{N_A1}^{(i)}\ \ldots\ \hat{\lambda}_{N_AN}^{(i)}\right]^\intercal \tag{2.45}$$

with $\hat{\lambda}_{jk}^{(i)}$ denoting the estimate of $\lambda_{jk}^{(i)}$ for $j = 1, \ldots, N_A$ and $k = 1, \ldots, N$. These estimated values represent the imperfect knowledge of the $\lambda_{jk}^{(i)}$ parameters at the eavesdropper nodes. Let $\boldsymbol{\Delta\lambda}_E^{(i)}$ denote the error vector that generates the uncertainty; that is,

$$\hat{\boldsymbol{\lambda}}_E^{(i)} = \boldsymbol{\lambda}_E^{(i)} + \boldsymbol{\Delta\lambda}_E^{(i)} \tag{2.46}$$

with

$$\begin{aligned}\boldsymbol{\Delta\lambda}_E^{(i)} \triangleq \big[&\Delta\lambda_{11}^{(i)}\ \ldots\ \Delta\lambda_{1N}^{(i)}\ \Delta\lambda_{21}^{(i)}\ \ldots\ \Delta\lambda_{2N}^{(i)} \\ &\ldots \Delta\lambda_{N_A1}^{(i)}\ \ldots\ \Delta\lambda_{N_AN}^{(i)}\big]^\intercal\end{aligned} \tag{2.47}$$

for $i = 1, 2, \ldots, N_T$. Also, let $\boldsymbol{\Delta\Lambda}_E$ and $\hat{\mathbf{\Lambda}}_E$ be the matrices containing the error vectors and the estimation vectors, respectively, as follows:

$$\boldsymbol{\Delta\Lambda}_E \triangleq \left[\boldsymbol{\Delta\lambda}_E^{(1)}\ \boldsymbol{\Delta\lambda}_E^{(2)} \ldots \boldsymbol{\Delta\lambda}_E^{(N_T)}\right] \tag{2.48}$$

$$\hat{\mathbf{\Lambda}}_E \triangleq \left[\hat{\boldsymbol{\lambda}}_E^{(1)}\ \hat{\boldsymbol{\lambda}}_E^{(2)} \ldots \hat{\boldsymbol{\lambda}}_E^{(N_T)}\right]. \tag{2.49}$$

In this scenario, the notation for the objective function $f(\mathbf{z}^E)$ is modified as $f(\mathbf{z}^E, \mathbf{\Lambda}_E)$ to emphasize the dependence on $\mathbf{\Lambda}$ (since $\boldsymbol{\Delta\Lambda}_E$ becomes another parameter of interest in the presence of uncertainty).

As in [107–109], we employ a bounded error model for the uncertainty. In particular, for the eavesdropper selection problem in the presence of parameter uncertainty, the following model is assumed for the error matrix $\boldsymbol{\Delta\Lambda}_E$:

$$\boldsymbol{\Delta\Lambda}_E \in \mathcal{E} \triangleq \left\{\boldsymbol{\Delta\lambda}^{(i)} \in \mathbb{R}^{N\times N_A} : |\Delta\lambda_{jk}^{(i)}| \leq \delta_{jk}^{(i)}, \forall i,j,k\right\} \tag{2.50}$$

where $\{\delta_{jk}^{(i)}\}_{i=1,j=1,k=1}^{N_T,N_A,N}$ determine the size of the uncertainty region $\mathcal{E}$ with $\delta_{jk}^{(i)} \geq 0$ for all i, j, and k.

The aim is to minimize the worst-case CRLB as in [6] and [109]. Therefore, under this setup, the proposed optimization problem can be formulated as

$$\min_{\mathbf{z}^E} \max_{\boldsymbol{\Delta\Lambda}_E\in\mathcal{E}} \quad f(\mathbf{z}^E, \mathbf{\Lambda}_E) \tag{2.51a}$$

$$\text{subject to} \quad \sum_{k=1}^{N} z_k^E = N_E, \tag{2.51b}$$

$$0 \leq z_k^E \leq 1 \text{ for } k = 1, 2, \ldots, N, \tag{2.51c}$$

$$\mathbf{\Lambda}_E = \hat{\mathbf{\Lambda}}_E - \boldsymbol{\Delta\Lambda}_E. \tag{2.51d}$$

To solve the optimization problem in (2.51), the following lemma is utilized.

Lemma 2.2: $f(\mathbf{z}^E, \mathbf{\Lambda}_E)$ is non-increasing in $\boldsymbol{\lambda}^{(i)}$ for all $i = 1, 2, \ldots, N_T$.

Proof: It is sufficient to show that $\text{tr}\left\{\left(\mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^E)\right)^{-1}\right\}$ is non-increasing in $\boldsymbol{\lambda}_E^{(i)}$ for any $i = 1, 2, \ldots, N_T$ (see (2.10)). As a consequence of Proposition 2.1, we can immediately observe that $\text{tr}\left\{\left(\mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^E)\right)^{-1}\right\}$ is non-increasing in $\boldsymbol{\lambda}_E^{(i)}$ if and only if $\text{tr}\left\{\left(\mathbf{J}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^E)\right)^{-1}\right\}$ is non-increasing in $\mathbf{z}^E$ due to the symmetric expression in (2.11). (That is, the elements of $\boldsymbol{\lambda}_E^{(i)}$ and $\mathbf{z}^E$ affect the expression in (2.11) in the same manner.) Therefore, via Lemma 2.1, we obtain the desired result. ■

Let the value of $\mathbf{\Delta\Lambda}_E$ that maximizes $f(\mathbf{z}^E, \mathbf{\Lambda}_E)$ over set $\mathcal{E}$ be denoted as $\mathbf{\Delta\Lambda}_E^*$ and let $\{\Delta\lambda_{jk}^{(i),*}\}_{i,j,k}$ represent the elements of $\mathbf{\Delta\Lambda}_E^*$ (see (2.47) and (2.48)). Based on Lemma 2.2, it is obtained that

$$\Delta\lambda_{jk}^{(i),*} = \delta_{jk}^{(i)}. \tag{2.52}$$

Therefore, solving (2.51) is equivalent to solving the following optimization problem:

$$\min_{\mathbf{z}^E} \quad f(\mathbf{z}^E, \hat{\mathbf{\Lambda}}_E - \mathbf{\Delta\Lambda}_E^*) \tag{2.53a}$$

$$\text{subject to} \quad \sum_{k=1}^{N} z_k^E = N_E, \tag{2.53b}$$

$$0 \leq z_k^E \leq 1 \text{ for } k = 1, 2, \ldots, N. \tag{2.53c}$$

It is noted that (2.53) is in the form of (2.44). Thus, the solution approaches discussed for the eavesdropper selection problem in the previous section can also be applied to this problem.

2.5 Jammer Selection Problem

In this section, we focus on the jammer selection problem under the assumption that there exist only jammer nodes in the environment, i.e., $N_E = 0$. The aim is to choose at most N_J locations from the set $\mathcal{N}$ for jamming purposes so that the target localization performance of the anchor nodes is degraded as much as possible. By using the CRLB of the anchor nodes related to the estimation of target node positions as the performance metric, the jammer selection problem is investigated in the presence and absence of perfect knowledge about the system parameters.

2.5.1 Problem Formulation

Let $\mathbf{z}^J = [z_1^J \ \ldots \ z_N^J]^\intercal$ denote a selection vector defined as

$$z_k^J = \begin{cases} 1, & \text{if } \mathbf{p}_k \in \mathcal{N}_J \\ 0, & \text{otherwise} \end{cases} \tag{2.54}$$

where $\sum_{k=1}^{N} z_k^J \leq N_J$. Via similar steps to those in [6, 25, 99], the EFIM related to the positioning of the target node located at $\mathbf{x}_i$ by the anchor nodes can be obtained as follows:

$$\tilde{\mathbf{J}}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^J) = \sum_{j \in \mathcal{A}_L^{(i)}} \frac{\tilde{\lambda}_j^{(i)}}{\tilde{\sigma}_j^2 + \sum_{k=1}^{N} z_k^J P_k^J \left|\gamma_{kj}\right|^2} \boldsymbol{\varphi}_{ij} \boldsymbol{\varphi}_{ij}^{\intercal} \tag{2.55}$$

In (2.55), $\tilde{\lambda}_j^{(i)}$ corresponds to λ_{ij} in [25, Eq. 3], $\boldsymbol{\varphi}_{ij} = [\cos\varphi_{ij} \;\; \sin\varphi_{ij}]^{\intercal}$, and φ_{ij} is the angle from the ith target location to $\mathbf{y}_j$, i.e., $\varphi_{ij} = \arctan\frac{x_{i2}-y_{j2}}{x_{i1}-y_{j1}}$, where $\mathbf{y}_j \triangleq [y_{j1} \; y_{j2}]^{\intercal}$.

Based on (2.55), we formulate the proposed jammer selection problem as follows:

$$\max_{\mathbf{z}^J} \;\; \sum_{i=1}^{N_T} w_i \operatorname{tr}\left\{ \left(\tilde{\mathbf{J}}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^J) \right)^{-1} \right\} \tag{2.56a}$$

$$\text{subject to} \;\; \sum_{k=1}^{N} z_k^J \leq N_J, \;\; \sum_{k=1}^{N} z_k^J P_k^J \leq P_T, \tag{2.56b}$$

$$z_k^J \in \{0, 1\} \text{ for } k = 1, 2, \ldots, N \tag{2.56c}$$

where P_T is total power budget.

For the jammer selection problem in (2.56), the distribution of the target node positions is assumed to be known. It is also assumed that the anchor node positions, LOS/NLOS conditions for possible target-anchor positions, and $\tilde{\lambda}_j^{(i)}$'s are known. Similar statements to those in Remark 2.2 can be made for the jammer selection problem, as well. As stated in [24], jammer nodes can obtain information about the localization parameters by various means such as using cameras to learn the locations of anchor nodes, performing prior measurements in the environment to form a database for the channel parameters, and listening to signals between anchor and target nodes. When this information is inaccurate, the robust formulation of the jammer selection problem in Section 2.5.3 can be employed by considering uncertainty in the knowledge of $\tilde{\lambda}_j^{(i)}$'s and LOS/NLOS conditions (please also see Remark 2.6). In addition, the effects of uncertainty in the anchor node positions and in the distribution of the target node position can be evaluated as in Section 2.7.2.

2.5.2 Theoretical Results

To simplify the notation, let $\tilde{f}(\mathbf{z}^J)$ and $\{g_{ij}(\mathbf{z}^J)\}_{i=1,j=1}^{N_T,N_A}$ be defined as

$$\tilde{f}(\mathbf{z}^J) \triangleq \sum_{i=1}^{N_T} w_i \operatorname{tr}\left\{\left(\tilde{\mathbf{J}}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^J)\right)^{-1}\right\}, \tag{2.57}$$

$$g_{ij}(\mathbf{z}^J) \triangleq \frac{\tilde{\lambda}_j^{(i)}}{\tilde{\sigma}_j^2 + \sum_{k=1}^N z_k^J P_k^J \left|\gamma_{kj}\right|^2}. \tag{2.58}$$

In the rest of this section, we analyze the convexity and monotonicity properties of $\tilde{f}$ with respect to $\mathbf{z}^J$.

Lemma 2.3: $\tilde{f}(\mathbf{z}^J)$ is non-decreasing in $\mathbf{z}^J$.

Proof: It is observed from the expression in (2.55) that if $\mathbf{z}^J \succeq \tilde{\mathbf{w}}$, then $\tilde{\mathbf{J}}_e^{(i)}(\mathbf{x}_i, \tilde{\mathbf{w}}) \succeq \tilde{\mathbf{J}}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^J)$ holds for any $i = 1, 2, \ldots, N_T$. Since the function $\operatorname{tr}\{(\cdot)^{-1}\}$ is non-increasing in its argument and $w_i \geq 0$ for any i, it is concluded that $\tilde{f}(\mathbf{z}^J)$ in (2.57) is non-decreasing in $\mathbf{z}^J$. ■

Lemma 2.4: $g_{ij}(\mathbf{z}^J)$ is a convex function of $\mathbf{z}^J$ for any i, j.

Proof: From (2.58), the second-order derivatives are calculated as

$$\frac{\partial^2 g_{ij}(\mathbf{z}^J)}{\partial z_k^J \partial z_l^J} = \frac{2\tilde{\lambda}_j^{(i)} P_k^J P_l^J \left|\gamma_{kj}\right|^2 \left|\gamma_{lj}\right|^2}{(\tilde{\sigma}_j^2 + \sum_{l=1}^N z_l^J P_l^J \left|\gamma_{lj}\right|^2)^3}. \tag{2.59}$$

Define a vector as $\boldsymbol{v}_j \triangleq [P_1^J \left|\gamma_{1j}\right|^2 \ \ldots \ P_N^J \left|\gamma_{Nj}\right|^2]^\intercal$ for $j = 1, 2, \ldots, N_A$. Then, for any $\mathbf{y} \in \mathbb{R}^N$, it follows from (2.59) that

$$\mathbf{y}^\intercal \nabla^2 g_{ij}(\mathbf{z}^J)\mathbf{y} = \frac{2\tilde{\lambda}_j^{(i)}}{(\tilde{\sigma}_j^2 + \sum_{l=1}^N z_l^J P_l^J \left|\gamma_{lj}\right|^2)^3} \mathbf{y}^\intercal \boldsymbol{v}_j \boldsymbol{v}_j^\intercal \mathbf{y} \geq 0. \tag{2.60}$$

Therefore, $\nabla^2 g_{ij}(\mathbf{z}^J)$ is a positive semi-definite matrix; hence, $g_{ij}(\mathbf{z}^J)$ is a convex function of $\mathbf{z}^J$. ■

Proposition 2.3: $\tilde{f}(\mathbf{z}^J)$ is a concave function $\mathbf{z}^J$.

Proof: As $w_i \geq 0$ for $i = 1, 2, \ldots, N_T$, it is sufficient to prove that $\operatorname{tr}\left\{\left(\tilde{\mathbf{J}}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^J)\right)^{-1}\right\}$

is a concave function of $\mathbf{z}^J$ for any i. We know that $\operatorname{tr}\left\{\left(\tilde{\mathbf{J}}_e^{(i)}(\mathbf{x}_i,\mathbf{z}^J)\right)^{-1}\right\}$ is concave with respect to $\mathbf{z}^J$ if and only if $\operatorname{tr}\left\{-\left(\tilde{\mathbf{J}}_e^{(i)}(\mathbf{x}_i,\mathbf{z}^J)\right)^{-1}\right\}$ convex with respect to $\mathbf{z}^J$. Hence, two auxiliary functions are defined as follows:

$$\tilde{c}:\mathbb{R}^{2\times 2}\to\mathbb{R} \text{ such that } \tilde{c}(\mathbf{X})=\operatorname{tr}\left\{\mathbf{X}^{-1}\right\} \tag{2.61}$$

$$c_i:\mathbb{R}^N\to\mathbb{R}^{2\times 2} \text{ such that } c_i(\mathbf{z}^J)=-\tilde{\mathbf{J}}_e^{(i)}(\mathbf{x}_i,\mathbf{z}^J). \tag{2.62}$$

Based on the preceding definitions, $\operatorname{tr}\left\{-\left(\tilde{\mathbf{J}}_e^{(i)}(\mathbf{x}_i,\mathbf{z}^J)\right)^{-1}\right\}=\tilde{c}(c_i(\mathbf{z}^J))$. It is known that $\tilde{c}(\cdot)$ is convex and non-increasing in its argument [105]. Thus, it is sufficient to prove that $c_i(\mathbf{z}^J)$ is concave with respect to $\mathbf{z}^J$, or equivalently, $\tilde{\mathbf{J}}_e^{(i)}(\mathbf{x}_i,\mathbf{z}^J)$ is convex with respect to $\mathbf{z}^J$.

To that aim, we should prove that for any $\mathbf{z}^J,\tilde{\mathbf{w}}\in\mathbb{R}^N$ and $\tilde{\gamma}\in[0,1]$, the following relation holds:

$$\tilde{\gamma}\tilde{\mathbf{J}}_e^{(i)}(\mathbf{x}_i,\mathbf{z}^J)+(1-\tilde{\gamma})\tilde{\mathbf{J}}_e^{(i)}(\mathbf{x}_i,\tilde{\mathbf{w}})\succeq\tilde{\mathbf{J}}_e^{(i)}(\mathbf{x}_i,\tilde{\gamma}\mathbf{z}^J+(1-\tilde{\gamma})\tilde{\mathbf{w}}). \tag{2.63}$$

For any $\mathbf{y}=[y_1\ y_2]^\intercal$, it follows from (2.55) and (2.58) that

$$\mathbf{y}^\intercal\tilde{\mathbf{J}}_e^{(i)}(\mathbf{x}_i,\mathbf{z}^J)\mathbf{y}=\sum_{j\in\mathcal{A}_i^L}g_{ij}(\mathbf{z}^J)(y_1\cos\varphi_{ij}+y_2\sin\varphi_{ij})^2. \tag{2.64}$$

By combining Lemma 2.4 and (2.64), the desired conclusion is reached. ■

From Lemma 2.3, we can conclude that if $\mathbf{z}^*=[z_1^*\ z_2^*\dots z_N^*]^\intercal$ is a solution of (2.56), then (2.56b) must be satisfied with equality, i.e., $\sum_{k=1}^N z_k^*=N_J$ must hold. By relaxing the last constraint in (2.56c), the following optimization problem is obtained:

$$\max_{\mathbf{z}^J}\ \sum_{i=1}^{N_T}w_i\operatorname{tr}\left\{\left(\tilde{\mathbf{J}}_e^{(i)}(\mathbf{x}_i,\mathbf{z}^J)\right)^{-1}\right\} \tag{2.65a}$$

$$\text{subject to}\ \sum_{k=1}^N z_k^J=N_J,\ \sum_{k=1}^N z_k^JP_k^J\le P_T, \tag{2.65b}$$

$$0\le z_k^J\le 1 \text{ for } k=1,2,\dots,N. \tag{2.65c}$$

Since the objective function in (2.65a) is concave due to Proposition 2.3 and all the constraints in (2.65b) and (2.65c) are affine, we reach the conclusion that (2.65) is a convex optimization problem. Thus, it can be solved via convex optimization tools for finding its globally optimal solution.

After finding the solution of (2.65), the largest-N_J algorithm and the proposed swap algorithm can be used for finding the solution of (2.56) as in the eavesdropper selection problem. However, in this case, we set the largest N_J components of the solution obtained from (2.65) to one, and while implementing the proposed swap algorithm, we check whether there is an increase in the objective function by simply swapping one of the N_J selected positions with one of the $N - N_J$ positions that are not selected. This discussion will lead us to the following remark.

Remark 2.4: For the formulation of (2.65), it is assumed that the transmit powers of the jammer nodes are given (fixed). If $\{P_k^J\}_{k=1}^N$ are considered as optimization variables as well, the following problem can be formulated (cf. (2.65)):

$$\max_{\mathbf{z}^J, \tilde{\mathbf{q}}} \quad \sum_{i=1}^{N_T} w_i \operatorname{tr}\left\{ \left(\sum_{j \in \mathcal{A}_L^{(i)}} \tilde{g}_{ij}(\tilde{\mathbf{q}}) \boldsymbol{\varphi}_{ij} \boldsymbol{\varphi}_{ij}^{\intercal} \right)^{-1} \right\} \tag{2.66a}$$

$$\text{subject to} \quad \sum_{k=1}^{N} z_k^J = N_J, \ \sum_{l=1}^{N} \tilde{q}_l \leq P_T, \tag{2.66b}$$

$$0 \leq z_k^J \leq 1 \text{ for } k = 1, 2, \ldots, N, \tag{2.66c}$$

$$0 \leq \tilde{q}_l \leq z_l^J P_l^{\text{peak}} \text{ for } l = 1, 2, \ldots, N \tag{2.66d}$$

where $\tilde{q}_l = z_l^J P_l^J$, $\tilde{\mathbf{q}} = [\tilde{q}_1 \ldots \tilde{q}_N]^{\intercal}$, $\tilde{g}_{ij}(\tilde{\mathbf{q}})$ is defined as (see (2.55))

$$\tilde{g}_{ij}(\tilde{\mathbf{q}}) \triangleq \frac{\tilde{\lambda}_j^{(i)}}{\tilde{\sigma}_j^2 + \sum_{l=1}^{N} \tilde{q}_l \left| \gamma_{lj} \right|^2}, \tag{2.67}$$

and P_l^{peak} is the peak power limit for the jammer node located at $\mathbf{p}_l$. It is observed that all the constraints are linear with respect to $\tilde{\mathbf{q}}$ and $\mathbf{z}^J$ in (2.66). Furthermore, as a corollary of Proposition 2.3, one can conclude that the objective function in (2.66a) is a concave function of $\tilde{\mathbf{q}}$. (This holds since there are no assumptions about $\{P_l^J\}_{l=1}^N$ in Proposition 2.3 while proving the concavity of the objective function $\tilde{f}(\mathbf{z}^J)$ with respect to $\mathbf{z}^J$.) Therefore, it is concluded that the optimization problem in (2.66) is convex, as well. This implies that the joint jammer selection and jammer power optimization problem can be solved via the convex problem in (2.66) (after relaxing the selection vector).

Remark 2.5: As a special case of (2.66), it can be shown that the following problem is

also convex.

$$\max_{\tilde{\mathbf{q}}} \sum_{i=1}^{N_T} w_i \operatorname{tr}\left\{ \left(\sum_{j \in \mathcal{A}_L^{(i)}} \frac{\tilde{\lambda}_j^{(i)}}{\tilde{\sigma}_j^2 + \sum_{l=1}^{N} \tilde{q}_l \left|\gamma_{lj}\right|^2} \boldsymbol{\varphi}_{ij} \boldsymbol{\varphi}_{ij}^{\mathsf{T}} \right)^{-1} \right\}$$
$$\text{s.t.} \sum_{j=1}^{N} \tilde{q}_j \leq P_T,\ 0 \leq \tilde{q}_l \leq P_l^{peak} \text{ for } l = 1, 2, \ldots, N. \tag{2.68}$$

It is noted that this problem is in the same form as the problem discussed in [25, Eq. 9]. In [25], the convexity of this problem is not taken into account. Instead, a series of geometric programming approximations are proposed in order to solve the optimization problem. Since the problem [25, Eq. 9] is in fact convex, it can also be solved via convex optimization tools.

2.5.3 Robust Jammer Selection Problem

In the previous section, the jammer nodes are assumed to have the perfect knowledge of $\{\tilde{\lambda}_j^{(i)}\}_{i=1,j=1}^{N_T,N_A}$ in (2.55). Similar to Section 2.4.3, some uncertainty in $\{\tilde{\lambda}_j^{(i)}\}_{i=1,j=1}^{N_T,N_A}$ is introduced for a robust formulation. (No uncertainty is considered for $|\gamma_{kj}|^2$'s in (2.55) since they mainly depend on the known positions of the jammer and anchor nodes.) For simplicity, it is assumed that $\mathcal{A}_i = \{\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_{N_A}\}$, i.e., all the anchor nodes are connected to the ith target position for any i.

To formulate the robust jammer selection problem, we first define $\boldsymbol{\Lambda}_J \triangleq [\boldsymbol{\lambda}_J^{(1)}\ \boldsymbol{\lambda}_J^{(2)} \ldots \boldsymbol{\lambda}_J^{(N_T)}]$, where $\boldsymbol{\lambda}_J^{(i)} \triangleq [\tilde{\lambda}_1^{(i)}\ \tilde{\lambda}_2^{(i)} \ldots \tilde{\lambda}_{N_A}^{(i)}]^{\mathsf{T}}$ for $i = 1, \ldots, N_T$.

The estimated versions of $\boldsymbol{\lambda}_J^{(i)}$ are defined as $\hat{\boldsymbol{\lambda}}_J^{(i)}$ for $i = 1, 2, \ldots, N_T$, where $\hat{\boldsymbol{\lambda}}_J^{(i)}$ denotes the estimate of $\boldsymbol{\lambda}_J^{(i)}$. Let $\boldsymbol{\Delta\lambda}_J^{(i)}$ represent the error vector that generates uncertainty, that is, $\hat{\boldsymbol{\lambda}}_J^{(i)} = \boldsymbol{\lambda}_J^{(i)} + \boldsymbol{\Delta\lambda}_J^{(i)}$ with

$$\boldsymbol{\Delta\lambda}_J^{(i)} \triangleq [\Delta\tilde{\lambda}_1^{(i)}\ \Delta\tilde{\lambda}_2^{(i)} \ldots \Delta\tilde{\lambda}_{N_A}^{(i)}]^{\mathsf{T}} \tag{2.69}$$

for $i = 1, 2, \ldots, N_T$. Also, $\boldsymbol{\Delta\Lambda}_J$ and $\hat{\boldsymbol{\Lambda}}_J$ are defined as

$$\boldsymbol{\Delta\Lambda}_J \triangleq [\boldsymbol{\Delta\lambda}_J^{(1)}\ \boldsymbol{\Delta\lambda}_J^{(2)} \ldots \boldsymbol{\Delta\lambda}_J^{(N_T)}], \tag{2.70}$$
$$\hat{\boldsymbol{\Lambda}}_J \triangleq [\hat{\boldsymbol{\lambda}}_J^{(1)}\ \hat{\boldsymbol{\lambda}}_J^{(2)} \ldots \hat{\boldsymbol{\lambda}}_J^{(N_T)}]. \tag{2.71}$$

In this scenario, the notation for the objective function $\tilde{f}(\mathbf{z}^J)$ is modified as $\tilde{f}(\mathbf{z}^J, \mathbf{\Lambda}_J)$ in order to emphasize the dependence on $\mathbf{\Lambda}_J$. We use the same bounded error model as in Section 2.4.3 for the error matrix $\mathbf{\Delta\Lambda}_J$:

$$\mathbf{\Delta\Lambda}_J \in \tilde{\mathcal{E}} \triangleq \big\{\mathbf{\Delta\lambda}_J^{(i)} \in \mathbb{R}^{N_A} : |\Delta\tilde{\lambda}_j^{(i)}| \leq \tilde{\delta}_j^{(i)}, \\ \forall i = 1, 2, \ldots, N_T \text{ and } \forall j = 1, 2, \ldots, N_A\big\} \tag{2.72}$$

where $\{\tilde{\delta}_j^{(i)}\}_{i=1,j=1}^{N_T,N_A}$ determine the size of the uncertainty region $\tilde{\mathcal{E}}$ with $\tilde{\delta}_j^{(i)} \geq 0$ for all $i = 1, 2, \ldots, N_T$ and $j = 1, 2, \ldots, N_A$. The aim is to maximize the minimum CRLB that can be achieved in $\tilde{\mathcal{E}}$. Therefore, under this setup, the proposed optimization problem can be formulated as

$$\max_{\mathbf{z}^J} \min_{\mathbf{\Delta\Lambda}_J \in \tilde{\mathcal{E}}} \quad \tilde{f}(\mathbf{z}^J, \mathbf{\Lambda}_J) \tag{2.73a}$$

$$\text{subject to} \quad \sum_{k=1}^{N} z_k^J = N_J, \ \sum_{k=1}^{N} z_k^J P_k^J \leq P_T, \tag{2.73b}$$

$$0 \leq z_k^J \leq 1 \text{ for } k = 1, 2, \ldots, N, \tag{2.73c}$$

$$\mathbf{\Lambda}_J = \hat{\mathbf{\Lambda}}_J - \mathbf{\Delta\Lambda}_J. \tag{2.73d}$$

To solve the optimization problem in (2.73), the following lemma is utilized. To solve the optimization problem in (2.73), the following lemma is utilized.

Lemma 2.5: $\tilde{f}(\mathbf{z}^J, \mathbf{\Lambda}_J)$ is non-increasing in $\mathbf{\lambda}_J^{(i)}$ for all $i = 1, 2, \ldots, N_T$.

Proof: It suffices to show that $\text{tr}\left\{\left(\tilde{\mathbf{J}}_e^{(i)}(\mathbf{x}_i, \mathbf{z}^J)\right)^{-1}\right\}$ is non-increasing in $\mathbf{\lambda}_J^{(i)}$ for any $i = 1, 2, \ldots, N_T$, which is evident from (2.55). ■

Let the value of $\mathbf{\Delta\Lambda}_J$ that minimizes $\tilde{f}(\mathbf{z}^J, \mathbf{\Lambda}_J)$ over set $\tilde{\mathcal{E}}$ be denoted as $\mathbf{\Delta\Lambda}_J^*$ and let $\{\Delta\tilde{\lambda}_j^{(i),*}\}_{i,j}$ represent the elements of $\mathbf{\Delta\Lambda}_J^*$ (see (2.69) and (2.70)). Based on Lemma 2.5, it is obtained that Therefore, solving (2.73) is equivalent to solving the following optimization problem:

$$\max_{\mathbf{z}^J} \quad \tilde{f}(\mathbf{z}^J, \hat{\mathbf{\Lambda}}_J - \mathbf{\Delta\Lambda}_J^*) \tag{2.74a}$$

$$\text{subject to} \quad \sum_{k=1}^{N} z_k^J = N_J, \ \sum_{k=1}^{N} z_k^J P_k^J \leq P_T, \tag{2.74b}$$

$$0 \leq z_k^J \leq 1 \text{ for } k = 1, 2, \ldots, N. \tag{2.74c}$$

This problem is exactly in the same form as the problem in (2.65), hence, it is a convex optimization problem. Therefore, the solution methods proposed for the jammer selection problem can also be used for the problem in (2.74).

Remark 2.6: The imperfect knowledge of LOS/NLOS conditions can be incorporated into the $\lambda_{jk}^{(i)}$ and $\tilde{\lambda}_{j}^{(i)}$ parameters in Sections 2.4 and 2.5. (In the case of a NLOS link, the corresponding $\lambda_{jk}^{(i)}$ and $\tilde{\lambda}_{j}^{(i)}$ parameters become zero; i.e., no position related information is gathered from that link.) Hence, the cases with imperfect knowledge of LOS/NLOS conditions can be treated in the robust eavesdropper and jammer selection approaches in Sections 2.4.3 and 2.5.3.

2.6 Joint Eavesdropper and Jammer Selection

In this section, we consider the eavesdropper and jammer selection problems jointly and place jammer and eavesdropper nodes by considering both the localization performance of the anchor nodes (which is to be degraded) and the accuracy of the eavesdropper nodes for estimating the location of the target node (which is to be enhanced). In this part, it is assumed that the jammer nodes do not cause any interference at the eavesdropper nodes; e.g., by using directional antennas towards the anchor nodes. In addition, we make the same assumptions as in the eavesdropper selection problem and the jammer selection problem.

Based on the selection vectors $\mathbf{z}^E$ and $\mathbf{z}^J$, the joint eavesdropper and jammer selection problem can be formulated as

$$\max_{\mathbf{z}^J, \mathbf{z}^E} \quad \tilde{f}(\mathbf{z}^J) \tag{2.75a}$$

$$\text{subject to} \quad f(\mathbf{z}^E) \leq \rho, \ \sum_{k=1}^{N} z_k^E = N_E, \tag{2.75b}$$

$$\sum_{k=1}^{N} z_k^J = N_J, \ \sum_{k=1}^{N} z_k^J P_k^J \leq P_T, \tag{2.75c}$$

$$z_k^E \in \{0,1\} \text{ for } k = 1,2,\ldots,N \tag{2.75d}$$

$$z_k^J \in \{0,1\} \text{ for } k = 1,2,\ldots,N \tag{2.75e}$$

$$z_k^E z_k^J = 0 \text{ for } k = 1,2,\ldots,N \tag{2.75f}$$

where $\tilde{f}(\mathbf{z}^J)$ is as in (2.57), $f(\mathbf{z}^E)$ is given by (2.10), and ρ is a given accuracy threshold related to eavesdropping. The last constraint (2.75f) guarantees that a node can be selected either as an eavesdropper or as a jammer. By relaxing the constraints in (2.75d) and (2.75e), and modifying (2.75f), we obtain the following optimization problem:

$$\max_{\mathbf{z}^J, \mathbf{z}^E} \quad \tilde{f}(\mathbf{z}^J) \tag{2.76a}$$

$$\text{subject to} \quad f(\mathbf{z}^E) \leq \rho, \ \sum_{k=1}^{N} z_k^E = N_E, \tag{2.76b}$$

$$\sum_{k=1}^{N} z_k^J = N_J, \ \sum_{k=1}^{N} z_k^J P_k^J \leq P_T, \tag{2.76c}$$

$$0 \leq z_k^E \leq 1 \text{ for } k = 1, 2, \ldots, N \tag{2.76d}$$

$$0 \leq z_k^J \leq 1 \text{ for } k = 1, 2, \ldots, N \tag{2.76e}$$

$$0 \leq z_k^E + z_k^J \leq 1 \text{ for } k = 1, 2, \ldots, N. \tag{2.76f}$$

As consequences of Proposition 2.2 and 2.3, it is noted that the optimization problem (2.76) is a convex optimization problem. The selection of ρ depends on the requirements in a given scenario. For instance, if learning the positions of the target nodes is more important than jamming the localization network, ρ should be small. Alternatively, one can try to minimize $f(\mathbf{z}^E)$ while keeping $\tilde{f}(\mathbf{z}^J)$ above a certain threshold. From Proposition 2.2 and 2.3 it can be argued that the resulting problem would also be convex. Hence, by using convex optimization tools, the solution of (2.76) or its alternative version can be obtained. Then, starting from that solution, the largest-N_J (or, largest-N_E) and swap algorithms can be used to obtain the solution of (2.75) or its alternative version.

Remark 2.7: In this chapter, the eavesdropper selection, the jammer selection, the joint eavesdropper and jammer selection problems and their robust versions are formulated based on the CRLB expressions. Since the CRLB expressions provide tight lower bounds in the high SNR regime, by optimizing the CRLB expressions we also optimize the corresponding estimators for each problem for high SNRs. In the low-SNR regime, since the localization accuracy is low, the optimal selection problems do not have practical importance. This is the main reasoning behind optimizing the CRLB expressions.

2.7 Simulation Results

In this section, simulations are conducted to investigate the performance of the proposed approaches. We consider a wireless source localization network, in which the target node is located at one of the 121 possible positions with equal probabilities (i.e., 1/121). In particular, the set of possible target positions is given by $\{\mathbf{x}_i\}_{i=1}^{121} = \{[2m, 2n] \mid -5 \leq m, n \leq 5, m, n \in \mathbb{Z}\}$ meters. Also, there are 10 anchor nodes at locations $\{\mathbf{y}_j\}_{j=1}^{10} = \{[18\cos(\psi_j), 18\sin(\psi_j)] \mid \psi_j = 2\pi(j-1)/10, j = 1, 2, \ldots, 10\}$ meters. In addition, there exists 100 possible positions for the eavesdropper and jammer nodes which are selected uniformly from the region $\mathcal{R} = ([20, 50] \times [-50, 50]) \cup ([-50, -20] \times [-50, 50]) \cup ([-20, 20] \times [-50, -30]) \cup ([-20, 20] \times [30, 50])$ meters. Such a region is selected in order to keep eavesdropper/jammer nodes away from the localization network by considering a practical application scenario as in Section 2.1. Figure 2.1 illustrates the positions of the target and anchor nodes, as well as the possible positions for the eavesdropper and jammer nodes.

In the simulations, we consider the eavesdropper selection problem, the jammer selection problem, and the joint eavesdropper and jammer selection problem, given by (2.9), (2.56), and (2.75), respectively. For the problem in (2.75), we assume that $N_E + N_J = N$. In other words, we have $\mathbf{z}_k^E = 1 - \mathbf{z}_k^J$ for any k, for the joint eavesdropper and jammer selection problem.

The following algorithms are investigated for performance comparisons:

- *Relaxed Algorithm*: The relaxed versions of (2.9), (2.56), and (2.75) (see (2.44), (2.65), and (2.76)) are solved via the fmincon$(\cdot)$ command of MATLAB by using the interior point algorithm, which has polynomial-time complexity in the worst case, and is very fast in practice. The solution of (2.44) provides a lower bound for (2.9), whereas the solutions of (2.65) and (2.75) provide upper bounds for (2.56) and (2.75), respectively.

- *Largest-N_E Algorithm*: We set the largest N_E components of the solution of (2.44) to one and the others to zero, and we evaluate the performance of this resulting selection vector using the expression in (2.11).

- *Largest-N_J Algorithm*: In this algorithm, we set the largest N_J components of the solution

of (2.65) to one, and the others to zero. For the problem in (2.75), if the relaxed solution pair obtained from (2.76) is denoted as $(\mathbf{z}^E_{\text{relaxed}}, \mathbf{z}^J_{\text{relaxed}})$, we simply set the largest N_J components of $\mathbf{z}^J_{\text{relaxed}}$ to one and the others to zero. The resulting vector is denoted as $\mathbf{z}^J_{\text{largest}}$, and $\mathbf{z}^E_{\text{largest}}$ is defined as $\mathbf{1}-\mathbf{z}^J_{\text{largest}}$, where $\mathbf{1}$ is the vector of ones. (The solution pair $(\mathbf{z}^E_{\text{largest}}, \mathbf{z}^J_{\text{largest}})$ may not be feasible for (2.75) unless the threshold value, ρ, is sufficiently large.)

- *Proposed Swap Algorithm:* In this algorithm, we start from the solutions obtained from the largest-N_E or the largest-N_J algorithms. The swap operation is performed as explained in Sections 2.4 and 2.5, the details of which are given in Algorithm 1. In all the simulations, μ in Algorithm 1 is selected as 0.01. During one swap operation, the number of objective function evaluations is given by $N_E(N-N_E)$. In other words, the total number of objective evaluations is upper bounded by $N^{\max}_{\text{swap}}(N-N_E)N_E$ (similarly for the jammer selection problem).

- *Swap Algorithm with Random Initialization:* This algorithm is considered for comparison purposes similar to the local optimization algorithm in [110]. In this algorithm, we use the proposed swap algorithm (Algorithm 1) with arbitrarily generated initial selection vectors (inputs) for the eavesdropper selection problem or the jammer selection problem. While generating the random initial vectors, we randomly choose N_E or N_J positions from N possible eavesdropper/jammer positions by using the *randperm(N,N_E)* or *randperm(N,N_J)* command of MATLAB with different seeds.

For the eavesdropper selection problem, we assume that $\sigma_k^2 = \sigma^2$ for each k. Moreover, $\alpha^{(E,1)}_{ijk}$ and $\chi^{(i)}_{jk}$ are modeled as $\left|\alpha^{(E,1)}_{ijk}\right|^2 = \|\mathbf{x}_i - \mathbf{p}_k\|^{-2}$ and $\chi^{(i)}_{jk} = 0$. Hence, $\lambda^{(i)}_{jk}$ is expressed as $\lambda^{(i)}_{jk} = 4\pi\beta^2_{ij}E_{ij}/(c^2\|\mathbf{x}_i - \mathbf{p}_k\|^2\sigma^2)$, where $E_{ij} = \int_{-\infty}^{\infty}|S_{ij}(f)|^2\,df$ is the energy of the signal $s_{ij}(t)$ (see Proposition 2.1). Then, the signal parameters are selected such that $\lambda^{(i)}_{jk}$ is given by $\lambda^{(i)}_{jk} = 1/(\|\mathbf{x}_i - \mathbf{p}_k\|^2\sigma^2)$ [25].

For the jammer selection problem, it is assumed that $\tilde{\sigma}_j^2 = \tilde{\sigma}^2$ for each j, $\tilde{\lambda}^{(i)}_j = 1/(\|\mathbf{x}_i - \mathbf{y}_j\|^2)$, and $|\gamma_{kj}|^2 = \|\mathbf{p}_k - \mathbf{y}_j\|^{-2}$. Regarding the transmit powers of the jammer nodes, $P^J_k = 10$ for each k and P_T is selected as $10N$, i.e., the constraint given by $\sum_k z^J_k P^J_k \leq P_T$ becomes ineffective.

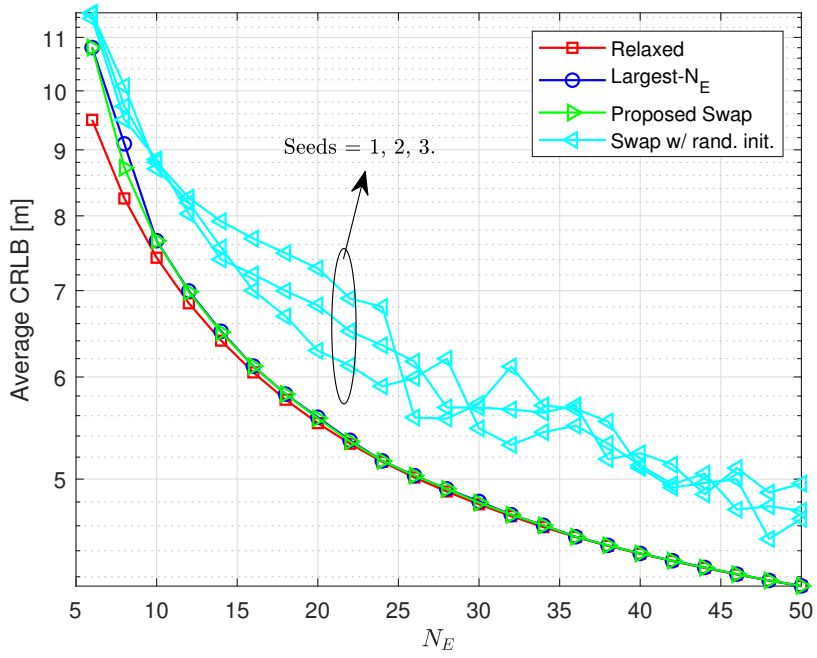


Figure 2.2: Average CRLB versus N_E when $\sigma^2 = 0.1$, $N_{\text{swap}}^{\max} = 5$, and the seeds of the random initial selection vectors are $1, 2, 3$ for the eavesdropper selection problem.

In order to perform simulations considering the shadowing effect, $\tilde{\lambda}_j^{(i)}$'s and $\lambda_{jk}^{(i)}$'s are multiplied with log-normal random variables with mean parameter -2 and variance parameter 1. Similarly, $|\gamma_{kj}|^2$'s are multiplied with log-normal random variables with mean parameter -2 and variance parameter 2.

In the simulations, for each problem, the square roots of the objectives are plotted, i.e., the average and the worst-case CRLB values are presented in terms of meters. The simulations are performed on an Intel Core i7 4.0 GHz PC with 16 GB of physical memory using MATLAB R2020b on a Windows 10 operating system.

2.7.1 Simulation Results with Perfect Knowledge of Parameters

In Figure 2.2, the eavesdropper selection problem is considered and the average CRLB performance of each algorithm is plotted versus N_E for the noise level $\sigma^2 = 0.1$ and $N_{\text{swap}}^{\max} = 5$. For the same setting, Figure 2.3 presents the average CRLB performance of each algorithm

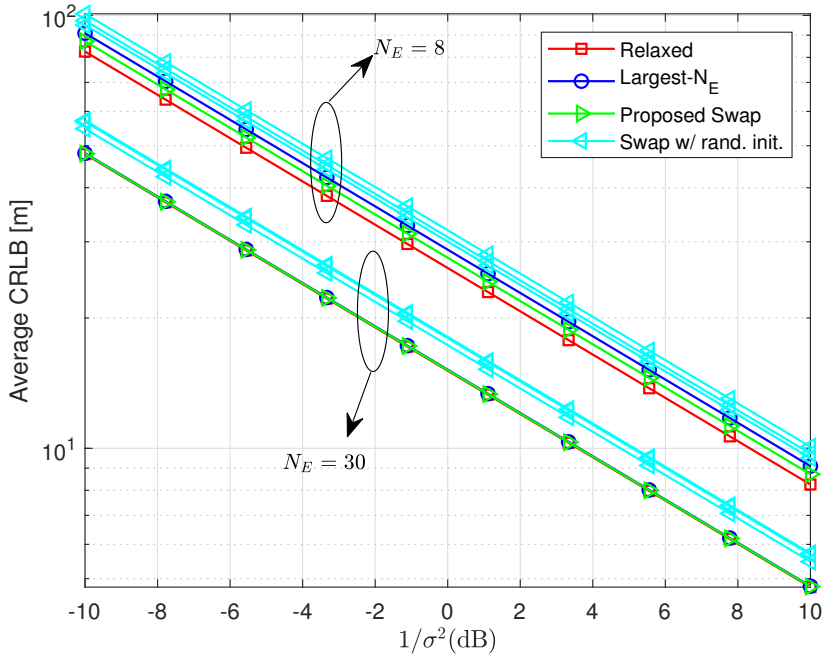


Figure 2.3: Average CRLB versus $1/\sigma^2$ when $N_E = 8$, $N_E = 30$, $N_{\text{swap}}^{\max} = 5$, and the seeds of the random initial selection vectors are $1, 2, 3$ for the eavesdropper selection problem.

versus $1/\sigma^2$ for $N_{\text{swap}}^{\max} = 5$ and two different levels of N_E's: $N_E = 8$ and $N_E = 30$. From Figures 2.2 and 2.3, it is observed that the solution of the relaxed problem provides a performance lower bound, as expected, and the largest-N_E algorithm and the proposed swap algorithm perform very similarly in this scenario. On the other hand, when the swap algorithm is executed based on three different random initial selection vectors (with seeds 1, 2, and 3), significant performance degradation is observed in comparison with the other algorithms. This implies that solving the relaxed problem and then obtaining the solution of the largest-N_E algorithm or the proposed swap algorithm is critical in achieving high localization accuracy.

As $\sigma_k^2 = \sigma^2$ for all $k = 1, 2, \ldots, N$, it is noted that by changing σ^2, we in fact scale all $\lambda_{jk}^{(i)}$'s with the same factor. Therefore, by Remark 2.1, it is concluded that the objective function is also scaled, as can be observed from Figure 2.3. Moreover, from Remark 2.1, it is known that the solution of the optimal eavesdropper selection problem (hence, that of the largest-N_E algorithm) remains the same for all σ^2's when N_E is fixed. For instance, when there are 8 eavesdroppers in the network, the $24, 33, 38, 39, 51, 77, 88, 92$th components of

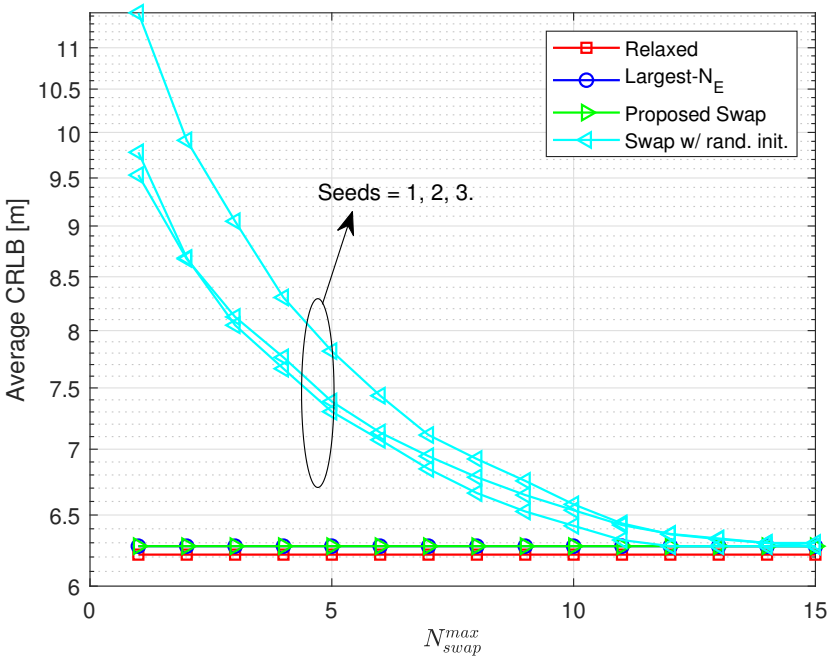


Figure 2.4: Average CRLB versus $N_{\text{swap}}^{\max}$ when $N_E = 15$, $\sigma^2 = 0.1$, and the seeds of the random initial selection vectors are $1, 2, 3$ for the eavesdropper selection problem.

