RELIABLE 5G SYSTEM DESIGN AND NETWORKING

By

Yuan Liang

A DISSERTATION

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

Electrical Engineering — Doctor of Philosophy

2019

ABSTRACT

RELIABLE 5G SYSTEM DESIGN AND NETWORKING

By

Yuan Liang

The upcoming fifth generation (5G) system is expected to support a variety of different devices and applications, such as ultra-reliable and low latency communications, Internet of Things (IoT) and mobile cloud computing. Reliable and effective communications lie in the core of the 5G system design. This dissertation is focused on the design and evaluation of robust 5G systems under both benign and malicious environments, with considerations on both the physical layer and higher layers.

For the physical layer, we study secure and efficient 5G transceiver under hostile jamming. We propose a securely precoded OFDM (SP-OFDM) system for efficient and reliable transmission under disguised jamming, a serious threat to 5G, where the jammer intentionally confuses the receiver by mimicking the characteristics of the authorized signal, and causes complete communication failure. We bring off a dynamic constellation by introducing secure randomness between the legitimate transmitter and receiver, and hence break the symmetricity between the authorized signal and the disguised jamming. It is shown that due to the secure randomness shared between the authorized transmitter and receiver, SP-OFDM can achieve a positive channel capacity under disguised jamming. The robustness of the proposed SP-OFDM scheme under disguised jamming is demonstrated through both theoretic and numerical analyses.

We further address the problem of finding the worst jamming distribution in terms of channel capacity for the SP-OFDM system. We consider a practical communication scenario, where the transmitting symbols are uniformly distributed over a discrete and finite alphabet, and the jamming interference is subject to an average power constraint, but may or may not have a peak power constraint. Using tools in functional analysis and complex analysis,

first, we prove the existence and uniqueness of the worst jamming distribution. Second, by analyzing the Kuhn-Tucker conditions for the worst jamming, we prove that the worst jamming distribution is discrete in amplitude with a finite number of mass points.

For the higher layers, we start with the modeling of 5G high-density heterogeneous networks. We investigate the effect of relay randomness on the end-to-end throughput in multi-hop wireless networks using stochastic geometry. We model the nodes as Poisson Point Processes and calculate the spatial average of the throughput over all potential geometrical patterns of the nodes. More specifically, for problem tractability, we first consider the simple nearest neighbor (NN) routing protocol, and analyze the end-to-end throughput so as to obtain a performance benchmark. Next, note that the ideal equal-distance routing is generally not realizable due to the randomness in relay distribution, we propose a quasi-equal-distance (QED) routing protocol. We derive the range for the optimal hop distance, and analyze the end-to-end throughput both with and without intra-route resource reuse. It is shown that the proposed QED routing protocol achieves a significant performance gain over NN routing.

Finally, we consider the malicious link detection in multi-