$\mathbf{z}_{\text{largest}}^{E}$ are equal to 1 for both $\sigma^2 = 0.1$ and $\sigma^2 = 10$.

The average CRLB performance and run time of each algorithm are evaluated versus $N_{\text{swap}}^{\max}$ in Figure 2.4 and Figure 2.5, respectively, for $\sigma^2 = 0.1$ and $N_E = 15$. The results indicate that it requires around 13 swap operations for the swap algorithm with random initialization (with seed 1) to converge to the performance of the proposed swap algorithm. Namely, the average CRLB of the swap algorithm with random initialization is 11.4 m at $N_{\text{swap}}^{\max} = 1$ and reduces to that of the proposed swap algorithm (i.e., 6.27 m) at $N_{\text{swap}}^{\max} = 13$.

On the other hand, the starting point obtained by the proposed largest-N_E algorithm (6.27 m) is not improved by the proposed swap algorithm, i.e., the largest-N_E algorithm provides the best selection vector in this scenario (please see Algorithm 1). When the corresponding run times in are compared, the benefits of the proposed swap and largest-N_E algorithms are observed. While the run time of the proposed swap algorithm is 0.9 sec. for each $N_{\text{swap}}^{\max}$, that of the swap algorithm with random initialization is 10.11 sec. for $N_{\text{swap}}^{\max} = 13$. Thanks to the relaxed algorithm, the proposed swap algorithm starts with a selection vector which is very

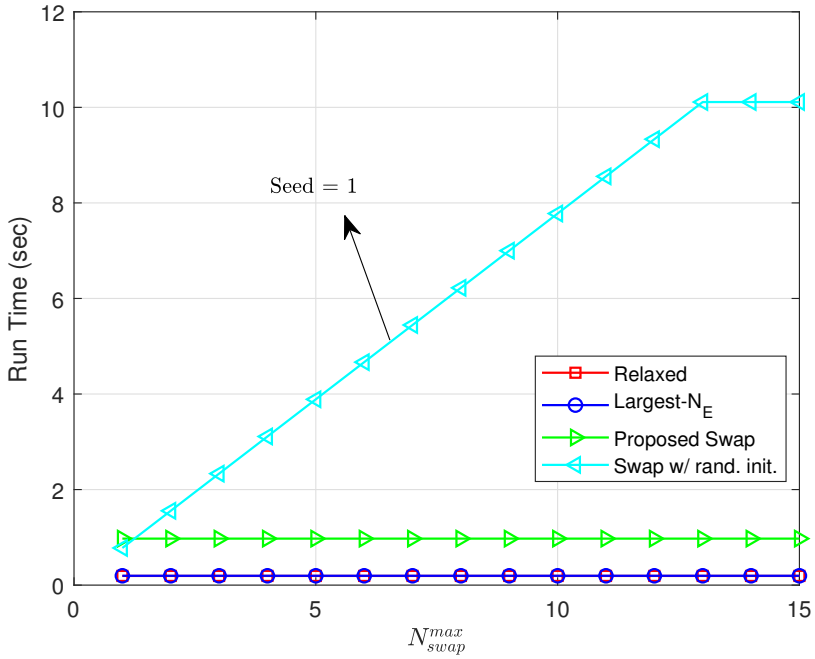


Figure 2.5: Run time versus $N_{\text{swap}}^{\max}$ when $N_E = 15$, $\sigma^2 = 0.1$, and the seed of the random initial selection vector is 1 for the eavesdropper selection problem.

close to the optimal selection vector; hence, it obtains the solution quickly. On the other hand, with random initial selection vectors, high localization accuracy cannot be obtained without performing a time-consuming search based on swap operations.

In Figure 2.6, the jammer selection problem is considered and the average CRLB performance of each algorithm is plotted versus N_J for the noise level $\tilde{\sigma}^2 = 0.1$. For the same setting, Figure 2.7 presents the average CRLB performance of each algorithm versus $1/\tilde{\sigma}^2$ for $N_J = 15$. From Figures 2.6 and 2.7, it is observed that the solution of the relaxed problem provides a performance upper bound, as expected, and the proposed largest-N_J algorithm and the proposed swap algorithm perform similarly. However, when the proposed swap algorithm is implemented based on three different random initial jammer selection vectors (instead of the solution of the largest-N_J algorithm), the obtained CRLB values reduce significantly. This indicates the advantage of the proposed approaches over the swap algorithm with random initialization.

The CRLB performance and run time of each algorithm are evaluated versus $N_{\text{swap}}^{\max}$ for

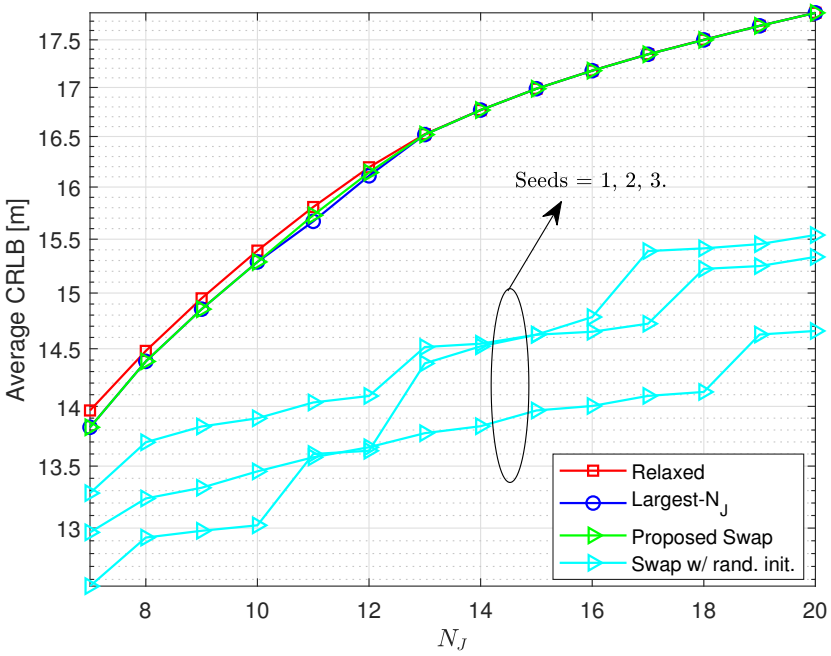


Figure 2.6: Average CRLB versus N_J when $\tilde{\sigma}^2 = 0.1$, $N_{\text{swap}}^{\max} = 5$, and the seeds of the random initial selection vectors are $1, 2, 3$ for the jammer selection problem.

$\tilde{\sigma}^2 = 0.1$ and $N_J = 15$ in Figures 2.8 and 2.9. The results indicate that after around 13 swap operations, the average CRLB of the swap algorithm with random initialization (which is initially 10.67 m.) converges that of the proposed swap algorithm (i.e., 16.98 m). (In this scenario, the starting point obtained by the proposed largest-N_J algorithm already corresponds to the best selection vector.) While the run time of the proposed swap algorithm is 0.2 sec., it takes around 5.24 sec. for the swap algorithm with random initialization (with seed 1) to converge to the proposed swap algorithm. Hence, the proposed swap and largest-N_J algorithms have significantly lower execution times than the swap algorithm with random initialization considering the same CRLB performance. This indicates that the proposed approach of solving the relaxed algorithm and using its solution as a basis for the largest-N_J and the swap algorithms provides significant benefits in obtaining the solution of the optimal jammer selection problem. In other words, the swap algorithm cannot achieve close to optimal performance in a short amount of time by starting from a random selection vector.

In Figure 2.10, the joint eavesdropper and jammer selection problem is investigated, and the average CRLB performances corresponding to the objective functions $f(\mathbf{z}^E)$ and $\tilde{f}(\mathbf{z}^J)$

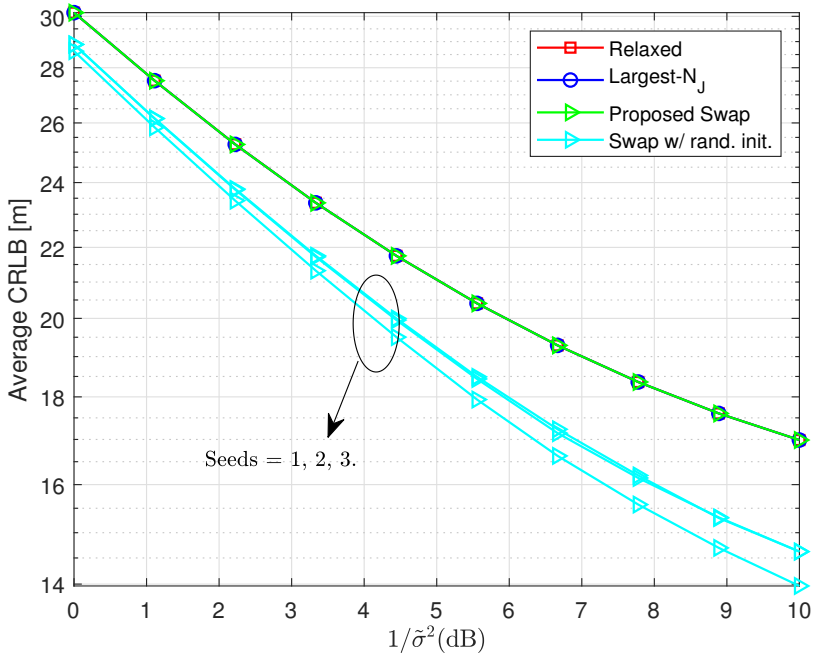


Figure 2.7: Average CRLB versus $1/\tilde{\sigma}^2$ when $N_J = 15$, $N_{\text{swap}}^{\max} = 5$, and the seeds of the random initial selection vectors are $1, 2, 3$ for the jammer selection problem.

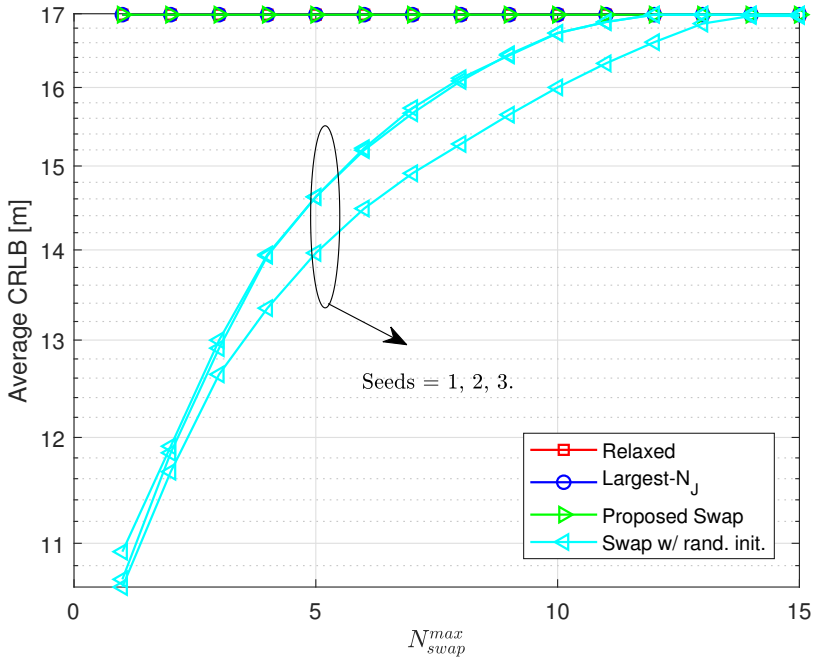


Figure 2.8: Average CRLB versus $N_{\text{swap}}^{\max}$ when $\tilde{\sigma}^2 = 0.1$, $N_J = 15$, and the seeds of the random initial selection vectors are $1, 2, 3$ for the jammer selection problem.

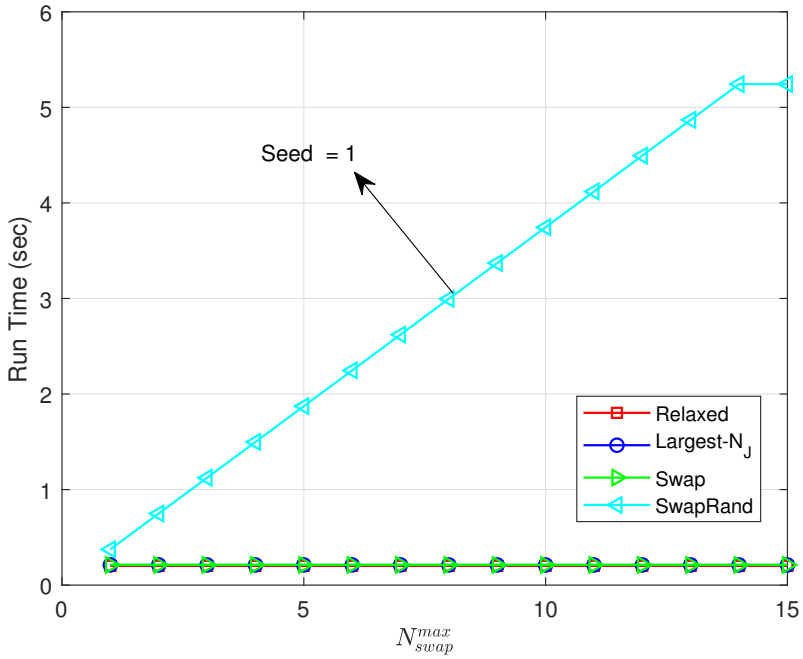


Figure 2.9: Run time versus $N_{\text{swap}}^{\max}$ when $\tilde{\sigma}^2 = 0.1$, $N_J = 15$, and the seed of the random initial vector is 1 for the jammer selection problem.

are plotted for each algorithm when $\rho = 50$ (see (2.75) and (2.76)). It is calculated that for $N_J = 60, 70, 90$, or equivalently $N_E = 40, 30, 10$, the solution of the largest-N_E algorithm is not a feasible solution for (2.75). For example, when $N_J = 60$, the average CRLB for the largest-N_E algorithm is 54.06, which is higher than $\rho = 50$. Also, even though the solutions of the largest-N_E algorithm are infeasible for $N_J = 60, 70$, starting from these solutions, via the proposed swap algorithm, it is possible obtain feasible selection vectors without reducing the value of $\tilde{f}(\mathbf{z}^J)$. However, when $N_J = 90$, via the proposed swap algorithm, it is not possible to obtain a feasible selection vector.

Moreover, a decrease is observed in the optimal value of $f(\mathbf{z}^E)$ from $N_J = 60$ to $N_J = 70$, or equivalently from $N_E = 40$ to $N_E = 30$. In other words, it is not possible to claim any monotonic behavior in $f(\mathbf{z}^E)$ with respect to N_E due to the constraint given by $f(\mathbf{z}^E) \leq \rho$ for the problem in (2.75). Furthermore, the relaxed problem does not necessarily provide a lower bound on $f(\mathbf{z}^E)$ as noted from the results at $N_J = 60$ and $N_J = 70$ (equivalently, $N_E = 40$ and $N_E = 30$).

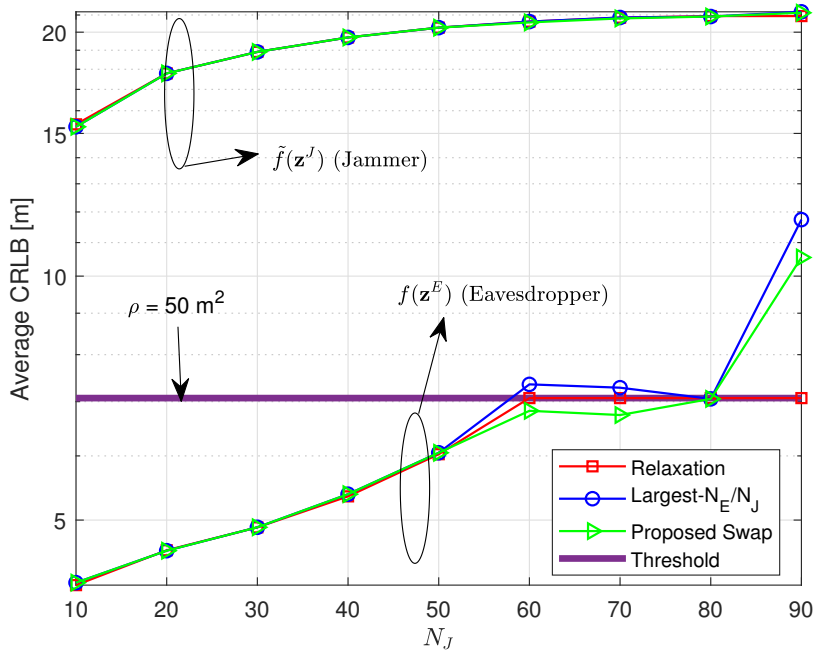


Figure 2.10: Average CRLB versus N_J when $\tilde{\sigma}^2 = \sigma^2 = 0.1$ and $\rho = 50$ for the joint eavesdropper and jammer selection problem.

2.7.2 Effects of Uncertainty in Knowledge of Target and/or Anchor Locations

In this part, we introduce some uncertainty to the knowledge related to the locations of the anchor and target nodes, and obtain the optimal selection strategies (using the relaxed formulations) for the cases of imperfect and perfect knowledge. Then, we apply the largest-N_E/N_J and proposed swap algorithms and evaluate their performance based on the actual system parameters. For the eavesdropper selection problem, we consider a scenario in which the eavesdropper nodes do not know the probability distribution of the target node location perfectly. (The knowledge of anchor node locations is not required for the eavesdropper selection problem.) In particular, for $i = 1, 2, \ldots, N_T$, the actual distribution of the target node location is given by

$$\tilde{w}_i = A \exp\left(-\frac{(x_{i1} - x_{01})^2}{2\nu^2} - \frac{(x_{i2} - x_{02})^2}{2\nu^2} \right) \tag{2.77}$$

where $\tilde{w}_i = \Pr\{\text{Target node is located at } \mathbf{x}_i\}$, $\mathbf{x}_i = [x_{i1}\, x_{i2}]^\intercal$, $\bar{x} = [x_{01}\, x_{02}]^\intercal$ is the mean of the target node location, and A is a normalization constant such that

$$\sum_{i=1}^{N_T} A \exp\left(-\frac{(x_{i1}-x_{01})^2}{2\nu^2} - \frac{(x_{i2}-x_{02})^2}{2\nu^2}\right) = 1. \tag{2.78}$$

On the other hand, the eavesdropper nodes assume that $\Pr\{\text{Target node is located at } \mathbf{x}_i\} = 1/N_T$ for $i = 1, 2, \ldots, N_T$. It is noted that as ν tends to infinity, $\tilde{w}_i$ approaches to $1/N_T$ for each i. In other words, as ν increases, the mismatch between the true distribution and the assumed one decreases. On the other extreme, when ν goes to zero, the target node is located at $\bar{x}$ with probability one; hence, the uniform distribution assumption becomes quite inaccurate.

In the simulations, we assume that $x_{01} = x_{02} = 0$ and $N_{\text{swap}}^{\max} = 5$. In Figure 2.11, the average CRLB performance of each algorithm is plotted versus ν (in dB) for $N_E = 20$, $\sigma^2 = 0.1$, and $\mu = 0.01$. It is observed that as long as the information about the distribution of the target node location is not very inaccurate, the proposed approach does not have a significant performance loss. Also, as the mismatch between the true distribution and the assumed one decreases (i.e., as ν increases), the proposed swap algorithm performs very similarly for both the true model and the assumed one.

For the jammer selection problem, we assume that the jammer nodes do not know the locations of the anchor nodes perfectly. It is assumed that for any $\mathbf{y}_j = [y_{j1}\, y_{j2}]^\intercal$, the jammer nodes have the knowledge of an erroneous version of $\mathbf{y}_j$. Let $\tilde{\mathbf{y}}_j$ be the assumed location of the jth anchor node by the jammer nodes. We model that $\tilde{\mathbf{y}}_j$ is uniformly chosen from a set $\{\mathbf{y} \mid \mathbf{y} = [y_1\, y_2]^\intercal, |y_1 - y_{j1}| \leq r \,\&\, |y_2 - y_{j2}| \leq r\}$. In Figure 2.12, when $\tilde{\sigma}^2 = 0.1$, $\nu = 1$, $r = 1$, and $\mu = 0.01$, the average CRLB performance of each algorithm is plotted versus N_J. It is observed that the proposed swap algorithm is quite robust to errors in the knowledge of anchor and target node locations. Even though the anchor node locations and the distribution of the target node location are not known perfectly, as N_J increases, the proposed swap algorithm performs very similarly for both the true model and the assumed one.

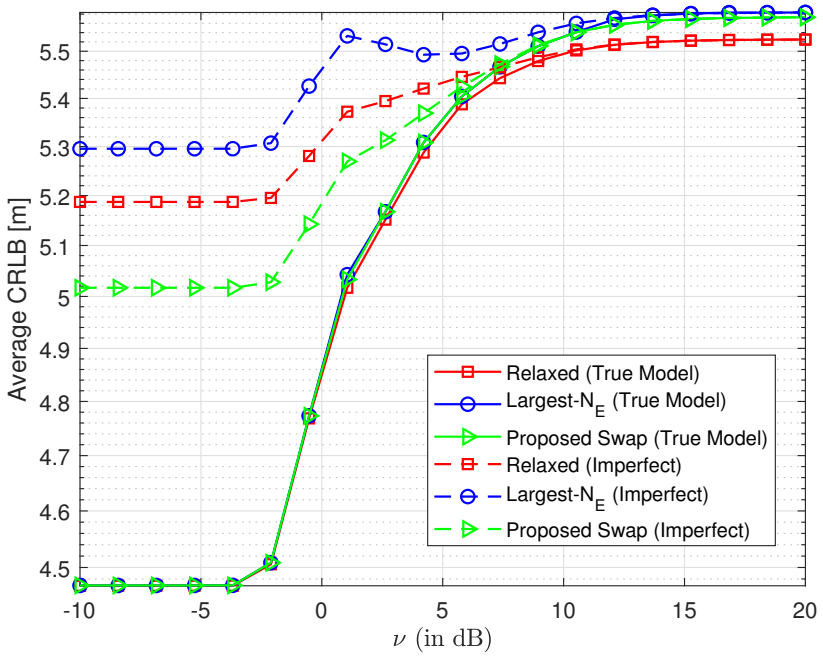


Figure 2.11: Average CRLB versus ν (in dB) when $N_E = 20$, $\sigma^2 = 0.1$, and $\mu = 0.01$.

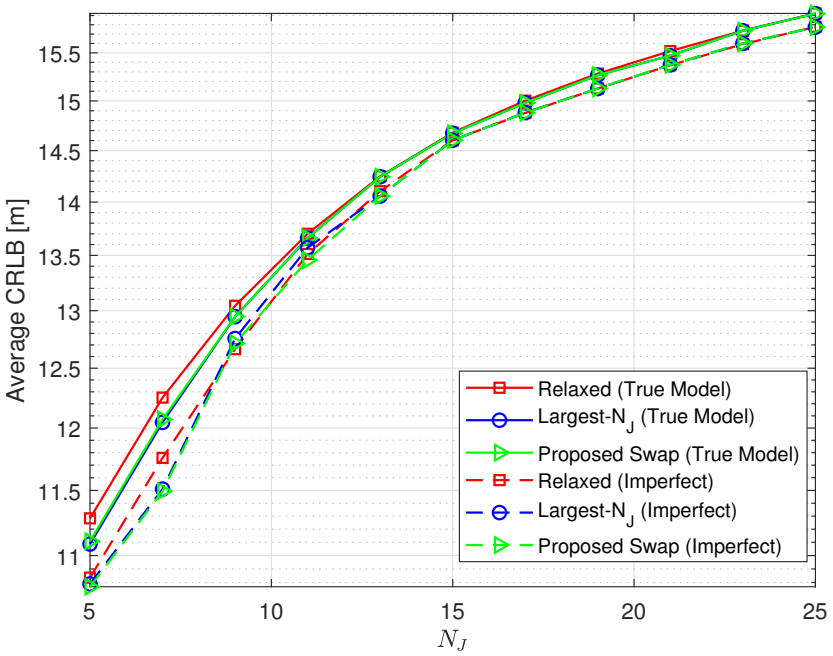


Figure 2.12: Average CRLB versus N_J when $\tilde{\sigma}^2 = 0.1$, $\nu = 1$, $r = 1$, and $\mu = 0.01$.

2.7.3 Simulation Results for Robust Approaches

In this part, the robust eavesdropper selection problem in Section 2.4.3 and the robust jammer selection problem in Section 2.5.3 are considered. The worst-case CRLB performances of the algorithms are compared for both the robust and non-robust approaches. In the robust approach, the problems given by (2.53) and (2.74) are considered for the robust eavesdropper and the robust jammer selection problems, respectively. However, in the non-robust case, the following optimization problems are considered: $\min_{\mathbf{z}^E} f(\mathbf{z}^E, \hat{\mathbf{\Lambda}}_E)$ subject to $\sum_{k=1}^{N} z_k^E = N_E$, $0 \leq z_k^E \leq 1$ for $k = 1, 2, \ldots, N$, which is the non-robust version of the eavesdropper selection problem, and $\max_{\mathbf{z}^J} \tilde{f}(\mathbf{z}^J, \hat{\mathbf{\Lambda}}_J)$ subject to $\sum_{k=1}^{N} z_k^J = N_J$, $0 \leq z_k^J \leq 1$ for $k = 1, 2, \ldots, N$, which is the non-robust version of the jammer selection problem.

For the eavesdropper selection problem, both the robust and non-robust approaches are considered, and two different selection vectors denoted as $\mathbf{z}_R^E$ and $\mathbf{z}_{NR}^E$ (corresponding to robust and non-robust, respectively) are obtained for each algorithm. Then, for $\mathbf{z}_R^E$ and $\mathbf{z}_{NR}^E$, the corresponding worst-case CRLBs are computed, which are given by $f(\mathbf{z}_R^E, \hat{\mathbf{\Lambda}}_E - \mathbf{\Delta\Lambda}_E^*)$ and $f(\mathbf{z}_{NR}^E, \hat{\mathbf{\Lambda}}_E - \mathbf{\Delta\Lambda}_E^*)$, respectively. Similarly, for the jammer selection problem, we define two different selection vectors as $\mathbf{z}_R^J$ and $\mathbf{z}_{NR}^J$, and evaluate $\tilde{f}(\mathbf{z}_R^J, \hat{\mathbf{\Lambda}}_J - \mathbf{\Delta\Lambda}_J^*)$ and $\tilde{f}(\mathbf{z}_{NR}^J, \hat{\mathbf{\Lambda}}_J - \mathbf{\Delta\Lambda}_J^*)$.

For the uncertainty region $\mathcal{E}$, each $\lambda_{jk}^{(i)}$ is modeled as $\lambda_{jk}^{(i)} \in [(1-\epsilon^{(i)})\hat{\lambda}_{jk}^{(i)},\ (1+\epsilon^{(i)})\hat{\lambda}_{jk}^{(i)}]$ for some $\epsilon^{(i)} \in [0, 1]$. Therefore, the eavesdropper selection is based on $(1-\epsilon^{(i)})\hat{\lambda}_{jk}^{(i)}$'s for the robust approach whereas $\hat{\lambda}_{jk}^{(i)}$'s are used for the non-robust approach. It is noted that $\delta_{jk}^{(i)}$ in (2.50) can be expressed as $\delta_{jk}^{(i)} = \epsilon^{(i)}\hat{\lambda}_{jk}^{(i)}$. If all $\epsilon^{(i)}$'s are not identical (which is commonly the case in practice), we expect performance difference between the robust and non-robust approaches. To that aim, we generate $N_T = 121$ realizations of independent uniform random variables distributed in $[0, 1]$ for $\epsilon^{(i)}$'s by using MATLAB (the seed is equal to 1).

For the jammer selection problem, we use a similar setup. For the uncertainty region $\tilde{\mathcal{E}}$, we generate $N_T = 121$ realizations of independent uniform random variables distributed in $[0, 1]$, denoted as $\kappa^{(i)}$, by using MATLAB (the seed is equal to 2). In this case, the jammer selection is based on the estimate of $\tilde{\lambda}_j^{(i)}$ multiplied with $(1 + \kappa^{(i)})$.

In Figures 2.13 and 2.14, the worst-case CRLB performances are presented respectively for

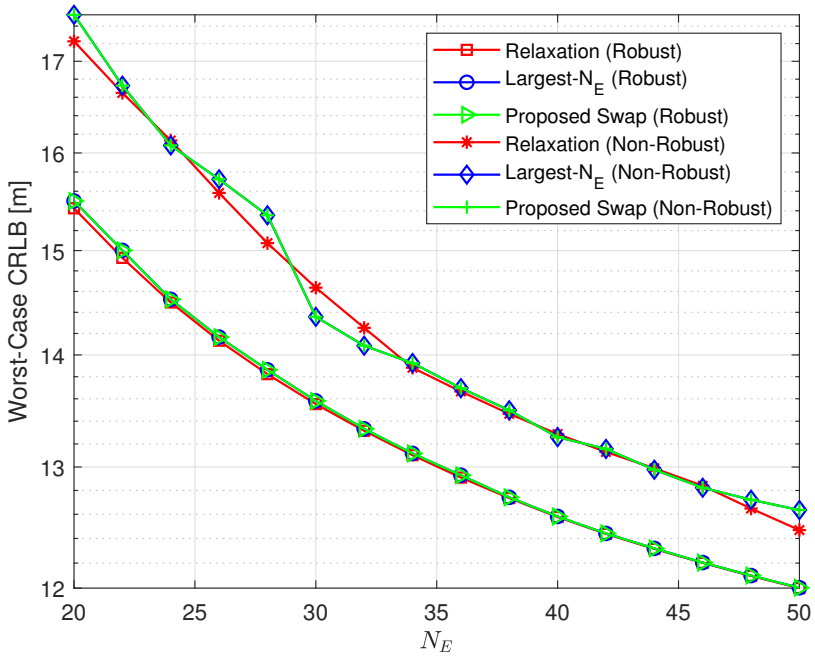


Figure 2.13: Worst-case CRLB versus N_E when $\sigma^2 = 0.1$ and $N_{\text{swap}}^{\max} = 5$ for the robust eavesdropper selection problem.

the eavesdropper selection and the jammer selection problems, considering both the robust and non-robust approaches. In Figure 2.13, as expected, the robust approaches yield lower worst-case CRLBs than the non-robust ones. On the other hand, the robust approach and the non-robust approach perform very similarly in Figure 2.14. In other words, for this system setup, without having the perfect knowledge of $\tilde{\lambda}_j^{(i)}$'s, one can achieve similar CRLB values to those achieved by the robust approach.

2.8 Concluding Remarks

For wireless source localization networks, the eavesdropper selection, jammer selection, and joint eavesdropper and jammer selection problems have been proposed. Related to the eavesdropper selection problem, a novel CRLB expression has been derived as the performance metric, and its convexity and monotonicity properties have been proved. After relaxing the integer constraints, a convex optimization problem has been obtained and eavesdropper

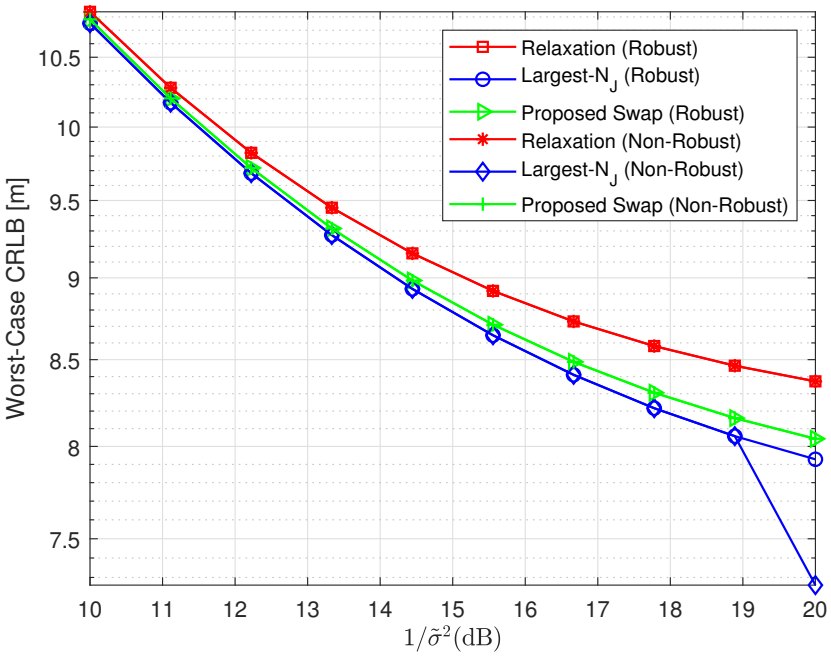


Figure 2.14: Worst-case CRLB versus $1/\tilde{\sigma}^2$ when $N_J = 5$ and $N_{\text{swap}}^{\max} = 5$ for the robust jammer selection problem.

selection algorithms have been proposed. Also, a robust approach has been developed in the presence of uncertainty about system parameters. For the jammer selection problem, a CRLB expression from the literature has been utilized, and its concavity and monotonicity properties have been derived. Similarly, a convex relaxation approach and a robust approach have also been developed for jammer selection. Moreover, the joint eavesdropper and jammer selection problem has been proposed and its relaxed version has been shown to reduce to a convex problem. Various simulation results have illustrated the benefits of the proposed algorithms in terms of performance and run time. In particular, the performance achieved by the proposed algorithms is very close to the performance bound specified by the relaxed problems, and the corresponding run times are significantly lower than the other alternatives such as the swap algorithm with random initialization and the exhaustive search. The results in this chapter reveal the capabilities of jammer and eavesdropper nodes, which can be useful for designing wireless source localization networks and taking appropriate precautions.

Chapter 3

Anchor Placement in TOA based Wireless Localization Networks via Convex Relaxation

In this chapter, we study the anchor placement problem by approximating it with an *anchor selection* problem for TOA based wireless localization networks. After studying the proposed eavesdropper selection and the jammer selection problems in Chapter 2, one can realize that the analyses in Chapter 2 can be utilized also for the anchor selection problem. By exploiting the ideas in Chapter 2, we prove that the anchor selection problem becomes a convex problem after relaxing the integer constraints. Moreover, we use similar algorithms proposed in Chapter 2 for the anchor selection problem. We also show that the analyses are valid also for TDOA or RSS based wireless localization networks.

3.1 System Model

Consider a two-dimensional wireless source localization network in which a target (source) node sends signals to anchor (reference) nodes for estimation of the target node location by anchor nodes. It is known that the target node is located at $\mathbf{x}_i \in \mathbb{R}^2$ with probability $w_i \geq 0$

for $i = 1, 2, \ldots, N_T$, where N_T is the number of possible target locations and $\sum_{i=1}^{N_T} w_i = 1$. Anchor nodes are located at $\{\mathbf{y}_j\}_{j=1}^{N_A} \subset \mathbb{R}^2$, where N_A is the number of anchor nodes in the network. ϕ_{ij} is the angle between jth anchor node and ith target node, i.e., $\phi_{ij} = \arctan \frac{x_{i2}-y_{j2}}{x_{i1}-y_{j1}}$, where $\mathbf{x}_i = [x_{i1}\, x_{i2}]^\intercal$ and $\mathbf{y}_j = [y_{j1}\, y_{j2}]^\intercal$.

In the following sections, we provide the signal model and formulate the corresponding anchor placement problems for TOA, TDOA and RSS based wireless localization networks.

3.2 TOA Based Anchor Placement Problem

3.2.1 Signal Model

Consider a scenario in which the clocks of the anchor and target nodes are perfectly synchronized. For the signal emitted from the target node located at $\mathbf{x}_i$, the signal received at the anchor node at location $\mathbf{y}_j$ is given by

$$r_{ij}(t) = \sum_{l=1}^{L_{ij}} \alpha_{ij}^{(l)} s_i\big(t - \tau_{ij}^{(l)}\big) + \eta_{ij}(t) \tag{3.1}$$

where $s_i(t)$ is a known signal transmitted from the ith target node, L_{ij} is the number of multipath components between the jth anchor node and the ith target node, $\alpha_{ij}^{(l)}$, and $\tau_{ij}^{(l)}$ denote, respectively, the amplitude and the delay of the lth multipath component between the jth anchor node and the ith target node, and $\eta_{ij}(t)$ is the measurement noise modeled as zero-mean white Gaussian noise with a power spectral density level of $N_0/2$. The delays of the paths are given by

$$\tau_{ij}^{(l)} = \frac{\|\mathbf{y}_j - \mathbf{x}_i\|_2 + b_{ij}^{(l)}}{c} \tag{3.2}$$

where c is the speed of the light and $b_{ij}^{(l)}$ is the range-bias term ($b_{ij}^{(l)} = 0$ for line-of-sight (LOS) propagation and $b_{ij}^{(l)} > 0$ for non-line-of-sight (NLOS) propagation).

3.2.2 Problem Formulation

In the considered wireless localization network, the aim is to determine the best N_A locations to place the anchor nodes in order to estimate the location of the target node as accurately as possible in the mean-square sense. In other words, $\mathbf{y}_j$'s are the optimization variables in the anchor placement problem. In order to emphasize that, we introduce a matrix $\mathbf{Y}$ as follows: $\mathbf{Y} \triangleq [\mathbf{y}_1\, \mathbf{y}_2\, \ldots\, \mathbf{y}_{N_A}]$. It is assumed that each anchor node can be placed in some bounded region $\mathcal{R} \subset \mathbb{R}^2$, that is, $\mathbf{y}_j \in \mathcal{R}$ for $j = 1, \ldots, N_A$.

After defining the anchor positions as optimization variables, the number, amplitudes and delays of the multipath components, and the angles between the anchor and target nodes become functions of the anchor positions. In order to emphasize the dependence on $\mathbf{Y}$, we replace L_{ij}, $\alpha_{ij}^{(l)}$, $\tau_{ij}^{(l)}$, and ϕ_{ij} with $L_i(\mathbf{y}_j)$, $\alpha_i^{(l)}(\mathbf{y}_j)$, $\tau_i^{(l)}(\mathbf{y}_j)$, and $\phi_i(\mathbf{y}_j)$, respectively, in the remainder of this chapter.

Via similar steps to those in [99], the equivalent Fisher information matrix (EFIM), $\mathbf{J}_i^{\mathrm{TOA}}(\mathbf{Y})$, corresponding to the target location $\mathbf{x}_i$ can be expressed as a function of the anchor locations $\{\mathbf{y}_j\}_{j=1}^{N_A}$ as

$$\mathbf{J}_i^{\mathrm{TOA}}(\mathbf{Y}) = \sum_{j \in \mathcal{A}_i^L(\mathbf{Y})} \lambda_i(\mathbf{y}_j) \boldsymbol{\varphi}_i(\mathbf{y}_j) \boldsymbol{\varphi}_i(\mathbf{y}_j)^{\intercal}, \tag{3.3}$$

$$\lambda_i(\mathbf{y}_j) \triangleq \frac{8\pi^2 \beta_i^2}{c^2}(1 - \xi_i(\mathbf{y}_j)) \frac{|\alpha_i^{(1)}(\mathbf{y}_j)|^2 \int_{-\infty}^{\infty} |S_i(f)|^2\, df}{N_0}, \tag{3.4}$$

$$\beta_i^2 \triangleq \frac{\int_{-\infty}^{\infty} f^2 |S_i(f)|^2\, df}{\int_{-\infty}^{\infty} |S_i(f)|^2\, df},\ \boldsymbol{\varphi}_i(\mathbf{y}_j) \triangleq [\cos(\phi_i(\mathbf{y}_j))\ \sin(\phi_i(\mathbf{y}_j))]^{\intercal} \tag{3.5}$$

where $\mathcal{A}_i^L(\mathbf{Y})$ is the set of indices of anchor nodes that are in LOS with the target node at location $\mathbf{x}_i$ for the anchor positions given by matrix $\mathbf{Y}$, $S_i(f)$ is the Fourier transform of $s_i(t)$, and $\xi_i(\mathbf{y}_j)$ is the path-overlap coefficient for the anchor location $\mathbf{y}_j$ and the target location $\mathbf{x}_i$ satisfying $0 \leq \xi_i(\mathbf{y}_j) \leq 1$ [99].

It is known that for any unbiased estimator $\hat{\mathbf{x}}_i$ of $\mathbf{x}_i$, the error vector satisfies [103]:

$$\mathbb{E}\{\|\hat{\mathbf{x}}_i - \mathbf{x}_i\|_2^2\} \geq \mathrm{tr}\left\{\mathbf{J}_i^{\mathrm{TOA}}(\mathbf{Y})^{-1}\right\} \tag{3.6}$$

where the expression on the right-hand-side corresponds to the CRLB. Then, by considering the CRLB as a performance metric, the proposed anchor placement problem can be

formulated as

$$\min_{\mathbf{Y}} \quad \sum_{i=1}^{N_T} w_i \operatorname{tr}\left\{\mathbf{J}_i^{\mathrm{TOA}}(\mathbf{Y})^{-1}\right\} \tag{3.7a}$$

$$\text{subject to} \quad \mathbf{y}_j \in \mathcal{R},\ j = 1, 2, \ldots, N_A. \tag{3.7b}$$

3.2.3 Theoretical Results and Algorithms

From (3.3) and (3.5), $\operatorname{tr}\left\{\mathbf{J}_i^{\mathrm{TOA}}(\mathbf{Y})^{-1}\right\}$ can be expressed after some algebraic manipulations as

$$\operatorname{tr}\left\{\mathbf{J}_i^{\mathrm{TOA}}(\mathbf{Y})^{-1}\right\} = \frac{2\sum_{k\in\mathcal{A}_i^L(\mathbf{Y})}\lambda_i(\mathbf{y}_k)}{\sum_{k\in\mathcal{A}_i^L(\mathbf{Y})}\sum_{l\in\mathcal{A}_i^L(\mathbf{Y})}\lambda_i(\mathbf{y}_k)\lambda_i(\mathbf{y}_l)\sin^2(\phi_i(\mathbf{y}_k)-\phi_i(\mathbf{y}_l))} \tag{3.8}$$

It is noted from (3.8) that the optimal anchor placement problem in (3.7) is quite challenging since the number of multipath components, the amplitudes, the delays, the angles between the anchor and target nodes, and the path-overlap coefficients become functions of the anchor locations (see (3.3)–(3.5)). Moreover, this problem is not convex in general. For example, the set $\mathcal{R}$ may not necessarily be a convex set.

In order to solve the anchor placement problem, we first discretize set $\mathcal{R}$ in (3.7b). Let $\widetilde{\mathcal{R}}$ be a finite subset of $\mathcal{R}$, and consider the problem in (3.7) for set $\widetilde{\mathcal{R}}$ by replacing the constraint in (3.7b) by $\mathbf{y}_j \in \widetilde{\mathcal{R}}$ for $j = 1, \ldots, N_A$. Since the objective function in (3.7a) is continuous with respect to the anchor locations, the optimal value of the discretized version of (3.7) gets closer to the optimal value of (3.7) as the number of elements in $\widetilde{\mathcal{R}}$ increases. Therefore, it is possible to achieve an accurate approximation to the original problem in (3.7) via discretization.

In the discretized version of (3.7), the aim is to identify a subset of $\widetilde{\mathcal{R}}$ with a cardinality of N_A. As $\widetilde{\mathcal{R}}$ is finite, we can represent its elements as $\widetilde{\mathcal{R}} = (\mathbf{y}^{(k)})_k$. Furthermore, we define $\lambda_i^{(k)} \triangleq \lambda_i(\mathbf{y}^{(k)})$, $\phi_i^{(k)} \triangleq \phi_i(\mathbf{y}^{(k)})$, and $\boldsymbol{\varphi}_i^{(k)} \triangleq \boldsymbol{\varphi}_i(\mathbf{y}^{(k)})$ for any i and k. Moreover, let the set of indices of anchor nodes in $\widetilde{\mathcal{R}}$ which are in LOS with the target node at location $\mathbf{x}_i$ be denoted as $\widetilde{\mathcal{A}_i^L}$ for any i. For any set $\mathcal{S}$, we define $\mathcal{S}_i^L \triangleq \mathcal{S} \cap \widetilde{\mathcal{A}_i^L}$. Then, the discretized

version of (3.7) is expressed as

$$\min_{\mathcal{S}\subset\mathbb{N}} \quad \sum_{i=1}^{N_T} w_i \, f_i^{\mathrm{TOA}}(\mathcal{S}) \tag{3.9a}$$

$$\text{subject to} \quad |\mathcal{S}| = N_A \tag{3.9b}$$

where $\mathbb{N}$ denotes the set of natural numbers and $f_i^{\mathrm{TOA}}(\mathcal{S})$ is given by

$$f_i^{\mathrm{TOA}}(\mathcal{S}) \triangleq \frac{2\sum_{k\in\mathcal{S}_i^L} \lambda_i^{(k)}}{\sum_{k\in\mathcal{S}_i^L}\sum_{l\in\mathcal{S}_i^L} \lambda_i^{(k)}\lambda_i^{(l)} \sin^2\left(\phi_i^{(k)} - \phi_i^{(l)}\right)} \tag{3.10}$$

The following lemma proves that solving (3.9) is equivalent to minimizing the ratio of non-decreasing supermodular functions subject to a cardinality constraint.

Lemma 3.1: The objective function in (3.9) is a ratio of two non-decreasing supermodular functions.

Proof: Define

$$p_i^{\mathrm{TOA}}(\mathcal{S}) \triangleq 2\sum_{k\in\mathcal{S}_i^L} \lambda_i^{(k)}, \text{ and } q_i^{\mathrm{TOA}}(\mathcal{S}) \triangleq \sum_{k\mathcal{S}_i^L}\sum_{l\in\mathcal{S}_i^L} \lambda_i^{(k)}\lambda_i^{(l)} \sin^2\left(\phi_i^{(k)} - \phi_i^{(l)}\right). \tag{3.11}$$

If $\mathcal{S} \subset \mathcal{W}$, then $p_i^{\mathrm{TOA}}(\mathcal{S}) \leq p_i^{\mathrm{TOA}}(\mathcal{W})$ and $q_i^{\mathrm{TOA}}(\mathcal{S}) \leq q_i^{\mathrm{TOA}}(\mathcal{W})$. In other words, both $p_i^{\mathrm{TOA}}(\cdot)$ and $q_i^{\mathrm{TOA}}(\cdot)$ are non-decreasing functions.

Take any $e \notin \mathcal{W}$. If $e \notin \widetilde{\mathcal{A}_i^L}$, then it is clear that $p_i^{\mathrm{TOA}}(\mathcal{W}\cup\{e\}) - p_i^{\mathrm{TOA}}(\mathcal{W}) = p_i^{\mathrm{TOA}}(\mathcal{S}\cup\{e\}) - p_i^{\mathrm{TOA}}(\mathcal{S}) = 0$, and $q_i^{\mathrm{TOA}}(\mathcal{W}\cup\{e\}) - q_i^{\mathrm{TOA}}(\mathcal{W}) = q_i^{\mathrm{TOA}}(\mathcal{S}\cup\{e\}) - q_i^{\mathrm{TOA}}(\mathcal{S}) = 0$. If $e \in \widetilde{\mathcal{A}_i^L}$, it is observed that

$$p_i^{\mathrm{TOA}}(\mathcal{W}\cup\{e\}) - p_i^{\mathrm{TOA}}(\mathcal{W}) = p_i^{\mathrm{TOA}}(\mathcal{S}\cup\{e\}) - p_i^{\mathrm{TOA}}(\mathcal{S})$$

$$\begin{aligned} q_i^{\mathrm{TOA}}(\mathcal{W}\cup\{e\}) - q_i^{\mathrm{TOA}}(\mathcal{W}) &= 2\lambda_i^{(e)} \sum_{k\in\mathcal{W}} \lambda_i^{(k)} \sin^2\left(\phi_i^{(k)} - \phi_i^{(e)}\right) \\ &\geq 2\lambda_i^{(e)} \sum_{k\in\mathcal{S}} \lambda_i^{(k)} \sin^2\left(\phi_i^{(k)} - \phi_i^{(e)}\right) \\ &= q_i^{\mathrm{TOA}}(\mathcal{S}\cup\{e\}) - q_i^{\mathrm{TOA}}(\mathcal{S}) \end{aligned}$$

Therefore, both $p_i^{\mathrm{TOA}}(\cdot)$ and $q_i^{\mathrm{TOA}}(\cdot)$ are non-decreasing supermodular functions [111]. Since the product of two non-decreasing, non-negative and supermodular functions is supermodular, it is concluded that $p_i^{\mathrm{TOA}}(\mathcal{S})\prod_{j\neq i} q_j^{\mathrm{TOA}}(\mathcal{S})$ and $\prod_j q_j(\mathcal{S})$ are supermodular functions as $p_i^{\mathrm{TOA}}(\cdot)$ and $q_i^{\mathrm{TOA}}(\cdot)$ are supermodular, non-negative and non-decreasing. Based on the definitions at the beginning of the proof, the objective function in (3.9), which is specified via (3.10), can be expressed as

$$\sum_{i=1}^{N_T} w_i f_i^{\mathrm{TOA}}(\mathcal{S}) = \frac{\sum_{i=1}^{N_T} w_i p_i^{\mathrm{TOA}}(\mathcal{S})\prod_{j\neq i} q_j^{\mathrm{TOA}}(\mathcal{S})}{\prod_j q_j^{\mathrm{TOA}}(\mathcal{S})}\,. \tag{3.12}$$

Since supermodularity is preserved under non-negative weighted summation, $\sum_{i=1}^{N_T} w_i p_i^{\mathrm{TOA}}(\mathcal{S})$ $\prod_{j\neq i} q_j^{\mathrm{TOA}}(\mathcal{S})$ is also supermodular. Therefore, both the numerator and the denominator of the objective function are supermodular. ■

In [54], it is stated that whether optimizing the ratio of monotone supermodular functions admits any polynomial time algorithm with bounded approximations is an open problem. Therefore, instead of employing integer programming approaches, we aim to transform (3.9) into an anchor selection problem that can be solved via convex optimization tools. To this aim, we introduce a selection vector $\mathbf{z} = [z_1\, z_2\, \ldots\, z_{|\widetilde{\mathcal{R}}|}]^\intercal$ as follows:

$$z_k = \begin{cases} 1, & \text{if an anchor node is placed at } \mathbf{y}^{(k)} \\ 0, & \text{otherwise} \end{cases}\,. \tag{3.13}$$

It is noted that (3.9) is equivalent to the following problem:

$$\min_{\mathbf{z}\in\mathbb{R}^{|\widetilde{\mathcal{R}}|}} \quad \sum_{i=1}^{N_T} w_i\, \widetilde{f}_i^{\mathrm{TOA}}(\mathbf{z}) \tag{3.14a}$$

$$\text{subject to} \quad \sum_{k=1}^{|\widetilde{\mathcal{R}}|} z_k = N_A \tag{3.14b}$$

$$z_k \in \{0,1\}\,,\ k = 1,2,\ldots,\left|\widetilde{\mathcal{R}}\right| \tag{3.14c}$$

where $\widetilde{f}_i^{\mathrm{TOA}}(\mathbf{z})$ is given by

$$\widetilde{f}_i^{\mathrm{TOA}}(\mathbf{z}) \triangleq \frac{2\sum_{k\in\widetilde{\mathcal{A}_i^L}} z_k \lambda_i^{(k)}}{\sum_{k\in\widetilde{\mathcal{A}_i^L}}\sum_{l\in\widetilde{\mathcal{A}_i^L}} z_k z_l \lambda_i^{(k)}\lambda_i^{(l)}\sin^2\left(\phi_i^{(k)}-\phi_i^{(l)}\right)} \tag{3.15}$$

The following proposition proves that the objective function in (3.14) is a convex function of the selection vector $\mathbf{z}$.

Proposition 3.1: The objective function in (3.14) is convex with respect to the selection vector $\mathbf{z}$.

Proof: It can be shown that $\widetilde{f}_i^{\mathrm{TOA}}(\mathbf{z})$ in (3.14) is equal to $\mathrm{tr}\left\{\tilde{\mathbf{J}}_i^{\mathrm{TOA}}(\mathbf{z})^{-1}\right\}$, where

$$\widetilde{\mathbf{J}}_i^{\mathrm{TOA}}(\mathbf{z}) \triangleq \sum_{k\in\widetilde{\mathcal{A}_i^L}} z_k \lambda_i^{(k)} \boldsymbol{\varphi}_i^{(k)} \big(\boldsymbol{\varphi}_i^{(k)}\big)^{\mathsf{T}}. \tag{3.16}$$

First, it is clear that $\widetilde{\mathbf{J}}_i^{\mathrm{TOA}}(\mathbf{z})$ is a linear function of $\mathbf{z}$. Moreover, it is known that $\mathrm{tr}\{\mathbf{A}^{-1}\}$ is a non-increasing convex function of the positive semi-definite matrix $\mathbf{A}$ [105]. Due to the concavity of $\widetilde{\mathbf{J}}_i^{\mathrm{TOA}}(\mathbf{z})$, we can argue, based on the chain rule, that $\widetilde{f}_i^{\mathrm{TOA}}(\mathbf{z})$ is convex with respect to $\mathbf{z}$ for any i. As w_i's in (3.14a) are non-negative, we have the desired conclusion about the convexity of the objective function in (3.14). ■

Since the objective function is convex with respect to $\mathbf{z}$, by relaxing the integer constraints in (3.14c), we obtain a convex optimization problem as follows:

$$\min_{\mathbf{z}\in\mathbb{R}^{|\mathcal{S}|}} \quad \sum_{i=1}^{N_T} w_i \, \widetilde{f}_i^{\mathrm{TOA}}(\mathbf{z}) \tag{3.17a}$$

$$\text{subject to} \quad \sum_{k=1}^{|\widetilde{\mathcal{R}}|} z_k = N_A \tag{3.17b}$$

$$0 \le z_k \le 1\,, \;\; k = 1, 2, \ldots, |\mathcal{S}| \tag{3.17c}$$

To summarize the main approach, we first formulate the anchor placement problem as a continuous and non-convex optimization problem as in (3.7). Then, we take finitely many points from the region $\mathcal{R}$ to discretize the problem as in (3.9). Next, we prove that this problem is equivalent to minimizing the ratio of two supermodular functions, for which there exists no polynomial time algorithms with bounded approximations in the literature. Therefore, we express this problem as an anchor selection problem as in (3.14), and by relaxing the integer constraints, it is proven that a convex formulation can be achieved as in (3.17). Thus, we propose the anchor selection problem in (3.17) as a convex approximation of the anchor placement problem in (3.7). After solving (3.17) via convex optimization tools

(such as CVX [112]), we propose the following two algorithms to obtain a solution of the original problem in (3.7). First, we can simply set the largest N_A components of the solution of (3.17) to one, and the others to zero (called largest-N_A algorithm). Second, starting from this solution, we can use the swap algorithm [44, 45]. In this algorithm, for each run, one checks whether there is a decrease in the objective function by simply swapping one of the N_A selected locations with one of the $\left|\widetilde{\mathcal{R}}\right| - N_A$ locations that are not selected. The overall procedure starting from $\mathcal{R}$ and N_A is outlined in Algorithm 2, where $\mathbf{z}_{\text{relaxed}}$, $\mathbf{z}_{\text{largest}}$ and $\mathbf{z}_{\text{swap}}$ denote the optimal selection vectors obtained from (3.17) (e.g., via CVX), the largest-N_A algorithm and the swap algorithm, respectively.

Algorithm 2 Proposed Anchor Placement Algorithm

Input: $\mathcal{R}$, N_A
Output: $\{\mathbf{y}^{(k)}\}_{k\in\mathcal{I}}$.

1: Discretize set $\mathcal{R}$ as $\widetilde{\mathcal{R}}$.
2: Find optimal selection vector $\mathbf{z}_{\text{relaxed}}$ by solving (3.17) (via CVX) for set $\widetilde{\mathcal{R}}$.
3: Obtain $\mathbf{z}_{\text{largest}}$ from $\mathbf{z}_{\text{relaxed}}$ by setting largest N_A components of $\mathbf{z}_{\text{relaxed}}$ to one, and others to zero.
4: Run swap algorithm starting from $\mathbf{z}_{\text{largest}}$ to obtain $\mathbf{z}_{\text{swap}}$.
5: $\mathcal{I} \leftarrow \{i \mid \mathbf{z}_{\text{swap}}(i) = 1\}$
6: Place anchors to $\{\mathbf{y}^{(k)}\}_{k\in\mathcal{I}}$.

3.2.4 Extension to Three-Dimensional Anchor Placement

Similar to the analysis in [99], our results can easily be extended to three dimensional scenarios. In that case, $\boldsymbol{\varphi}_i(\mathbf{y}_j)$ in (3.5) becomes

$$\boldsymbol{\varphi}_i(\mathbf{y}_j) = [\sin\theta_i(\mathbf{y}_j)\cos\phi_i(\mathbf{y}_j) \;\; \sin\theta_i(\mathbf{y}_j)\sin\phi_i(\mathbf{y}_j) \;\; \cos\theta_i(\mathbf{y}_j)]^{\mathsf{T}}$$

where $\theta_i(\mathbf{y}_j)$ and $\phi_i(\mathbf{y}_j)$ denote, respectively, the azimuth and polar angles in the direction from the target node at location $\mathbf{x}_i$ to the anchor node located at $\mathbf{y}_j$.

It is observed that after discretization and approximating the anchor placement problem as the anchor selection problem, Proposition 3.1 holds also for the three dimensional case as the FIM is a linear function of the selection vector $\mathbf{z}$ (cf. (3.16)). Hence, the proposed algorithms can be used for the three dimensional anchor placement problem, as well.

3.3 TDOA Based Anchor Placement Problem

In the TDOA based approach, the anchor nodes are synchronized among themselves but they are not synchronized with the target node. Therefore, there are additional unknown parameters $\{\Delta_i\}_{i=1}^{N_T}$, where Δ_i characterizes the time offset between the clocks of the target node located at $\mathbf{x}_i$ and the anchor nodes. Hence, (3.2) changes as follows:

$$\tau_{ij}^{(l)} = \frac{1}{c}\left(\|\mathbf{y}_j - \mathbf{x}_i\|_2 + b_{ij}^{(l)} + \Delta_i\right) \tag{3.18}$$

As in the previous section, due to the difficulty of the continuous optimization problem (see (3.7)), we discretize the set $\mathcal{R}$ as $\widetilde{\mathcal{R}}$. After the discretization, via similar steps to those in [44, 45], one can show that the CRLB related to the estimation of the ith target location, $\mathbf{x}_i$, by anchor nodes is given by

$$f_i^{\mathrm{TDOA}}(\mathcal{S}) \triangleq \frac{3\sum_{k\in\mathcal{S}_i^L}\sum_{l\in\mathcal{S}_i^L}\lambda_i^{(k)}\lambda_i^{(l)}a_i^{(k,l)}}{4\sum_{k\in\mathcal{S}_i^L}\sum_{l\in\mathcal{S}_i^L}\sum_{m\in\mathcal{S}_i^L}\lambda_i^{(k)}\lambda_i^{(l)}\lambda_i^{(m)}\tilde{a}_i^{(k,l,m)}}, \tag{3.19}$$

$$a_i^{(k,l)} \triangleq \sin^2\left(\frac{\phi_i^{(k)} - \phi_i^{(l)}}{2}\right),\ \tilde{a}_i^{(k,l,m)} \triangleq a_i^{(k,l)}a_i^{(l,m)}a_i^{(m,k)}.$$

Similar to Lemma 3.1, it can be proven that the objective function $\sum_{i=1}^{N_T} w_i f_i^{\mathrm{TDOA}}(\mathcal{S})$ can be written as a ratio of two non-decreasing supermodular functions. In addition, after relaxation, from Proposition 2 in [44], the anchor selection problem for the TDOA based approach can be shown to be convex, as well. Hence, the algorithms proposed for the TOA based approach in the previous section can also be used for TDOA based wireless localization networks.

3.4 RSS Based Anchor Placement Problem

In this section, after calculating the power of the received signal according to the model in (3.1), anchor nodes estimate the position of the target node. We adopt the model given in [104].

The received signal power at the anchor node located at $\mathbf{y}_j$ due to the transmission of

$s_i(t)$, $P_i^{(r)}(\mathbf{y}_j)$, is given by

$$P_i^{(r)}(\mathbf{y}_j) = P_i^{(s)}(\mathbf{y}_j) + P_i^{(n)}, \tag{3.20}$$

where $P_i^{(s)}(\mathbf{y}_j)$ and $P_i^{(n)}$ are the signal and the noise powers, respectively. $P_i^{(s)}(\mathbf{y}_j)$ is expressed as follows:

$$P_i^{(s)}(\mathbf{y}_j) = k_i(\mathbf{y}_j) P_i \frac{g_i(\mathbf{y}_j)^2 \gamma_i(\mathbf{y}_j)}{\big(d_i(\mathbf{y}_j)\big)^{\epsilon}} \tag{3.21}$$

where P_i is the (known) transmitted power, $g_i(\mathbf{y}_j)$ and $\gamma_i(\mathbf{y}_j)$ are variables that conform to Rayleigh and log-normal distributions, $d_i(\mathbf{y}_j) = \|\mathbf{y}_j - \mathbf{x}_i\|_2$, ϵ is the path loss factor, and $k_i(\mathbf{y}_j)$ is the known constant given by

$$k_i(\mathbf{y}_j) = \frac{G_t^{(i)} G_r^{(i)}(\mathbf{y}_j)}{4\pi} \tag{3.22}$$

with $G_t^{(i)}$ and $G_r^{(i)}(\mathbf{y}_j)$ being the antenna gains at the target node $\mathbf{x}_i$ and the anchor node located at $\mathbf{y}_j$, respectively.

By taking the steps in [104], the equivalent Fisher information matrix (EFIM), $\mathbf{J}_i^{\mathrm{RSS}}(\mathbf{Y})$ corresponding to the target position i, as a function of anchor positions $\{\mathbf{y}_j\}_{j=1}^{N_A}$ is given by

$$\mathbf{J}_i^{\mathrm{RSS}}(\mathbf{Y}) = \mathbf{H}_i(\mathbf{Y}) \mathbf{X}_i(\mathbf{Y}) \mathbf{H}_i(\mathbf{Y})^{\intercal} \tag{3.23}$$

where

$$\mathbf{H}_i(\mathbf{Y}) = \frac{10\epsilon}{c \ln 10} \begin{bmatrix} \cos(\phi_i(\mathbf{y}_1)) & \dots & \cos(\phi_i(\mathbf{y}_{N_A})) \\ \sin(\phi_i(\mathbf{y}_1)) & \dots & \sin(\phi_i(\mathbf{y}_{N_A})) \end{bmatrix} \left[\mathrm{diag}\left(d_i(\mathbf{y}_1), \dots, d_i(\mathbf{y}_{N_A})\right)\right]^{-1}, \tag{3.24}$$

$$\mathbf{X}_i(\mathbf{Y}) = \left[\mathrm{diag}(\kappa_i(\mathbf{y}_1), \dots, \kappa_i(\mathbf{y}_{N_A}))\right]^{-1}, \tag{3.25}$$

$$\kappa_i(\mathbf{y}_j) = \frac{100}{(\ln 10)^2} \sum_{m=1}^{N_i(\mathbf{y}_j)} \mathrm{var}(\ln \gamma_i(\mathbf{y}_j)) \tag{3.26}$$

and $N_i(\mathbf{y}_j)$ is the number of path elements concatenated in tandem between target $\mathbf{x}_i$ and anchor $\mathbf{y}_j$. Via some algebraic manipulations, the CRLB related to the position of the target node i based on the RSS approach can be computed as follows:

$$\mathrm{tr}\left\{\mathbf{J}_i^{\mathrm{RSS}}(\mathbf{Y})^{-1}\right\} = \frac{2c^2 \ln(10)^2}{(100\epsilon^2)} \frac{\sum_{k=1}^{N_A} \mu_i(\mathbf{y}_k)}{\sum_{k=1}^{N_A} \sum_{l=1}^{N_A} \mu_i(\mathbf{y}_k) \mu_i(\mathbf{y}_l) \sin^2\left(\phi_i(\mathbf{y}_k) - \phi_i(\mathbf{y}_l)\right)} \tag{3.27}$$

where $\mu_i(\mathbf{y}_k) = 1/\big(\kappa_i(\mathbf{y}_{N_k}) d_i(\mathbf{y}_k)^2\big)$.

As in the previous sections, due to the difficulty of the continuous optimization problem, we discretize the set $\mathcal{R}$ as $\widetilde{\mathcal{R}} = (\mathbf{y}^{(k)})_k$. Let $\mu_i^{(k)} \triangleq \mu_i(\mathbf{y}^{(k)})$ for any $k = 1, 2, \ldots, N_A$.

It is noted that the expression in (3.27) is quite similar to (3.8). Hence, after the discretization, we can express $\sum_{i=1}^{N_T} w_i f_i^{\text{RSS}}(\mathcal{S})$ as a ratio of two non-decreasing supermodular functions, where

$$f_i^{\text{RSS}}(\mathcal{S}) = \frac{2c^2 \ln(10)^2}{(100\epsilon^2)} \frac{\sum_{k\in\mathcal{S}} \mu_i^{(k)}}{\sum_{k\in\mathcal{S}} \sum_{l\in\mathcal{S}} \mu_i^{(k)} \mu_i^{(l)} \sin^2\left(\phi_i^{(k)} - \phi_i^{(l)}\right)}. \tag{3.28}$$

Furthermore, by applying the steps in Proposition 3.1, one can prove that, after relaxing the integer constraints, the anchor selection problem based on the RSS approach is convex. Thus, Algorithm 2 is applicable for the RSS based anchor placement problem as well.

Remark 3.1: Throughout this chapter, a source localization network is considered. However, due to the similarity of the expressions for the FIMs, all the preceding analyses and the proposed algorithms are also valid for self localization networks (for TOA, TDOA and RSS approaches).

Remark 3.2: In this chapter, we rely on the perfect knowledge of $\lambda_i^{(k)}$'s. In fact, due to the monotonic behavior of the CRLB with respect to $\lambda_i^{(k)}$'s, it is straightforward to extend the analyses if we have some uncertainty region for each $\lambda_i^{(k)}$'s as in [44, 45].

3.5 Simulation Results and Conclusions

In this section, numerical examples are presented to evaluate the proposed approaches in Section 3.2. Examples are provided for two different setups in which two and three dimensional source localization networks are considered. In both setups, we evaluate the performance of two algorithms, namely, the largest-N_A and the swap algorithms. We also compare their performance with the lower bound provided by the solution of the relaxed problem in (3.17).

3.5.1 Example of Two Dimensional Wireless Network

Consider a wireless source localization network as shown in Figure 3.1 (all locations are in meters). In particular, the anchor nodes are placed in the region $\mathcal{R} = \mathcal{R}_1 \cup \mathcal{R}_2$, where $\mathcal{R}_1 = [0,3] \times ([0,3] \cup [8,11])$ and $\mathcal{R}_2 = [8,11] \times ([0,3] \cup [8,11])$. We provide two different discretizations of $\mathcal{R}$ by taking 196 and 676 points from $\mathcal{R}$. (We take points from $\mathcal{R}$ for each 0.5 and 0.25 meters along both x and y directions for the first and second setups, respectively.) Moreover, the number of possible locations for the target node, N_T, is equal to 129 as illustrated in Figure 3.1.

In the simulations, the same parameters as in [25, 44] are used. In particular, $\alpha_i^{(l)}(\mathbf{y}_j)$ and $\xi_i(\mathbf{y}_j)$ are modeled as $\alpha_i^{(l)}(\mathbf{y}_j) = \|\mathbf{x}_i - \mathbf{y}_j\|_2^{-2}$ and $\xi_i(\mathbf{y}_j) = 0$. Hence, $\lambda_i^{(k)}$ is expressed as $\lambda_i^{(k)} = 8\pi\beta_i^2 E_i / \left(c^2 \left\|\mathbf{x}_i - \mathbf{y}^{(k)}\right\|_2^2 N_0\right)$. Also, the signal parameters are selected such that $\lambda_i^{(k)} = 1/\left(\left\|\mathbf{x}_i - \mathbf{y}^{(k)}\right\|_2^2 N_0\right)$ as in [25]. Also we set $w_i = 1/N_T$ for $i = 1, \ldots, N_T$. The average CRLBs are presented in terms of meters, i.e., we take the square roots of the objectives.

Figure 3.1 shows the cases of $\left|\widetilde{\mathcal{R}}\right| = 196$ and $\left|\widetilde{\mathcal{R}}\right| = 676$, together with the optimal anchor locations obtained from the swap algorithm when $N_A = 10$ and $N_0 = 1$. It is noted that even though the number of points in $\widetilde{\mathcal{R}}$ increases, the optimal placement strategy does not change effectively. Hence, it is expected that the resulting CRLBs do not differ significantly with respect to discretization once a sufficiently dense grid is employed. Therefore, in the remaining examples, we use the first setup and take 196 points from $\widetilde{\mathcal{R}}$, i.e., $\left|\widetilde{\mathcal{R}}\right| = 196$.

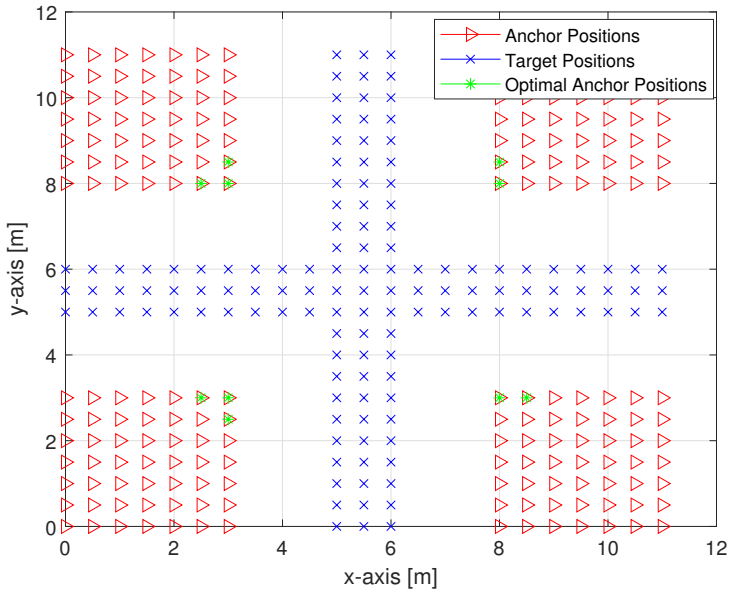
Figure 3.2 presents the average CRLB performance of each algorithm versus N_A for two different noise levels: $N_0 = 1$ and $N_0 = 10$. For the same setting, in Figure 3.3, the average CRLB performance of each algorithm is plotted versus $1/N_0$ for $N_A = 3$ and 5. It is observed that the solution of the relaxed problem is very close to the other two algorithms in both Figures 3.2 and 3.3. Therefore, the optimal solution of the discretized anchor placement problem in (3.9) is practically achieved in this scenario. Another important observation is that the optimal placement strategy does not change with the noise power, N_0 since by changing N_0, we scale all $\lambda_i^{(k)}$'s with the same factor. For example, in Figure 3.2, the curve corresponding to $N_0 = 10$ is just the scaled version of the curve for $N_0 = 1$.

3.5.2 Example of Three Dimensional Wireless Network

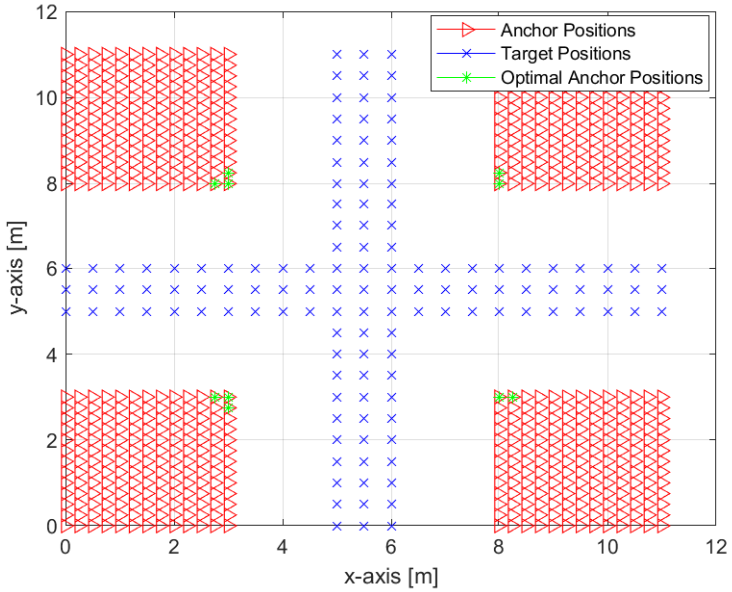
In this part, we consider a wireless localization network as in Figure 3.4. In particular, the anchor nodes are placed in $\mathcal{R} = \{[x, y, z] \mid 0 \leq x, y \leq 10, z = 10\}$ and for the discretization we take points from $\mathcal{R}$ for each 0.5 meter along both x and y directions such that the number of all points in $\widetilde{\mathcal{R}}$ is equal to 441. Furthermore, the number of possible target positions is equal to 121 as illustrated in Figure 3.4. We use the same simulation parameters as in the two dimensional example except that to realize the shadowing effect, $\lambda_i^{(k)}$'s are multiplied by independent log-normal random variables with a mean parameter of -3 and a variance parameter of 3. For this purpose, we generate a matrix with dimensions 121×441 by using MATLAB (the seed is equal to 1), where the (i, k)th element of this matrix corresponds to the log-normal random variable for the channel between $\mathbf{x}_i$ and $\mathbf{y}^{(k)}$ as in [44].

Figure 3.5 presents the average CRLB performance of each algorithm versus N_A for two different noise levels: $N_0 = 1$ and $N_0 = 10$. We see that when $N_A = 3$, starting from the solution of the largest-N_A, via the swap algorithm, we obtain a solution very close to that of the relaxed algorithm. In other words, in this scenario, we benefit from the swap algorithm. Moreover, in Figure 3.5 we again observe that by changing the noise power, we only scale the objective value. For the same setting, in Figure 3.6, the average CRLB performance of each algorithm is plotted versus $1/N_0$ for $N_A = 3$ and 5. Again the same observations can be made as those for $N_A = 3$.

Overall, the proposed approach provides an effective solution to the anchor placement problem via discretization and convex relaxation. The performance loss due to discretization can be remedied by using a dense grid, and the suboptimality due to convex relaxation can be mitigated via the swap algorithm, as seen in the numerical examples.



(a) $\left|\widetilde{\mathcal{R}}\right| = 196$



(b) $\left|\widetilde{\mathcal{R}}\right| = 676$

Figure 3.1: Illustration of possible locations of target and anchor nodes, together with optimal anchor locations (obtained from the swap algorithm) when $N_A = 10$ and $N_0 = 1$ for two different cases: (a) $\left|\widetilde{\mathcal{R}}\right| = 196$ and (b) $\left|\widetilde{\mathcal{R}}\right| = 676$.

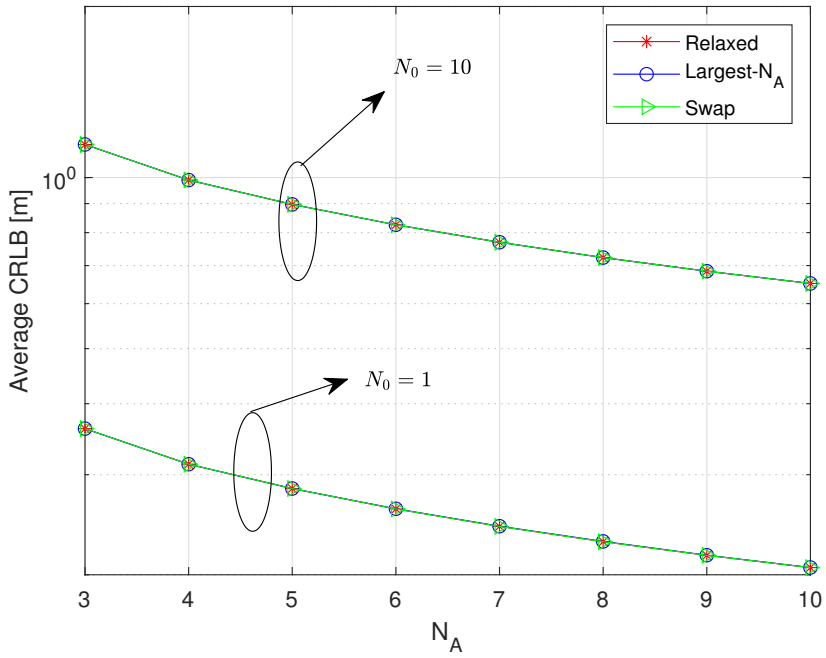


Figure 3.2: Average CRLB versus N_A for different algorithms when $N_0 = 1$ and 10.

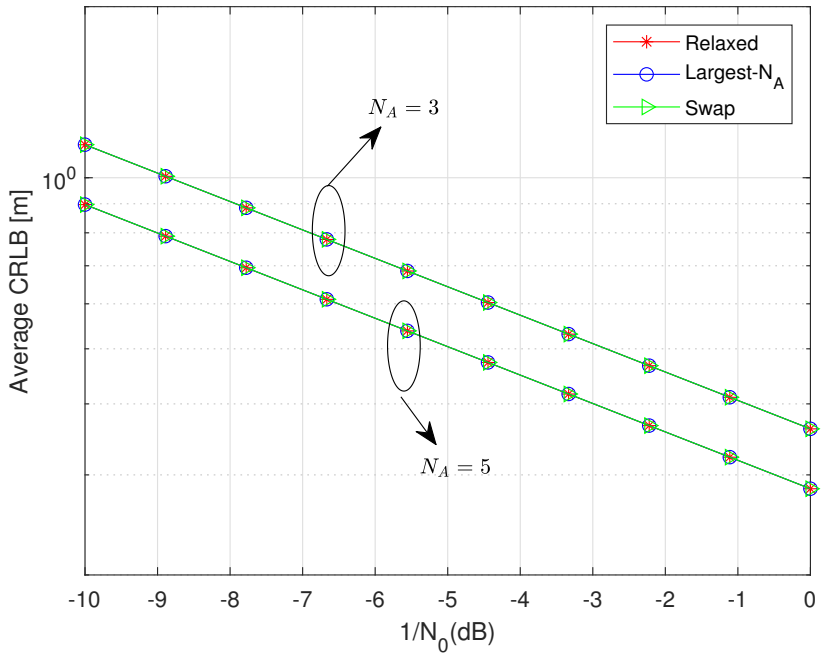


Figure 3.3: Average CRLB versus $1/N_0$ for different algorithms when $N_A = 3$ and 5.

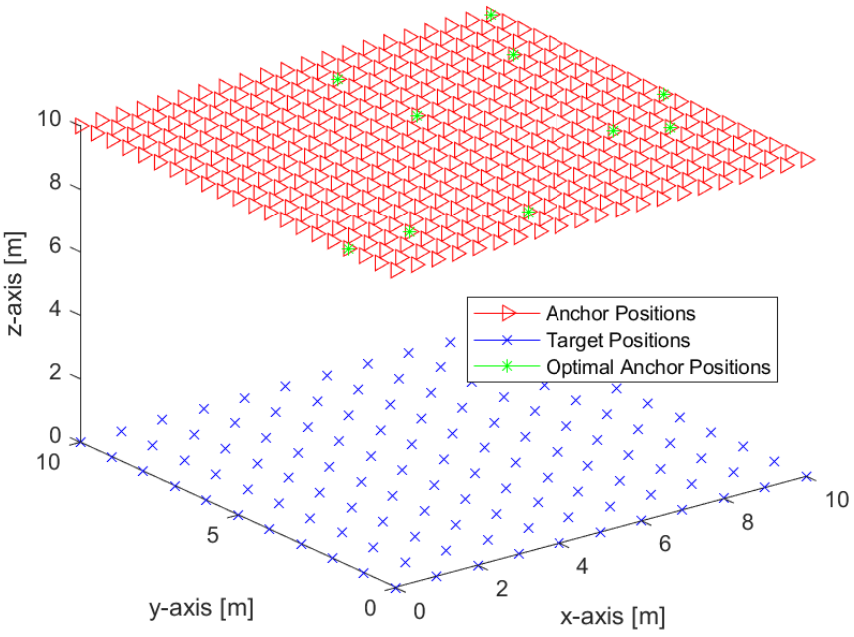


Figure 3.4: Illustration of possible locations of target and anchor nodes, together with the optimal anchor locations (obtained from the swap algorithm) when $N_A = 10$ and $N_0 = 1$.

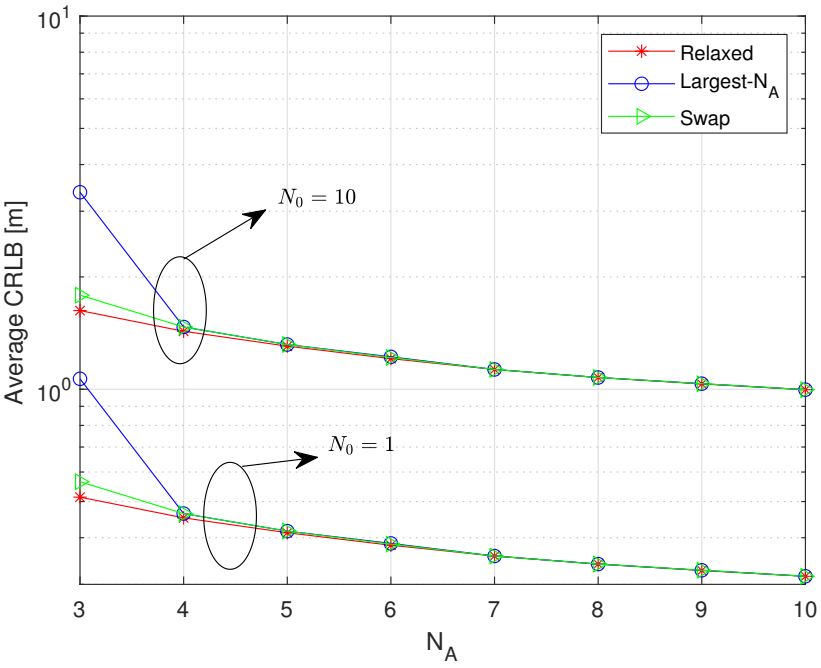


Figure 3.5: Average CRLB versus N_A for different algorithms when $N_0 = 1$ and 10.

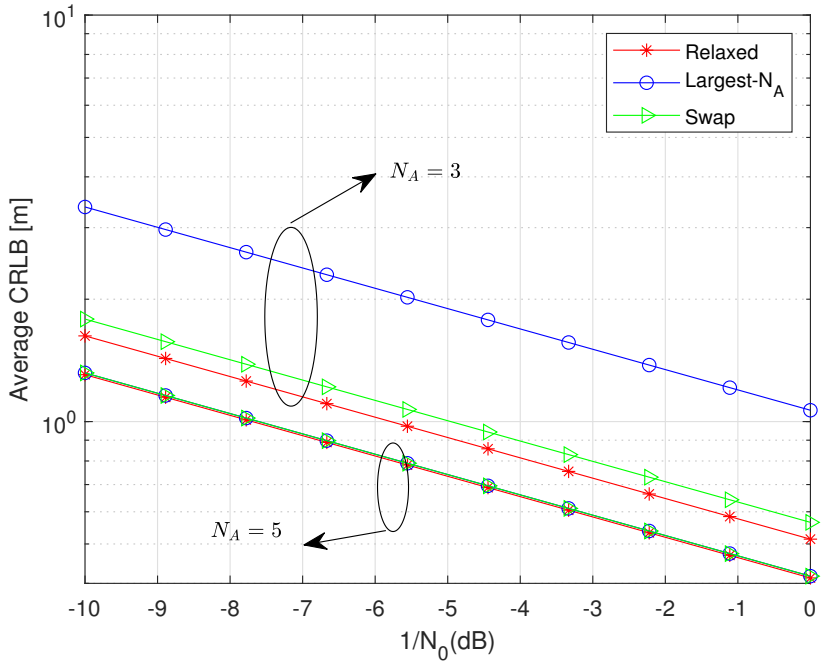


Figure 3.6: Average CRLB versus $1/N_0$ for different algorithms when $N_A = 3$ and 5.

Chapter 4

RIS-aided Near-Field Localization under Phase-Dependent Amplitude Variations

In this chapter, we investigate the problem of RIS-aided geometric near-field localization of a single-antenna UE served by a single-antenna BS under LoS blockage [59, 71, 73, 113], considering a realistic RIS amplitude model [78], which relies on equivalent circuit models of individual reflecting elements. Specifically, we quantify degradation in localization performance due to mismatch between an *ideal model* with unit-amplitude RIS element responses and a *realistic model* with phase-dependent amplitude variations [78,114], by resorting to the MCRB analysis [85,115]. In addition, we develop novel localization and online RIS calibration algorithms for cases with and without the knowledge of the underlying RIS amplitude model.

4.1 System Model

In this section, we describe the system geometry, present the signal model and the RIS model, and formulate the problem of interest.

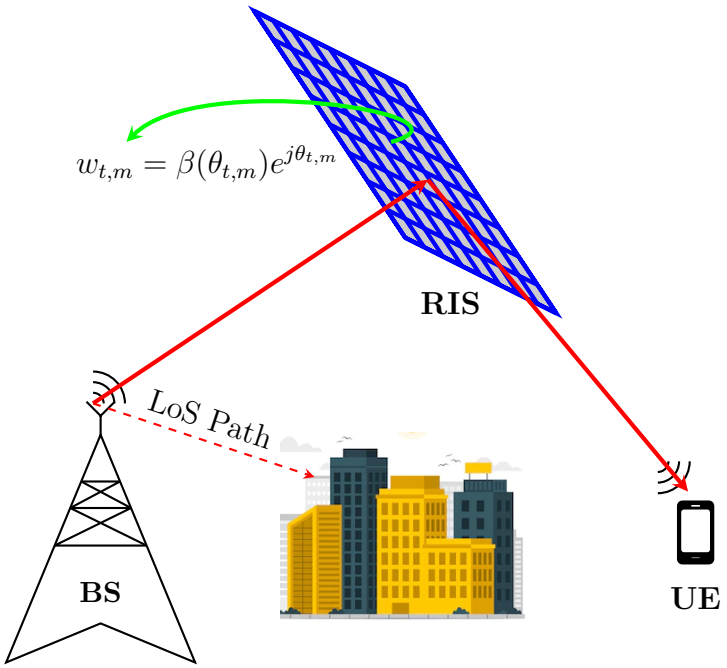


Figure 4.1: Configuration of a RIS-aided localization system with LoS blockage.

4.1.1 Geometry and Signal Model

We consider an RIS-aided localization system (see Figure 4.1) with a single-antenna BS, an M-element RIS, and a single-antenna UE having the following three-dimensional locations: $\boldsymbol{p}_{\text{BS}}$ denotes the known BS location, $\boldsymbol{p}_{\text{RIS}} = [\text{x}_\text{R}\, \text{y}_\text{R}\, \text{z}_\text{R}]^\mathsf{T}$ is the known center of the RIS, $\boldsymbol{p}_m = [\text{x}_m\, \text{y}_m\, \text{z}_m]^\mathsf{T}$ represents the known location of the mth RIS element for $1 \leq m \leq M$, and $\overline{\boldsymbol{p}} = [\overline{\text{x}}\, \overline{\text{y}}\, \overline{\text{z}}]^\mathsf{T}$ is the unknown UE location. For convenience, following the notation given in [85, 116], we use $\overline{(\cdot)}$ for the true values of the parameters of interest throughout this chapter.

In the considered setting, the BS broadcasts a narrowband signal s_t over T transmissions under the constraint of $\mathbb{E}\{|s_t|^2\} = E_s$. For simplicity, we assume that $s_t = \sqrt{E_s}$ for any t. Assuming LoS blockage [59,71] and the absence of uncontrolled multipath, the signal received by the UE involves only reflections from the RIS and can be expressed at transmission t as

$$y_t = \overline{\alpha}\, \underbrace{\boldsymbol{a}^\mathsf{T}(\overline{\boldsymbol{p}})\text{diag}(\mathbf{w}_t)\boldsymbol{a}(\boldsymbol{p}_{\text{BS}})}_{\triangleq \boldsymbol{b}^\mathsf{T}(\overline{\boldsymbol{p}})\mathbf{w}_t} s_t + n_t\,, \tag{4.1}$$

where $\overline{\alpha}$ is the unknown channel gain, $\mathbf{w}_t = [w_{t,1}\ \ldots\ w_{t,M}]^\mathsf{T}$ is the RIS profile at transmission

t, and n_t is uncorrelated zero-mean additive Gaussian noise with variance $N_0/2$ per real dimension.

Moreover, $\boldsymbol{b}(\overline{\boldsymbol{p}}) = \boldsymbol{a}(\overline{\boldsymbol{p}}) \odot \boldsymbol{a}(\boldsymbol{p}_{\mathrm{BS}})$, where $\boldsymbol{a}(\boldsymbol{p})$ is the near-field RIS steering vector for a given position $\boldsymbol{p}$, defined as

$$[\boldsymbol{a}(\boldsymbol{p})]_m = \exp\left(-j\frac{2\pi}{\lambda}\left(\|\boldsymbol{p}-\boldsymbol{p}_m\|_2 - \|\boldsymbol{p}-\boldsymbol{p}_{\mathrm{RIS}}\|_2\right)\right) \tag{4.2}$$

for $m \in \{1,\ldots,M\}$, in which λ denotes the signal wavelength.

4.1.2 Model for RIS Elements

Following the practical model in [78], we consider *phase-dependent amplitude variations* of the RIS elements given by

$$w_{t,m} = \beta(\theta_{t,m})e^{j\theta_{t,m}}, \tag{4.3}$$

with $\theta_{t,m} \in [-\pi,\pi)$ and $\beta(\theta_{t,m}) \in [0,1]$ denoting the phase shift and the corresponding amplitude, respectively. In particular, $\beta(\theta_{t,m})$ is expressed as

$$\beta(\theta_{t,m}) = (1-\overline{\beta}_{\min})\left(\frac{\sin(\theta_{t,m}-\overline{\phi})+1}{2}\right)^{\overline{\kappa}} + \overline{\beta}_{\min}, \tag{4.4}$$

where $\overline{\beta}_{\min} \geq 0$, $\overline{\phi} \geq 0$, and $\overline{\kappa} \geq 0$ are the constants related to the specific circuit implementation [78]. To illustrate amplitude variations in (4.4), Figure 4.2 plots $\beta(\theta)$ as a function of the applied phase shift θ for various values of $\overline{\beta}_{\min}$ when $\overline{\kappa} = 1.5$ and $\overline{\phi} = 0$. As seen from the figure, larger amplitude fluctuations occur as $\overline{\beta}_{\min}$ approaches 0. The resulting performance penalties in location estimation will be quantified through the MCRB analysis in Section 4.2.

4.1.3 Problem Description

Given the observations y_t in (4.1) over T transmission instances, our goal is to derive theoretical performance bounds and develop low-complexity algorithms for estimating the position of

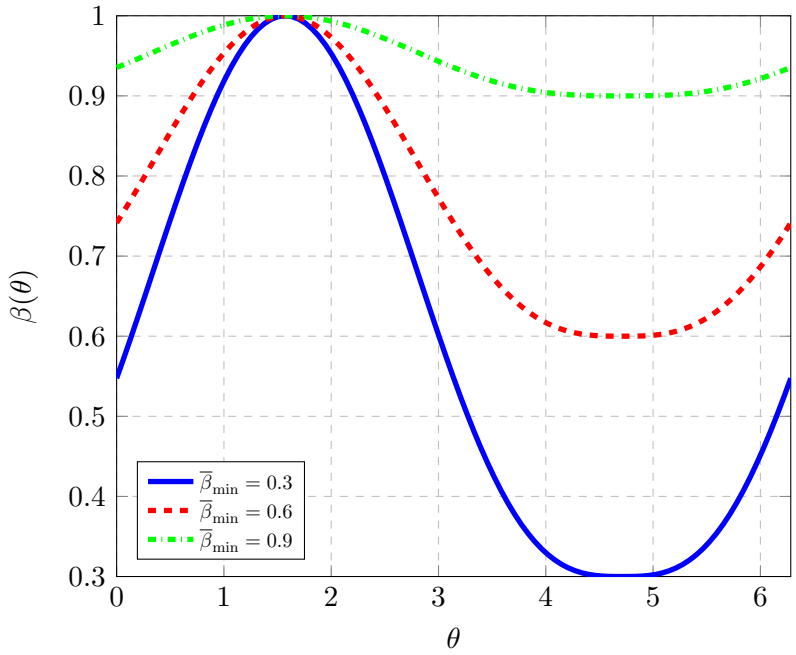


Figure 4.2: $\beta(\theta)$ in (4.4) for three different values of $\overline{\beta}_{\min}$, when $\overline{\kappa} = 1.5$ and $\overline{\phi} = 0$.

the UE $\overline{\boldsymbol{p}}$ (and the channel gain $\overline{\boldsymbol{\alpha}}$ as an unknown nuisance parameter) under three different scenarios:

- *Scenario-I*: There is a mismatch between the assumption and the reality in this scenario. It is assumed that the amplitudes of the RIS elements are equal to 1 (which is equivalent to assuming $\overline{\beta}_{\min} = 1$ or $\overline{\kappa} = 0$); however, the *true model* is as in (4.3).
- *Scenario-II*: The *true model* in (4.3) is known, but the RIS related parameters, $\overline{\beta}_{\min}, \overline{\kappa}$, and $\overline{\phi}$, are assumed to be unknown.
- *Scenario-III*: Both the *true model* in (4.3) and the RIS related parameters, $\overline{\beta}_{\min}, \overline{\kappa}$, and $\overline{\phi}$, are known.

To handle the different scenarios, the remainder of the chapter is organized as follows. In Section 4.2, the MCRB analysis of near-field localization under Scenario I is performed while Section 4.3 focuses on the estimator design for Scenario I. Then, the localization algorithms and the theoretical bounds for Scenario II and Scenario III are presented in Section 4.4. Finally, numerical examples for all the three scenarios are provided in Section 4.5.

4.2 Scenario-I: Misspecified Cramér-Rao Bound (MCRB) Analysis

In this scenario, we aim to quantify the localization performance loss due to the model mismatch resulting from the phase-dependent amplitude variations specified in (4.3). To that end, we will resort to the MCRB analysis [85, 115–118]. In the following, we first describe the *true model*, which corresponds to the realistic RIS response model in (4.3), and the *assumed model*, which is the ideal unit-amplitude RIS model commonly employed in the literature. Then, we provide theoretical background on the MCRB, propose a method to find the *pseudo-true parameter*, and derive the MCRB and the corresponding LB.

4.2.1 True and Assumed RIS Amplitude Models

4.2.1.1 True Model

The true parameter vector $\overline{\boldsymbol{\eta}}$ is given by $\overline{\boldsymbol{\eta}} \triangleq [\mathrm{Re}(\overline{\alpha})\, \mathrm{Im}(\overline{\alpha})\, \overline{\boldsymbol{p}}^{\mathsf{T}}]^{\mathsf{T}}$. We define μ_t as

$$\mu_t \triangleq \overline{\alpha} \sum_{m=1}^{M} [\boldsymbol{b}(\overline{\boldsymbol{p}})]_m w_{t,m} s_t \tag{4.5}$$

for $t = 1, \ldots, T$. Then, the probability density function (pdf) of the true observation, $p(\mathbf{y})$, can be expressed as

$$p(\mathbf{y}) = \left(\frac{1}{\pi N_0}\right)^T \exp\left(-\frac{1}{N_0} \|\mathbf{y} - \boldsymbol{\mu}\|_2^2\right), \tag{4.6}$$

where $\mathbf{y} \triangleq [y_1 \ \ldots \ y_T]^{\mathsf{T}}$ and $\boldsymbol{\mu} \triangleq [\mu_1 \ \ldots \ \mu_T]^{\mathsf{T}}$.

4.2.1.2 Assumed Model

In practice, the knowledge of the exact amplitude model in (4.4), which is hardware dependent, may not be available. In that case, the ideal model of $\beta(\theta_{t,m}) = 1$ can be used. For

this *assumed model*, we represent $w_{t,m}$ as $\tilde{w}_{t,m}$, which is given by

$$\tilde{w}_{t,m} = e^{j\theta_{t,m}} \tag{4.7}$$

for any t and m. Therefore, the misspecified parametric pdf for $\boldsymbol{\eta} \triangleq [\mathrm{Re}(\alpha)\, \mathrm{Im}(\alpha)\, \boldsymbol{p}^{\mathsf{T}}]^{\mathsf{T}}$ under the assumed model, denoted by $\tilde{p}(\mathbf{y}|\boldsymbol{\eta})$, can be expressed as

$$\tilde{p}(\mathbf{y}|\boldsymbol{\eta}) = \left(\frac{1}{\pi N_0}\right)^T \exp\left(-\frac{1}{N_0}\left\|\mathbf{y} - \tilde{\boldsymbol{\mu}}(\boldsymbol{\eta})\right\|_2^2\right), \tag{4.8}$$

where $\tilde{\boldsymbol{\mu}}(\boldsymbol{\eta}) \triangleq [\tilde{\mu}_1(\boldsymbol{\eta}) \ \ldots \ \tilde{\mu}_T(\boldsymbol{\eta})]^{\mathsf{T}}$, and

$$\tilde{\mu}_t(\boldsymbol{\eta}) \triangleq \alpha \sum_{m=1}^{M} [\boldsymbol{b}(\boldsymbol{p})]_m \tilde{w}_{t,m} s_t \tag{4.9}$$

for $t = 1, \ldots, T$. It is noted that when $\overline{\beta}_{\min} = 1$ or $\overline{\kappa} = 0$, $p(\mathbf{y})$ and $\tilde{p}(\mathbf{y}|\overline{\boldsymbol{\eta}})$ coincide with each other for any $\mathbf{y}$.

4.2.2 MCRB Definition

We introduce the pseudo-true parameter [85, 115], which minimizes the Kullback-Leibler (KL) divergence between the true pdf in (4.6) and the misspecified parametric pdf in (4.8); namely,

$$\boldsymbol{\eta}_0 = \underset{\boldsymbol{\eta} \in \mathbb{R}^5}{\arg\min}\, D\left(p(\mathbf{y}) \| \tilde{p}(\mathbf{y}|\boldsymbol{\eta})\right), \tag{4.10}$$

where $D\left(p(\mathbf{y}) \| \tilde{p}(\mathbf{y}|\boldsymbol{\eta})\right)$ denotes the KL divergence between the densities $p(\mathbf{y})$ and $\tilde{p}(\mathbf{y}|\boldsymbol{\eta})$. Next, let $\hat{\boldsymbol{\eta}}(\mathbf{y})$ be a misspecified-unbiased (MS-unbiased) estimator of $\overline{\boldsymbol{\eta}}$, i.e., the mean of the estimator $\hat{\boldsymbol{\eta}}(\mathbf{y})$ under the true model is equal to $\boldsymbol{\eta}_0$. The MCRB is a lower bound for the covariance matrix of any MS-unbiased estimator of $\overline{\boldsymbol{\eta}}$, $\hat{\boldsymbol{\eta}}(\mathbf{y})$ [84, 85, 115, 116]:

$$\mathbb{E}_p\{(\hat{\boldsymbol{\eta}}(\mathbf{y}) - \boldsymbol{\eta}_0)(\hat{\boldsymbol{\eta}}(\mathbf{y}) - \boldsymbol{\eta}_0)^{\mathsf{T}}\} \succeq \mathrm{MCRB}(\boldsymbol{\eta}_0), \tag{4.11}$$

where $\mathbb{E}_p\{\cdot\}$ denotes the expectation operator under the true model $p(\mathbf{y})$ and

$$\mathrm{MCRB}(\boldsymbol{\eta}_0) \triangleq \boldsymbol{A}_{\boldsymbol{\eta}_0}^{-1} \boldsymbol{B}_{\boldsymbol{\eta}_0} \boldsymbol{A}_{\boldsymbol{\eta}_0}^{-1}, \tag{4.12}$$

in which the (i,j)-th elements of the matrices $\boldsymbol{A}_{\boldsymbol{\eta}_0}$ and $\boldsymbol{B}_{\boldsymbol{\eta}_0}$ are calculated as

$$[\boldsymbol{A}_{\boldsymbol{\eta}_0}]_{ij} = \mathbb{E}_p\left\{\frac{\partial^2}{\partial \eta_i \partial \eta_j} \log \tilde{p}(\mathbf{y}|\boldsymbol{\eta})\Big|_{\boldsymbol{\eta}=\boldsymbol{\eta}_0}\right\}, \tag{4.13}$$

$$[\boldsymbol{B}_{\boldsymbol{\eta}_0}]_{ij} = \mathbb{E}_p \left\{ \frac{\partial}{\partial \eta_i} \log \tilde{p}(\mathbf{y}|\boldsymbol{\eta}) \frac{\partial}{\partial \eta_j} \log \tilde{p}(\mathbf{y}|\boldsymbol{\eta}) \Big|_{\boldsymbol{\eta}=\boldsymbol{\eta}_0} \right\}, \tag{4.14}$$

for $1 \leq i, j \leq 5$, with η_i denoting the ith element of $\boldsymbol{\eta}$. Note that without model mismatch, $\boldsymbol{A}_{\boldsymbol{\eta}_0} = \boldsymbol{A}_{\overline{\boldsymbol{\eta}}} = -\boldsymbol{B}_{\boldsymbol{\eta}_0} = -\boldsymbol{B}_{\overline{\boldsymbol{\eta}}}$ so that the MCRB reverts to the classical Cramér-Rao bound (CRB) [116].

Since the value of the pseudo-true parameter is generally not of interest, the MCRB is used to establish the LB of any MS-unbiased estimator with respect to the true parameter value [85]

$$\mathbb{E}_p\{(\hat{\boldsymbol{\eta}}(\mathbf{y}) - \overline{\boldsymbol{\eta}})(\hat{\boldsymbol{\eta}}(\mathbf{y}) - \overline{\boldsymbol{\eta}})^{\mathsf{T}}\} \succeq \mathrm{LB}(\boldsymbol{\eta}_0), \tag{4.15}$$

where $\mathrm{LB}(\boldsymbol{\eta}_0) \triangleq \mathrm{MCRB}(\boldsymbol{\eta}_0) + (\overline{\boldsymbol{\eta}} - \boldsymbol{\eta}_0)(\overline{\boldsymbol{\eta}} - \boldsymbol{\eta}_0)^{\mathsf{T}}$. The last term is a bias term; that is, $\mathrm{Bias}(\boldsymbol{\eta}_0) \triangleq (\overline{\boldsymbol{\eta}} - \boldsymbol{\eta}_0)(\overline{\boldsymbol{\eta}} - \boldsymbol{\eta}_0)^{\mathsf{T}}$, and it is independent of the SNR. Hence, as the SNR tends to infinity, the MCRB term goes to zero, and the bias term becomes a tight bound for the MSE of any MS-unbiased estimator.

4.2.3 MCRB Derivation for RIS-aided Localization

4.2.3.1 Determining the Pseudo-True Parameter

To derive the MCRB for estimating the UE position under mismatch between the amplitude models for the RIS elements, we should first calculate the $\boldsymbol{\eta}_0$ parameter in (4.10) for the system model described in Section 4.1; that is, we should find the value of $\boldsymbol{\eta}$ that minimizes the KL divergence between $p(\mathbf{y})$ in (4.6) and $\tilde{p}(\mathbf{y}|\boldsymbol{\eta})$ in (4.8). The following lemma characterizes $\boldsymbol{\eta}_0$ for the considered system model.

Lemma 4.1: The value of $\boldsymbol{\eta}$ that minimizes the KL divergence between $p(\mathbf{y})$ in (4.6) and $\tilde{p}(\mathbf{y}|\boldsymbol{\eta})$, which is a parameterized version of (4.8), can be expressed as

$$\boldsymbol{\eta}_0 = \underset{\boldsymbol{\eta} \in \mathbb{R}^5}{\arg\min} \left\| \boldsymbol{\epsilon}(\boldsymbol{\eta}) \right\|_2 \tag{4.16}$$

where $\boldsymbol{\epsilon}(\boldsymbol{\eta}) \triangleq [\epsilon_1(\boldsymbol{\eta}) \ \ldots \ \epsilon_T(\boldsymbol{\eta})]^{\mathsf{T}}$ and $\epsilon_t(\boldsymbol{\eta}) \triangleq \mu_t - \tilde{\mu}_t(\boldsymbol{\eta})$ for $t = 1, \ldots, T$.

Proof: Based on the definition of the KL divergence and the system model in Section 4.1, (4.10) can be expressed as

$$\boldsymbol{\eta}_0 = \underset{\boldsymbol{\eta}\in\mathbb{R}^5}{\arg\min} \int p(\mathbf{y}) \log\left(\frac{p(\mathbf{y})}{\tilde{p}(\mathbf{y}|\boldsymbol{\eta})}\right) \mathrm{d}\mathbf{y} \tag{4.17}$$

$$= \underset{\boldsymbol{\eta}\in\mathbb{R}^5}{\arg\min} - \int p(\mathbf{y}) \log \tilde{p}(\mathbf{y}|\boldsymbol{\eta}) \,\mathrm{d}\mathbf{y} \tag{4.18}$$

$$= \underset{\boldsymbol{\eta}\in\mathbb{R}^5}{\arg\min} \int p(\mathbf{y}) \left\|\mathbf{y} - \tilde{\boldsymbol{\mu}}(\boldsymbol{\eta})\right\|_2^2 \mathrm{d}\mathbf{y} \tag{4.19}$$

where the second equality is due to the independence of $p(\mathbf{y})$ from $\boldsymbol{\eta}$, and the last equality is obtained from (4.8). Then, it can be shown that the following equations hold:

$$\begin{aligned}\int p(\mathbf{y}) \left\|\mathbf{y} - \tilde{\boldsymbol{\mu}}(\boldsymbol{\eta})\right\|_2^2 d\mathbf{y} &= \sum_{t=1}^{T} \int p(\mathbf{y}) \left|y_t - \tilde{\mu}_t(\boldsymbol{\eta})\right|^2 \mathrm{d}\mathbf{y} \\ &= \sum_{t=1}^{T} \underbrace{\left(\prod_{t'\neq t} \int p(y_{t'}) \,\mathrm{d}y_{t'}\right)}_{=1} \left(\int p(y_t) \left|y_t - \tilde{\mu}_t(\boldsymbol{\eta})\right|^2 \mathrm{d}y_t\right) \\ &= \sum_{t=1}^{T} \int p(y_t) \left|y_t - \tilde{\mu}_t(\boldsymbol{\eta})\right|^2 \mathrm{d}y_t. \end{aligned} \tag{4.20}$$

We now introduce $\epsilon_t(\boldsymbol{\eta}) = \mu_t - \tilde{\mu}_t(\boldsymbol{\eta})$, so that $\left|y_t - \tilde{\mu}_t(\boldsymbol{\eta})\right|^2 = \left|y_t - \mu_t + \epsilon_t(\boldsymbol{\eta})\right|^2$, and the integral expression in (4.20) can be manipulated as follows:

$$\begin{aligned}\int p(y_t) \left|y_t - \tilde{\mu}_t(\boldsymbol{\eta})\right|^2 \mathrm{d}y_t &= \int p(y_t) \left|y_t - \mu_t\right|^2 \mathrm{d}y_t \\ &\quad + \left|\epsilon_t(\boldsymbol{\eta})\right|^2 \int p(y_t) \,\mathrm{d}y_t + 2 \int p(y_t) \mathrm{Re}\left((y_t - \mu_t)^* \epsilon_t(\boldsymbol{\eta})\right) \mathrm{d}y_t. \end{aligned} \tag{4.21}$$

Since $y_t \sim \mathcal{CN}(\mu_t, N_0)$ and $\int p(y_t) \,\mathrm{d}y_t = 1$, the expression in (4.21) can be simplified as

$$\int p(y_t) \left|y_t - \tilde{\mu}_t(\boldsymbol{\eta})\right|^2 \mathrm{d}y_t = N_0 + \left|\epsilon_t(\boldsymbol{\eta})\right|^2. \tag{4.22}$$

By combining (4.19), (4.20) and (4.22), we finally obtain that

$$\bar{\boldsymbol{\eta}} = \underset{\boldsymbol{\eta}\in\mathbb{R}^5}{\arg\min} \sum_{t=1}^{T} \left(N_0 + \left|\epsilon_t(\boldsymbol{\eta})\right|^2\right) = \underset{\boldsymbol{\eta}\in\mathbb{R}^5}{\arg\min} \sum_{t=1}^{T} \left|\epsilon_t(\boldsymbol{\eta})\right|^2,$$

which completes the proof. ■

Lemma 4.1 states that the pseudo-true parameter minimizes the Euclidean distance between the noise-free observations under the true and assumed models.

Let $\gamma(\boldsymbol{\eta}) \triangleq \|\boldsymbol{\epsilon}(\boldsymbol{\eta})\|_2 = \|\boldsymbol{\mu} - \tilde{\boldsymbol{\mu}}(\boldsymbol{\eta})\|_2$. It is noted from (4.5) and (4.9) that $\gamma(\boldsymbol{\eta})$ is non-convex with respect to $\boldsymbol{\eta}$; hence, it is challenging to solve (4.16) in its current form. Based on (4.8) and (4.9), we can re-write (4.16) as

$$(\boldsymbol{\alpha}_0, \boldsymbol{p}_0) = \arg\min_{(\boldsymbol{\alpha},\boldsymbol{p})} \|\boldsymbol{\mu} - \alpha\, \boldsymbol{c}(\boldsymbol{p})\|_2 \,, \tag{4.23}$$

where $[\boldsymbol{c}(\boldsymbol{p})]_t \triangleq \sum_{m=1}^{M} [\boldsymbol{b}(\boldsymbol{p})]_m \tilde{w}_{t,m} s_t$. The optimal complex-valued α for any given $\boldsymbol{p}$ can be expressed as

$$\alpha = \frac{\boldsymbol{c}^{\mathsf{H}}(\boldsymbol{p})\boldsymbol{\mu}}{\boldsymbol{c}^{\mathsf{H}}(\boldsymbol{p})\boldsymbol{c}(\boldsymbol{p})} \,. \tag{4.24}$$

Inserting (4.24) into (4.23), the minimization problem can be reduced to a three-dimensional search as follows:

$$\boldsymbol{p}_0 = \arg\max_{\boldsymbol{p}} \boldsymbol{\mu}^{\mathsf{H}} \boldsymbol{\Pi}_{\boldsymbol{c}(\boldsymbol{p})} \boldsymbol{\mu} \;, \tag{4.25}$$

where $\boldsymbol{\Pi}_{\mathbf{x}} \triangleq \mathbf{x}\mathbf{x}^{\mathsf{H}}/\mathbf{x}^{\mathsf{H}}\mathbf{x}$. Therefore, $\boldsymbol{\eta}_0 = [\boldsymbol{\alpha}_0^{\mathsf{T}}\ \boldsymbol{p}_0^{\mathsf{T}}]^{\mathsf{T}}$ can be found by first performing a three-dimensional optimization as in (4.25), and then calculating α_0 via (4.24) and obtaining $\boldsymbol{\alpha}_0$ as $\boldsymbol{\alpha}_0 = [\mathrm{Re}(\alpha_0)\ \mathrm{Im}(\alpha_0)]^{\mathsf{T}}$.

Remark 4.1: In order to determine the pseudo-true parameter or equivalently to find $\boldsymbol{p}_0$ in (4.25), the true location $\overline{\boldsymbol{p}}$ can be used for initialization, which reduces the computational complexity of MCRB calculation significantly.

Remark 4.2: It is noted that the proof of Lemma 4.1 does not rely on the amplitude model given in (4.3). Thus, Lemma 4.1 is not only valid for (4.3). That is, for any kind of phase-dependent amplitude variations, Lemma 4.1 can be used.

4.2.3.2 Deriving the MCRB

After finding $\boldsymbol{\eta}_0$, we compute the matrices $\boldsymbol{A}_{\boldsymbol{\eta}_0}$ from (4.13) and $\boldsymbol{B}_{\boldsymbol{\eta}_0}$ from (4.14) for evaluating the MCRB in (4.11). Based on the pdf expressions in (4.6)–(4.8), (4.13) becomes

$$[\boldsymbol{A}_{\boldsymbol{\eta}_0}]_{ij} = -\frac{1}{N_0}\left(\int \frac{\partial^2}{\partial\eta_i\partial\eta_j}\left\|\mathbf{y}-\tilde{\boldsymbol{\mu}}(\boldsymbol{\eta})\right\|_2^2 p(\mathbf{y})\,d\mathbf{y}\right)\Bigg|_{\boldsymbol{\eta}=\boldsymbol{\eta}_0} \tag{4.26}$$

$$= -\frac{1}{N_0}\left(\sum_{t=1}^{T}\int \frac{\partial^2}{\partial\eta_i\partial\eta_j}\left|y_t-\tilde{\mu}_t(\boldsymbol{\eta})\right|^2 p(\mathbf{y})\,d\mathbf{y}\right)\Bigg|_{\boldsymbol{\eta}=\boldsymbol{\eta}_0} \tag{4.27}$$

$$= -\frac{1}{N_0}\left(\sum_{t=1}^{T}\int \frac{\partial^2}{\partial\eta_i\partial\eta_j}\left|y_t-\tilde{\mu}_t(\boldsymbol{\eta})\right|^2 p(y_t)\,dy_t\right)\Bigg|_{\boldsymbol{\eta}=\boldsymbol{\eta}_0} \tag{4.28}$$

$$= \frac{2}{N_0}\mathrm{Re}\left\{\sum_{t=1}^{T}\epsilon_t(\boldsymbol{\eta})^*\frac{\partial^2\tilde{\mu}_t(\boldsymbol{\eta})}{\partial\eta_i\eta_j} - \frac{\partial\tilde{\mu}_t^*(\boldsymbol{\eta})}{\partial\eta_i}\frac{\partial\tilde{\mu}_t(\boldsymbol{\eta})}{\partial\eta_j}\right\}\Bigg|_{\boldsymbol{\eta}=\boldsymbol{\eta}_0} \tag{4.29}$$

In addition, after some algebraic manipulation, the (i,j)th entry of matrix $\boldsymbol{B}_{\boldsymbol{\eta}_0}$ in (4.14) can be written as the sum of four terms as $[\boldsymbol{B}_{\boldsymbol{\eta}_0}]_{ij} = T_1 + T_2 + T_3 + T_4$, where

$$T_1 = \frac{1}{N_0^2}\left(\sum_{t=1}^{T}\frac{\partial\tilde{\mu}_t(\boldsymbol{\eta})}{\partial\eta_i}\epsilon_t(\boldsymbol{\eta})^*\right)\left(\sum_{l=1}^{T}\frac{\partial\tilde{\mu}_l(\boldsymbol{\eta})}{\partial\eta_j}\epsilon_l(\boldsymbol{\eta})^*\right)\Bigg|_{\boldsymbol{\eta}=\boldsymbol{\eta}_0} \tag{4.30}$$

$$T_2 = \left[\frac{1}{N_0^2}\left(\sum_{t=1}^{T}\frac{\partial\tilde{\mu}_t(\boldsymbol{\eta})}{\partial\eta_i}\epsilon_t(\boldsymbol{\eta})^*\right)\left(\sum_{l=1}^{T}\frac{\partial\tilde{\mu}_l^*(\boldsymbol{\eta})}{\partial\eta_j}\epsilon_l(\boldsymbol{\eta})\right) + \frac{1}{N_0}\sum_{t=1}^{T}\frac{\partial\tilde{\mu}_t(\boldsymbol{\eta})}{\partial\eta_i}\frac{\partial\tilde{\mu}_t^*(\boldsymbol{\eta})}{\partial\eta_j}\right]\Bigg|_{\boldsymbol{\eta}=\boldsymbol{\eta}_0} \tag{4.31}$$

$$T_3 = \frac{1}{N_0^2}\left(\sum_{t=1}^{T}\frac{\partial\tilde{\mu}_t^*(\boldsymbol{\eta})}{\partial\eta_i}\epsilon_t(\boldsymbol{\eta})\right)\left(\sum_{t=1}^{T}\frac{\partial\tilde{\mu}_l^*(\boldsymbol{\eta})}{\partial\eta_j}\epsilon_l(\boldsymbol{\eta})\right)\Bigg|_{\boldsymbol{\eta}=\boldsymbol{\eta}_0} \tag{4.32}$$

$$T_4 = \left[\frac{1}{N_0^2}\left(\sum_{t=1}^{T}\frac{\partial\tilde{\mu}_t^*(\boldsymbol{\eta})}{\partial\eta_i}\epsilon_t(\boldsymbol{\eta})\right)\left(\sum_{l=1}^{T}\frac{\partial\tilde{\mu}_l(\boldsymbol{\eta})}{\partial\eta_j}\epsilon_l(\boldsymbol{\eta})^*\right) + \frac{1}{N_0}\sum_{t=1}^{T}\frac{\partial\tilde{\mu}_t^*(\boldsymbol{\eta})}{\partial\eta_i}\frac{\partial\tilde{\mu}_t(\boldsymbol{\eta})}{\partial\eta_j}\right]\Bigg|_{\boldsymbol{\eta}=\boldsymbol{\eta}_0} \tag{4.33}$$

Hence, $[\boldsymbol{A}_{\boldsymbol{\eta}_0}]_{ij}$ and $[\boldsymbol{B}_{\boldsymbol{\eta}_0}]_{ij}$ can be written in more compact forms as follows:

$$[\boldsymbol{A}_{\boldsymbol{\eta}_0}]_{ij} = \frac{2}{N_0}\mathrm{Re}\left\{\boldsymbol{\epsilon}(\boldsymbol{\eta})^{\mathsf{H}}\frac{\partial^2\tilde{\boldsymbol{\mu}}(\boldsymbol{\eta})}{\partial\eta_i\partial\eta_j} - \Big(\frac{\partial\tilde{\boldsymbol{\mu}}(\boldsymbol{\eta})}{\partial\eta_i}\Big)^{\mathsf{H}}\frac{\partial\tilde{\boldsymbol{\mu}}(\boldsymbol{\eta})}{\partial\eta_j}\right\}\Bigg|_{\boldsymbol{\eta}=\boldsymbol{\eta}_0} \tag{4.34}$$

$$[\boldsymbol{B}_{\boldsymbol{\eta}_0}]_{ij} = \frac{2}{N_0}\left[\frac{2}{N_0}\mathrm{Re}\left\{\boldsymbol{\epsilon}(\boldsymbol{\eta})^{\mathsf{H}}\frac{\partial\tilde{\boldsymbol{\mu}}(\boldsymbol{\eta})}{\partial\eta_i}\right\}\mathrm{Re}\left\{\boldsymbol{\epsilon}(\boldsymbol{\eta})^{\mathsf{H}}\frac{\partial\tilde{\boldsymbol{\mu}}(\boldsymbol{\eta})}{\partial\eta_j}\right\} + \mathrm{Re}\left\{\left(\frac{\partial\tilde{\boldsymbol{\mu}}(\boldsymbol{\eta})}{\partial\eta_i}\right)^{\mathsf{H}}\frac{\partial\tilde{\boldsymbol{\mu}}(\boldsymbol{\eta})}{\partial\eta_j}\right\}\right]\Bigg|_{\boldsymbol{\eta}=\boldsymbol{\eta}_0}. \tag{4.35}$$

where

$$\frac{\partial^2\tilde{\boldsymbol{\mu}}(\boldsymbol{\eta})}{\partial\eta_i\partial\eta_j} \triangleq \left[\frac{\partial^2\tilde{\mu}_1(\boldsymbol{\eta})}{\partial\eta_i\partial\eta_j}\ \cdots\ \frac{\partial^2\tilde{\mu}_T(\boldsymbol{\eta})}{\partial\eta_i\partial\eta_j}\right]^{\mathsf{T}}. \tag{4.36}$$

Therefore, once we compute the first and the second derivatives of $\tilde{\mu}_t(\boldsymbol{\eta})$ with respect to $\boldsymbol{\eta}$, we can easily compute the matrices $\boldsymbol{A}_{\boldsymbol{\eta}_0}$ and $\boldsymbol{B}_{\boldsymbol{\eta}_0}$ as specified above. Based on $\boldsymbol{A}_{\boldsymbol{\eta}_0}$ and $\boldsymbol{B}_{\boldsymbol{\eta}_0}$, the MCRB in (4.11) and the lower bound in (4.15) can be evaluated in a straightforward manner. Next, we present the derivatives of $\tilde{\mu}_t(\boldsymbol{\eta})$ as follows.

Derivatives of $\tilde{\mu}_t(\boldsymbol{\eta})$:

Let $\boldsymbol{\eta}$ be given by $\boldsymbol{\eta} = [\alpha_r\, \alpha_i\, \mathrm{x}\, \mathrm{y}\, \mathrm{z}]^{\mathsf{T}}$. Also, define $\boldsymbol{p} \triangleq [\mathrm{x}\, \mathrm{y}\, \mathrm{z}]^{\mathsf{T}}$, $b_m \triangleq [\boldsymbol{b}(\boldsymbol{p})]_m$, and $\alpha \triangleq \alpha_r + j\alpha_i$. We also introduce $\boldsymbol{u} = \frac{\boldsymbol{p}-\boldsymbol{p}_{\mathrm{RIS}}}{\|\boldsymbol{p}-\boldsymbol{p}_{\mathrm{RIS}}\|_2}$and for any $1 \leq m \leq M$, $\boldsymbol{u}_m = \frac{\boldsymbol{p}-\boldsymbol{p}_m}{\|\boldsymbol{p}-\boldsymbol{p}_m\|_2}$, where $\boldsymbol{u} = [u_x\, u_y\, u_z]^{\mathsf{T}}$ and $\boldsymbol{u}_m = [u_{m,x}\, u_{m,y}\, u_{m,z}]^{\mathsf{T}}$.Then, the first and second derivatives of $\tilde{\mu}_t(\boldsymbol{\eta})$ with respect to $\boldsymbol{\eta}$ are given as follows:

$$\frac{\partial \tilde{\mu}_t(\boldsymbol{\eta})}{\partial \alpha_r} = \sum_{m=1}^{M} b_m \tilde{w}_{t,m} s_t,\ \frac{\partial \tilde{\mu}_t(\boldsymbol{\eta})}{\partial \alpha_i} = j \sum_{m=1}^{M} b_m \tilde{w}_{t,m} s_t.$$

For $\nu \in \{\mathrm{x}\, \mathrm{y}\, \mathrm{z}\}$, we can write

$$\begin{aligned}
\frac{\partial \tilde{\mu}_t(\boldsymbol{\eta})}{\partial \nu} &= -j\frac{2\pi}{\lambda}\alpha \sum_{m=1}^{M} b_m \left(u_{m,\nu} - u_x\right) \tilde{w}_{t,m} s_t, \\
\frac{\partial^2 \tilde{\mu}_t(\boldsymbol{\eta})}{\partial \alpha_r \partial \nu} &= -j\frac{2\pi}{\lambda} \sum_{m=1}^{M} b_m \left(u_{m,\nu} - u_\nu\right) \tilde{w}_{t,m} s_t, \\
\frac{\partial^2 \tilde{\mu}_t(\boldsymbol{\eta})}{\partial \alpha_i \partial \nu} &= j\frac{\partial^2 \tilde{\mu}_t(\boldsymbol{\eta})}{\partial \alpha_r \partial \nu}, \\
\frac{\partial^2 \tilde{\mu}_t(\boldsymbol{\eta})}{\partial \nu \partial \nu} &= -\alpha\frac{4\pi^2}{\lambda^2} \sum_{m=1}^{M} b_m \left(u_{m,\nu} - u_\nu\right)^2 \tilde{w}_{t,m} s_t - j\frac{2\pi}{\lambda}\alpha \sum_{m=1}^{M} b_m \left(\frac{1-u_{m,\nu}^2}{\|\boldsymbol{p}-\boldsymbol{p}_m\|_2} - \frac{1-u_\nu^2}{\|\boldsymbol{p}-\boldsymbol{p}_{\mathrm{RIS}}\|_2}\right) \tilde{w}_{t,m} s_t.
\end{aligned}$$

Moreover, if $\nu_1, \nu_2 \in \{\mathrm{x}\, \mathrm{y}\, \mathrm{z}\}$ and they correspond to different coordinates, it is possible to express

$$\begin{aligned}
\frac{\partial^2 \tilde{\mu}_t(\boldsymbol{\eta})}{\partial \nu_1 \partial \nu_2} = &-\alpha\frac{4\pi^2}{\lambda^2} \sum_{m=1}^{M} b_m \left(u_{m,\nu_1} - u_{\nu_1}\right)\left(u_{m,\nu_2} - u_{\nu_2}\right) \tilde{w}_{t,m} s_t \\
&+ j\frac{2\pi}{\lambda}\alpha \sum_{m=1}^{M} b_m \left(\frac{u_{m,\nu_1}u_{m,\nu_2}}{\|\boldsymbol{p}-\boldsymbol{p}_m\|_2} - \frac{u_{\nu_1}u_{\nu_2}}{\|\boldsymbol{p}-\boldsymbol{p}_{\mathrm{RIS}}\|_2}\right) \tilde{w}_{t,m} s_t.
\end{aligned}$$

4.3 Scenario-I: Mismatched Estimator

In this section, we focus on estimator design for Scenario-I. First, we derive the plain MML estimator, which entails computationally prohibitive high-dimensional non-convex optimization. To circumvent this, we then propose a low-complexity estimator capitalizing on the Jacobi-Anger expansion, which reduces the problem to a series of line searches over range, azimuth, and elevation domains.

4.3.1 Mismatched Maximum Likelihood (MML) Estimator

The MML estimator is given by [85]

$$\hat{\boldsymbol{\eta}}_{\mathrm{MML}}(\mathbf{y}) = \underset{\boldsymbol{\eta}\in\mathbb{R}^5}{\arg\max} \log \tilde{p}(\mathbf{y}|\boldsymbol{\eta}). \tag{4.37}$$

Under some regularity conditions, it can be shown that $\hat{\boldsymbol{\eta}}_{\mathrm{MML}}(\mathbf{y})$ is asymptotically MS-unbiased and its error covariance matrix is asymptotically equal to the MCRB($\boldsymbol{\eta}_0$) [85, Thm. 2]. Hence, the covariance matrix of the MML estimator is asymptotically tight to the MCRB.

From (4.8) and (4.37), the MML estimator based on the received signal $\mathbf{y}$ in (4.1) can be expressed as

$$\hat{\boldsymbol{\eta}}_{\mathrm{MML}}(\mathbf{y}) = \underset{\boldsymbol{\eta}\in\mathbb{R}^5}{\arg\max} \log \tilde{p}(\mathbf{y}|\boldsymbol{\eta}) = \underset{\boldsymbol{\eta}\in\mathbb{R}^5}{\arg\min} \left\|\mathbf{y} - \tilde{\boldsymbol{\mu}}(\boldsymbol{\eta})\right\|_2. \tag{4.38}$$

Since this problem is in the same form as in (4.16), it can be reduced to a three-dimensional optimization problem as discussed in Section 4.2.3. In order to solve the resulting problem, initialization can be very critical as we are faced with a non-convex optimization problem. During the estimation process, we do not have access to the true position $\overline{\boldsymbol{p}}$. Hence, we cannot use the true position vector $\overline{\boldsymbol{p}}$ for the initialization. If an arbitrarily chosen position vector is used for the initialization, the global optimal solution of (4.37) cannot always be obtained. To find a remedy for this issue, we next propose an approximated version of the MML estimator, namely, the approximate mismatched maximum likelihood (AMML) estimator, based on the Jacobi-Anger expansion approach [70, 82].

4.3.2 AMML Estimator Structure

Let $\overline{\vartheta} \in [0,\, \pi/2]$ denote the angle between the Z axis and $\overline{\boldsymbol{p}}$, and $\overline{\varphi} \in [0,\, 2\pi]$ represent the angle between the projection of $\overline{\boldsymbol{p}}$ on the X-Y plane and the X axis, measured counter-clockwise. Hence, we can write $\overline{\boldsymbol{p}} = \overline{d}\,[\sin\overline{\vartheta}\cos\overline{\varphi}\ \sin\overline{\vartheta}\sin\overline{\varphi}\ \cos\overline{\vartheta}]^{\mathsf{T}}$, where $\overline{d} = \|\overline{\boldsymbol{p}}\|_2$. When $\overline{d} \gg \|\mathbf{p}_m\|_2$, the near-field steering vector $[\boldsymbol{a}(\overline{\boldsymbol{p}})]_m$ in (4.2) reverts to its standard far-field counterpart as follows [70]:

$$[\boldsymbol{a}(\overline{\boldsymbol{p}})]_m = \exp\left(j\frac{2\pi}{\lambda}\mathbf{p}_m^{\mathsf{T}}\boldsymbol{k}(\overline{\vartheta},\overline{\varphi})\right)\ . \tag{4.39}$$

By employing the Jacobi-Anger expansion to (4.39), $\boldsymbol{a}(\overline{\boldsymbol{p}})$ can be expanded as [119]

$$[\boldsymbol{a}(\overline{\boldsymbol{p}})]_m = \sum_{n=-\infty}^{\infty} j^n J_n\left(\frac{2\pi}{\lambda}\|\boldsymbol{p}_m\|_2 \sin\overline{\vartheta}\right) e^{jn(\overline{\varphi}-\psi_m)}\ , \tag{4.40}$$

where $\boldsymbol{p}_m = \|\boldsymbol{p}_m\|_2\,[\cos(\psi_m)\ \sin(\psi_m)\ 0]^{\mathsf{T}}$ and $J_n(\cdot)$ is the nth order Bessel function of the first kind. As $|J_n(\cdot)|$ decays to 0 as $|n|$ increases, by neglecting the terms with $|n| > N$, for some $N \in \mathbb{N}$, $\boldsymbol{a}(\overline{\boldsymbol{p}})$ in (4.39) can be approximated by

$$[\boldsymbol{a}(\overline{\boldsymbol{p}})]_m \approx \sum_{n=-N}^{N} j^n J_n\left(\frac{2\pi}{\lambda}\|\boldsymbol{p}_m\|_2 \sin\overline{\vartheta}\right) e^{jn(\overline{\varphi}-\psi_m)}. \tag{4.41}$$

We define $[\boldsymbol{g}_m(\overline{\vartheta})]_n$ and $[\boldsymbol{h}(\overline{\varphi})]_n$ for $n \in \{-N, \ldots, N\}$ as follows:

$$[\boldsymbol{g}_m(\overline{\vartheta})]_n = j^n J_n\left(\frac{2\pi}{\lambda}\|\boldsymbol{p}_m\|_2 \sin\overline{\vartheta}\right) e^{-jn\psi_m}\ , \tag{4.42}$$

$$[\boldsymbol{h}(\overline{\varphi})]_n = e^{jn\overline{\varphi}}\ . \tag{4.43}$$

Then, inserting (4.42) and (4.43) into (4.41) yields

$$\boldsymbol{a}(\overline{\boldsymbol{p}}) \approx \boldsymbol{G}^{\mathsf{T}}(\overline{\vartheta})\boldsymbol{h}(\overline{\varphi}), \tag{4.44}$$

where

$$\boldsymbol{G}(\overline{\vartheta}) = [\boldsymbol{g}_1(\overline{\vartheta})\ \ldots\ \boldsymbol{g}_M(\overline{\vartheta})] \in \mathbb{C}^{(2N+1)\times M}. \tag{4.45}$$

Next, we define a matrix $\boldsymbol{Q} \in \mathbb{C}^{T\times M}$ with the elements $[\boldsymbol{Q}]_{t,m} = \tilde{w}_{t,m}[\boldsymbol{a}(\boldsymbol{p}_{\mathrm{BS}})]_m$ for any t, m. Hence, (4.9) can be approximated as

$$\tilde{\boldsymbol{\mu}}(\overline{\boldsymbol{\eta}}) \approx \overline{\alpha}\boldsymbol{Q}\boldsymbol{G}^{\mathsf{T}}(\overline{\vartheta})\boldsymbol{h}(\overline{\varphi})\sqrt{E_s} \tag{4.46}$$

where $s_t = \sqrt{E_s}$ for any t. That is, for the assumed model, we can write the observations as

$$\mathbf{y} \approx \overline{\alpha}\boldsymbol{Q}\boldsymbol{G}^{\mathsf{T}}(\overline{\vartheta})\boldsymbol{h}(\overline{\varphi})\sqrt{E_s} + \boldsymbol{n} \ , \tag{4.47}$$

where $\boldsymbol{n} \triangleq [n_1 \ \ldots \ n_T]^{\mathsf{T}}$. By using the three-step simple line searches given in [70, Eqs. (31), (32), (33)], the estimates of $\overline{\varphi}$, $\overline{\vartheta}$ and $\overline{d}$ are obtained as follows:

$$\hat{\vartheta} = \underset{\vartheta\in[0,\,\pi/2]}{\arg\min} \left\| \mathbf{y} - \boldsymbol{Q}\boldsymbol{G}^{\mathsf{T}}(\vartheta) \left(\boldsymbol{Q}\boldsymbol{G}^{\mathsf{T}}(\vartheta)\right)^{\dagger} \mathbf{y} \right\|_2 , \tag{4.48}$$

$$\hat{\varphi} = \underset{\varphi\in[0,\,2\pi]}{\arg\min} \left\| \mathbf{y} - \sqrt{E_s}\hat{\alpha}\left(\varphi\right) \boldsymbol{Q}\boldsymbol{G}^{\mathsf{T}}(\hat{\vartheta})\boldsymbol{h}(\varphi) \right\|_2 , \tag{4.49}$$

$$\hat{d} = \underset{d\in(0,\infty)}{\arg\min} \left\| \mathbf{y} - \sqrt{E_s}\hat{\alpha}\left(\boldsymbol{p}(d)\right) \boldsymbol{Q}\boldsymbol{a}(\boldsymbol{p}(d)) \right\|_2 , \tag{4.50}$$

where $(\cdot)^{\dagger}$ denotes pseudo-inverse,

$$\boldsymbol{p}(d) \triangleq d[\sin(\hat{\vartheta})\cos(\hat{\varphi}) \ \sin(\hat{\vartheta})\sin(\hat{\varphi}) \ \cos(\hat{\vartheta})]^{\mathsf{T}} \ , \tag{4.51}$$

$$\hat{\alpha}(\varphi) \triangleq \frac{\sqrt{E_s}\left(\boldsymbol{Q}\boldsymbol{G}^{\mathsf{T}}(\hat{\vartheta})\boldsymbol{h}(\varphi)\right)^{\mathsf{H}}\mathbf{y}}{\left(\boldsymbol{Q}\boldsymbol{G}^{\mathsf{T}}(\hat{\vartheta})\boldsymbol{h}(\varphi)\right)^{\mathsf{H}}\boldsymbol{Q}\boldsymbol{G}^{\mathsf{T}}(\hat{\vartheta})\boldsymbol{h}(\varphi)} \ , \tag{4.52}$$

$$\hat{\alpha}(\boldsymbol{p}(d)) \triangleq \frac{\sqrt{E_s}\left(\boldsymbol{Q}\boldsymbol{a}(\boldsymbol{p}(d))\right)^{\mathsf{H}}\mathbf{y}}{\left(\boldsymbol{Q}\boldsymbol{a}(\boldsymbol{p}(d))\right)^{\mathsf{H}}\boldsymbol{Q}\boldsymbol{a}(\boldsymbol{p}(d))} \ . \tag{4.53}$$

After obtaining the estimates of $\overline{\vartheta}, \overline{\varphi}$, and $\overline{d}$, we use $\boldsymbol{p}(\hat{d})$ as the AMML estimate for the UE location. The entire algorithm is summarized in Algorithm 3. As discussed in [70], these three-step simple line searches have a low computational complexity. Based on the AMML estimate for the UE location, the search intervals in (4.48)-(4.50) can be made narrower, and we run the AMML estimator again.

Next, we analyze how the performance bounds and the estimator structures are affected when the true RIS amplitude model given in (4.3) is known.

Algorithm 3 AMML Algorithm for RIS-aided Near-Field Localization via Jacobi-Anger Expansion

Input: Observation $\mathbf{y}$ in (4.1).
Output: Location estimate $\widehat{\mathbf{p}}$.

(a) Find an estimate of azimuth $\hat{\vartheta}$ by solving (4.48).

(b) Using $\hat{\vartheta}$, find an estimate of elevation $\hat{\varphi}$ by solving (4.49).

(c) Using $\hat{\vartheta}$ and $\hat{\varphi}$, find an estimate of distance $\hat{d}$ by solving (4.50).

(d) Compute the location estimate via (4.51).

4.4 Scenario-II & Scenario-III: RIS-aided Localization Under Known RIS Amplitude Model

In this section, we investigate RIS-aided localization under Scenario-II and Scenario-III, where the UE is assumed to be aware of the RIS amplitude model in (4.3).

4.4.1 Scenario-II: Known RIS Amplitude Model with Unknown Parameters

In this scenario, in order to parameterize the unknown system parameters, we will use $\boldsymbol{\eta} = [\mathrm{Re}(\alpha)\, \mathrm{Im}(\alpha)\, \boldsymbol{p}^{\mathsf{T}}\, \beta_{\min}\, \kappa\, \phi]^{\mathsf{T}}$, which consists of both the channel parameters and the RIS model parameters. Then, by [70, Eq. 9], the Fisher Information matrix (FIM), $\boldsymbol{J}(\boldsymbol{\eta}) \in \mathbb{R}^{8\times 8}$, can be expressed as

$$\boldsymbol{J}(\boldsymbol{\eta}) = \frac{2}{N_0}\mathrm{Re}\left\{ \left(\frac{\partial \boldsymbol{\mu}}{\partial \boldsymbol{\eta}}\right)^{\mathsf{H}} \frac{\partial \boldsymbol{\mu}}{\partial \boldsymbol{\eta}} \right\}. \tag{4.54}$$

In order to compute the derivatives of $\boldsymbol{\mu}$ with respect to the first five entries of $\boldsymbol{\eta}$, we can use the derivatives given in Chapter 4.2.3.2 by replacing the $\tilde{w}_{t,m}$ terms with $w_{t,m}$. For the last three entries of $\boldsymbol{\eta}$, i.e., for the RIS related parameters, the FIM entries are given as follows:

$$\frac{\partial \mu_t(\boldsymbol{\eta})}{\partial \beta_{\min}} = \alpha\sqrt{E_s}\sum_{m=1}^{M}[\boldsymbol{b}(\boldsymbol{p})]_m e^{j\theta_{t,m}}\left(1-\left(\frac{\sin(\theta_{t,m}-\phi)+1}{2}\right)^{\kappa}\right),$$

$$\frac{\partial \mu_t(\boldsymbol{\eta})}{\partial \kappa} = \alpha\sqrt{E_s}\sum_{m=1}^{M}[\boldsymbol{b}(\boldsymbol{p})]_m e^{j\theta_{t,m}}(1-\beta_{\min})\left(\frac{\sin(\theta_{t,m}-\phi)+1}{2}\right)^{\kappa}\log\left(\frac{\sin(\theta_{t,m}-\phi)+1}{2}\right),$$

$$\frac{\partial \mu_t(\boldsymbol{\eta})}{\partial \phi} = -\alpha\sqrt{E_s}\sum_{m=1}^{M}[\boldsymbol{b}(\boldsymbol{p})]_m e^{j\theta_{t,m}}(1-\beta_{\min})\kappa\left(\frac{\sin(\theta_{t,m}-\phi)+1}{2}\right)^{\kappa-1}\left(\frac{\cos(\theta_{t,m}-\phi)}{2}\right).$$

After obtaining the FIM, by computing $\mathrm{Tr}\{\boldsymbol{J}^{-1}(\boldsymbol{\eta})\}_{3:5,3:5}$, we can obtain the CRB for estimating the UE position. Moreover, the ML estimator can be stated as

$$\hat{\boldsymbol{\eta}}_{\mathrm{ML}}(\mathbf{y}) = \underset{\boldsymbol{\eta}\in\mathbb{R}^8}{\arg\max}\log p(\mathbf{y}). \tag{4.55}$$

As discussed in Section 4.2.3, the estimate for $\overline{\alpha}$ can uniquely be determined for given estimates of $\overline{\boldsymbol{p}}$, $\overline{\beta}_{\min}$, $\overline{\kappa}$, and $\overline{\phi}$. That is, this problem can be reduced to a 6-dimensional optimization problem. Similar to the mismatched scenario (Scenario-I), the initialization is an important issue for this scenario, as well. For practical implementations, we propose an approximate version of the ML estimator, called the approximate maximum likelihood (AML) estimator, in the next section.

4.4.2 Scenario-II: AML Estimator

In this part, our goal is to solve the problem of *joint localization and online RIS calibration* in (4.55), which involves estimating the UE location $\overline{\boldsymbol{p}}$ and the RIS model parameters $\overline{\beta}_{\min}$, $\overline{\kappa}$, and $\overline{\phi}$ simultaneously. To accomplish this in an efficient manner, we propose a low-complexity estimator as an alternative to the high-dimensional non-convex optimization in (4.55).

Let us write the observations in (4.1) in a vector form as

$$\mathbf{y} = \bar{\alpha}\,\mathbf{W}^{\mathsf{T}}(\overline{\boldsymbol{\zeta}})\boldsymbol{b}(\overline{\boldsymbol{p}})\sqrt{E_s} + \mathbf{n}, \tag{4.56}$$

where $\mathbf{W}(\overline{\boldsymbol{\zeta}}) = [\mathbf{w}_1(\overline{\boldsymbol{\zeta}}) \ldots \mathbf{w}_T(\overline{\boldsymbol{\zeta}})] \in \mathbb{C}^{M\times T}$ is the matrix of RIS profiles as a function of the parameters $\overline{\boldsymbol{\zeta}} = [\overline{\beta}_{\min}\ \overline{\kappa}\ \overline{\phi}]^{\mathsf{T}}$ of the RIS amplitude model in (4.3) and (4.4), and $\mathbf{n} = [n_1 \ldots n_T]^{\mathsf{T}}$ is the additive noise vector. From (4.3) and (4.4), $\mathbf{W}(\overline{\boldsymbol{\zeta}})$ can be expressed as

$$\mathbf{W}(\overline{\boldsymbol{\zeta}}) = \big(\overline{\beta}_{\min}\boldsymbol{\Gamma}_1(\overline{\kappa},\overline{\phi}) + \boldsymbol{\Gamma}_2(\overline{\kappa},\overline{\phi})\big)\odot e^{j\boldsymbol{\Theta}}, \tag{4.57}$$

where $\boldsymbol{\Theta} \in \mathbb{R}^{M\times T}$ denotes the RIS phase shifts with $[\boldsymbol{\Theta}]_{m,t} = \theta_{m,t}$,

$$\boldsymbol{\Gamma}_1(\overline{\kappa}, \overline{\phi}) \triangleq \mathbf{1}_M \mathbf{1}_T^{\mathsf{T}} - \left(\frac{\sin(\boldsymbol{\Theta} - \overline{\phi}) + 1}{2}\right)^{\overline{\kappa}}, \tag{4.58}$$

$$\boldsymbol{\Gamma}_2(\overline{\kappa}, \overline{\phi}) \triangleq \left(\frac{\sin(\boldsymbol{\Theta} - \overline{\phi}) + 1}{2}\right)^{\overline{\kappa}}, \tag{4.59}$$

$\mathbf{1}_M$ is an all-ones vector of size M, and $\sin(\cdot)$ and $(\cdot)^{\overline{\kappa}}$ operations are element-wise. Plugging $\boldsymbol{b}(\overline{\boldsymbol{p}}) = \boldsymbol{a}(\overline{\boldsymbol{p}}) \odot \boldsymbol{a}(\mathbf{p}_{\mathrm{BS}})$ and (4.57) into (4.56) yields

$$\mathbf{y} = \overline{\alpha}\left(\overline{\beta}_{\min}\widetilde{\boldsymbol{\Gamma}}_1(\overline{\kappa}, \overline{\phi}) + \widetilde{\boldsymbol{\Gamma}}_2(\overline{\kappa}, \overline{\phi})\right)^{\mathsf{T}} \boldsymbol{a}(\overline{\boldsymbol{p}})\sqrt{E_s} + \mathbf{n}, \tag{4.60}$$

where

$$\begin{aligned}\widetilde{\boldsymbol{\Gamma}}_1(\overline{\kappa}, \overline{\phi}) &\triangleq \boldsymbol{\Gamma}_1(\overline{\kappa}, \overline{\phi}) \odot e^{j\boldsymbol{\Theta}} \odot \boldsymbol{a}(\mathbf{p}_{\mathrm{BS}})\mathbf{1}_T^{\mathsf{T}}, \\ \widetilde{\boldsymbol{\Gamma}}_2(\overline{\kappa}, \overline{\phi}) &\triangleq \boldsymbol{\Gamma}_2(\overline{\kappa}, \overline{\phi}) \odot e^{j\boldsymbol{\Theta}} \odot \boldsymbol{a}(\mathbf{p}_{\mathrm{BS}})\mathbf{1}_T^{\mathsf{T}}.\end{aligned} \tag{4.61}$$

The ML estimator corresponding to the observation model in (4.60) is given by

$$\min_{\alpha,\mathbf{p},\boldsymbol{\zeta}} \left\|\mathbf{y} - \alpha\left(\beta_{\min}\widetilde{\boldsymbol{\Gamma}}_1(\kappa, \phi) + \widetilde{\boldsymbol{\Gamma}}_2(\kappa, \phi)\right)^{\mathsf{T}} \boldsymbol{a}(\mathbf{p})\sqrt{E_s}\right\|_2^2. \tag{4.62}$$

To solve the ML optimization problem in (4.62), we now propose a three-step procedure consisting of location initialization, online RIS calibration and location refinement.

4.4.2.1 Step 0: Initialization of UE Location

First, by assuming $\beta_{\min} = 1$, the initial location estimate $\widehat{\mathbf{p}}$ is obtained by using the Jacobi-Anger expansion based algorithm in Algorithm 3. Inserting $\widehat{\mathbf{p}}$ into the ML estimator in (4.62), the optimization problem becomes

$$\min_{\alpha,\boldsymbol{\zeta}} \left\|\mathbf{y} - \alpha\left(\beta_{\min}\widetilde{\boldsymbol{\Gamma}}_1(\kappa, \phi) + \widetilde{\boldsymbol{\Gamma}}_2(\kappa, \phi)\right)^{\mathsf{T}} \boldsymbol{a}(\widehat{\mathbf{p}})\sqrt{E_s}\right\|_2^2. \tag{4.63}$$

4.4.2.2 Step 1: Online RIS Calibration

As noted from (4.63), $\overline{\alpha}$ and $\overline{\beta}_{\min}$ can now be estimated in closed-from as a function of the remaining unknown parameters, while the estimates of $\overline{\kappa}$ and $\overline{\phi}$ can be found via a 2-D

search. This motivates an alternating optimization algorithm where we alternate among updates of α, $\beta_{\min}$, and (κ, ϕ):

- *Update* α: Given $\boldsymbol{\zeta}$, a closed-form estimate of α in (4.63) is given by

$$\widehat{\alpha} = \left(\boldsymbol{\Upsilon}^{\mathsf{H}}(\boldsymbol{\zeta})\boldsymbol{\Upsilon}(\boldsymbol{\zeta})\right)^{-1}\boldsymbol{\Upsilon}^{\mathsf{H}}(\boldsymbol{\zeta})\mathbf{y}, \tag{4.64}$$

  where

$$\boldsymbol{\Upsilon}(\boldsymbol{\zeta}) \triangleq \left(\beta_{\min}\widetilde{\boldsymbol{\Gamma}}_1(\kappa,\phi) + \widetilde{\boldsymbol{\Gamma}}_2(\kappa,\phi)\right)^{\mathsf{T}}\boldsymbol{a}(\widehat{\mathbf{p}})\sqrt{E_s}. \tag{4.65}$$

- *Update* $\beta_{\min}$: Given α, κ, and ϕ, under the constraint of $0 \leq \beta_{\min} \leq 1$, the Lagrangian can be expressed as follows:

$$L(\beta_{\min}, \lambda_1, \lambda_2) = \|\mathbf{z} - \beta_{\min}\boldsymbol{\omega}\|_2^2 + \lambda_1(\beta_{\min} - 1) - \lambda_2\beta_{\min}$$

  where $\mathbf{z} = \mathbf{y} - \alpha\widetilde{\boldsymbol{\Gamma}}_2(\kappa,\phi)^{\mathsf{T}}\boldsymbol{a}(\widehat{\mathbf{p}})\sqrt{E_s}$ and $\boldsymbol{\omega} = \alpha\widetilde{\boldsymbol{\Gamma}}_1(\kappa,\phi)^{\mathsf{T}}\boldsymbol{a}(\widehat{\mathbf{p}})\sqrt{E_s}$. From Karush-Kuhn-Tucker conditions, the closed-form estimate of $\beta_{\min}$ in (4.63) can be obtained from the following set of equations:

$$\lambda_1 - \lambda_2 + 2\widehat{\beta}_{\min}\boldsymbol{\omega}^{\mathsf{H}}\boldsymbol{\omega} = \mathbf{z}^{\mathsf{H}}\boldsymbol{\omega} + \boldsymbol{\omega}^{\mathsf{H}}\mathbf{z} \tag{4.66}$$

$$\lambda_1(\widehat{\beta}_{\min} - 1) = 0, \;\; \lambda_2\widehat{\beta}_{\min} = 0. \tag{4.67}$$

  Hence, we can conclude that $\widehat{\beta}_{\min}$ admits one of the three alternative forms: $\widehat{\beta}_{\min} = 1$, $\widehat{\beta}_{\min} = 0$, or $\widehat{\beta}_{\min} = \mathrm{Re}\{\mathbf{z}^{\mathsf{H}}\boldsymbol{\omega}\}/(\boldsymbol{\omega}^{\mathsf{H}}\boldsymbol{\omega})$. Among these three solutions, the one which yields the smallest objective is chosen.

- *Update* κ *and* ϕ: Given α and $\beta_{\min}$, we can estimate κ and ϕ via a 2-D search:

$$(\widehat{\kappa}, \widehat{\phi}) = \underset{\substack{\kappa\in[0,\infty)\\ \phi\in[0,2\pi)}}{\arg\min} \left\| \mathbf{y} - \alpha\left(\beta_{\min}\widetilde{\boldsymbol{\Gamma}}_1(\kappa,\phi) + \widetilde{\boldsymbol{\Gamma}}_2(\kappa,\phi)\right)^{\mathsf{T}}\boldsymbol{a}(\widehat{\mathbf{p}})\sqrt{E_s}\right\|_2 \tag{4.68}$$

4.4.2.3 Step 2: Refinement of UE Location

As the output of this alternating procedure, we obtain the estimates of $\overline{\alpha}$, $\overline{\beta}_{\min}$, $\overline{\kappa}$, and $\overline{\phi}$. By plugging the estimates of $\overline{\beta}_{\min}$, $\overline{\kappa}$, and $\overline{\phi}$ (representing the *calibrated* RIS parameters)

Algorithm 4 AML Algorithm for Joint UE Localization and Online RIS Calibration

Input: Observation $\mathbf{y}$ in (4.60).

Output: Location estimate $\widehat{\mathbf{p}}$, channel gain estimate $\widehat{\alpha}$ and estimates of RIS amplitude model parameters $\widehat{\boldsymbol{\zeta}} = [\widehat{\beta}_{\min}, \widehat{\kappa}, \widehat{\phi}]^{\mathsf{T}}$.

1: **Step 0:** *Initialization of UE Location*

   (a) Set $\beta_{\min} = 1$.

   (b) Compute the initial location estimate $\widehat{\mathbf{p}}$ using Algorithm 3.

2: **Step 1:** *Alternating Iterations for Online RIS Calibration*

3: **while** the objective function in (4.63) does not converge

   (a) Update the channel estimate $\widehat{\alpha}$ via (4.64).

   (b) Update $\widehat{\beta}_{\min}$ via (4.66).

   (c) Update $\widehat{\kappa}$ and $\widehat{\phi}$ via (4.68).

4: **end while**

5: **Step 2:** *Refinement of UE Location with Calibrated RIS Model*

   (a) Use Algorithm 3 to estimate the UE location, $\widehat{\mathbf{p}}$, and the channel gain, $\widehat{\alpha}$, from (4.62) by plugging the estimates $\widehat{\beta}_{\min}$, $\widehat{\kappa}$ and $\widehat{\phi}$ obtained at the output of **Step 1**.

back into the ML estimator in (4.62), the estimate of the UE location $\overline{\boldsymbol{p}}$ can be refined via Algorithm 3. The overall algorithm for joint UE localization and online RIS calibration is summarized in Algorithm 4.

Remark 4.3: If we skip Step 1 of Algorithm 4 (i.e., online RIS calibration) and choose $\widehat{\beta}_{\min} = 1$ (i.e., uncalibrated, unit-amplitude RIS model in (4.7)), the AML algorithm gives the same estimate as the AMML algorithm.

4.4.3 Scenario-III: Known RIS Amplitude Model with Known Parameters

In this scenario, the unknown system parameters are given by $\boldsymbol{\eta} = [\mathrm{Re}(\alpha)\, \mathrm{Im}(\alpha)\, \boldsymbol{p}^{\mathsf{T}}]^{\mathsf{T}}$ and the values of the RIS related parameters are perfectly known. For this scenario, the FIM,

$\boldsymbol{J}(\boldsymbol{\eta}) \in \mathbb{R}^{5\times 5}$, can be computed as in (4.54). In addition, the derivatives presented in Chapter 4.2.3.2 can be used by replacing $\tilde{w}_{t,m}$'s with $w_{t,m}$'s.

To estimate the UE location, we can employ the same AML algorithm, Algorithm 4, as used in Scenario-II. As the values of $\overline{\beta}_{\min}, \overline{\kappa}$, and $\overline{\phi}$ are available, we can skip Step 0 and Step 1 of Algorithm 4 and run Step 2 with the known values of the RIS amplitude model parameters.

4.5 Numerical Results

In this section, we first present numerical examples for evaluating the theoretical bounds in three different scenarios, and then compare the performance of the AMML and AML estimators against the theoretical bounds.

4.5.1 Simulation Setup

We consider an RIS with $M = 50 \times 50$ elements, where the inter-element spacing is $\lambda/2$ and the area of each element is $A = \lambda^2/4$ [70]. The carrier frequency is equal to $f_c = 28$ GHz. The RIS is modeled to lie in the X-Y plane with $\boldsymbol{p}_{\text{RIS}} = [0\,0\,0]^{\mathsf{T}}$. Moreover, for the RIS elements, the $\theta_{t,m}$ values are generated uniformly and independently between $-\pi$ and π. The BS is located at $\boldsymbol{p}_{\text{BS}} = 5.77 \times [-1\,1\,1]^{\mathsf{T}}$ meters. For given distance d to the RIS, the UE is located at $d \times [1\,1\,1]^{\mathsf{T}}/\|[1\,1\,1]\|_2$ meters. We set the number of transmission to $T = 200$. For simplicity, we assume that $s_t = \sqrt{E_s}$ for any t. Also, the SNR is defined as

$$\text{SNR} = \frac{E_s\,|\overline{\alpha}|^2}{TN_0} \sum_{t=1}^{T} \left|\boldsymbol{b}^{\mathsf{T}}(\overline{\boldsymbol{p}})\mathbf{w}_t\right|^2 . \tag{4.69}$$

To solve (4.25) for the LB computation, we employ the GlobalSearch algorithm of MATLAB by providing $\overline{\boldsymbol{p}}$ as the initial vector. In addition, N in (4.41) is taken as 50 for using the Jacobi-Anger expansion approach.

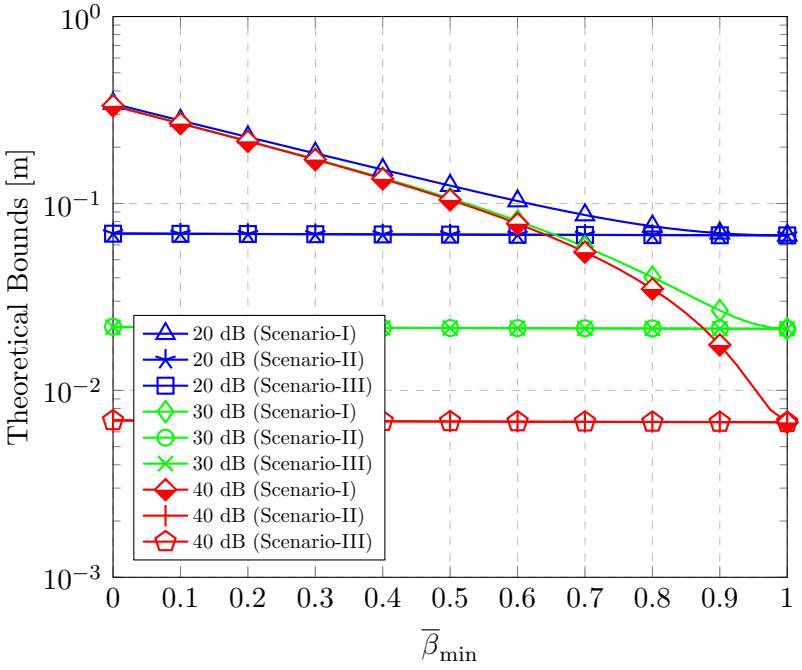


Figure 4.3: Theoretical bounds versus $\overline{\beta}_{\min}$ for SNR = 20 dB, 30 dB and 40 dB when the UE distance is 5 meters, $\overline{\kappa} = 1.5$ and $\overline{\phi} = 0$.

4.5.2 Results and Discussions

4.5.2.1 Theoretical Limits vs. RIS Model Parameters

In Figure 4.3, for all the three scenarios, we show the theoretical bounds as a function of $\overline{\beta}_{\min}$ for SNRs of 20, 30, and 40 dB when the UE distance is 5 meters from the center of the RIS, $\overline{\kappa} = 1.5$, and $\overline{\phi} = 0$. We observe from the figure that as $\overline{\beta}_{\min}$ decreases, i.e., as the mismatch between the true and the assumed models increases, the LB increases and raising the SNR level does not improve the LB values significantly. In addition, the sensitivity to the model mismatch is more pronounced at higher SNRs, while for an SNR of 20 dB, the performance is relatively insensitive for $\overline{\beta}_{\min} > 0.7$. This shows that being unaware of the true RIS amplitude model can constitute a crucial limiting factor for RIS-aided localization at high SNRs. Interestingly, we note that when the true model and the true values of $\overline{\beta}_{\min}$, $\overline{\kappa}$ and $\overline{\phi}$ are known, the value of $\overline{\beta}_{\min}$ does not influence the CRB values notably. In fact, as the CRB values for the Scenario-II and Scenario-III are almost the same, it can be inferred that once we know the true model, knowing the true values of $\overline{\beta}_{\min}$, $\overline{\kappa}$ and $\overline{\phi}$ is not critical.

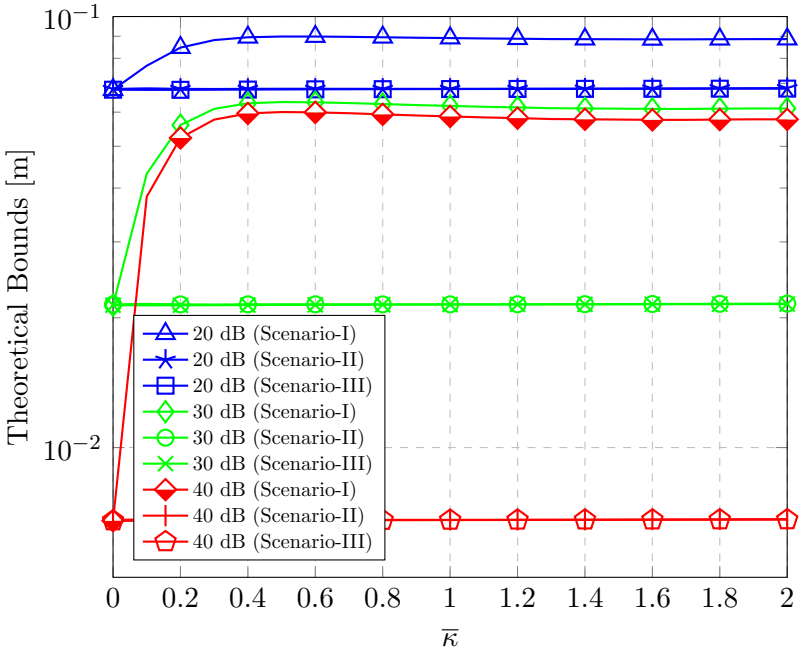


Figure 4.4: Theoretical bounds versus $\overline{\kappa}$ for SNR $= 20\,\text{dB}$, $30\,\text{dB}$ and $40\,\text{dB}$ when the UE distance is 5 meters, $\overline{\beta}_{\text{min}} = 0.7$ and $\overline{\phi} = 0$.

In Figure 4.4, for all the three scenarios, the theoretical bounds are plotted versus κ for SNRs of 20, 30, and 40 dB when the UE distance is 5 meters from the center of the RIS, $\overline{\beta}_{\text{min}} = 0.7$, and $\overline{\phi} = 0$. Similar to Figure 4.3, the CRB values for Scenario-II and Scenario-III are almost the same. We also observe that as κ approaches 0, i.e., as the mismatch between the true and assumed models decreases, the LB and the CRB values for Scenario-II and Scenario-III become closer to each other similarly to Figure 4.3. In addition, as the SNR increases, the performance loss due to the mismatch becomes more significant. Moreover, increasing $\overline{\kappa}$ beyond $\overline{\kappa} = 0.4$ does not have any notable impacts on the LB values.

4.5.2.2 Effect of RIS Size

To investigate the effects of the number of RIS elements, the average LB and CRB values are plotted versus the RIS size in Figure 4.5 for all the three scenarios by averaging over 200 different random phase profiles for the RIS elements, where the SNR is $20\,\text{dB}$, the UE distance is 5 meters, $\overline{\beta}_{\text{min}} \in \{0.3, 0.7\}$, $\overline{\kappa} = 1.5$, and $\overline{\phi} = 0$. We observe that as the RIS size or $\overline{\beta}_{\text{min}}$ increases, we obtain lower LB values in general. In addition, the curves for different

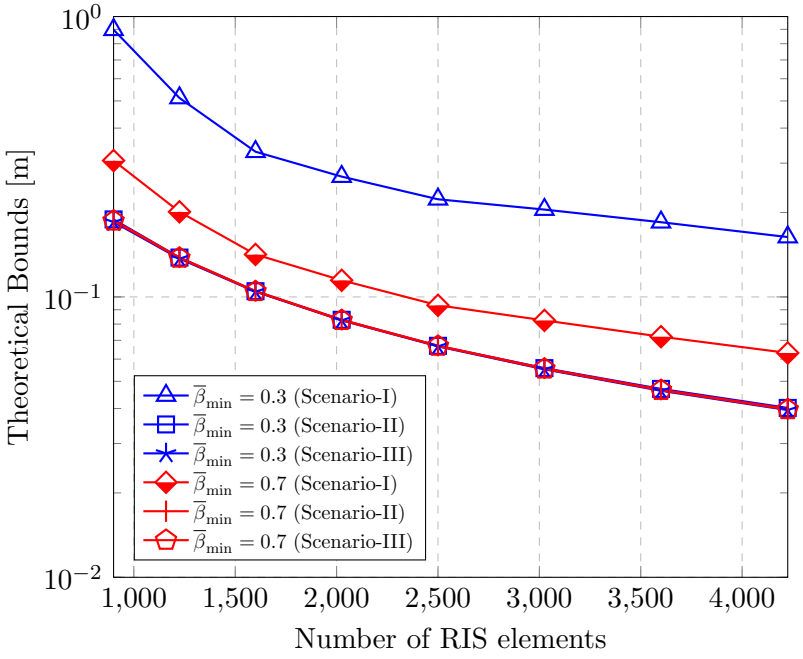


Figure 4.5: Theoretical bounds versus number of RIS elements and for $\overline{\beta}_{\min} \in \{0.3, 0.7\}$ when the UE distance is 5 meters, SNR = 20 dB, $\overline{\kappa} = 1.5$ and $\overline{\phi} = 0$.

$\overline{\beta}_{\min}$ values are almost parallel. We also note the significant price paid due to the model mismatch: With the perfect knowledge of the RIS model and with 1000 elements, a similar performance can only be attained using a RIS with 4225 elements when $\overline{\beta}_{\min} = 0.3$ under the model mismatch.

4.5.2.3 Performance of Algorithm 3 and Algorithm 4 vs. SNR

To provide a comparative analysis of the three scenarios, in Figure 4.6, the performances of the AMML algorithm in Algorithm 3 and the AML algorithm in Algorithm 4 are plotted versus SNR, and compared with the corresponding LB and CRB values when $\overline{\beta}_{\min} = 0.5$. It is noted that the AMML and AML algorithms achieve the theoretical bounds in the high SNR regime in all the three scenarios. This indicates that the proposed Jacobi-Anger expansion based low-complexity approach in Algorithm 3 can successfully provide near-optimal solutions to the near-field localization problem in (4.38). Moreover, by comparing the AMML and the AML curves at high SNRs, we observe that the AML algorithm completely recovers the performance loss due to model misspecification, which verifies the effectiveness of

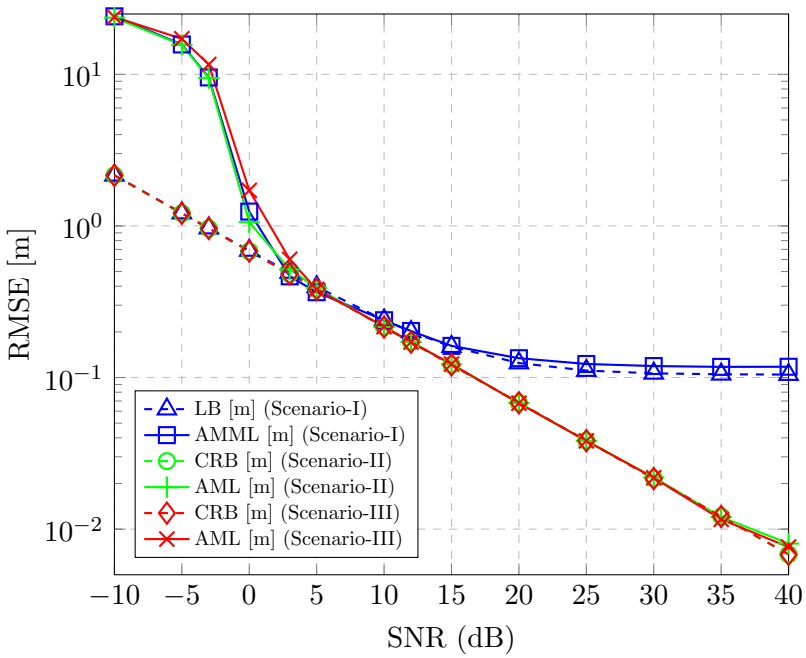


Figure 4.6: Performance of the AMML and the AML algorithms along with the corresponding theoretical bounds versus SNR (dB) when the UE distance is 5 meters, $\overline{\kappa} = 1.5$, $\overline{\beta}_{\min} = 0.5$ and $\overline{\phi} = 0$.

the online RIS calibration in Step 1 and the UE location refinement in Step 2 of Algorithm 4.

To explore the asymptotic behavior of the AMML algorithm in Scenario I, its performance with respect to SNR is illustrated in Figure 4.7 for $\overline{\beta}_{\min} = 0.5$ and 0.7 when the UE distance is 5 meters. In addition to the performance of the AMML estimator, the LB, the MCRB, and the bias term values are also plotted. We observe that the AMML estimator exhibits three distinct regimes: a low-SNR regime where the AMML is limited by noise peaks and thus far away from the LB; a medium-SNR regime where the AMML is close to the LB, which itself is dominated by the MCRB; and a high-SNR regime, where the AMML and LB are limited by the bias term Bias($\boldsymbol{\eta}_0$).

4.5.2.4 Performance of Algorithm 3 and Algorithm 4 vs. RIS Model Parameters

To investigate the performance of the proposed localization methods under varying values of RIS model parameters, in Figure 4.8, the RMSEs of the AMML and AML algorithms are

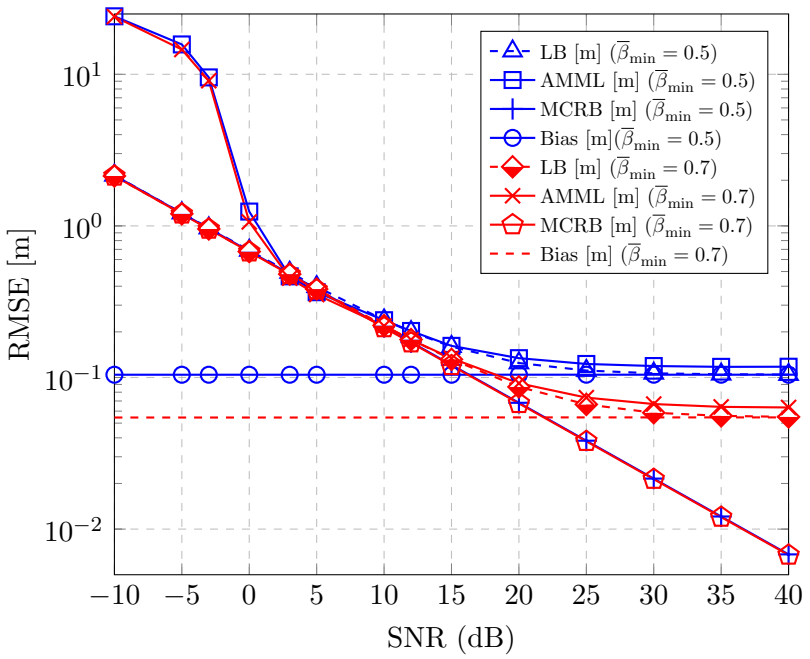


Figure 4.7: AMML, LB, MCRB, and Bias term versus SNR (dB) for $\overline{\beta}_{\min} \in \{0.5, 0.7\}$ when the UE distance is 5 meters, $\overline{\kappa} = 1.5$ and $\overline{\phi} = 0$.

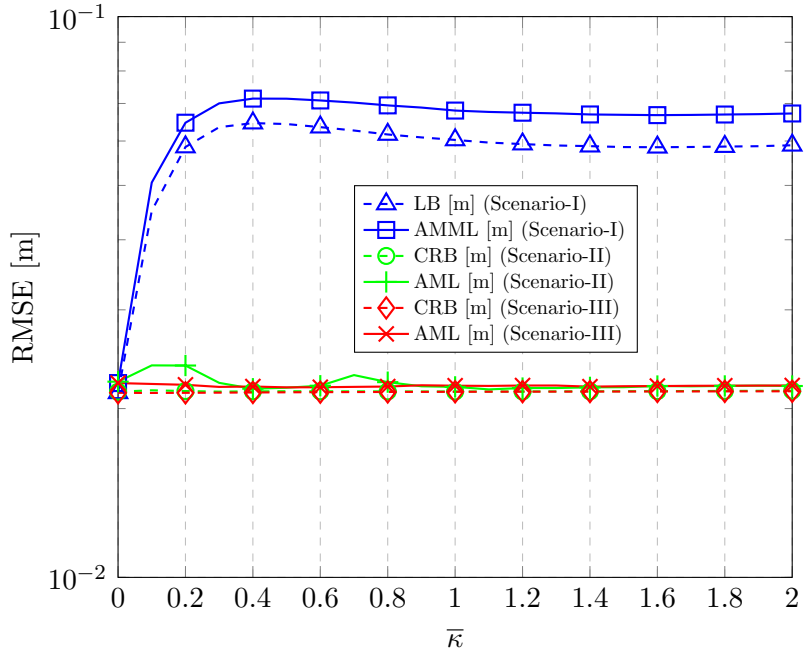


Figure 4.8: Performance of the AMML and the AML algorithms along with the corresponding theoretical bounds versus $\overline{\kappa}$ when the UE distance is 5 meters, SNR = 30 dB, $\overline{\beta}_{\min} = 0.7$, and $\overline{\phi} = 0$.

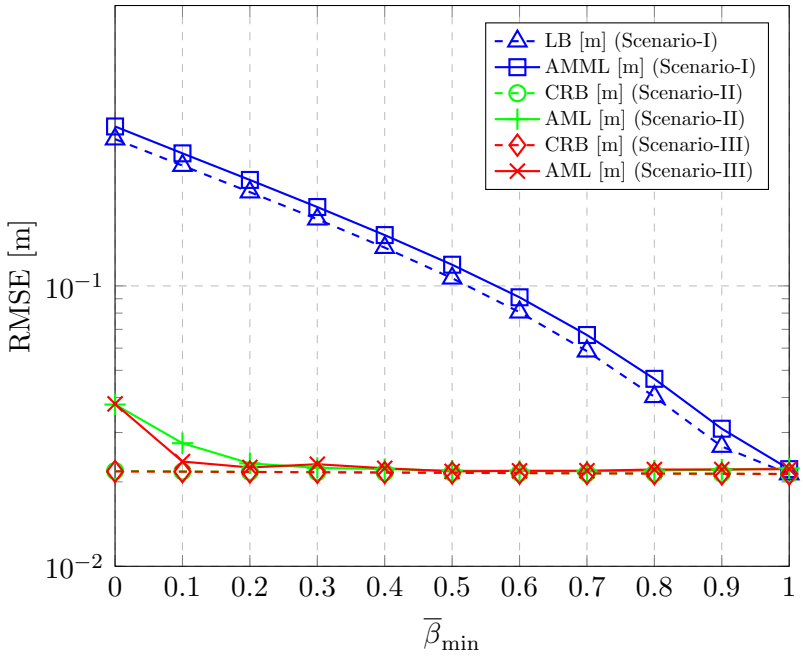


Figure 4.9: Performance of the AMML and the AML algorithms along with the corresponding theoretical bounds versus $\overline{\beta}_{\min}$ when the UE distance is 5 meters, SNR = 30 dB, $\overline{\kappa} = 1.5$, and $\overline{\phi} = 0$.

evaluated versus $\overline{\kappa}$ when SNR = 30 dB, $\overline{\beta}_{\min} = 0.7$, $\overline{\phi} = 0$, and the UE distance is 5 meters. Similarly, in Figure 4.9, the performances of the AMML and AML algorithms versus $\overline{\beta}_{\min}$ are shown when SNR = 30 dB, $\overline{\kappa} = 1.5$, $\overline{\phi} = 0$, and the UE distance is 5 meters. From Figures 4.8 and 4.9, it is noted that for Scenario-II and Scenario-III, the AML algorithm achieves the CRB, which is insensitive to the values of $\overline{\kappa}$ and $\overline{\beta}_{\min}$. In addition, a combined evaluation of Figure 4.6, Figure 4.8 and Figure 4.9 demonstrates that both of the proposed algorithms can attain the corresponding bounds under a wide variety of settings concerning different SNR levels and RIS model parameters.

4.5.2.5 Convergence Behavior of Algorithm 4

Finally, for a single realization, Figure 4.10 illustrates the errors of the position estimates at each alternating iteration in Step 1 of Algorithm 2. In the figure, $\hat{\boldsymbol{p}}(k)$ denotes the estimate of the position $\overline{\boldsymbol{p}}$ obtained from the Jacobi-Anger approach by using the estimate of $\overline{\boldsymbol{\zeta}}$ at the kth iteration.

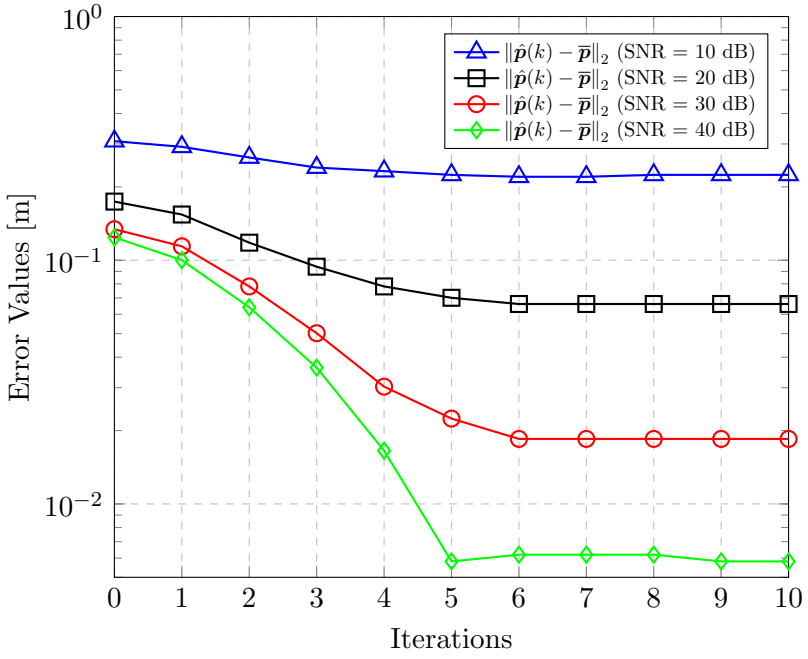


Figure 4.10: Errors of estimates of $\overline{\boldsymbol{p}}$ at each iteration in Step 1 of Algorithm 2 when $\overline{\beta}_{\min} = 0.5$, $\overline{\kappa} = 1.5$, $\overline{\phi} = 0$, SNR = 30 dB, and UE distance is 5 meters.

We observe that, starting from the initial location estimate given by Algorithm 3, Algorithm 4 provides significant performance gains through the iterations of the online RIS calibration in Step 1. In particular, at an SNR of 40 dB, Algorithm 4 achieves the error value of 0.0058 m, while the error corresponding to Algorithm 3 is 0.1241 m.

4.6 Concluding Remarks

We have studied the problem of RIS-aided near-field localization under amplitude variations of individual RIS elements as a function of the applied phase shifts, which is a practical model based on equivalent RIS circuit models of reflecting elements [78]. First, through the MCRB analysis, we have quantified localization performance losses due to model misspecification when the UE is unaware of the RIS amplitude model, and developed an algorithm that achieves the corresponding LB. Second, under a known RIS amplitude model, we have derived the corresponding CRB and proposed a low-complexity algorithm for joint UE localization and online calibration of RIS model parameters. Extensive simulations over a broad

range of operating conditions demonstrate the following key results:

- *Significance of the Knowledge of RIS Amplitude Model:* Being unaware of the true RIS amplitude model and assuming conventional unit-amplitude RIS responses can severely degrade the localization accuracy, with the losses being more pronounced at higher SNRs and higher amplitude fluctuations (small $\overline{\beta}_{\min}$ and large $\overline{\kappa}$ in (4.4)).
- *Localization under Model Mismatch:* Under the unknown RIS amplitude model, the proposed Jacobi-Anger expansion based low-complexity method in Algorithm 3 can provide near-optimal localization performance very close to the corresponding LB.
- *Joint Localization and RIS Calibration:* Under the known RIS amplitude model, it is possible to recover the performance losses incurred by model misspecification using the proposed algorithm in Algorithm 4, which can calibrate the RIS model online with the aid of an unknown-location UE and subsequently refine the UE location with an accuracy that asymptotically attains the CRB.

Based on these outcomes, future research will focus on localization-optimal passive beamforming at the RIS under the realistic RIS amplitude model in (4.4), considering wideband signals and unobstructed LoS scenarios.

Chapter 5

RIS-aided Localization under Pixel Failures

In this chapter, the aim is to perform RIS-aided localization when some of RIS elements (pixels) fail.

5.1 System Model

In this section, we present the system geometry and the signal model, describe RIS failure models, and formulate the problems of interest under pixel failures.

5.1.1 Geometry and Signal Model

We consider a RIS-aided localization system with a single-antenna BS, an N-element RIS, and a single-antenna UE having the following three-dimensional locations: $\mathbf{p}_{\text{BS}} \in \mathbb{R}^3$ denotes the known BS location, $\mathbf{p}_{\text{RIS}} \in \mathbb{R}^3$ is the known center of the RIS, $\mathbf{p}_n \in \mathbb{R}^3$ represents the known location of the n-th RIS element for $1 \leq n \leq N$, and $\overline{\boldsymbol{p}} \in \mathbb{R}^3$ is the unknown UE location.

Without loss of generality, the BS broadcasts a narrowband signal s_t over T transmissions under the constraint of $\mathbb{E}\left\{|s_t|^2\right\} = E_s$. Assuming LoS blockage and the absence of uncontrolled multipath, the signal received by the UE involves only reflections from the RIS and can be expressed at transmission t as

$$y_t = \bar{\alpha}\, \boldsymbol{a}^{\mathsf{T}}(\overline{\boldsymbol{p}})\mathrm{diag}(\boldsymbol{\gamma}_t)\boldsymbol{a}(\mathbf{p}_{\mathrm{BS}})s_t + n_t\,, \tag{5.1}$$

where α is the unknown channel gain, $\boldsymbol{\gamma}_t \in \mathbb{C}^{N\times 1}$ is the RIS phase profile at transmission t, and n_t is uncorrelated zero-mean additive Gaussian noise with variance $N_0/2$ per real dimension. Moreover, $\boldsymbol{a}(\mathbf{p}) \in \mathbb{C}^{N\times 1}$ is the near-field RIS steering vector for a given position $\mathbf{p}$, defined as

$$[\boldsymbol{a}(\mathbf{p})]_n = \exp\left(-j\frac{2\pi}{\lambda}\left(\|\mathbf{p}-\mathbf{p}_n\|_2 - \|\mathbf{p}-\mathbf{p}_{\mathrm{RIS}}\|_2\right)\right) \tag{5.2}$$

for $n \in \{1,\ldots,N\}$, where λ denotes the signal wavelength.

5.1.2 RIS Pixel Failure Model

Based on [18], we consider the biased type of failure. The element switches to a valid, biased state with a certain distance from the desired state due to bit-flipping or external biases. Under such element failures, the RIS phase profile $\boldsymbol{\gamma}_t$ in (5.1) can be modeled as

$$\boldsymbol{\gamma}_t = \boldsymbol{\phi}_t \odot \overline{\mathbf{m}}\,, \tag{5.3}$$

where $\boldsymbol{\phi}_t \in \mathbb{C}^{N\times 1}$ represents the *configurable* RIS weights under the designer's control, and $\overline{\mathbf{m}} \in \mathbb{C}^{N\times 1}$ denotes the unknown *failure masks* quantifying the effect of faulty elements, which can be defined as [19, 86]

$$\overline{m}_n = \begin{cases} \zeta_n, & \text{if the } n\text{-th RIS element is faulty (biased)} \\ 1, & \text{if the } n\text{-th RIS element is properly functioning} \end{cases}. \tag{5.4}$$

Based on (5.3), the RIS phase profile takes the following values in the presence of failures:

$$[\boldsymbol{\gamma}_t]_n = \begin{cases} [\boldsymbol{\phi}_t]_n, & \text{if the } n\text{-th RIS element is functioning} \\ [\boldsymbol{\phi}_t]_n\overline{m}_n, & \text{if the } n\text{-th RIS element is biased} \end{cases} \tag{5.5}$$

In (5.4), $\zeta_n = \kappa_n e^{j\psi_n}$ denotes the failure related complex response of the n-th element, with $0 < \kappa_n \leq 1$ and $0 \leq \psi_n < 2\pi$ representing the resulting attenuation and phase shift, respectively.

We model that each RIS element fails independent and identically with given probability p_{fail}. Also, if pixel n fails, we assume that $\kappa_n \sim \mathcal{U}(0,1)$ and $\psi_n \sim \mathcal{U}(-\pi, \pi)$.

5.1.3 Problem Description

Given the observations $\{y_t\}_{t=1}^T$ in (5.1) over T transmission instances, the problems under RIS pixel failures specified in (5.4) can be described as follows:

1. To what extent are RIS pixel failures detrimental for RIS-aided localization of the UE? How is the performance degradation affected by the percentage of failing elements?
2. How can we identify which pixels are failing and recover the failure mask $\mathbf{m}$ in order to find the position of the UE?

5.2 Problem 1: Theoretical Performance Evaluation Under Pixel Failures

In this section, we tackle Problem 1 in Sec. 5.1.3 by resorting to the MCRB [85] as a tool for assessing degradation in localization performance due to model misspecification. We employ a similar approach to that in [82, 83].

5.2.1 True and Assumed Models

We describe the true and assumed models in the presence of pixel failures specified through the failure mask $\overline{\mathbf{m}}$ in (5.3) as follows:

- **True Model:** $\overline{\mathbf{m}} \neq \mathbf{1}$.
- **Assumed Model:** $\overline{\mathbf{m}} = \mathbf{1}$ (no pixel failures)

Both models have the perfect knowledge of $\boldsymbol{\phi}_t$ in (5.5). Under the true model, the noiseless part of the received signal at transmission t can be expressed as follows

$$\mu_t = \overline{\alpha}\, \boldsymbol{a}^{\mathsf{T}}(\overline{\boldsymbol{p}})\mathrm{diag}(\boldsymbol{\gamma}_t)\boldsymbol{a}(\mathbf{p}_{\mathrm{BS}})s_t. \tag{5.6}$$

On the other hand, under the assumed model, for the misspecification parameter $\boldsymbol{\eta}$, the noiseless part of the received signal at transmission t is given by

$$\widetilde{\mu}_t(\boldsymbol{\eta}) = \alpha\, \boldsymbol{a}^{\mathsf{T}}(\boldsymbol{p})\mathrm{diag}(\boldsymbol{\phi}_t)\boldsymbol{a}(\mathbf{p}_{\mathrm{BS}})s_t, \tag{5.7}$$

where

$$\boldsymbol{\eta} \triangleq \left[\mathrm{Re}\{\alpha\}\, \mathrm{Im}\{\alpha\}\, \boldsymbol{p}^{\mathsf{T}}\right]^{\mathsf{T}}. \tag{5.8}$$

If there is no mismatch between the assumption and the reality, i.e., if $\overline{\mathbf{m}} = \mathbf{1}$, we have $\widetilde{\mu}_t(\overline{\boldsymbol{\eta}}) = \mu_t$ for the true set of parameters, $\overline{\boldsymbol{\eta}} \triangleq \left[\mathrm{Re}\{\overline{\alpha}\}\, \mathrm{Im}\{\overline{\alpha}\}\, \overline{\boldsymbol{p}}^{\mathsf{T}}\right]^{\mathsf{T}}$. Next, based on the MCRB definition in Chapter 4.2.2, we provide how to compute the theoretical performance bounds for estimating the UE position under the mismatch between the reality and the assumption as described above.

5.2.2 MCRB derivation

For the considered setup, we can use the methodology in Chapter 4 to determine the corresponding MCRB and LB values. Based on Lemma 4.1 in Chapter 4, it is possible to observe that pseudotrue parameter, $\boldsymbol{\eta}_0$, which minimizes the KL divergence between the true pdf and the misspecified parametric pdfs, can be expressed as

$$\boldsymbol{\eta}_0 = \underset{\boldsymbol{\eta}\in\mathbb{R}^5}{\arg\min} \left\|\boldsymbol{\epsilon}(\boldsymbol{\eta})\right\|_2 \tag{5.9}$$

where $\boldsymbol{\epsilon}(\boldsymbol{\eta}) \triangleq [\epsilon_1(\boldsymbol{\eta}) \ \ldots \ \epsilon_T(\boldsymbol{\eta})]^{\mathsf{T}}$ and $\epsilon_t(\boldsymbol{\eta}) \triangleq \mu_t - \tilde{\mu}_t(\boldsymbol{\eta})$ for $t = 1, \ldots, T$. The corresponding MCRB and LB values can be computed in a similar fashion to that in Chapter 4.2.3. Next, we discuss how to jointly recover the unknown failure mask $\overline{\mathbf{m}}$ and estimate the position of the UE.

5.3 Problem 2: Joint Localization and Recovery of Failure Masks

Let $\mathbf{y} = [y_1 \dots y_T]^\mathsf{T}$, $\mathbf{n} = [n_1 \dots n_T]^\mathsf{T}$, $\boldsymbol{b}(\overline{\boldsymbol{p}}) = \boldsymbol{a}(\overline{\boldsymbol{p}}) \odot \boldsymbol{a}(\mathbf{p}_{\text{BS}})$, $\boldsymbol{\Gamma} = [\boldsymbol{\gamma}_1 \dots \boldsymbol{\gamma}_T] \in \mathbb{C}^{N \times T}$ and $\boldsymbol{S} = \text{diag}(s_1, \dots, s_T)$. Then, the observations in (5.1) can be written compactly as

$$\mathbf{y} = \overline{\alpha} \boldsymbol{S} \boldsymbol{\Gamma}^\mathsf{T} \boldsymbol{b}(\overline{\boldsymbol{p}}) + \mathbf{n} \, . \tag{5.10}$$

Here, using (5.3), $\boldsymbol{\Gamma}$ can be expressed as

$$\boldsymbol{\Gamma} = \boldsymbol{\Phi} \odot \overline{\mathbf{m}} \mathbf{1}^\mathsf{T} \, , \tag{5.11}$$

where $\boldsymbol{\Phi} = [\boldsymbol{\phi}_1 \dots \boldsymbol{\phi}_T] \in \mathbb{C}^{N \times T}$. Our aim is to recover $\overline{\mathbf{m}}$ from (5.10) while simultaneously estimating $\overline{\boldsymbol{p}}$ (as usual, $\overline{\alpha}$ can be estimated in closed-form as a function of $\overline{\boldsymbol{p}}$ and $\overline{\mathbf{m}}$). Since $T < N$ in practice due to large RIS sizes, we need to make certain assumptions on the structure of $\overline{\mathbf{m}}$ for joint estimation of $\overline{\boldsymbol{p}}$, $\overline{\mathbf{m}}$ from $\mathbf{y}$. A common approach in the literature is to make a sparsity assumption that the number of faulty elements is small compared to the RIS size [19] or the array size [86]. Following a similar approach, we assume that $\overline{\mathbf{m}} - \mathbf{1}$ is a sparse vector.

Under the sparsity assumption, we first propose an ℓ_1 regularization based joint localization and failure diagnosis method. Then, we try to accomplish joint localization and failure diagnosis via recovering the unknown mask vector $\overline{\mathbf{m}}$ with a successive approach.

5.3.1 ℓ_1-regularization based Joint Localization and Failure Diagnosis

To perform joint localization and failure diagnosis, we can update estimates of $\overline{\mathbf{m}}$, $\overline{\boldsymbol{p}}$ and $\overline{\alpha}$ in an alternating manner. To that aim, we estimate $\overline{\boldsymbol{p}}$ and $\overline{\alpha}$ for a given estimate of $\overline{\mathbf{m}}$ via the Jacobi-Anger method described in Chapter 4.3.2. For given estimates of $\overline{\boldsymbol{p}}$ and $\overline{\alpha}$, the estimate of $\overline{\mathbf{m}}$ is found by the ℓ_1-regularization approach.

More specifically, let us analyze what happens in the ith iteration. Let $\mathbf{m}^{(i)}$ be the estimate of $\overline{\mathbf{m}}$ that we have at the beginning of the ith iteration. Then, the estimates of $\overline{\boldsymbol{p}}$ and $\overline{\alpha}$, $\mathbf{p}^{(i)}$

Algorithm 5 ℓ_1 regularization based Joint Localization and Failure Diagnosis Algorithm

Input: Observation $\mathbf{y}$, RIS phase profiles $\mathbf{\Phi}$, convergence threshold ε and maximum number of iterations M.
Output: UE location $\widehat{\mathbf{p}}$, failure mask $\widehat{\mathbf{m}}$ and channel gain $\widehat{\alpha}$.
Initialization: Set $i = 0$. Initialize the failure mask to be the all-ones vector, i.e., $\mathbf{m}^{(0)} = \mathbf{1}$.
Iterations:
while $i < I$ **do**
  Estimate $\mathbf{p}^{(i)}$ and $\alpha^{(i)}$ by using Jacobi-Anger expansion for the mask $\mathbf{m}^{(i)}$.
  Estimate $\mathbf{m}^{(i+1)}$ by using ℓ_1-regularized mask-recover approach for $\mathbf{p}^{(i)}$ and $\alpha^{(i)}$.
  if ($i \geq 1$ and $\left\|\mathbf{p}^{(i)} - \mathbf{p}^{(i-1)}\right\|_2 \leq \varepsilon$) or $i = M$ **then**
    Set $\widehat{\mathbf{m}} = \mathbf{m}^{(i)}$
    break
  end if
  Set $i = i + 1$.
end while
Localization: Estimate the UE location and channel gain for the failure mask $\widehat{\mathbf{m}}$, by using Jacobi-Anger approach and establishing finer search around $\mathbf{p}^{(i)}$.

and $\alpha^{(i)}$, can be found via the Jacobi-Anger method by using the mask estimate $\mathbf{m}^{(i)}$. By denoting $\boldsymbol{h}^{(i)} \triangleq \alpha^{(i)}\boldsymbol{b}(\mathbf{p}^{(i)})$, the estimate of $\overline{\mathbf{m}}$ can be updated as

$$\mathbf{m}^{(i+1)} = \arg\min_{\mathbf{m}} \left\|\mathbf{y} - \boldsymbol{S}(\mathbf{\Phi}^{\mathsf{T}} \odot \mathbf{1}\mathbf{m}^{\mathsf{T}})\boldsymbol{h}^{(i)}\right\|_2^2 + \lambda \left\|\mathbf{m} - 1\right\|_1 . \tag{5.12}$$

The details are summarized in Algorithm 5. Moreover, one can write the following identity:

$$\boldsymbol{S}(\mathbf{\Phi}^{\mathsf{T}} \odot \mathbf{1}\mathbf{m}^{\mathsf{T}})\boldsymbol{h}^{(i)} = \boldsymbol{S}\left(\mathbf{\Phi}^{\mathsf{T}} \odot \mathbf{1}(\boldsymbol{h}^{(i)})^{\mathsf{T}}\right)\mathbf{m}. \tag{5.13}$$

For simplicity, we define $\boldsymbol{U}^{(i)} \triangleq \boldsymbol{S}(\mathbf{\Phi}^{\mathsf{T}} \odot \mathbf{1}\boldsymbol{h}^{\mathsf{T}})$. Then, we can re-write (5.12) as follows:

$$\mathbf{m}^{(i+1)} = \arg\min_{\mathbf{m}} \left\|\mathbf{y} - \boldsymbol{U}^{(i)}\mathbf{m}\right\|_2^2 + \lambda \left\|\mathbf{m} - 1\right\|_1 . \tag{5.14}$$

5.3.2 Successive Joint Localization and Failure Diagnosis

In this algorithm, we successively determine which pixel fails and capture the mask vector, and estimate the position of the UE and the channel gain in an alternating manner. In each iteration, we update the set of failing pixels by assuming there is at most one failure. In the following, the details of the algorithm are explained starting from the first iteration.

Algorithm 6 First Iteration of the Successive Joint Localization and Failure Diagnosis Algorithm

Input: Observation $\mathbf{y}$, RIS phase profiles $\mathbf{\Phi}$, convergence threshold ε and maximum number of alternating steps C, initial position and channel gain estimates $\mathbf{p}^{(0)}$, $\alpha^{(0)}$.
Output: $\mathbf{p}^{(1)}$,$\alpha^{(1)}$, $\mathbf{m}^{(1)}$,$\mathcal{I}^{(1)}$
Set bool = 1, $l = 0$, $\mathbf{p}^{(1,0)} = \mathbf{p}^{(0)}$, $\alpha^{(1,0)} = \alpha^{(0)}$, and $\mathbf{m}^{(1,0)} = \mathbf{1}$
while bool **do**
  Set $l = l + 1$.
  Given $\mathbf{p}^{(1,l)}$, $\alpha^{(1,l)}$, find $(\widehat{k}, \hat{\kappa}_k, \hat{\theta}_k) = \arg\max_{k,\hat{\kappa}_k,\hat{\theta}_k} f(\mathbf{y}|\mathcal{H}_k) \Pr\{\mathcal{H}_k|\text{There is at most one failure}\}$
  if $\widehat{k} = 0$ **then**
    bool = 0. Set $\mathbf{p}^{(1)} = \mathbf{p}^{(1,l)}$, $\alpha^{(1)} = \alpha^{(1,l)}$, and $\mathbf{m}^{(1)} = \mathbf{m}^{(1,l)}$
    Set $\mathcal{I}^{(1)} = \emptyset$.
  else
    Update the mask $\mathbf{m}^{(1,l)}$ accordingly.
    For that mask, update $\mathbf{p}^{(1,l)}$ and $\alpha^{(1,l)}$ via Jacobi-Anger expansion.
    if $l \geq C$ or $\left\|\mathbf{p}^{(1,l)} - \mathbf{p}^{(1,l-1)}\right\|_2 \leq \varepsilon$ **then**
      Set bool = 0. Set $\mathbf{p}^{(1)} = \mathbf{p}^{(1,l)}$, $\alpha^{(1)} = \alpha^{(1,l)}$, and $\mathbf{m}^{(1)} = \mathbf{m}^{(1,l)}$
      Set $\mathcal{I}^{(1)} = \{\widehat{k}\}$.
    end if
  end if
end while

5.3.2.1 First Iteration:

We have the position and channel gain estimates $\mathbf{p}^{(0)}$, $\alpha^{(0)}$ obtained by the Jacobi-Anger algorithm for $\mathbf{m}^{(0)} = \mathbf{1}$. In the first iteration, we have $N + 1$ different hypotheses. That is,

$$\begin{aligned}
&\mathcal{H}_0 : \text{no failure},\\
&\mathcal{H}_k : k\text{th pixel fails for } 1 \leq k \leq N.
\end{aligned}$$

Or, equivalently,

$$\begin{aligned}
&\mathcal{H}_0 : \mathbf{y} = \boldsymbol{U}^{(0)}\widetilde{\mathbf{m}}^{(0)} + \mathbf{n},\\
&\mathcal{H}_k : \mathbf{y} = \boldsymbol{U}^{(0)}\widetilde{\mathbf{m}}^{(k)} + \mathbf{n} \text{ for } 1 \leq k \leq N,
\end{aligned}$$

where $\boldsymbol{U}^{(0)} = \boldsymbol{S}\left(\mathbf{\Phi}^{\mathsf{T}} \odot \mathbf{1}(\boldsymbol{h}^{(0)})^{\mathsf{T}}\right)$ for $\boldsymbol{h}^{(0)} = \alpha^{(0)}\boldsymbol{b}(\mathbf{p}^{(0)})$. Moreover, $\widetilde{\mathbf{m}}^{(0)} = \mathbf{1}$, and

$$\left[\widetilde{\mathbf{m}}^{(k)}\right]_n = \begin{cases} 1, & \text{if } n \neq k,\\ \kappa_k e^{j\theta_k} & \text{if } n = k. \end{cases}$$

The prior probabilities of hypotheses $\mathcal{H}_0$ and $\{\mathcal{H}_k\}_{k=1}^{N}$ can be computed as follows:

$$\Pr\{\mathcal{H}_0|\text{There is at most one failure}\} = \frac{(1-\mathrm{p_{fail}})^{\mathrm{N}}}{(1-\mathrm{p_{fail}})^{\mathrm{N}} + \mathrm{N}\mathrm{p_{fail}}(1-\mathrm{p_{fail}})^{\mathrm{N}-1}} = \frac{1-\mathrm{p_{fail}}}{1-\mathrm{p_{fail}}+\mathrm{N}\mathrm{p_{fail}}} \tag{5.15}$$

$$\Pr\{\mathcal{H}_k|\text{There is at most one failure}\} = \frac{(1-\mathrm{p_{fail}})^{\mathrm{N}-1}\mathrm{p_{fail}}}{(1-\mathrm{p_{fail}})^{\mathrm{N}} + \mathrm{N}\mathrm{p_{fail}}(1-\mathrm{p_{fail}})^{\mathrm{N}-1}} = \frac{\mathrm{p_{fail}}}{1-\mathrm{p_{fail}}+\mathrm{N}\mathrm{p_{fail}}} \tag{5.16}$$

For $k \geq 1$, we determine $\hat{\kappa}_k$ and $\hat{\theta}_k$ which maximize $f(\mathbf{y}|\mathcal{H}_k)$, where $f(\cdot|\mathcal{H}_k)$ is the likelihood function under the hypothesis $\mathcal{H}_k$. In other words, we need to determine

$$(\hat{\kappa}_k, \hat{\theta}_k) = \arg\max_{\kappa,\theta} f(\mathbf{y}|\mathcal{H}_k) = \arg\max_{\kappa,\theta} \exp\left(-\frac{\left\|\mathbf{y} - \boldsymbol{U}^{(0)}\widetilde{\mathbf{m}}^{(k)}\right\|_2^2}{N_0}\right) \tag{5.17}$$

The following lemma characterizes the solution of (5.17).

Lemma 5.1: The solution of (5.17) can be speficied as follows:

$$\hat{\theta}_k = \angle\left(\sum_{t=1}^{T}\left([\boldsymbol{U}^{(0)}]_{t,k}\right)^* v_{t,k}\right) \tag{5.18}$$

$$\hat{\kappa}_k = \frac{\left|\left(\sum_{t=1}^{T}\left([\boldsymbol{U}^{(0)}]_{t,k}\right)^* v_{t,k}\right)\right|}{\sum_{t=1}^{T}\left|[\boldsymbol{U}^{(0)}]_{t,k}\right|^2} \tag{5.19}$$

where $v_{t,k}$ is defined as

$$v_{t,k} \triangleq y_t - \sum_{l=1, l\neq k}^{N} [\boldsymbol{U}^{(0)}]_{t,l} \tag{5.20}$$

Proof: One can note that the following chain of equations must hold:

$$(\hat{\kappa}_k, \hat{\theta}_k) = \arg\min_{\kappa,\theta} \left\|\mathbf{y} - \boldsymbol{U}^{(0)}\widetilde{\mathbf{m}}^{(k)}\right\|_2^2 = \arg\min_{\kappa,\theta} \sum_{t=1}^{T}\left|y_t - \sum_{l=1}^{N}[\boldsymbol{U}^{(0)}]_{t,l}[\widetilde{\mathbf{m}}^{(k)}]_l\right|^2 \tag{5.21}$$

$$= \arg\min_{\kappa,\theta} \sum_{t=1}^{T}\left|y_t - \sum_{l=1, l\neq k}^{N}[\boldsymbol{U}^{(0)}]_{t,l} - [\boldsymbol{U}^{(0)}]_{t,k}\kappa e^{j\theta}\right|^2 \tag{5.22}$$

$$= \arg\min_{\kappa,\theta} \sum_{t=1}^{T}\left|v_{t,k} - [\boldsymbol{U}^{(0)}]_{t,k}\kappa e^{j\theta}\right|^2 \tag{5.23}$$

$$= \arg\min_{\kappa,\theta} \sum_{t=1}^{T}\kappa^2\left|[\boldsymbol{U}^{(0)}]_{t,k}\right|^2 - v_{t,k}^*[\boldsymbol{U}^{(0)}]_{t,k}\kappa e^{j\theta} - v_{t,k}\left([\boldsymbol{U}^{(0)}]_{t,k}\right)^*\kappa e^{-j\theta} \tag{5.24}$$

Let $g^{(k)}(\kappa,\theta)$ be defined as the objective in (5.24). First, by taking the derivative of $g^{(k)}(\kappa,\theta)$ with respect to θ, we obtain that

$$\frac{\partial g^{(k)}(\kappa,\theta)}{\partial\theta} = j\kappa e^{-j\theta}\sum_{t=1}^{T} v_{t,k}\left([\boldsymbol{U}^{(0)}]_{t,k}\right)^{*} - j\kappa e^{j\theta}\sum_{t=1}^{T} v_{t,k}^{*}[\boldsymbol{U}^{(0)}]_{t,k}\Bigg|_{\theta=\hat{\theta}_k} = 0 \tag{5.25}$$

if and only if

$$e^{j\hat{\theta}_k}\sum_{t=1}^{T} v_{t,k}^{*}[\boldsymbol{U}^{(0)}]_{t,k} = e^{-j\hat{\theta}_k}\sum_{t=1}^{T} v_{t,k}\left([\boldsymbol{U}^{(0)}]_{t,k}\right)^{*} \tag{5.26}$$

Since the RHS of (5.26) is the conjugate of the LHS of (5.26), (5.26) is possible only if both sides of (5.26) is real. This implies that

$$\hat{\theta}_k = \angle\left(\sum_{t=1}^{T}\left([\boldsymbol{U}^{(0)}]_{t,k}\right)^{*} v_{t,k}\right) \tag{5.27}$$

Now, taking the derivative of $g^{(k)}(\kappa,\hat{\theta}_k)$ with respect to κ, we obtain that

$$\frac{\partial g^{(k)}(\kappa,\hat{\theta}_k)}{\partial\kappa} = \sum_{t=1}^{T} 2\kappa\left|[\boldsymbol{U}^{(0)}]_{t,k}\right|^2 - v_{t,k}^{*}[\boldsymbol{U}^{(0)}]_{t,k}e^{j\hat{\theta}_k} - v_{t,k}\left([\boldsymbol{U}^{(0)}]_{t,k}\right)^{*} e^{-j\hat{\theta}_k}\Bigg|_{\kappa=\hat{\kappa}_k} = 0 \tag{5.28}$$

if and only if

$$2\hat{\kappa}_k\sum_{t=1}^{T}\left|[\boldsymbol{U}^{(0)}]_{t,k}\right|^2 = \sum_{t=1}^{T} v_{t,k}^{*}[\boldsymbol{U}^{(0)}]_{t,k}e^{j\hat{\theta}_k} + v_{t,k}\left([\boldsymbol{U}^{(0)}]_{t,k}\right)^{*} e^{-j\hat{\theta}_k} \tag{5.29}$$

By using (5.27), one can see that the RHS of (5.29) is equal to $2\left|\sum_{t=1}^{T} v_{t,k}\left([\boldsymbol{U}^{(0)}]_{t,k}\right)^{*}\right|$. Thus, $\hat{\kappa}_k$ is can be written as

$$\hat{\kappa}_k = \frac{\left|\left(\sum_{t=1}^{T}\left([\boldsymbol{U}^{(0)}]_{t,k}\right)^{*} v_{t,k}\right)\right|}{\sum_{t=1}^{T}\left|[\boldsymbol{U}^{(0)}]_{t,k}\right|^2} \tag{5.30}$$

Now, to show that $\hat{\theta}_k$ and $\hat{\kappa}_k$ in (5.27) and (5.30) are the minimizers of $g^{(k)}(\kappa,\theta)$ we check the second order conditions. To that aim, we compute the Hessian matrix.

$$\frac{\partial^2 g^{(k)}(\kappa,\theta)}{\partial\kappa^2} = 2\sum_{t=1}^{T}\left|[\boldsymbol{U}^{(0)}]_{t,k}\right|^2\Bigg|_{\kappa=\hat{\kappa}_k,\theta=\hat{\theta}_k} = 2\sum_{t=1}^{T}\left|[\boldsymbol{U}^{(0)}]_{t,k}\right|^2 \geq 0. \tag{5.31}$$

$$\frac{\partial^2 g^{(k)}(\kappa,\theta)}{\partial\kappa\partial\theta} = je^{-j\theta}\sum_{t=1}^{T} v_{t,k}\left([\boldsymbol{U}^{(0)}]_{t,k}\right)^{*} - je^{j\theta}\sum_{t=1}^{T} v_{t,k}^{*}[\boldsymbol{U}^{(0)}]_{t,k}\Bigg|_{\kappa=\hat{\kappa}_k,\theta=\hat{\theta}_k} = 0. \tag{5.32}$$

$$\frac{\partial^2 g^{(k)}(\kappa,\theta)}{\partial\theta^2} = \kappa e^{-j\theta}\sum_{t=1}^{T} v_{t,k}\left([\boldsymbol{U}^{(0)}]_{t,k}\right)^* + \kappa e^{j\theta}\sum_{t=1}^{T} v_{t,k}^*[\boldsymbol{U}^{(0)}]_{t,k}\Bigg|_{\kappa=\hat{\kappa}_k,\theta=\hat{\theta}_k} \tag{5.33}$$

$$= 2\hat{\kappa}_k\left|\left(\sum_{t=1}^{T}\left([\boldsymbol{U}^{(0)}]_{t,k}\right)^* v_{t,k}\right)\right| \geq 0. \tag{5.34}$$

From (5.31), (5.32), and (5.34), we conclude that the Hessian matrix is positive definite, hence $\hat{\theta}_k$ and $\hat{\kappa}_k$ in (5.27) and (5.30) are the minimizers of $g^{(k)}(\kappa,\theta)$. ■

After calculating $\hat{\kappa}_k$ and $\hat{\theta}_k$ for all hypotheses $\{\mathcal{H}_k\}_{k=1}^{N}$, we compare the posterior probability of each hypothesis. Then, we choose the hypothesis which yields the maximum posterior probability. More specifically, we choose

$$\widehat{k} = \arg\max_k \Pr\{\mathcal{H}_k|\text{There is at most one failure}\}\exp\left(-\frac{1}{N_0}\left\|\mathbf{y}-\boldsymbol{U}^{(0)}\widehat{\widetilde{\mathbf{m}}}^{(k)}\right\|_2^2\right) \tag{5.35}$$

where $\widehat{\widetilde{\mathbf{m}}}^{(0)} = \widetilde{\mathbf{m}}^{(0)}$, and for $k \geq 1$, $\widehat{\widetilde{\mathbf{m}}}^{(k)}$ is defined as

$$\left[\widehat{\widetilde{\mathbf{m}}}^{(k)}\right]_n = \begin{cases} 1, & \text{if } n \neq k, \\ \hat{\kappa}_k e^{j\hat{\theta}_k} & \text{if } n = k. \end{cases}$$

If $\widehat{k}$ in (5.35) is equal to 0, we declare that there is no pixel failure and we do not proceed to the second iteration. If $\widehat{k} \neq 0$, then for $\widehat{\widetilde{\mathbf{m}}}^{(\widehat{k})}$, we update the position and the channel gain estimates. For that estimated position and the channel gain, we update $\boldsymbol{U}^{(0)}$ and we again compute the posterior probabilities and update the mask estimate. We perform these alternating steps until the number of allowed alternating steps is exceeded or the change in the position estimates becomes negligible. At the end of the first iteration, we have the position, channel gain, mask and the failing pixel estimates as $\mathbf{p}^{(1)}$,$\alpha^{(1)}$, $\mathbf{m}^{(1)}$,$\mathcal{I}^{(1)}$, respectively. The details of this step are summarized in Algorithm 6. Next, we discuss what happens in the ith iteration.

5.3.2.2 ith Iteration:

In the ith iteration, we basically perform the same operations as in the first iteration with some changes. This time, the number of hypotheses reduces to $N+1-\left|\mathcal{I}^{(i-1)}\right|$, which can

be expressed as

$$\mathcal{H}_0 : \mathbf{y} = \boldsymbol{U}^{(i-1)}\widetilde{\mathbf{m}}^{(0)} + \mathbf{n},$$
$$\mathcal{H}_k : \mathbf{y} = \boldsymbol{U}^{(i-1)}\widetilde{\mathbf{m}}^{(k)} + \mathbf{n} \text{ for } k \notin \mathcal{I}^{(i-1)}$$

where $\boldsymbol{U}^{(i-1)} = \boldsymbol{S}\left(\boldsymbol{\Phi}^{\mathsf{T}} \odot \mathbf{1}(\boldsymbol{h}^{(i-1)})^{\mathsf{T}}\right)$ for $\boldsymbol{h}^{(i-1)} = \alpha^{(i-1)}\boldsymbol{b}(\mathbf{p}^{(i-1)})$. Moreover, $\widetilde{\mathbf{m}}^{(0)} = \mathbf{m}^{(i-1)}$, and for $k \notin \mathcal{I}^{(i-1)}$,

$$\left[\widetilde{\mathbf{m}}^{(k)}\right]_n = \begin{cases} 1, & \text{if } n \neq k, \text{and } n \notin \mathcal{I}^{(i-1)}, \\ \left[\mathbf{m}^{(i-1)}\right]_n & \text{if } n \neq k, \text{and } n \in \mathcal{I}^{(i-1)}, \\ \kappa_k e^{j\theta_k} & \text{if } n = k. \end{cases}$$

The prior probabilities of hypotheses $\mathcal{H}_0$ and $\{\mathcal{H}_k\}_{k\notin\mathcal{I}^{(i-1)}}$ are updated as

$$\Pr\{\mathcal{H}_0|\text{There is at most one failure except for } \mathcal{I}^{(i-1)}\} = \frac{1 - \mathrm{p_{fail}}}{1 - \mathrm{p_{fail}} + (\mathrm{N} - |\mathcal{I}^{(\mathrm{i-1})}|)\,\mathrm{p_{fail}}} \tag{5.36}$$

$$\Pr\{\mathcal{H}_k|\text{There is at most one failure except for } \mathcal{I}^{(i-1)}\} = \frac{\mathrm{p_{fail}}}{1 - \mathrm{p_{fail}} + (\mathrm{N} - |\mathcal{I}^{(\mathrm{i-1})}|)\,\mathrm{p_{fail}}} \tag{5.37}$$

Moreover, for the statement in Lemma 5.1, $\boldsymbol{U}^{(0)}$ is replaced by $\boldsymbol{U}^{(i-1)}$, and $v_{t,k}$ is modified as

$$v_{t,k} = y_t - \sum_{l\neq k, l=1}^{N} [\boldsymbol{U}^{(i-1)}]_{t,l} \left[\mathbf{m}^{(i-1)}\right]_l \tag{5.38}$$

After determining $\widehat{k}$, i.e., the hypothesis with the highest posterior, for the given set $\mathcal{J}^{(i)} \triangleq \mathcal{I}^{(i-1)} \cup \widehat{k}$, we determine the optimal values of $\{\hat{\kappa}_k, \hat{\theta}_k\}_{k\in\mathcal{J}^{(i)}}$ by formulating this problem as a convex problem. Now, we discuss how we end up with a convex problem for obtaining the estimates $\{\hat{\kappa}_k, \hat{\theta}_k\}_{k\in\mathcal{J}^{(i)}}$.

We need to solve the following problem:

$$\{\hat{\kappa}_k, \hat{\theta}_k\}_{k\in\mathcal{J}^{(i)}} = \underset{\{\kappa_k,\theta_k\}_{k\in\mathcal{J}^{(i)}}}{\arg\min} \left\|\mathbf{y} - \boldsymbol{U}^{(i-1)}\mathbf{m}\right\|_2^2 \tag{5.39}$$

$$= \underset{\{\kappa_k,\theta_k\}_{k\in\mathcal{J}^{(i)}}}{\arg\min} \sum_{t=1}^{T} \left| \underbrace{y_t - \sum_{k\notin\mathcal{J}^{(i)}} [\boldsymbol{U}^{(i-1)}]_{t,k}}_{q_t} - \sum_{k\in\mathcal{J}^{(i)}} [\boldsymbol{U}^{(i-1)}]_{t,k}\kappa_k e^{j\theta_k} \right|^2 \tag{5.40}$$

$$= \underset{\{\kappa_k,\theta_k\}_{k\in\mathcal{J}^{(i)}}}{\arg\min} \sum_{t=1}^{T} \left| q_t - \sum_{k\in\mathcal{J}^{(i)}} [\boldsymbol{U}^{(i-1)}]_{t,k}\kappa_k e^{j\theta_k} \right|^2 \tag{5.41}$$

Since $0 \leq \kappa_k \leq 1$, we can re-formulate this problem as follows:

$$\min_{\{x_k\}_{k\in\mathcal{J}^{(i)}}} \sum_{t=1}^{T} \left| q_t - \sum_{k\in\mathcal{J}^{(i)}} [\boldsymbol{U}^{(i-1)}]_{t,k} x_k \right|^2 \tag{5.42}$$

$$\text{such that } |x_k| \leq 1 \text{ for any } k. \tag{5.43}$$

Clearly, (5.42) is a convex problem with respect to $\{x_k\}_{k\in\mathcal{J}^{(i)}}$. Hence, by solving this problem via convex programming techniques, we obtain our estimates $\{\hat{\kappa}_k, \hat{\theta}_k\}_{k\in\mathcal{J}^{(i)}}$. One should note that, as $\mathcal{I}^{(i-1)} \subseteq \mathcal{J}^{(i)}$, by solving (5.42), we also refine our previous estimates.

Again, based on this resulting mask vector, we update the position and the channel gain estimates. For that estimated position and the channel gain, we update $\boldsymbol{U}^{(i-1)}$ and we again compute the posterior probabilities and update the mask estimate. We perform these alternating steps until the number of allowed alternating steps is exceeded or the change in the position estimates becomes negligible, as we do in the first iteration. The whole algorithm is summarized in Algorithm 7. To determine the stopping time of this algorithm, we put a bound on the number of iterations. If the number of successive iterations exceeds I, then the algorithm stops.

To compare the performances of the proposed algorithms, we use two types of CRBs as explained below.

- **CRB-perfect**: This corresponds to the CRB when the perfect knowledge of the mask vector is available. This CRB is exactly in the same form as the CRB presented in Chapter 4.4.3.

- **CRB-known-loc**: This corresponds to the CRB when the failure locations are known, but κ_k and θ_k values are taken as unknowns. That is, in addition to the derivatives we use for calculating CRB-perfect, we need to determine the derivatives of μ_t with respect to κ_k and θ_k when there is a failure in the kth pixel.

  If we denote $\overline{\boldsymbol{U}} \triangleq \boldsymbol{S}(\boldsymbol{\Phi}^{\mathsf{T}} \odot \mathbf{1}\bar{\boldsymbol{h}}^{\mathsf{T}})$, where $\bar{\boldsymbol{h}} = \overline{\alpha}\boldsymbol{b}(\overline{\boldsymbol{p}})$, for given set of failure indices $\mathcal{I}$, it

is possible to express that

$$\mu_t = \sum_{k \notin \mathcal{I}} \left[\overline{\boldsymbol{U}}\right]_{t,k} + \sum_{k \in \mathcal{I}} \left[\overline{\boldsymbol{U}}\right]_{t,k} \kappa_k e^{j\theta_k} \tag{5.44}$$

Hence, we can write

$$\frac{\partial \mu_t}{\partial \kappa_k} = \left[\overline{\boldsymbol{U}}\right]_{t,k} e^{j\theta_k}, \text{ and } \frac{\partial \mu_t}{\partial \theta_k} = j \left[\overline{\boldsymbol{U}}\right]_{t,k} \kappa_k e^{j\theta_k}. \tag{5.45}$$

5.4 Numerical Results

In this section, we first present numerical examples for evaluating the theoretical bounds, and then compare the performance of the ℓ_1-regularization based algorithm and successive algorithm against the theoretical bounds.

5.4.1 Simulation Setup

We consider an RIS with $N = 20 \times 20$ elements, where the inter-element spacing is $\lambda/2$ and the area of each element is $A = \lambda^2/4$ [70]. The carrier frequency is equal to $f_c = 28$ GHz. The RIS is modeled to lie in the X-Y plane with $\boldsymbol{p}_{\text{RIS}} = [0\,0\,0]^{\mathsf{T}}$. Moreover, for the RIS elements, the entries of $\boldsymbol{\phi}_t$ are generated uniformly and independently between $-\pi$ and π. The BS is located at $\boldsymbol{p}_{\text{BS}} = 5.77 \times [-1\,1\,1]^{\mathsf{T}}$ meters. The UE is located at $5 \times [1\,1\,1]^{\mathsf{T}} / \|[1\,1\,1]\|_2$ meters. We set the number of transmissions to $T = 200$. For simplicity, we assume that $s_t = \sqrt{E_s}$ for any t. Also, the SNR is defined as

$$\text{SNR} = \frac{\left\|\overline{\alpha} \boldsymbol{S} \boldsymbol{\Gamma}^{\mathsf{T}} \boldsymbol{b}(\overline{\boldsymbol{p}})\right\|_2^2}{T N_0}. \tag{5.46}$$

To solve (5.9) for the LB computation, we employ the GlobalSearch algorithm of MATLAB by providing $\overline{\boldsymbol{p}}$ as the initial vector. In addition, N in (4.41) is taken as 50 for using the Jacobi-Anger expansion approach.

While implementing Algorithm 7, the number of maximum allowed iterations, I, is selected as $2N\text{p}_{\text{fail}}$. The reasoning behind this selection can be explained as follows. Since

the number of pixel failures estimated by Algorithm 7, is upper bounded by I, we need to choose I such that $\Pr\{\text{Number of failures} > I\} \leq \epsilon$, where $\epsilon > 0$ is a small number. Or equivalently,

$$\Pr\{\text{Number of failures} > I\} = 1 - \sum_{m=0}^{I} (\mathrm{p_{fail}})^{\mathrm{m}} (1 - \mathrm{p_{fail}})^{\mathrm{N-m}} \binom{\mathrm{N}}{\mathrm{m}} \tag{5.47}$$

should be small. In our simulations, we consider $\mathrm{p_{fail}} \in \{0.01, 0.02, 0.03, 0.04, 0.05\}$. For these values of $\mathrm{p_{fail}}$, for $I = 2N\mathrm{p_{fail}}$, $\Pr\{\text{Number of failures} > I\} \leq 0.02$.

Also, we set $C = 15$ in Algorithm 7. Moreover, for the ℓ_1-regularization based algorithm, we set $\lambda = 0.05\sqrt{\mathrm{SNR}}$ and $M = 15$. For both algorithms, ε is set to be 0.001. The simulations are performed on an Intel Core i7 4.0 GHz PC with 16 GB of physical memory using MATLAB R2020b on a Windows 10 operating system.

5.4.2 Results and Discussions

5.4.2.1 Theoretical Performance Bounds

In Figure 5.1, we present the theoretical bounds as a function of $\mathrm{p_{fail}}$ for SNRs 10, 20, and 30 dB when the UE distance is 5 meters from the center of the RIS. In this figure, both CRB-perfect and CRB-known-loc bounds are presentend. It can be noted that CRB-perfect and CRB-known-loc values are very close to each other. This observation suggests that once the failure locations are known, knowing the values of κ_k, θ_k is not essential.

The gap between the blue and red or green curves shows the effect of the pixel failures on the position estimates. We observe from the figure that as $\mathrm{p_{fail}}$ increases, i.e., as the mismatch between the true and the assumed models increases, the LB increases. We also observe that after $\mathrm{p_{fail}} = 0.04$, raising the SNR level from 20 to 30 dB does not improve the LB values, significantly.

In Figure 5.2, we show the theoretical bounds as a function of SNR for $\mathrm{p_{fail}}$ values 0.01, 0.03, and 0.05 when the UE distance is 5 meters from the center of the RIS. In parallel to Figure 5.1, we observe that CRB-perfect and CRB-known-loc behave very similarly. We

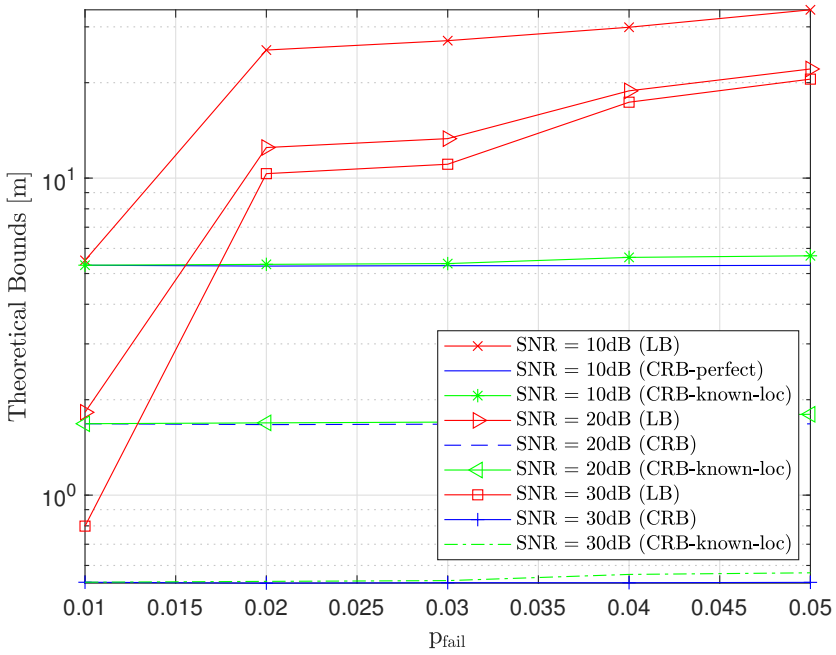


Figure 5.1: Theoretical bounds versus p_{fail} for SNR = 10, 20, 30 dB, when the UE distance is 5 meters from the center of the RIS.

also see that for $p_{fail} \geq 0.03$, raising the SNR after 30 dB does not improve the LB values notably. In both Figures 5.1 and 5.2 , we conclude that failures can degrade the estimation performance significantly. We note that when $p_{fail} \geq 0.02$, the degradation is significant in both high and low SNR regimes. Moreover, even for $p_{fail} = 0.01$, the degradation becomes notable in the high SNR regime.

5.4.2.2 Performances of Algorithm 5 and Algorithm 7

In this part, we investigate the performances of Algorithm 5 and Algorithm 7. While generating the failure mask vector, we set $\kappa_k = 1$ and ψ_k is generated uniformly between $-\pi$ and π, if the kth pixel fails. In addition to the performances of Algorithm 5 and Algorithm 7, we also plot the performance of the AMML estimator discussed in Chapter 4.3.2, in which localization is performed by assuming that there is no pixel failure even though the reality is different.

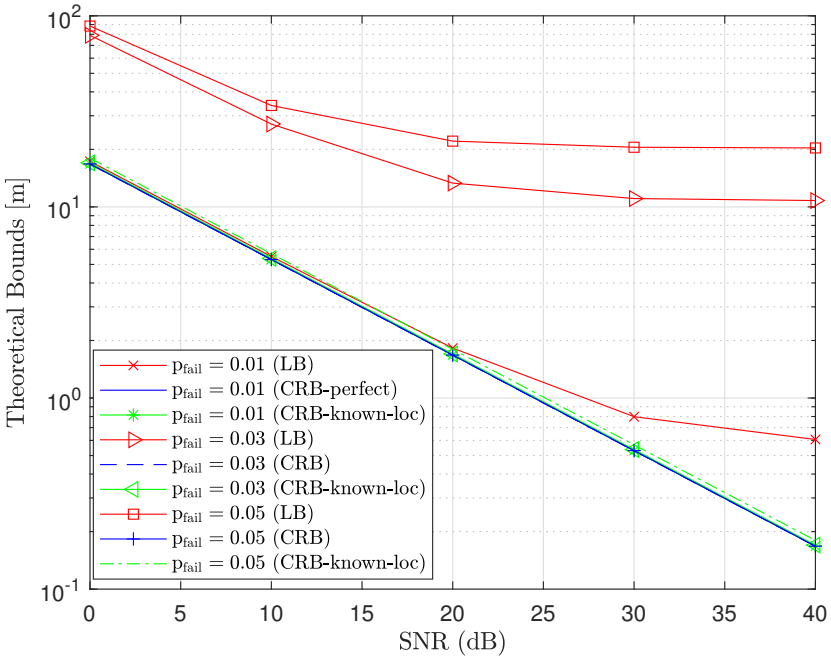


Figure 5.2: Theoretical bounds versus SNR for $p_{\text{fail}} = 0.01, 0.03$ and 0.05, when the UE distance is 5 meters from the center of the RIS.

In Figure 5.3, when the UE distance is 5 meters from the center of the RIS and $p_{\text{fail}} = 0.02$, the performances of the AMML algorithm, the ℓ_1 regularization based joint localization and failure diagnosis algorithm, and the succesive joint localization and failure diagnosis algorithm are shown versus SNR, together with the theoretical bounds. For this setting, in Figure 5.4, the mask-recovery performances of Algorithm 5 and Algorithm 7 versus SNR are also shown. To define the mask recovery performance, we use the square root of the normalized mean squared error (NMSE), i.e., for the mask vector estimate $\widehat{\mathbf{m}}$, we use

$$\text{NMSE} = \frac{\|\widehat{\mathbf{m}} - \overline{\mathbf{m}}\|_2^2}{\|\overline{\mathbf{m}}\|_2^2} = \frac{\|\widehat{\mathbf{m}} - \overline{\mathbf{m}}\|_2^2}{N} \tag{5.48}$$

We can observe from Figure 5.3 that via both successive and ℓ_1 regularization based approaches, localization error is greatly reduced compared to the AMML algorithm. Moreover, it can be noted that after SNR $= 20$ dB, the successive algorithm performs very similarly to the theoretical bounds. On the other hand, as the SNR increases, the performance of the ℓ_1 regularization based approach does not improve as much as the successive approach, and it deviates from the theoretical bounds. The main reason behind this observation can

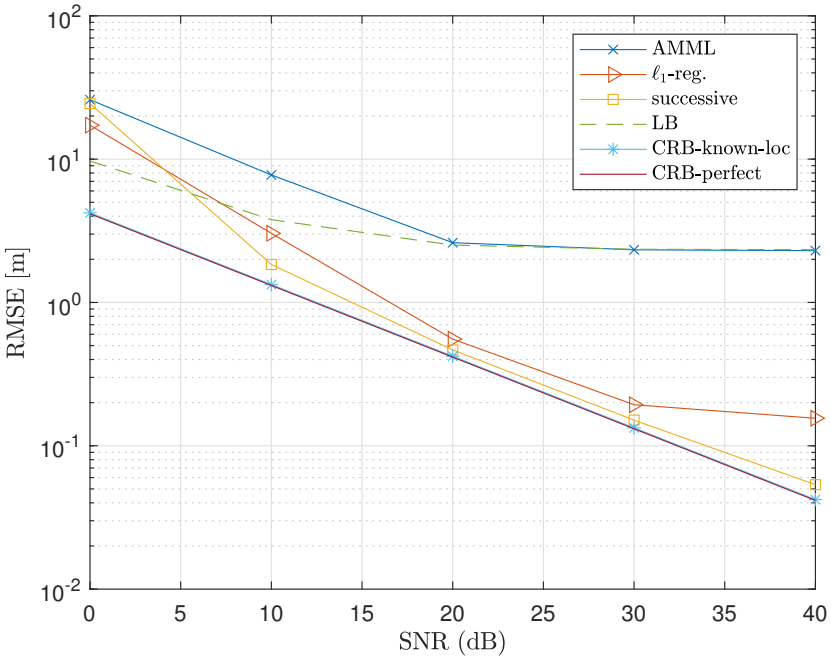


Figure 5.3: Localization performances of the AMML algorithm, Algorithm 5 and Algorithm 7 together with the theoretical bounds versus SNR, when the UE distance is 5 meters from the center of the RIS and $p_{\text{fail}} = 0.02$.

be explained from Figure 5.4. In this figure, it is observed that via the successive approach, the failure mask is captured better than the ℓ_1-regularization approach, hence the resulting positioning errors in Figure 5.3 become lower than those in the ℓ_1-regularization approach.

In Figure 5.5, when the UE distance is 5 meters from the center of the RIS and SNR = 40 dB, the performances of the AMML algorithm, ℓ_1-regularization based approach and successive approach versus p_{fail} are shown. For this setting, in Figure 5.6, the mask-recovery performances of Algorithm 5 and Algorithm 7 versus p_{fail} are also plotted. We again observe that by using Algorithm 5 and Algorithm 7, the positioning error is greatly reduced with respect to the AMML algorithm. Moreover, from Figure 5.5, it can be inferred that as p_{fail} increases, the performance difference between the ℓ_1-regularizaton based approach and the successive approach becomes more evident since via Algorithm 7, the unknown failure mask vector is recovered more effectively as observed in Figure 5.6.

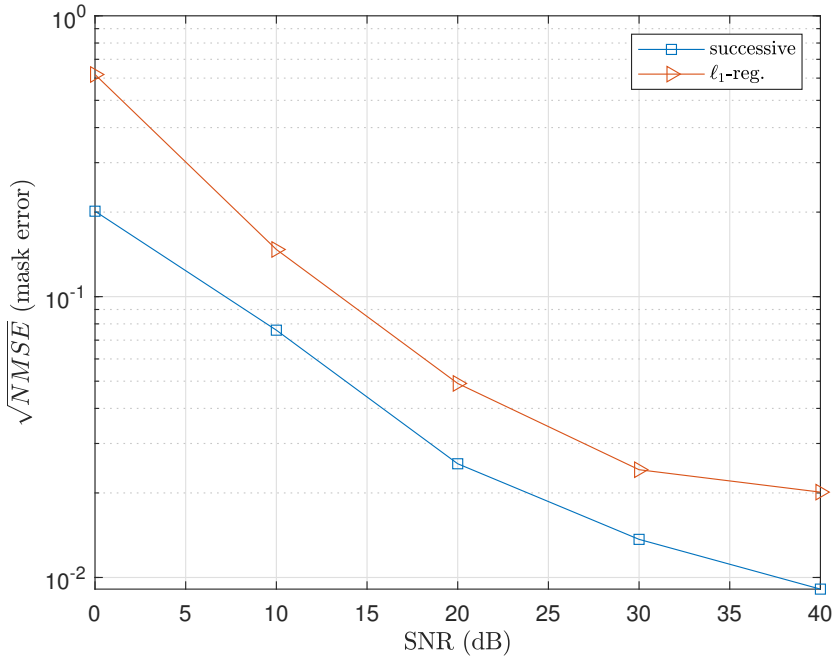


Figure 5.4: Mask recovery performances of Algorithm 5 and Algorithm 7 versus SNR, when the UE distance is 5 meters from the center of the RIS and $p_{\text{fail}} = 0.02$.

5.4.3 Run Time Comparison of Algorithm 5 and Algorithm 7

In terms of localization and mask recovery performances, the successive algorithm is better than the ℓ_1-regularization based algorithm. In this part, we compare the corresponding run times of Algorithm 5 and Algorithm 7. At an SNR of 40 dB, the average run time performances of Algorithm 5 and Algorithm 7 are given in Table 5.1. From these results, it can be noted that as $p_{\text{fail}} \leq 0.03$, the average run times of Algorithm 5 and Algorithm 7 are very close to each other. As $p_{\text{fail}} > 0.03$, in terms of average run time performance, the ℓ_1-regularization based algorithm is more efficient than the successive one. This result is quite expected since the required number of successive iterations increases as p_{fail} increases. However, even for $p_{\text{fail}} > 0.03$, the run time performances of Algorithm 5 and Algorithm 7 are comparable. That is, considering the localization and mask recovery performance of Algorithm 7, the additional run time cost that Algorithm 7 brings can be considered as acceptable.

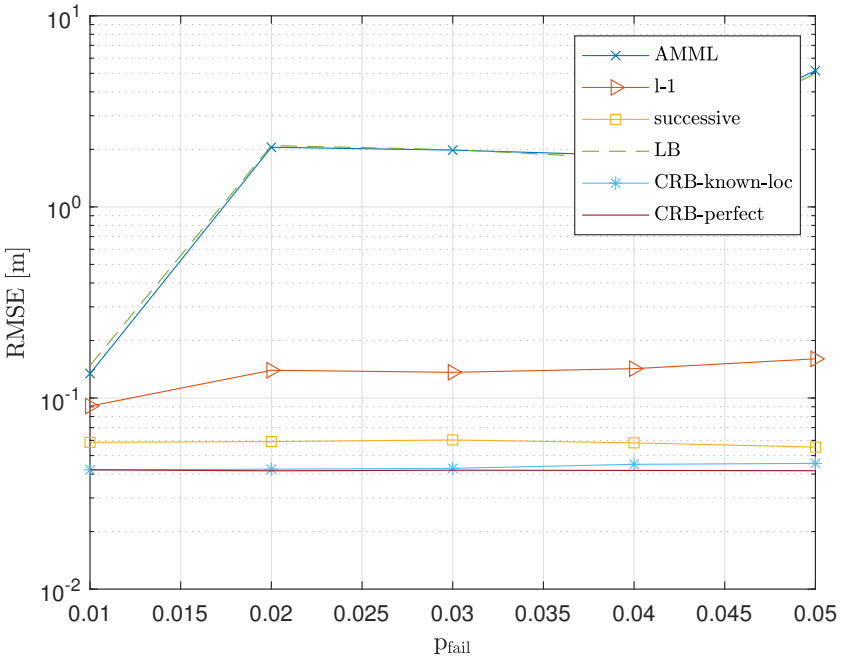


Figure 5.5: Localization performances of the AMML algorithm, Algorithm 5 and Algorithm 7 together with the theoretical bounds versus p_{fail}, when the UE distance is 5 meters from the center of the RIS and SNR = 40dB.

Table 5.1: Average Run Times of Algorithm 5 and Algorithm 7 in seconds

Algo.	$p_{fail} = 0.01$	$p_{fail} = 0.02$	$p_{fail} = 0.03$	$p_{fail} = 0.04$	$p_{fail} = 0.05$
ℓ_1	19.5	44.9	42.6	40.9	50.8
Successive	23.27	41.7	58.5	92.2	116.4

5.5 Concluding Remarks and Extensions

In this chapter, we have formulated the problem of RIS-aided localization under pixel failures and analyzed how detrimental pixel failures can be for localization by deriving corresponding theoretical performance bounds. We have also proposed Algorithms 5 and 7 for joint localization and mask recovery. Via simulation results, it has been shown that degradation in localization due to pixel failures can be significant. By using the proposed algorithms, positioning errors have been greatly reduced significantly. Especially, for the successive approach, estimation errors have been very close to the theoretical bounds in the high SNR regime.

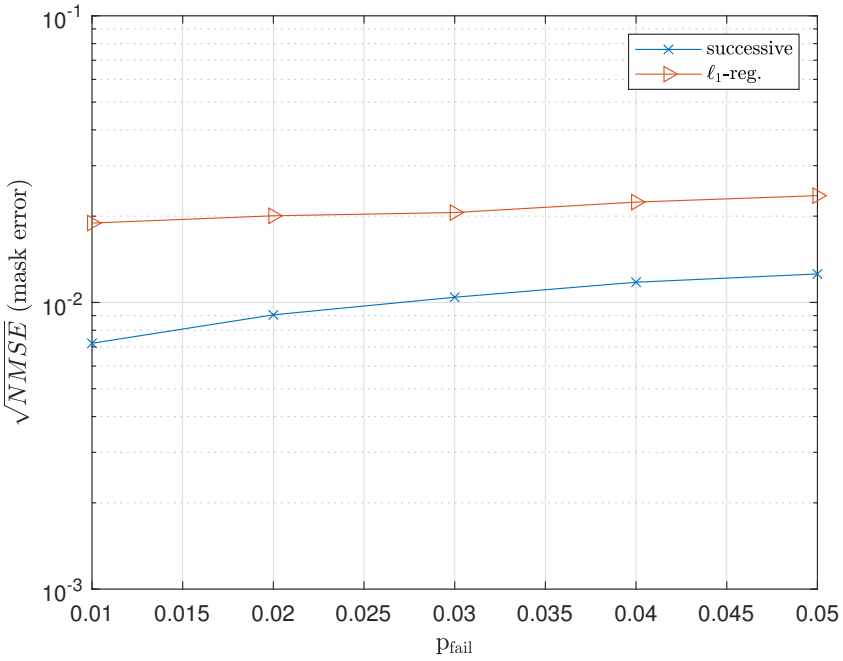


Figure 5.6: Mask recovery performances of Algorithm 5 and Algorithm 7 versus p_{fail}, when the UE distance is 5 meters from the center of the RIS and SNR = 40dB.

We can extend some of the results in this chapter as follows: While formulating the problem of RIS-aided localization under pixel failures, we have considered only-biased type of failures. As mentioned in [19, 86], disconnectedness is another type of failure. Under the disconnectedness case, the RIS profile $\boldsymbol{\gamma}_t$, and $\mathbf{m}$ can be expressed as

$$\boldsymbol{\gamma}_t = \boldsymbol{\phi}_t \odot \mathbf{m} + \boldsymbol{c}\,, \tag{5.49}$$

where $\boldsymbol{c} \in \mathbb{C}^{N\times 1}$ denotes the unknown *failure mask* quantifying the effect of disconnected pixels, which can be defined as [19, 86]

$$m_n = \begin{cases} 0, & \text{if the } n\text{-th RIS element is faulty (disconnected)} \\ \zeta_n, & \text{if the } n\text{-th RIS element is faulty (biased)} \\ 1, & \text{if the } n\text{-th RIS element is properly functioning} \end{cases}, \tag{5.50}$$

$$c_n = \begin{cases} \zeta_n, & \text{if the } n\text{-th RIS element is faulty (disconnected)} \\ 0, & \text{otherwise} \end{cases}. \tag{5.51}$$

Based on (5.49)–(5.51), the RIS phase profile takes the following values in the presence of

disconnected- and biased-type failures:

$$[\boldsymbol{\gamma}_t]_n = \begin{cases} [\boldsymbol{\phi}_t]_n, & \text{if the } n\text{-th RIS element is functioning} \\ [\boldsymbol{\phi}_t]_n m_n, & \text{if the } n\text{-th RIS element is biased} \\ c_n, & \text{if the } n\text{-th RIS element is disconnected} \end{cases} \tag{5.52}$$

For the case of $\mathbf{m} = \mathbf{1}$, i.e., for the disconnected-only scenario, both Algorithm 5 and Algorithm 7 can be used with minor modifications. However, for the case of $\mathbf{m} \neq \mathbf{1}$ and $\boldsymbol{c} \neq \mathbf{0}$, ℓ_1-regularization based methods could be ineffective. The reason is that, based on (5.49)-(5.51), we should enforce that $m_n c_n = 0$ for any $1 \leq n \leq N$. Due to the non-convexity of this constraint, ℓ_1-regularization based methods could be inefficient. However, even for this difficult scenario, the successive approach could be effective. For the considered problem, in the first iteration, we can consider that there are $2N + 1$ hypotheses as follows:

$$\begin{aligned} \mathcal{H}_0 &: \text{no failure}, \\ \mathcal{H}_k^{(b)} &: k\text{th pixel is biased for } 1 \leq k \leq N. \\ \mathcal{H}_k^{(d)} &: k\text{th pixel is disconnected for } 1 \leq k \leq N. \end{aligned}$$

We can again compute the posterior probabilities of the hypotheses and determine the one that yields the maximum one. For instance if $\mathcal{H}_k^{(b)}$ has the highest posterior probability, then we consider that pixel k is biased, and not consider hypothesis $\mathcal{H}_k^{(d)}$ in the remaining iterations. In the remaining iterations, we continue by assuming that pixel k is biased.

Algorithm 7 Successive Joint Localization and Failure Diagnosis Algorithm

Input: Observation $\mathbf{y}$, RIS phase profiles $\mathbf{\Phi}$, convergence threshold ε and maximum number of alternating steps C, maximum number of successive iterations I.
Output: $\widehat{\mathbf{p}}$, $\widehat{\alpha}$ and $\widehat{\mathbf{m}}$.
Obtain the initial position and channel gain estimates by Jacobi-Anger algorithm for $\mathbf{m}^{(0)} = \mathbf{1}$.
Set bool-out = 1, $i = 0$, $\mathcal{I}^{(0)} = \emptyset$.
while bool-out **do**
  Set $l = 0$, $i = i + 1$. $\mathbf{p}^{(i,0)} = \mathbf{p}^{(i-1)}$, $\alpha^{(i,0)} = \alpha^{(i-1)}$, and $\mathbf{m}^{(i,0)} = \mathbf{m}^{(i-1)}$.
  while bool-in **do**
    Given $\mathbf{p}^{(i,l)}$, $\alpha^{(i,l)}$ and $\mathbf{m}^{(i,l)}$,for $k \notin \mathcal{I}^{(i-1)}$ solve
    $(\widehat{k}, \hat{\kappa}_k, \hat{\theta}_k) = \arg\max_{k,\kappa_k,\theta_k} f(\mathbf{y}|\mathcal{H}_k) \Pr\{\mathcal{H}_k|\text{There is at most one failure except for } \mathcal{I}^{(i-1)}\}$.
    Set $l = l + 1$.
    if $\hat{k} = 0$ **then**
      Set bool-in = 0, bool-out = 0. Set $\mathbf{p}^{(i)} = \mathbf{p}^{(i,l)}$, $\alpha^{(i)} = \alpha^{(i,l)}$, and $\mathbf{m}^{(i)} = \mathbf{m}^{(i,l)}$
      Set $\mathcal{I}^{(i)} = \mathcal{I}^{(i-1)}$.
    else
      For given set of failure indices $\mathcal{I}^{(i-1)} \cup \{\widehat{k}\}$, find the $\hat{\kappa}_k, \hat{\theta}_k$'s by using (5.42), and update the mask accordingly.
      For the updated mask, update $\mathbf{p}^{(i,l)}$ and $\alpha^{(i,l)}$ via Jacobi-Anger algorithm.
      if $l \geq C$ or $\left\|\mathbf{p}^{(i,l)} - \mathbf{p}^{(i,l-1)}\right\|_2 \leq \varepsilon$ **then**
        Set bool-in = 0. Set $\mathbf{p}^{(i)} = \mathbf{p}^{(i,l)}$, $\alpha^{(i)} = \alpha^{(i,l)}$, and $\mathbf{m}^{(i)} = \mathbf{m}^{(i,l)}$
        Set $\mathcal{I}^{(i)} = \mathcal{I}^{(i-1)} \cup \{\widehat{k}\}$.
      end if
    end if
  end while
  if $i \geq I$ or $\hat{k} = 0$ **then**
    Set bool-out = 0, $\widehat{\mathbf{p}} = \mathbf{p}^{(i)}$, $\widehat{\alpha} = \alpha^{(i)}$ and $\widehat{\mathbf{m}} = \mathbf{m}^{(i)}$.
  end if
end while

Chapter 6

Parameter Encoding for ECRB Minimization in the Presence of Jamming

In this chapter, the optimal encoding strategy of a transmitter is investigated in the presence of a jammer from an estimation theoretic perspective [120]. In the considered problem, the ECRB at an intended receiver is used as the performance metric. The optimal encoding strategy is determined first by restricting the set of possible encoding functions of the transmitter to the set of monotone increasing functions. Then, by removing the monotonicity assumption on the encoding function of the transmitter, the optimal encoding strategy is analyzed.

6.1 System Model and Problem Formulation

A transmitter sends a scalar parameter $\theta \in \Lambda$ to a receiver over a noisy and flat-fading channel in the presence of a jammer, as shown in Figure 6.1. The jammer has access to parameter θ (as in [97]), encodes it via a differentiable, real valued function $g : \Lambda \to \Gamma$, and sends the encoded parameter to the receiver. The aim is to perform accurate estimation of

parameter θ at the receiver in the presence of jamming. To this aim, parameter θ is encoded by a differentiable, real valued function $f : \Lambda \to \Upsilon$ at the transmitter. Accordingly, the received signal Y can be expressed as

$$Y = h_T f(\theta) + h_J g(\theta) + N, \tag{6.1}$$

where h_T and h_J denote the channel fading coefficients between the transmitter and the receiver and between the jammer and the receiver, respectively, N is the noise term, which is modeled as a zero-mean Gaussian random variable with a known variance denoted by σ^2, and N and θ are assumed to be independent.

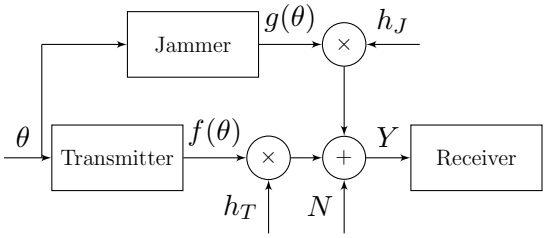


Figure 6.1: System model for parameter encoding in the presence of jamming.

The prior information on parameter θ is represented by a probability density function (PDF) denoted by $w(\theta)$ for $\theta \in \Lambda$. Also, the channel coefficients are supposed to be known by the transmitter and the receiver. In addition, it is assumed that the receiver knows both mappings $f(\cdot)$ and $g(\cdot)$, and the transmitter has the knowledge of $g(\cdot)$. The motivation and justification for these assumptions are as follows: (i) In a sensor network in which jamming is caused by another transmitter in the same network unintentionally, these assumptions can hold. (ii) Under these assumptions, we obtain an upper bound on the estimation performance at the receiver in the presence of jamming. (This bound becomes tight when the transmitter is smart and the jammer is dummy.) (iii) The analysis under these assumptions leads to the best response strategy of the transmitter for a given jammer strategy, which forms an important step towards a game theoretic analysis.

To quantify the estimation accuracy at the receiver, the ECRB is employed as a performance metric since it converges to the MSE of the maximum a-posteriori probability (MAP) estimator in the high SNR regime [121], does not depend on specific estimator structures, and facilitates theoretical analyses (leading to explicit expressions for the optimal encoder

function at the transmitter). The ECRB is defined as the expectation of the conditional Cramér-Rao bound [121] and calculated as follows:

$$\mathbb{E}_\theta \left\{ \mathcal{I}(\theta)^{-1} \right\} = \int_\Lambda w(\theta) \frac{1}{\mathcal{I}(\theta)} \, d\theta \tag{6.2}$$

where $\mathcal{I}(\theta)$ denotes the Fisher information, i.e.,

$$\mathcal{I}(\theta) = \int \left(\frac{\partial \log p_{Y|\theta}(y)}{\partial \theta} \right)^2 p_{Y|\theta}(y) \, dy \tag{6.3}$$

with $p_{Y|\theta}(y)$ representing the conditional PDF of Y for a given value of θ. For the considered system model in (6.1), $p_{Y|\theta}(y)$ is expressed as

$$p_{Y|\theta}(y) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{\left(y - h_T f(\theta) - h_J g(\theta)\right)^2}{2\sigma^2} \right). \tag{6.4}$$

by taking logarithm of both sides in (6.4), we would obtain

$$\log p_{Y|\theta}(y) = \log\left(\frac{1}{\sqrt{2\pi\sigma^2}} \right) - \frac{\left(y - h_T f(\theta) - h_J g(\theta)\right)^2}{2\sigma^2}. \tag{6.5}$$

By some algebraic manipulations, it is possible to show that the Fisher information, $\mathcal{I}(\theta)$, is given by

$$\mathcal{I}(\theta) = \left(h_T f'(\theta) + h_J g'(\theta)\right)^2 / \sigma^2 \tag{6.6}$$

where $f'(\theta)$ and $g'(\theta)$ denotes the derivatives of $f(\theta)$ and $g(\theta)$, respectively. Intuitively, the jammer would like to cancel the transmitted signal to set the Fisher information to zero. However, it does not know the encoder at the transmitter and can design its encoder based on previous experience. When the transmitter employs a differential encoding strategy for ease of implementation, the jammer can also be modeled to employ a different encoding strategy for cancellation purposes.

Based on a reasoning similar to that in [90], the ranges of θ, $g(\theta)$, and $f(\theta)$ are modeled as $\Lambda = [a, b]$, $\Gamma = [k, l]$, and $\Upsilon = [c, d]$, respectively, for some $a, b, c, d, k, l \in \mathbb{R}$. In particular, for $\theta \in [a, b]$, $f(\cdot)$ must be a differentiable function that satisfies $c \leq f(\theta) \leq d$. By setting lower and upper limits on $f(\theta)$, we effectively impose a peak power constraint on the transmitted signal, which in turn limits the average transmit power, as well. Hence, for given $g(\cdot)$, we propose the following optimization problem for parameter encoding at the transmitter:

$$\min_f \qquad \int_a^b w(\theta) \frac{\sigma^2}{\left(h_T f'(\theta) + h_J g'(\theta)\right)^2} \, d\theta \tag{6.7a}$$

$$\text{subject to} \quad c \leq f(\theta) \leq d\,,\ \forall\, \theta \in [a,b] \tag{6.7b}$$

That is, the aim is to obtain the optimal encoding function at the transmitter that minimizes the ECRB at the receiver ((6.2) and (6.6)) for a given jammer and under the constraint in (6.7b). In order to solve this problem, we need some theoretical background of variational calculus, which will be given in the next section.

6.2 Preliminaries for Calculus of Variations

First, we should clarify the distinction between two types of extremals: the weak and the strong minimizer/maximizer. Throughout this chapter, we will concentrate on minimizers, especially on the weak minimizer. Similar conclusions can easily be made for maximizers, as well.

6.2.1 Weak and Strong Minimizers/Maximizers

In order to explain weak and strong minimizers, we need to define norms $\|\cdot\|_0$ and $\|\cdot\|_1$. Let $\mathcal{C}^k([a,b],\mathbb{R}^n)$ be a space of k-times continuously differentiable functions (here, $k \geq 0$ is an integer and $k=0$ corresponds to functions that are just continuous), mapping the closed interval $[a,b]$ to $\mathbb{R}^n$ for some integer $n \geq 1$. For a given function $y(x) \in \mathcal{C}^0([a,b],\mathbb{R}^n)$, $\|y\|_0$ is defined as [122, pp. 6], [123, Eq. 1.30, pp. 15]

$$\|y\|_0 \triangleq \max_{a\leq x\leq b} |y(x)| \tag{6.8}$$

where $|\cdot|$ corresponds to the standard Euclidean norm defined on $\mathbb{R}^n$. Similarly, for $y(x) \in \mathcal{C}^1([a,b],\mathbb{R}^n)$, $\|y\|_1$ is defined as [122, pp. 6], [123, Eq. 1.30, pp. 15]

$$\|y\|_1 \triangleq \max_{a\leq x\leq b} |y(x)| + \max_{a\leq x\leq b} |y'(x)| \tag{6.9}$$

where $y'(\cdot)$ denotes the derivative of $y(\cdot)$.

Let $J[y]$ be a real-valued functional defined on some space V equipped with a norm $\|\cdot\|$. Then, $\hat{y}$ is a local minimizer of $J[\cdot]$ if there exists an $\epsilon > 0$ such that for any y satisfying $\|y-\hat{y}\| \leq \epsilon$, we have $J(\hat{y}) \leq J(y)$ [122, pp. 12], [123, pp. 15]. The local minimum

with respect to the $\|\cdot\|_0$ and $\|\cdot\|_1$ norms are called as the strong minimizer and the weak minimizer, respectively [122, pp. 13], [123, pp. 26]. In other words, both the weak and the strong minimizers are local minimizers.

Let us consider the problem of minimizing $J[y] = \int_a^b L(x, y, y')\, dx$ subject to $y(a) = A$ and $y(b) = B$, where y lies on a function space V. (Similar conclusions can be made for the functional optimization problems containing integral constraints.)

6.2.2 Definitions of First and Second Variations

The first variation is defined as [122, pp. 12]

$$\delta J|_y(\eta) = \lim_{\|\eta\| \to 0} J[y + \eta] - J[y] \tag{6.10}$$

Analogously, in [123, Eq. 1.34, pp. 16], the first variation is defined as

$$\delta J|_y(\eta) \triangleq \lim_{\alpha \to 0} \frac{J[y + \alpha\eta] - J[y]}{\alpha} \tag{6.11}$$

where for sufficiently small α, $y + \alpha\eta$ must be an element of V. One can clearly see that (6.10) and (6.11) are equivalent to each other. In addition, the second variation is defined as [122, pp. 99]

$$\delta^2 J|_y(\eta) = \lim_{\|\eta\| \to 0} J[y + \eta] - J[y] - \delta J|_y(\eta). \tag{6.12}$$

Analogously, in [123, Eq. 1.39, pp. 18], the second variation is defined as

$$\delta^2 J|_y(\eta) \triangleq \lim_{\alpha \to 0} \frac{J[y + \alpha\eta] - J[y] - \delta J|_y(\eta)\alpha}{\alpha^2} \tag{6.13}$$

Again, one can clearly see that (6.12) and (6.13) are equivalent to each other.

6.2.3 Necessary and Sufficient Conditions for Weak Minimizers

Necessary condition for a function to be a local minimizer is determined by Euler-Lagrange equations as given in [122, Thm. 1, pp. 15] and [123, Eq. 2.18, pp. 30]. One should note that Euler-Lagrange equations must hold for both types of minimizers. In particular, we must have

$$L_y = \frac{d}{dx} L_{y'} \tag{6.14}$$

where $L_y = \frac{\partial L}{\partial y}$ and $L_{y'} = \frac{\partial L}{\partial y'}$. One should note that these partial derivatives are taken with respect to the functions. On the other hand, in the RHS of (6.14), we are taking the regular derivative of the function $L_{y'}$ with respect to x. This is the reason why some of the derivatives are regular while some of them are partial.

Let $P(x) \triangleq \frac{1}{2}L_{y'y'}$ and $Q(x) \triangleq \frac{1}{2}\left(L_{yy} - \frac{d}{dx}L_{yy'}\right)$, where $L_{y'y'} = \frac{\partial^2 L}{\partial y' \partial y'}$, $L_{yy'} = \frac{\partial^2 L}{\partial y \partial y'}$, and $L_{yy} = \frac{\partial^2 L}{\partial y \partial y}$. These definitions are taken from [122, Eq. 41, pp. 112] and [123, Eq. 2.59, pp. 48]. It is noted that the second variation can be written as [122, Eq. 10, pp. 102], [123, Eq. 2.58, pp. 48]

$$\delta^2 J|_y(\eta) = \int_a^b P(x)(\eta'(x))^2 + Q(x)(\eta(x))^2\, dx \tag{6.15}$$

If the equation $Qv = \frac{d}{dx}(Pv')$ has admits a solution such that $v(a) = 0$ and $v(c) = 0$ for some $c > a$ and $c \leq b$, this point c is said to be conjugate to a [122, pp. 106], [123, pp. 52]. Now, we are ready to express the sufficient condition for optimality in the sense of weak minimizers as follows:

$y(.)$ is a weak minimizer if $y(.)$ satisfies Euler-Lagrange equations, $L_{y',y'}(x, y(x), y'(x)) > 0$ for all $x \in [a, b]$ and $[a, b]$ contains no points conjugate to a [122, pp. 116], [123, pp. 53].

Furthermore, in [122, Thm. 2, pp. 109], it is stated that if the integral expression in (6.15), hence, the second variation, is positive definite for all $\eta(\cdot)$ such that $\eta(a) = \eta(b) = 0$, then the interval $[a, b]$ contains no points conjugate to a, where $P(x) > 0$ for all $x \in [a, b]$. The definition of positive definiteness is given in [122, pp. 98]. In fact, this definition is equivalent to the second variation being positive.

6.3 Optimal Encoding Function at Transmitter

We characterize the solution of (6.7) in various scenarios by first restricting f to be monotone strictly increasing or monotone strictly decreasing, and then by removing the monotonicity assumption on f.

6.3.1 f is strictly monotone increasing

If f is strictly monotone increasing, $f'(\theta) > 0$ for each $\theta \in [a, b]$. By adding the constraint $f'(\theta) > 0$ to (6.7), we formulate the proposed optimization problem as follows:

$$\min_{f} \quad \int_a^b w(\theta)(h_T f'(\theta) + h_J g'(\theta))^{-2}\, d\theta \tag{6.16a}$$

$$\text{subject to} \quad c \le f(\theta) \le d\,,\ \forall\, \theta \in [a, b] \tag{6.16b}$$

$$f'(\theta) > 0,\ \forall\, \theta \in [a, b] \tag{6.16c}$$

where the constant term σ^2 is removed from the objective function for notational convenience. It is noted that the objective function in (6.16a) remains constant if we shift all $f(\theta)$ values by the same scalar number. Due to the monotonicity of $f(\cdot)$, if we ensure that $f(b)-f(a) \le d-c$, we can find the optimal $f(\cdot)$ up to a constant. We can then adjust this constant term such that $f(\cdot)$ remains in $[c, d]$. Another way of writing $f(b) - f(a) \le d - c$ is $\int_a^b f'(\theta)\, d\theta \le d - c$. Hence, by replacing (6.16b) with $\int_a^b f'(\theta)\, d\theta \le d - c$, we can concentrate on the following problem:

$$\min_{f} \quad \int_a^b w(\theta)(h_T f'(\theta) + h_J g'(\theta))^{-2}\, d\theta \tag{6.17a}$$

$$\text{subject to} \quad \int_a^b f'(\theta)\, d\theta \le d - c \tag{6.17b}$$

$$f'(\theta) > 0,\ \forall\, \theta \in [a, b] \tag{6.17c}$$

Next, we replace the constraint in (6.17c) by the equality constraint $f'(\theta) = \epsilon + \mu^2(\theta)$ for a sufficiently small number $\epsilon > 0$ and for some function μ. We also define a function $t(\cdot)$ such that

$$\int_a^b f'(\theta) + t^2(\theta)\, d\theta = d - c \tag{6.18}$$

Hence, we can reformulate (6.17) as follows:

$$\min_{f,t,\mu} \quad \int_a^b w(\theta)(h_T f'(\theta) + h_J g'(\theta))^{-2}\, d\theta \tag{6.19a}$$

$$\text{subject to} \quad \int_a^b f'(\theta) + t^2(\theta)\, d\theta = d - c \tag{6.19b}$$

$$f'(\theta) = \mu^2(\theta) + \epsilon\,,\ \forall\, \theta \in [a, b] \tag{6.19c}$$

The following proposition characterizes the solution of (6.19).

Proposition 6.1: A solution to (6.19) admits one of the following two alternative forms:

- either $f'(\theta) = \epsilon$ for all $\theta \in [a, b]$,
- or, there exists $\emptyset \subseteq S \subseteq [a, b]$ such that

$$f'(\theta) = \epsilon, \text{ if } \theta \in S, \tag{6.20}$$

$$f'(\theta) = \frac{(\tilde{K} w(\theta))^{1/3} - h_J g'(\theta)}{h_T} > 0, \text{ if } \theta \in S^c, \tag{6.21}$$

where $S^c = [a, b] \setminus S$ and $\tilde{K}$ is chosen such that

$$\int_a^b f'(\theta)\, d\theta = d - c. \tag{6.22}$$

Proof: Let $H(\theta, f', \mu, t, \gamma, \lambda)$ be given by

$$H(\theta, f', \mu, t, \gamma, \lambda) = w(\theta)(h_T f'(\theta) + h_J g'(\theta))^{-2} + \lambda \left(f'(\theta) + t^2(\theta)\right) + \gamma(\theta) \left(\mu^2(\theta) + \epsilon - f'(\theta)\right). \tag{6.23}$$

where λ and $\gamma(\theta)$ are Lagrange multipliers. Finding the extremals of (6.19) is equivalent to finding the extremals of $\mathcal{H}[f', \mu, t, \gamma]$, where

$$\mathcal{H}[f', \mu, t, \gamma] = \int_a^b H(\theta, f', \mu, t, \gamma, \lambda)\, d\theta\,. \tag{6.24}$$

From (6.23), Euler-Lagrange equations [122, pp. 36] lead to

$$\frac{\partial H}{\partial f} - \frac{d}{d\theta}\frac{\partial H}{\partial f'} = -\frac{d}{d\theta}\left(- \frac{2h_T w(\theta)}{\left(h_T f'(\theta) + h_J g'(\theta)\right)^3} + \lambda - \gamma(\theta)\right) = 0 \tag{6.25}$$

$$\frac{\partial H}{\partial \mu} - \frac{d}{d\theta}\frac{\partial H}{\partial \mu'} = 2\gamma(\theta)\mu(\theta) = 0 \tag{6.26}$$

$$\frac{\partial H}{\partial \gamma} - \frac{d}{d\theta}\frac{\partial H}{\partial \gamma'} = \mu^2(\theta) + \epsilon - f'(\theta) = 0 \tag{6.27}$$

$$\frac{\partial H}{\partial t} - \frac{d}{d\theta}\frac{\partial H}{\partial t'} = 2\lambda t(\theta) = 0. \tag{6.28}$$

(We use the partial derivative notation for the derivatives with respect to functions, otherwise we use the regular derivative notation.) (6.25) implies that there exists a constant $K \in \mathbb{R}$ such that

$$\frac{2h_T w(\theta)}{\left(h_T f'(\theta) + h_J g'(\theta)\right)^3} + \gamma(\theta) = K + \lambda\,. \tag{6.29}$$

Multiplying both sides of (6.29) with $\mu(\theta)$ and using (6.26) and (6.27), we obtain

$$\frac{2h_T w(\theta)\mu(\theta)}{\left(h_T\mu^2(\theta)+h_T\epsilon+h_J g'(\theta)\right)^3} = (K+\lambda)\mu(\theta). \tag{6.30}$$

It is noted from (6.23) that the following relations hold:

$$H_f = \frac{\partial H}{\partial f} = 0, \tag{6.31}$$

$$H_{ff'} = \frac{\partial^2 H}{\partial f \partial f'} = 0, \tag{6.32}$$

$$H_{ff} = \frac{\partial^2 H}{\partial f^2} = 0, \tag{6.33}$$

$$H_{f'f'} = \frac{\partial^2 H}{\partial f'^2} = \frac{6h_T^2 w(\theta)}{\left(h_T f'(\theta)+h_J g'(\theta)\right)^4} > 0. \tag{6.34}$$

Then, the second variation $\delta^2\mathcal{H}|_f(\eta)$ is given by

$$\begin{aligned}\delta^2\mathcal{H}|_f(\eta) &= \frac{1}{2}\int_a^b \left[\eta^2\left(H_{ff}-\frac{d}{d\theta}H_{ff'}\right)\right] + \eta'^2 H_{f'f'}\,d\theta \\ &= \frac{1}{2}\int_a^b \eta'^2 H_{f'f'}\,d\theta > 0\end{aligned} \tag{6.35}$$

for any perturbation $\eta(\theta)$ [122, p. 25]. One should note that as (6.35) holds for any perturbation, it holds also for the admissible perturbations. Hence, it is deduced that the interval $[a,b]$ contains no points conjugate to a [122, Thm. 2, p. 109]. Based on (6.35), any $f(\cdot)$ satisfying (6.25)–(6.28) also satisfies the sufficient conditions to be a minimizer of (6.19) [122, p. 116]. Hence, it is concluded that the resulting $f(\cdot)$ is a minimizer of (6.19). Therefore, the aim becomes finding a solution $f(\cdot)$ that satisfies the Euler-Lagrange equations. To obtain a solution, K can be set to zero; i.e., $K=0$. Then, based on (6.28), there exist two cases; namely, $\lambda=0$ or $\lambda\neq 0$:

$\underline{\lambda=0}$: From (6.30), $\mu(\theta)=0$ is obtained for any θ. Hence, $f'(\theta)=\epsilon$ for all $\theta\in[a,b]$ due to (6.27).

$\underline{\lambda\neq 0}$: From (6.28), $t(\theta)=0$ for any θ. Hence, the solution $f(\cdot)$ should satisfy

$$\int_a^b f'(\theta)\,d\theta = d-c. \tag{6.36}$$

Moreover, $\mu(\cdot)$ should satisfy the following equation:

$$\mu(\theta)\left[\left(h_T\mu^2(\theta)+h_T\epsilon+h_J g'(\theta)\right)^3 - \tilde{K}w(\theta)\right] = 0 \tag{6.37}$$

where $\tilde{K} = 2h_T/\lambda$, meaning that there exists a set $S \subseteq [a, b]$ such that $f'(\theta)$ is specified by (6.20) and (6.21), and $\tilde{K}$ is chosen to satisfy (6.22). ■

By comparing the ECRB values corresponding to the encoding functions obtained for the two alternatives in Proposition 6.1, we can select the encoding function that yields the lower ECRB. The following corollary characterizes the closed form solution for the optimal encoding function when θ is uniformly distributed and $g(\cdot)$ is a linear encoding function.

Corollary 1: If θ is uniformly distributed and $g(\cdot)$ is a linear mapping, the optimal encoding function is given by

$$f(\theta) = c + (d - c)(\theta - a)/(b - a) \tag{6.38}$$

regardless of the value of h_J.

Proof: If θ is distributed uniformly and the encoding function of the jammer is taken as a linear mapping, the ratio $\big((\tilde{K}w(\theta))^{1/3} - h_J g'(\theta)\big)/h_T$ becomes a constant value that is independent of θ, which we call L. If we choose $L = (d-c)/(b-a)$ and $S = \emptyset$, it is seen that all of the Euler-Lagrange equations are satisfied. Therefore, if θ is uniformly distributed and $g(\cdot)$ is a linear mapping, $f'(\theta)$ must be equal to $(d-c)/(b-a)$ for all $\theta \in [a, b]$. In other words, f also becomes a linear mapping. Namely, $f(\theta)$ is given by $f(\theta) = f(a)+(d - c)(\theta-a)/(b-a)$. By choosing $f(a) = c$, we find a solution that satisfies all of the Euler-Lagrange equations and is feasible for (6.16). ■

To find the encoding function specified by Proposition 6.1, we should determine set S and parameter $\tilde{K}$ such that (6.20)–(6.22) are satisfied. To determine S, Algorithm 8 is proposed.

In Algorithm 8, if $S^{(0)}$ is not empty, in each iteration $i \geq 1$, we exclude the interval in which $\alpha_i(\theta) < 0$. Since we have $d - c - \epsilon(b - a) = \int_{[a,b]} \alpha_i(\theta)\, d\theta < \int_{R^{(i)}} \alpha_i(\theta)\, d\theta$ and $\tilde{K}^{(i+1)}$ is computed such that the integral of $\alpha_{i+1}(\theta)$ over the region $R^{(i)}$ is equal to $d - c - \epsilon(b - a)$, it is evident that $\tilde{K}^{(i)} \geq \tilde{K}^{(i+1)}$. This also means that $S^{(i)} \subseteq S^{(i+1)}$. By comparing the ECRB values corresponding to the encoding functions obtained by the proposed algorithm and $f'(\theta) = \epsilon$, we can determine an optimal encoding function.

Remark 6.1: When $f(\cdot)$ is strictly monotone decreasing, $-f(\cdot)$ becomes a strictly monotone increasing function. Therefore, if we define $p(\theta) \triangleq -f(\theta)$ for each θ, an optimization

Algorithm 8 Proposed Algorithm for Determining S and $f'(\cdot)$

Input: $w(\cdot), g'(\cdot), h_T, h_J, \epsilon$.
Output: $S, f'(\cdot)$.

To find $\tilde{K}^{(0)}$, solve the following integral equation $\int_a^b \frac{(\tilde{K}^{(0)}w(\theta))^{1/3}-h_T\epsilon-h_Jg'(\theta)}{h_T}\,d\theta = d-c-\epsilon(b-a)$
Set $\alpha_0(\theta) = \frac{(\tilde{K}^{(0)}w(\theta))^{1/3}-h_T\epsilon-h_Jg'(\theta)}{h_T}$ for all $\theta \in [a,b]$.
Find $S^{(0)} = \{\theta \in [a,b] \mid \alpha_0(\theta) < 0\}$
if $S^{(0)} = \emptyset$ **then**
    $\rho = 0$, $S \leftarrow S^{(0)}, \alpha(\cdot) \leftarrow \alpha_0(\cdot), f'(\cdot) \leftarrow \alpha(\cdot) + \epsilon$.
else
    $\rho = 1$, $i \leftarrow 0$, $R^{(0)} \leftarrow [a,b] \setminus S^{(0)}$.
end if
while $\rho = 1$ **do**
    $i \leftarrow i+1$, and compute $\tilde{K}^{(i)}$ by solving the integral equation $\int_{R^{(i-1)}} \frac{(\tilde{K}^{(i)}w(\theta))^{1/3}-h_T\epsilon-h_Jg'(\theta)}{h_T}\,d\theta = d-c-\epsilon(b-a)$.
    Set $\alpha_i(\theta) = \frac{(\tilde{K}^{(i)}w(\theta))^{1/3}-h_T\epsilon-h_Jg'(\theta)}{h_T}$ for all $\theta \in R^{(i-1)}$.
    Find $S^{(i)} = \{\theta \in [a,b] \mid \alpha_i(\theta) < 0\}$
    $R^{(i)} \leftarrow [a,b] \setminus S^{(i)}$
    if $S^{(i)} \setminus S^{(i-1)} = \emptyset$ **then**
        $\rho = 0$, $S \leftarrow S^{(i)}, \alpha(\cdot) \leftarrow \alpha_i(\cdot), f'(\cdot) \leftarrow \alpha(\cdot) + \epsilon$.
    end if
end while

problem in the same form as that in (6.16) can be formulated and the same approach as in Section 6.3.1 can be employed.

6.3.2 f is not necessarily monotone

In this case, $c \le f(\theta) \le d$ implies that there exist $\mu(\cdot)$ and $t(\cdot)$ such that $f(\theta) = c + \mu^2(\theta)$ and $f(\theta) = d - t^2(\theta)$ for each θ. Then, (6.7) can be reformulated as

$$\min_{f} \quad \int_a^b w(\theta)(h_T f'(\theta) + h_J g'(\theta))^{-2}\,d\theta \tag{6.39a}$$

$$\text{subject to} \quad f(\theta) = c + \mu^2(\theta), \forall\, \theta \in [a,b], \tag{6.39b}$$

$$f(\theta) = d - t^2(\theta), \forall\, \theta \in [a,b]. \tag{6.39c}$$

The following proposition characterizes the solution of (6.39).

Proposition 6.2: If $\mathcal{P} = \{\theta \mid f(\theta) = c \text{ or } f(\theta) = d\}$ has zero measure and there exists $\xi \in \mathbb{R}$ such that

$$\max_{\theta\in[a,b]} \frac{c - \psi(\theta) - f(a)}{W(\theta)} < \xi < \min_{\theta\in[a,b]} \frac{d - \psi(\theta) - f(a)}{W(\theta)}, \tag{6.40}$$

then any $f(\theta) = f(a) + \psi(\theta) + \xi W(\theta)$ that satisfies the Euler-Lagrange equations is an optimal solution for (6.39), where

$$\psi(\theta) \triangleq -\frac{h_J(g(\theta) - g(a))}{h_T}, \tag{6.41}$$

$$W(\theta) \triangleq \int_a^\theta w(\tau)^{1/3}\, d\tau. \tag{6.42}$$

Proof: Let $F(\theta, f, f', \mu, t, \gamma^{(1)}, \gamma^{(2)})$ be given by

$$\begin{aligned} F(\theta, f, f', \mu, t, \gamma^{(1)}, \gamma^{(2)}) = w(\theta)\frac{1}{\left(h_T f'(\theta) + h_J g'(\theta)\right)^2} + \gamma^{(1)}(\theta)(\mu^2(\theta) + c - f(\theta)) \\ + \gamma^{(2)}(\theta)(f(\theta) - d + t^2(\theta)) \end{aligned} \tag{6.43}$$

where $\gamma^{(1)}(\theta)$ and $\gamma^{(2)}(\theta)$ are Lagrange multipliers. Finding the extremals of (6.39) is equivalent to finding the extremals of $\mathcal{F}(f, f', \mu, t, \gamma^{(1)}, \gamma^{(2)})$, which is given by

$$\mathcal{F}(f, f', \mu, t, \gamma^{(1)}, \gamma^{(2)}) = \int_a^b F(\theta, f, f', \mu, t, \gamma^{(1)}, \gamma^{(2)})\, d\theta.$$

From (6.43), the Euler-Lagrange equations can be obtained as

$$\frac{\partial F}{\partial f} - \frac{d}{d\theta}\frac{\partial F}{\partial f'} = -\gamma^{(1)}(\theta) + \gamma^{(2)}(\theta) + \frac{d}{d\theta}\left(\frac{2h_T w(\theta)}{\left(h_T f'(\theta) + h_J g'(\theta)\right)^3}\right) = 0, \tag{6.44}$$

$$\frac{\partial F}{\partial \mu} - \frac{d}{d\theta}\frac{\partial F}{\partial \mu'} = 2\mu(\theta)\gamma^{(1)}(\theta) = 0, \tag{6.45}$$

$$\frac{\partial F}{\partial t} - \frac{d}{d\theta}\frac{\partial F}{\partial t'} = 2t(\theta)\gamma^{(2)}(\theta) = 0, \tag{6.46}$$

$$\frac{\partial F}{\partial \gamma^{(1)}} - \frac{d}{d\theta}\frac{\partial F}{\partial \gamma^{(1)'}} = \mu^2(\theta) + c - f(\theta) = 0 \tag{6.47}$$

$$\frac{\partial F}{\partial \gamma^{(2)}} - \frac{d}{d\theta}\frac{\partial F}{\partial \gamma^{(2)'}} = f(\theta) - d + t^2(\theta) = 0. \tag{6.48}$$

As $\mathcal{P}$ defined in Proposition 6.2 is assumed to have zero measure, we concentrate on the case of $\mu(\theta) \neq 0$ and $t(\theta) \neq 0$. From (6.44), for some $\beta \in \mathbb{R}$, the following relation is obtained:

$$\frac{2h_T w(\theta)}{\left(h_T f'(\theta) + h_J g'(\theta)\right)^3} = \beta + \int_a^\theta \left(-\gamma^{(1)}(\tau) + \gamma^{(2)}(\tau)\right)\, d\tau$$

$$= \beta + \int_{[a,\theta]\cap\mathcal{P}} \left(-\gamma^{(1)}(\tau) + \gamma^{(2)}(\tau)\right) d\tau = \beta. \tag{6.49}$$

Therefore, $f'(\theta)$ is given by

$$f'(\theta) = ((\tilde{\beta} w(\theta))^{1/3} - h_J g'(\theta))/h_T, \tag{6.50}$$

where $\tilde{\beta} = 2h_T/\beta$. Then, $f(\theta)$ is expressed as

$$f(\theta) = f(a) + \int_a^\theta \frac{(\tilde{\beta} w(\tau))^{1/3} - h_J g'(\tau)}{h_T}\, d\tau. \tag{6.51}$$

Let $\xi \triangleq \tilde{\beta}^{1/3}/h_T$. Then, $f(\theta)$ can be written as

$$f(\theta) = f(a) + \psi(\theta) + \xi W(\theta). \tag{6.52}$$

We must find ξ such that $c < f(\theta) < d$ for any $\theta \in [a, b]$. Equivalently, ξ must satisfy the condition in (6.40) of Proposition 6.2. If there exists no ξ satisfying (6.40), the Euler-Lagrange equations do not yield any solution; otherwise, $f(\theta)$ can be found from (6.52). If there is such a ξ, similar to the proof of Proposition 6.1, one can see that $F_f = F_{ff'} = F_{ff} = 0$ and $F_{f'f'} > 0$ for each θ. Hence, via similar arguments to those in the proof of Proposition 6.1, we can argue that f is the local minimizer of (6.39). ■

As a corollary to Proposition 6.2, if θ is distributed uniformly, g is a linear function of θ, and the condition in Proposition 6.2 holds, it is concluded that the encoding function at the transmitter is linear as in the monotone case. Furthermore, once $g(\cdot)$ and $w(\cdot)$ are known, the knowledge of $\psi(\cdot)$ and $W(\cdot)$ also becomes available. Hence, $\max_{\theta\in[a,b]} (c - \psi(\theta) - f(a))/W(\theta)$ and $\min_{\theta\in[a,b]} (d - \psi(\theta) - f(a))/W(\theta)$ can easily be found in terms of $f(a)$. By adjusting the value of $f(a)$, one can determine whether the condition in (6.40) is satisfied.

Remark 6.2: Since the optimal encoding functions in Propositions 6.1 and 6.2 are local minimizers, we can compare the ECRBs achieved by these encoding functions and choose the one that achieves the lower ECRB.

Next, we discuss what happens for the multiple transmitters-single receiver and single transmitter-multiple receivers cases.

6.4 Extension to the Multiple Transmitters-Single Receiver Case

Let $f_m(\cdot)$ and $h_T^{(m)}$ denote the encoding function of the mth transmitter and the channel fading coefficient between the mth transmitter and the receiver for $1 \leq m \leq M$, respectively. Furthermore, assume that $f_m(\cdot) \in [c_m, d_m]$ for all m. Then, the received signal Y can be expressed as

$$Y = \sum_{m=1}^{M} h_T^{(m)} f_m(\theta) + h_J g(\theta) + N \tag{6.53}$$

By using similar steps and assuming that $f_m(\cdot)$'s are differentiable, it can be shown that the Fisher information, $\mathcal{I}(\theta)$, can be expressed as

$$\mathcal{I}(\theta) = \frac{\left(\sum_{m=1}^{M} h_T^{(m)} f_m'(\theta) + h_J g'(\theta)\right)^2}{\sigma^2} \tag{6.54}$$

where $f_m'(\cdot)$ denotes the derivative of $f_m(\cdot)$ for $1 \leq m \leq M$. Hence, the proposed optimization problem can be stated as

$$\min_{\{f_m\}_{m=1}^{M}} \quad \int_a^b w(\theta) \frac{\sigma^2}{\left(\sum_{m=1}^{M} h_T^{(m)} f_m'(\theta) + h_J g'(\theta)\right)^2} \, d\theta \tag{6.55a}$$

$$\text{subject to} \quad c_m \leq f_m(\theta) \leq d_m \,, \ \forall\, \theta \in [a, b] \ \text{ and } \forall m. \tag{6.55b}$$

The difficulty of solving this problem stems from the fact that we try to minimize the objective function with respect to M different functions. After solving the Euler-Lagrange equations, it is not easy to obtain a closed form solution as in Proposition 6.1, and it is unclear that the solution obtained by the Euler-Lagrange equations is a local (weak) minimizer. As the multiple transmitters-multiple receivers case is the generalization of this case, finding a closed form solution as in Proposition 6.1 for the multiple transmitters-multiple receivers

case is even harder.

6.5 Extension to the Single Transmitter-Multiple Receivers Case

In this case, assume that the transmitter broadcasts the signal $f(\theta)$ to each intended receiver. Let the number of the receivers be equal to K. Let $h_T^{(k)}$ and $h_J^{(k)}$ denote the channel fading coefficients between the transmitter and the kth receiver, and between the jammer and the kth receiver for $1 \leq k \leq K$, respectively. Hence, for $1 \leq k \leq K$, the received signal at the kth receiver, Y_k, can be expressed as

$$Y_k = h_T^{(k)} f(\theta) + h_J^{(k)} g(\theta) + N_k \tag{6.56}$$

where $N_k \sim \mathcal{N}(0, \sigma_k^2)$. Assuming N_k's are independent, one can express the conditional probability $p(\underline{Y}|\theta)$, as follows:

$$p(\underline{Y}|\theta) = \prod_{k=1}^{K} \frac{1}{\sqrt{2\pi\sigma_k^2}} \exp\left(-\frac{\left(Y_k - h_T^{(k)} f(\theta) - h_J^{(k)} g(\theta)\right)^2}{2\sigma_k^2} \right) \tag{6.57}$$

where $\underline{Y} = [Y_1\, Y_2\, \ldots\, Y_K]^\intercal$. Then, one can observe that the partial derivative of $\log p(\underline{Y}|\theta)$ with respect to θ is given by

$$\frac{\partial \log p(\underline{Y}|\theta)}{\partial \theta} = \sum_{k=1}^{K} \frac{1}{\sigma_k^2} \left(Y_k - h_T^{(k)} f(\theta) - h_J^{(k)} g(\theta)\right) \left(h_T^{(k)} f'(\theta) + h_J^{(k)} g'(\theta)\right). \tag{6.58}$$

For the notation simplicity, we can define

$$\gamma(Y_k, \theta) \triangleq \left(Y_k - h_T^{(k)} f(\theta) - h_J^{(k)} g(\theta)\right) \left(h_T^{(k)} f'(\theta) + h_J^{(k)} g'(\theta)\right) \tag{6.59}$$

Then, the Fisher information, $\mathcal{I}(\theta)$, is given by

$$\mathcal{I}(\theta) = \int \left(\sum_{k=1}^{K} \frac{\gamma(Y_k, \theta)}{\sigma_k^2} \right)^2 p(\underline{Y}|\theta)\, d\underline{Y} \tag{6.60}$$

$$= \sum_{k=1}^{K} \sum_{l=1}^{K} \int \frac{\gamma(Y_k, \theta)\gamma(Y_l, \theta)}{\sigma_k^2 \sigma_l^2} p(\underline{Y}|\theta)\, d\underline{Y} \tag{6.61}$$

Let us compute the integral $\int \frac{\gamma(Y_k,\theta)\gamma(Y_l,\theta)}{\sigma_k^2\sigma_l^2} p(\underline{Y}|\theta)\, d\underline{Y}$ for each k, l. First, consider the case of $k \neq l$. One can see that the integral expression can be manipulated as

$$\int \frac{\gamma(Y_k,\theta)\gamma(Y_l,\theta)}{\sigma_k^2\sigma_l^2} p(\underline{Y}|\theta)\, d\underline{Y} = \int \frac{\gamma(Y_k,\theta)\gamma(Y_l,\theta)}{\sigma_k^2\sigma_l^2} p(Y_k|\theta)p(Y_l|\theta) \prod_{u\neq k,l} p(Y_u|\theta)\, d\underline{Y} \tag{6.62}$$

$$= \int \frac{\gamma(Y_k,\theta)}{\sigma_k^2} p(Y_k|\theta)\, dY_k \int \frac{\gamma(Y_l,\theta)}{\sigma_l^2} p(Y_l|\theta)\, dY_l \prod_{u\neq k,l} \underbrace{\int p(Y_u|\theta)\, dY_u}_{=1} \tag{6.63}$$

$$= \int \frac{\gamma(Y_k,\theta)}{\sigma_k^2} p(Y_k|\theta)\, dY_k \int \frac{\gamma(Y_l,\theta)}{\sigma_l^2} p(Y_l|\theta)\, dY_l \tag{6.64}$$

For any k, it can be shown that

$$\int \frac{\gamma(Y_k,\theta)}{\sigma_k^2} p(Y_k|\theta)\, dY_k = 0. \tag{6.65}$$

Hence, we can conclude that $\mathcal{I}(\theta)$ is equal to the following expression:

$$\mathcal{I}(\theta) = \sum_{k=1}^{K} \int \frac{\gamma^2(Y_k,\theta)}{\sigma_k^4} p(Y_k|\theta)\, dY_k \tag{6.66}$$

$$= \sum_{k=1}^{K} \frac{\left(h_T^{(k)} f'(\theta) + h_J^{(k)} g'(\theta)\right)^2}{\sigma_k^4} \underbrace{\int \left(Y_k - h_T^{(k)} f(\theta) - h_J^{(k)} g(\theta)\right)^2 p(Y_k|\theta)\, dY_k}_{=\sigma_k^2} \tag{6.67}$$

$$= \sum_{k=1}^{K} \frac{\left(h_T^{(k)} f'(\theta) + h_J^{(k)} g'(\theta)\right)^2}{\sigma_k^2} \tag{6.68}$$

Our aim is to minimize the ECRB, i.e, to minimize the integral expression $\int_a^b w(\theta) \frac{1}{\mathcal{I}(\theta)}\, d\theta$. Therefore, we can formulate the proposed optimization problem as follows:

$$\min_{f} \qquad \int_a^b w(\theta) \frac{1}{\sum_{k=1}^{K} \frac{\left(h_T^{(k)} f'(\theta) + h_J^{(k)} g'(\theta)\right)^2}{\sigma_k^2}}\, d\theta \tag{6.69a}$$

$$\text{subject to} \quad c \leq f(\theta) \leq d\,, \ \forall\, \theta \in [a,b]\,. \tag{6.69b}$$

Let H_T, H_{TJ}, and H_J be defined as

$$H_T \triangleq \sum_{k=1}^{K} \left(\frac{h_T^{(k)}}{\sigma_k}\right)^2,\ H_{TJ} \triangleq \sum_{k=1}^{K} \frac{2h_T^{(k)} h_J^{(k)}}{\sigma_k^2} \text{ and } H_J \triangleq \sum_{k=1}^{K} \left(\frac{h_J^{(k)}}{\sigma_k}\right)^2. \tag{6.70}$$

As all the channel fading coefficients and the variances are assumed to be known, H_T, H_{TJ}, and H_J are known. Then, we can reformulate the proposed optimization problem as follows:

$$\min_{f} \quad \int_a^b w(\theta) \frac{\sigma^2}{H_T f'(\theta)^2 + H_{TJ} f'(\theta) g'(\theta) + H_J g'(\theta)^2} \, d\theta \tag{6.71a}$$

$$\text{subject to} \quad c \leq f(\theta) \leq d \,, \; \forall \, \theta \in [a, b] \tag{6.71b}$$

It is noted that this problem is in a very similar form to the optimization problem described in (6.7). In (6.7), a second-degree polynomial with respect to $f'(\cdot)$ appears in the denominator of the integrand, too. Hence, via similar techniques as in the proof of the Proposition 6.1, we can characterize the optimal encoding strategy for the problem in (6.71) above.

6.6 Numerical Results and Conclusions

In this section, a numerical example is presented when parameter θ is uniformly distributed between 0 and 1; that is, $\Lambda = [a, b]$ with $a = 0$ and $b = 1$. In other words, $w(\theta) = 1$ if $\theta \in [0, 1]$ and $w(\theta) = 0$ otherwise. We restrict our search space to strictly monotone increasing mappings for the encoding function $f(\cdot)$ at the transmitter. Also, two different encoding functions are considered for the jammer as $g(\theta) = \theta$ and $g(\theta) = \theta^2$. Hence, $g(\theta) \in \Gamma = [k, l]$ with $k = 0$ and $l = 1$. In addition, it is assumed that the range of the encoding function $f(\cdot)$ is given by $[0, 1]$. In the simulations, ϵ in (6.19) is set to 0.001 and the variance of N in (6.1) is given by $\sigma^2 = 1$.

In Figure 6.2, the optimal encoding functions, $f(\theta)$, are plotted for $g(\theta) = \theta$ and $g(\theta) = \theta^2$ when $h_T/h_J \in \{0.01, 0.1, 1, 10, 100\}$. It is observed that $f(\theta) = \theta$ regardless of the value of h_T/h_J when $g(\theta) = \theta$; that is, $f(\theta)$ is also linear in accordance with Corollary 1. When $g(\theta) = \theta^2$ and $h_T = h_J$, it is known via (6.20) and (6.21) that

$$f'(\theta) = \begin{cases} \epsilon, & \theta \in S \\ \nu - 2\theta, & \text{if } \theta \in [0, 1] \setminus S \end{cases} \tag{6.72}$$

for some $\nu \in \mathbb{R}$. By choosing $\nu = 2$ and $S = \emptyset$, we obtain the desired solution. Hence, the optimal encoding function is given by $f(\theta) = 2\theta - \theta^2$ in that case, as can be verified from

Figure 6.2. It is also noted that as h_T gets significantly larger than h_J, the optimal encoding function converges to the linear one. This is intuitive since it is known via [90, Prop.1] that in the absence of jamming, the optimal encoding function is a linear mapping. For comparison purposes, we consider the encoding function in [90], which is optimal in the absence of jamming (and would be used if the transmitter were unaware of jamming). In that case, the encoding function, denoted by $\tilde{f}(\theta)$, has the following derivative [90]:

$$\tilde{f}'(\theta) = \frac{(d-c)w(\theta)}{\int_a^b w(\theta)^{1/3}\, d\theta}. \tag{6.73}$$

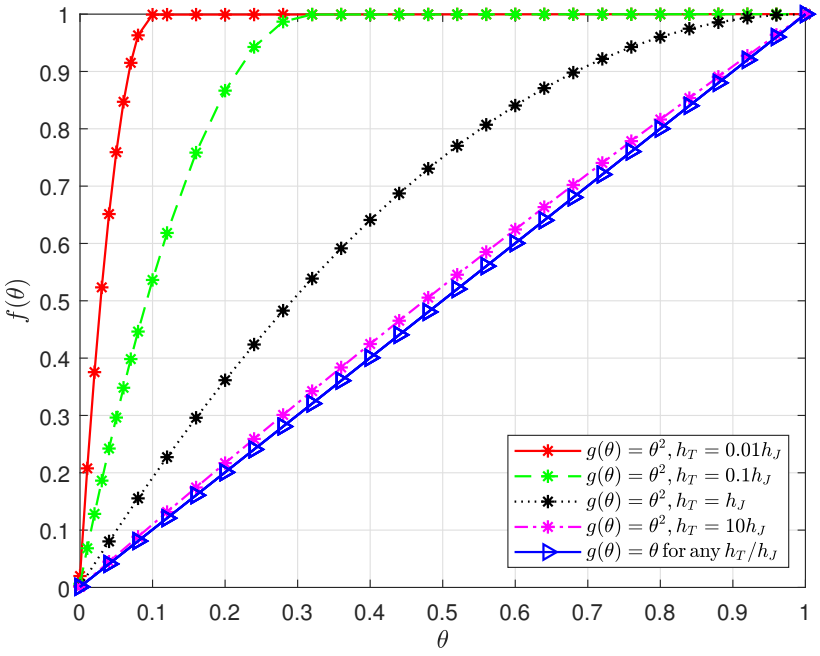


Figure 6.2: $f(\theta)$ versus θ for two different encoding functions of jammer when $h_T/h_J \in \{0.01, 0.1, 1, 10, 100\}$.

In Figure 6.3, the ECRB values achieved by $f(\theta)$ (proposed in this work) and $\tilde{f}(\theta)$ are plotted versus h_T/h_J for $g(\theta) = \theta$ and $g(\theta) = \theta^2$. For $g(\theta) = \theta$, $f(\theta) = \tilde{f}(\theta)$; hence, the same ECRB performance is attained. For $g(\theta) = \theta^2$, the proposed encoding function leads to lower ECRB values especially for $h_T < h_J$, demonstrating the benefits of the proposed optimal encoding approach.

Also, for $h_T < h_J$, the ECRB values are lower for the case of $g(\theta) = \theta$ than the case with $g(\theta) = \theta^2$. We also observe that, for $g(\theta) = \theta$ and h_T is much smaller than h_J, ECRB values

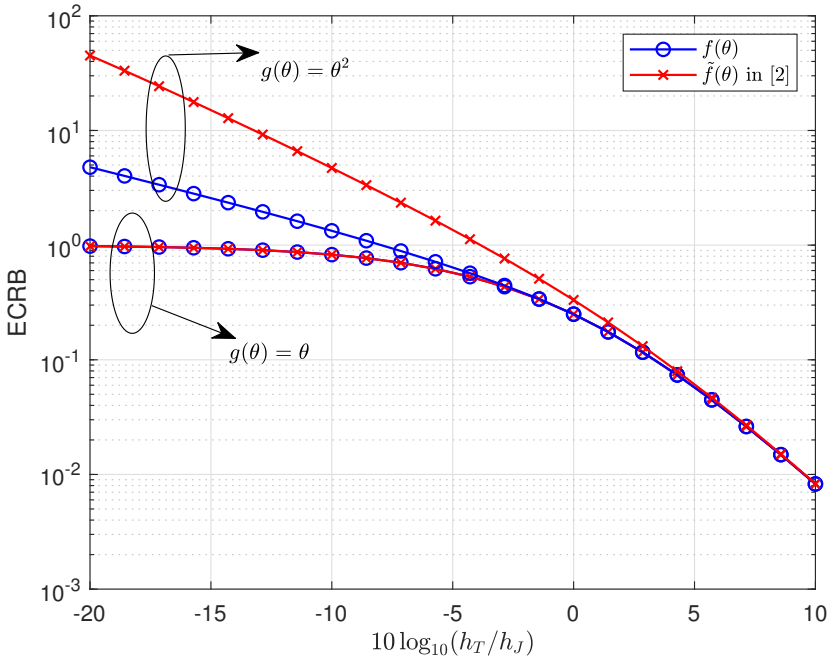


Figure 6.3: ECRB versus $10\log_{10}(h_T/h_J)$ for two different jammer encoding functions.

are lower than the case $g(\theta) = \theta^2$. This means that the linear mapping at the jammer is not as destructive for the ECRB performance at the receiver as the nonlinear one in this scenario. The reason is that when $g(\theta) = \theta$, as we observe from the Figure 6.2, the optimal encoding function $f(\theta) = \theta$. In other words, when jammer chooses $g(\theta) = \theta$, transmitter benefits from this mapping. On the other hand, when $g(\theta) = \theta^2$, transmitter needs to act differently than the jammer in order to remove the destructive effects introduced by the jammer. Moreover, when h_T is significantly larger than h_J, all the ECRB values converge since the signal component due to the transmitter becomes dominant at the receiver and the encoding functions become the same as seen in Figure 6.2. In conclusion, the proposed optimal encoding approach can lead to improved estimation performance in the presence of jamming.

Chapter 7

Conclusion and Future Work

In this dissertation, estimation theoretic analyses of location secrecy and RIS-aided localization under hardware impairments have been presented. First, in Chapter 2, a wireless localization network consisting of eavesdropper and jammer nodes has been considered. For the considered network, optimal selection strategies of eavesdropper and jammer nodes have been investigated. We have first formulated the eavesdropper selection problem. The CRLB related to the estimation of the target node position by eavesdropper nodes has been selected as the performance metric. This CRLB has been derived, and its analytical properties including monotonicity and convexity have been examined. We have proved that the CRLB is a convex function of the eavesdropper selection vector. After relaxing the integer constraints, we have approximated the eavesdropper selection problem by a convex problem. Then, we have formulated the jammer selection problem in which jammer nodes aim to degrade the localization accuracy of the network as much as possible. We have used a CRLB expression from the literature as the performance metric, and we have analyzed its convexity and monotonicity properties with respect to the jammer selection vector. After these analyses and relaxation of the integer constraints, we have approximated the jammer selection problem by a convex problem, too. Then, by combining the results obtained for the eavesdropper selection problem and the jammer selection problem, we have formulated the joint eavesdropper and jammer selection problem. We have proposed some algorithms for solving these problems, and simulation results have been presented to examine performance of the proposed algorithms. Numerical results have shown that the proposed algorithms perform very

closely to the theoretical bounds.

In Chapter 3, we have formulated the anchor placement problem to minimize the CRLB related to estimation of target node position by anchor nodes. We have approximated the anchor placement problem as an anchor selection problem after discretization of the region where anchor nodes are allowed to be placed. Using similar analysis techniques in Chapter 2, it has been proved that after relaxing the integer constraints, the anchor selection problem becomes a convex problem. In the considered problem, anchor and target nodes have been assumed to be synchronous. However, extensions to quasi-synchronous wireless localization networks have been also examined. By conducting simulations, we have shown that the performance loss due to discretization can be mitigated by using a dense grid. Also, the proposed algorithms have provided effective solutions to the anchor placement as they have achieved the theoretical performance bounds.

As a possible future work, we can come up with game-theoretic formulations by combining the works presented in Chapter 2 and Chapter 3. That is, placement games among the anchor nodes and adverserial nodes (eavesdropper and jammer) can be formulated. For a given anchor placement or selection strategy, we have already characterized the optimal eavesdropper and jammer selection strategies and vice versa. Whether this game admits any Nash equilibrium or not can be considered in future studies.

In Chapters 4 and 5, RIS-aided localization under hardware impairments has been investigated. In Chapter 4, RIS-aided localization has been investigated when the perfect knowledge of RIS amplitudes is missing. In the formulation, RIS amplitudes have been assumed to be equal to one; however, in the reality, RIS amplitudes have been considered as a function of applied phase shifts based on a practical RIS circuit model [78]. First, we have analyzed the localization performance loss due to mismatch between the reality and the belief about the RIS amplitudes. To quantify this performance, we have used MCRB analysis and computed the corresponding LB. It has been shown that being unaware of the true RIS amplitude model can cause severe degradation in the localization accuracy. When the RIS amplitude model is known, but the actual parameters of the model are not known, we have derived the corresponding CRB. We also have proposed a joint localization and RIS calibration algorithm when the RIS amplitude model is known. Our proposed algorithm can calibrate the RIS model online and refine the UE location with an accuracy that

asymptotically attains the CRB.

In Chapter 5, we have investigated RIS-aided localization when RIS pixels fail independently with a certain probability denoted by p_{fail}. First, we have analyzed how detrimental pixel failures can be for localization. To quantify the effect of pixel failures, we have devised an MCRB analysis as in Chapter 4. Numerical results have suggested that even for small values of p_{fail}, the degradation could be significant. To remedy this issue, we have proposed two different joint localization and failure mask recovery algorithms. Both algorithms have reduced the performance loss due to pixel failures significantly. The successive joint localization and mask recovery algorithm has been shown to be asymptotically efficient as it attains the CRB in the high-SNR regime.

In Chapters 4 and 5, we have considered only the LoS path between the UE and the receiver. In future work, we can try to analyze multipath effects for the considered problems. Moreover, for RIS-aided localization under pixel failures, we have worked on only biased type of failures. In addition to the biased type of failure, disconnected type of failure can be also considered. As discussed at the end of Chapter 5, our analyses can be extended to the only disconnected case and the joint biased and disconnected cases as well.

In Chapter 6, we have investigated the optimal encoding strategy of the transmitter in the presence of the jammer. In the considered setting, we have used the ECRB as the performance metric. First, by using tools from the calculus of variations, we have characterized the optimal encoding strategy of the transmitter when the set of possible encoding strategies are confined to the set of monotone functions. Then, this analysis has been extended to set of non-monotone functions. Via numerical results we have shown that the proposed encoding strategy can improve the estimation performance under jamming attacks. In the formulation, we have assumed that the transmitter has the knowledge of the encoding strategy of the jammer. As a possible direction for future work, we can extend our analyses when the transmitter does not know the jammer strategy exactly, but has access to statistics of the possible jammer encoding strategies. In that scenario, while deriving the Fisher information, we need to consider averaging over possible jammer encoding functions.

Bibliography

[1] R. Zekavat and R. M. Buehrer, *Handbook of Position Location: Theory, Practice and Advances*. Wiley-IEEE Press, 1st ed., 2011.

[2] M. Z. Win, W. Dai, Y. Shen, G. Chrisikos, and H. Vincent Poor, "Network operation strategies for efficient localization and navigation," *Proc. IEEE*, vol. 106, pp. 1224–1254, July 2018.

[3] J. Jiang, G. Han, C. Zhu, Y. Dong, and N. Zhang, "Secure localization in wireless sensor networks: A survey," *J. Commun.*, vol. 6, pp. 460–470, Sep. 2011.

[4] W. Dai and M. Z. Win, "A theoretical foundation for location secrecy," in *Proc. IEEE Int. Conf. Commun. (ICC)*, pp. 1–6, May 2017.

[5] T. Zhang, X. Li, and Q. Zhang, "Location privacy protection: A power allocation approach," *IEEE Trans. Commun.*, vol. 67, pp. 748–761, Jan. 2019.

[6] S. Gezici, M. R. Gholami, S. Bayram, and M. Jansson, "Jamming of wireless localization systems," *IEEE Trans. Commun.*, vol. 64, pp. 2660–2676, June 2016.

[7] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, 2019.

[8] T. S. Rappaport, Y. Xing, O. Kanhere, S. Ju, A. Madanayake, S. Mandal, A. Alkhateeb, and G. C. Trichopoulos, "Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond," *IEEE Access*, vol. 7, pp. 78729–78757, 2019.

[9] H. Tataria, M. Shafi, A. F. Molisch, M. Dohler, H. Sjöland, and F. Tufvesson, "6G wireless systems: Vision, requirements, challenges, insights, and opportunities," *Proc. IEEE*, vol. 109, no. 7, pp. 1166–1199, 2021.

[10] A. R. Chiriyath, B. Paul, and D. W. Bliss, "Radar-communications convergence: Coexistence, cooperation, and co-design," *IEEE Trans. Cogn. Commun. Netw.*, vol. 3, no. 1, pp. 1–12, 2017.

[11] F. Liu, Y. Cui, C. Masouros, J. Xu, T. X. Han, Y. C. Eldar, and S. Buzzi, "Integrated sensing and communications: Towards dual-functional wireless networks for 6G and beyond," 2021.

[12] C. De Lima, D. Belot, R. Berkvens, A. Bourdoux, D. Dardari, M. Guillaud, M. Isomursu, E. S. Lohan, Y. Miao, A. N. Barreto, M. R. K. Aziz, J. Saloranta, T. Sanguanpuak, H. Sarieddeen, G. Seco-Granados, J. Suutala, T. Svensson, M. Valkama, B. Van Liempd, and H. Wymeersch, "Convergent communication, sensing and localization in 6G systems: An overview of technologies, opportunities and challenges," *IEEE Access*, vol. 9, pp. 26902–26925, 2021.

[13] H. Wymeersch, D. Shrestha, C. M. de Lima, V. Yajnanarayana, B. Richerzhagen, M. F. Keskin, K. Schindhelm, A. Ramirez, A. Wolfgang, M. F. de Guzman, K. Haneda, T. Svensson, R. Baldemair, and S. Parkvall, "Integration of communication and sensing in 6G: a joint industrial and academic perspective," 2021.

[14] D. K. Pin Tan, J. He, Y. Li, A. Bayesteh, Y. Chen, P. Zhu, and W. Tong, "Integrated sensing and communication in 6G: Motivations, use cases, requirements, challenges and future directions," in *Proc. 1st IEEE Int. Online Symp. Joint Commun. Sens. (JC&S)*, pp. 1–6, 2021.

[15] Q. Wu, S. Zhang, B. Zheng, C. You, and R. Zhang, "Intelligent reflecting surface-aided wireless communications: A tutorial," *IEEE Trans. Commun.*, vol. 69, no. 5, pp. 3313–3351, 2021.

[16] A. Elzanaty, A. Guerra, F. Guidi, D. Dardari, and M.-S. Alouini, "Towards 6G holographic localization: Enabling technologies and perspectives," 2021.

[17] H. Wymeersch, J. He, B. Denis, A. Clemente, and M. Juntti, "Radio localization and mapping with reconfigurable intelligent surfaces: Challenges, opportunities, and research directions," *IEEE Veh. Technol. Mag.*, vol. 15, no. 4, pp. 52–61, 2020.

[18] H. Taghvaee, A. Cabellos-Aparicio, J. Georgiou, and S. Abadal, "Error analysis of programmable metasurfaces for beam steering," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 10, no. 1, pp. 62–74, 2020.

[19] R. Sun, W. Wang, L. Chen, G. Wei, and W. Zhang, "Diagnosis of intelligent reflecting surface in millimeter-wave communication systems," *IEEE Transactions on Wireless Communications*, vol. 21, no. 6, pp. 3921–3934, 2022.

[20] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[21] W. Dai and M. Z. Win, "On protecting location secrecy," in *Proc. Int. Symp. Wireless Commun. Systems (ISWCS)*, pp. 31–36, Aug. 2017.

[22] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: A survey," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 17, pp. 197–215, Dec. 2014.

[23] S. Vadlamani, H. Medal, B. Eksioglu, and P. Li, "A bi-level programming model for the wireless network jamming placement problem," in *Proc. Industrial and Systems Eng. Res. Conf.*, Jan. 2014.

[24] S. Gezici, S. Bayram, M. N. Kurt, and M. R. Gholami, "Optimal jammer placement in wireless localization systems," *IEEE Trans. Signal Process.*, vol. 64, pp. 4534–4549, Sep. 2016.

[25] M. F. Keskin, C. Ozturk, S. Bayram, and S. Gezici, "Jamming strategies in wireless source localization systems," *IEEE Wireless Commun. Lett.*, vol. 8, pp. 1141–1145, Aug. 2019.

[26] A. Houjeij, W. Saad, and T. Bagar, "Optimal deployment of wireless small cell base stations with security considerations," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, pp. 607–612, Dec. 2014.

[27] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attack strategies and network defense policies in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 9, pp. 1119–1133, Aug. 2010.

[28] Z. Liu, H. Liu, W. Xu, and Y. Chen, "Error minimizing jammer localization through smart estimation of ambient noise," in *Proc. IEEE 9th Int. Conf.Mobile Adhoc Sensor Syst. (MASS)*, pp. 308–316, Oct. 2012.

[29] Y. Sun and X. Wang, "Jammer localization in wireless sensor networks," in *Proc. 5th Int. Conf. Wireless Commun., Netw., Mobile Comput. (WiCom)*, pp. 1–4, Sep. 2009.

[30] T. Cheng, P. Li, and S. Zhu, "Multi-jammer localization in wireless sensor networks," in *Proc. 7th Int. Conf. Comput. Intell. Secur. (CIS)*, pp. 736–740, Dec. 2011.

[31] A. Hussein, T. Rahman, and C. Y. Leow, "A survey and open issues of jammer localization techniques in wireless sensor networks," *J. Theor. Appl. Inf. Technol.*, vol. 71, pp. 293–301, Jan. 2015.

[32] J. Feng, X. Li, E. L. Pasiliao, and J. M. Shea, "Jammer placement to partition wireless network," in *Proc. GLOBECOM Workshops*, pp. 1487–1492, Dec. 2014.

[33] S. Sankararaman, K. Abu-Affash, A. Efrat, S. Bique, V. Polishchuk, S. Ramasubramanian, and M. Segal, "Optimization schemes for protective jamming," *Mobile Netw. Appl.*, vol. 19, pp. 45–60, Feb. 2014.

[34] A. D. Sezer and S. Gezici, "Power control games between anchor and jammer nodes in wireless localization networks," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 4, pp. 564–575, Sep. 2018.

[35] S. Bayram, M. F. Keskin, S. Gezici, and O. Arikan, "Optimal power allocation for jammer nodes in wireless localization systems," *IEEE Trans. Signal Process.*, vol. 65, pp. 6489–6504, Dec. 2017.

[36] A. Shankar, "Optimal jammer placement to interdict wireless network services," *M.S. Thesis, Naval Postgraduate School, Monterey, CA, USA*, 2008.

[37] C. Liu, J. Lee, and T. Q. S. Quek, "Safeguarding UAV communications against full-duplex active eavesdropper," *IEEE Trans. Wireless Commun.*, vol. 18, pp. 2919–2931, June 2019.

[38] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Trans. Signal Process.*, vol. 61, pp. 82–91, Jan. 2013.

[39] Q. Zhu, W. Saad, Z. Han, H. V. Poor, and T. Basar, "Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach," *IEEE Military Commun. Conf. (MILCOM)*, pp. 119–124, Nov. 2011.

[40] J. Isaacs, D. Klein, and J. Hespanha, "Optimal sensor placement for time difference of arrival localization," in *Proc. Joint 48th IEEE Conf. on Decision and Control and 28th Chinese Control Conf.*, pp. 7878–7884, Dec. 2009.

[41] S. Xu, Y. Ou, and X. Wu, "Optimal sensor placement for 3-D time-of-arrival target localization," *IEEE Trans. Signal Process.*, vol. 67, pp. 5018–5031, Oct. 2019.

[42] Z. Liu, W. Dai, and M. Z. Win, "Node placement for localization networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, pp. 1–6, May 2017.

[43] C. Ozturk and S. Gezici, "Anchor placement in toa based wireless localization networks via convex relaxation," in *2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, pp. 1–6, 2021.

[44] C. Ozturk and S. Gezici, "Eavesdropper selection strategies in wireless source localization networks," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, 2020.

[45] C. Ozturk and S. Gezici, "Eavesdropper and jammer selection in wireless source localization networks," *IEEE Transactions on Signal Processing*, vol. 69, pp. 4341–4356, 2021.

[46] H. Zhang, "Two-dimensional optimal sensor placement," *IEEE Trans. Syst., Man, Cybern.*, vol. 25, no. 5, pp. 781–792, 1995.

[47] D. B. Jourdan and N. Roy, "Optimal sensor placement for agent localization," in *Proc. IEEE Position, Location, and Navigation Symp. (PLANS)*, pp. 128–139, 2006.

[48] S. Martínez and F. Bullo, "Optimal sensor placement and motion coordination for target tracking," *Automatica*, vol. 42, no. 4, pp. 661 – 668, 2006.

[49] Y. Shen and M. Z. Win, "Energy efficient location-aware networks," in *Proc. IEEE Int. Conf. on Commun.*, pp. 2995–3001, 2008.

[50] A. N. Bishop, B. Fidan, B. Anderson, K. Doğançay, and P. N. Pathirana, "Optimality analysis of sensor-target localization geometries," *Automatica*, vol. 46, no. 3, pp. 479 – 492, 2010.

[51] J. Y. Zhou, J. Shi, and X. L. Qiu, "Landmark placement for wireless localization in rectangular-shaped industrial facilities," *IEEE Trans. Veh. Technol.*, vol. 59, pp. 3081 – 3090, 08 2010.

[52] W. Meng, L. Xie, and W. Xiao, "Optimality analysis of sensor-source geometries in heterogeneous sensor networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 4, pp. 1958–1967, 2013.

[53] S. Xu and K. Doğançay, "Optimal sensor placement for 3-D angle-of-arrival target localization," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 53, no. 3, pp. 1196–1211, 2017.

[54] W. Bai, R. Iyer, K. Wei, and J. Bilmes, "Algorithms for optimizing the ratio of submodular functions," in *Proc. Int. Conf. on Mach. Learn.*, p. 2751–2759, 2016.

[55] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116753–116773, 2019.

[56] C. Pan, H. Ren, K. Wang, J. F. Kolb, M. Elkashlan, M. Chen, M. Di Renzo, Y. Hao, J. Wang, A. L. Swindlehurst, X. You, and L. Hanzo, "Reconfigurable intelligent surfaces for 6G systems: Principles, applications, and research directions," *IEEE Commun. Mag.*, vol. 59, no. 6, pp. 14–20, 2021.

[57] X. Yuan, Y.-J. A. Zhang, Y. Shi, W. Yan, and H. Liu, "Reconfigurable-intelligent-surface empowered wireless communications: Challenges and opportunities," *IEEE Wireless Commun.*, vol. 28, no. 2, pp. 136–143, 2021.

[58] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4157–4170, 2019.

[59] D. Dardari, N. Decarli, A. Guerra, and F. Guidi, "LOS/NLOS near-field localization with a large reconfigurable intelligent surface," *IEEE Trans. Wireless Commun.*, pp. 1–1, 2021.

[60] Z. Yang, M. Chen, W. Saad, W. Xu, M. Shikh-Bahaei, H. V. Poor, and S. Cui, "Energy-efficient wireless communications with distributed reconfigurable intelligent surfaces," *IEEE Trans. Wireless Commun.*, vol. 21, no. 1, pp. 665–679, 2022.

[61] B. Di, H. Zhang, L. Song, Y. Li, Z. Han, and H. V. Poor, "Hybrid beamforming for reconfigurable intelligent surface based multi-user communications: Achievable rates with limited discrete phase shifts," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1809–1822, 2020.

[62] C. Huang, R. Mo, and C. Yuen, "Reconfigurable intelligent surface assisted multiuser MISO systems exploiting deep reinforcement learning," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1839–1850, 2020.

[63] H. Guo, Y.-C. Liang, J. Chen, and E. G. Larsson, "Weighted sum-rate maximization for reconfigurable intelligent surface aided wireless networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 5, pp. 3064–3076, 2020.

[64] Z. Zhou, N. Ge, Z. Wang, and L. Hanzo, "Joint transmit precoding and reconfigurable intelligent surface phase adjustment: A decomposition-aided channel estimation approach," *IEEE Trans. Commun.*, vol. 69, no. 2, pp. 1228–1243, 2021.

[65] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5394–5409, 2019.

[66] M.-M. Zhao, A. Liu, and R. Zhang, "Outage-constrained robust beamforming for intelligent reflecting surface aided wireless communication," *IEEE Trans. Signal Process.*, vol. 69, pp. 1301–1316, 2021.

[67] S. Hu, F. Rusek, and O. Edfors, "Beyond massive MIMO: The potential of positioning with large intelligent surfaces," *IEEE Trans. Signal Process.*, vol. 66, no. 7, pp. 1761–1774, 2018.

[68] K. Keykhosravi, M. F. Keskin, G. Seco-Granados, and H. Wymeersch, "SISO RIS-enabled joint 3D downlink localization and synchronization," in *IEEE Int. Conf. Commun.*, pp. 1–6, 2021.

[69] A. Elzanaty, A. Guerra, F. Guidi, and M.-S. Alouini, "Reconfigurable intelligent surfaces for localization: Position and orientation error bounds," *IEEE Trans. Signal Process.*, vol. 69, pp. 5386–5402, 2021.

[70] Z. Abu-Shaban, K. Keykhosravi, M. F. Keskin, G. C. Alexandropoulos, G. Seco-Granados, and H. Wymeersch, "Near-field localization with a reconfigurable intelligent surface acting as lens," in *IEEE Int. Conf. Commun.*, pp. 1–6, 2021.

[71] O. Rinchi, A. Elzanaty, and M.-S. Alouini, "Compressive near-field localization for multipath RIS-aided environments," *IEEE Commun. Lett.*, pp. 1–1, 2022.

[72] F. Guidi and D. Dardari, "Radio positioning with EM processing of the spherical wavefront," *IEEE Trans. Wireless Commun.*, vol. 20, no. 6, pp. 3571–3586, 2021.

[73] M. Rahal, B. Denis, K. Keykhosravi, B. Uguen, and H. Wymeersch, "RIS-enabled localization continuity under near-field conditions," in *Proc. IEEE 22nd Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, pp. 436–440, 2021.

[74] A. Guerra, F. Guidi, D. Dardari, and P. M. Djurić, "Near-field tracking with large antenna arrays: Fundamental limits and practical algorithms," *IEEE Trans. Signal Process.*, vol. 69, pp. 5723–5738, 2021.

[75] M. Rahal, B. Denis, K. Keykhosravi, M. F. Keskin, B. Uguen, and H. Wymeersch, "Constrained RIS phase profile optimization and time sharing for near-field localization," 2022.

[76] Z. Wang, Z. Liu, Y. Shen, A. Conti, and M. Z. Win, "Location awareness in beyond 5G networks via reconfigurable intelligent surfaces," *IEEE J. Sel. Areas Commun.*, pp. 1–1, 2022.

[77] K. Keykhosravi and H. Wymeersch, "Multi-RIS discrete-phase encoding for interpath-interference-free channel estimation," 2021.

[78] S. Abeywickrama, R. Zhang, Q. Wu, and C. Yuen, "Intelligent reflecting surface: Practical phase shift model and beamforming optimization," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5849–5863, 2020.

[79] P. Xu, G. Chen, Z. Yang, and M. D. Renzo, "Reconfigurable intelligent surfaces-assisted communications with discrete phase shifts: How many quantization levels are required to achieve full diversity?," *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 358–362, 2021.

[80] G. Gradoni and M. Di Renzo, "End-to-end mutual coupling aware communication model for reconfigurable intelligent surfaces: An electromagnetic-compliant approach based on mutual impedances," *IEEE Wireless Commun. Lett.*, vol. 10, no. 5, pp. 938–942, 2021.

[81] W. Wang and W. Zhang, "Joint beam training and positioning for intelligent reflecting surfaces assisted millimeter wave communications," *IEEE Trans. Wireless Commun.*, vol. 20, no. 10, pp. 6282–6297, 2021.

[82] C. Ozturk, M. F. Keskin, H. Wymeersch, and S. Gezici, "On the impact of hardware impairments on RIS-aided localization," in *IEEE Int. Conf. Commun.*, 2022.

[83] C. Ozturk, M. F. Keskin, H. Wymeersch, and S. Gezici, "Ris-aided near-field localization under phase-dependent amplitude variations," *arXiv preprint arXiv:2204.12783*, 2022.

[84] C. D. Richmond and L. L. Horowitz, "Parameter bounds on estimation accuracy under model misspecification," *IEEE Trans. Signal Process.*, vol. 63, no. 9, pp. 2263–2278, 2015.

[85] S. Fortunati, F. Gini, M. S. Greco, and C. D. Richmond, "Performance bounds for parameter estimation under misspecified models: Fundamental findings and applications," *IEEE Signal Process. Mag.*, vol. 34, no. 6, pp. 142–157, 2017.

[86] M. E. Eltayeb, T. Y. Al-Naffouri, and R. W. Heath, "Compressive sensing for millimeter wave antenna array diagnosis," *IEEE Transactions on Communications*, vol. 66, no. 6, pp. 2708–2721, 2018.

[87] B. Sun, C. Wu, J. Shi, H.-L. Ruan, and W.-Q. Ye, "Direction-of-arrival estimation under array sensor failures with ULA," *IEEE Access*, vol. 8, pp. 26445–26456, 2020.

[88] S. Ma, J. Li, X. Bu, and J. An, "Joint diagnosis of RIS and BS for RIS-aided millimeter-wave system," *Electronics*, vol. 10, no. 20, 2021.

[89] B. Li, Z. Zhang, Z. Hu, and Y. Chen, "Joint array diagnosis and channel estimation for RIS-aided mmwave MIMO system," *IEEE Access*, vol. 8, pp. 193992–194006, 2020.

[90] C. Goken and S. Gezici, "ECRB-based optimal parameter encoding under secrecy constraints," *IEEE Transactions on Signal Processing*, vol. 66, no. 13, pp. 3556–3570, 2018.

[91] C. Goken, S. Gezici, and O. Arikan, "Estimation theoretic optimal encoding design for secure transmission of multiple parameters," *IEEE Transactions on Signal Processing*, vol. 67, no. 16, pp. 4302–4316, 2019.

[92] C. Goken and S. Gezici, "Estimation theoretic secure communication via encoder randomization," *IEEE Transactions on Signal Processing*, vol. 67, no. 23, pp. 6105–6120, 2019.

[93] T. Basar, "The Gaussian test channel with an intelligent jammer," *IEEE Transactions on Information Theory*, vol. 29, no. 1, pp. 152–157, 1983.

[94] E. Akyol, K. Rose, and T. Basar, "On optimal jamming over an additive noise channel," in *52nd IEEE Conference on Decision and Control*, pp. 3079–3084, 2013.

[95] E. Akyol, K. Rose, and T. Basar, "Optimal zero-delay jamming over an additive noise channel," *IEEE Transactions on Information Theory*, vol. 61, no. 8, pp. 4331–4344, 2015.

[96] X. Gao, E. Akyol, and T. Basar, "On communication scheduling and remote estimation in the presence of an adversary as a nonzero-sum game," in *2018 IEEE Conference on Decision and Control (CDC)*, pp. 2710–2715, 2018.

[97] E. Akyol, "On optimal jamming in strategic communication," in *2019 IEEE Information Theory Workshop (ITW)*, pp. 1–5, 2019.

[98] M. Weiss and S. C. Schwartz, "On optimal minimax jamming and detection of radar signals," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-21, pp. 385–393, May 1985.

[99] Y. Shen and M. Z. Win, "Fundamental limits of wideband localization - Part I: A general framework," *IEEE Trans. Inf. Theory*, vol. 56, pp. 4956–4980, Oct. 2010.

[100] Y. Shen, W. Dai, and M. Win, "Power optimization for network localization," *IEEE/ACM Trans. Netw.*, vol. 22, pp. 1337–1350, Aug. 2014.

[101] J. Overman, "Wireless clock synchronisation for UWB positioning," *M.S. Thesis, Delft University of Technology*, Aug. 2019.

[102] C.-Y. Han, "Clock synchronization and localization for wireless sensor network," *Ph.D. Thesis, Université Paris Saclay*, Nov. 2018.

[103] H. V. Poor, *An Introduction to Signal Detection and Estimation*. New York: Springer-Verlag, 1994.

[104] Y. Qi, "Wireless geolocation in a non-line-of-sight environment," *Ph.D. Thesis, Princeton University*, Nov. 2003.

[105] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[106] S. Joshi and S. Boyd, "Sensor selection via convex optimization," *IEEE Trans. Signal Process.*, vol. 57, pp. 451–462, Feb. 2009.

[107] D. Bertsimas, D. Pachamanova, and M. Sim, "Robust linear optimization under general norms," *Oper. Res. Lett.*, vol. 32, pp. 510–516, Nov. 2004.

[108] D. Bertsimas, D. B. Brown, and C. Caramanis, "Theory and applications of robust optimization," *SIAM Review*, vol. 53, no. 3, pp. 464–501, 2011.

[109] M. F. Keskin, A. D. Sezer, and S. Gezici, "Optimal and robust power allocation for visible light positioning systems under illumination constraints," *IEEE Trans. Commun.*, vol. 67, pp. 527–542, Jan. 2019.

[110] B. Oymak, B. Dulek, and S. Gezici, "Sensor selection and design for binary hypothesis testing in the presence of a cost constraint," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 6, pp. 617–632, 2020.

[111] S. Fujishige, *Submodular Functions and Optimization*. ISSN, Elsevier Science, 2005.

[112] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1." `http://cvxr.com/cvx`, Mar. 2014.

[113] J. He, H. Wymeersch, and M. Juntti, "Channel estimation for RIS-aided mmWave MIMO systems via atomic norm minimization," *IEEE Trans. Wireless Commun.*, vol. 20, no. 9, pp. 5786–5797, 2021.

[114] Y. Zhang, J. Zhang, M. D. Renzo, H. Xiao, and B. Ai, "Performance analysis of RIS-aided systems with practical phase shift and amplitude response," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4501–4511, 2021.

[115] Q. H. Vuong, "Cramer-Rao bounds for misspecified models." `https://resolver.caltech.edu/CaltechAUTHORS:20170823-162930200`, Oct. 1986. Unpublished.

[116] S. Fortunati, F. Gini, and M. S. Greco, "Chapter 4: Parameter bounds under misspecified models for adaptive radar detection," in *Academic Press Library in Signal Processing, Volume 7* (R. Chellappa and S. Theodoridis, eds.), pp. 197–252, Academic Press, 2018.

[117] T. T. Le, K. Abed Meraim, and N. Linhtrung, "Misspecified Cramer-Rao bounds for blind channel estimation under channel order misspecification," *IEEE Trans. Signal. Process.*, pp. 1–1, 2021.

[118] F. Roemer, "Misspecified Cramer-Rao bound for delay estimation with a mismatched waveform: A case study," in *IEEE Int. Conf. Acoustics, Speech Signal Process.*, pp. 5994–5998, 2020.

[119] A. A. Cuyt, V. Petersen, B. Verdonk, H. Waadeland, and W. B. Jones, *Handbook of Continued Fractions for Special Functions*. Springer Publishing Company, Incorporated, 1 ed., 2008.

[120] C. Ozturk, C. Goken, and S. Gezici, "Parameter encoding for ecrb minimization in the presence of jamming," *IEEE Signal Processing Letters*, vol. 29, pp. 419–423, 2022.

[121] H. L. V. Trees and K. L. Bell, *Bayesian Bounds for Parameter Estimation and Nonlinear Filtering/Tracking*. Wiley-IEEE Press, 2007.

[122] I. M. Gelfand and S. V. Fomin, *Calculus of Variations*. Upper Saddle River, NJ, USA: Prentice-Hall, 1963. Revised English edition translated and edited by Richard A. Silverman.

[123] D. Liberzon, *Calculus of Variations and Optimal Control Theory: A Concise Introduction*. USA: Princeton University Press, 2011.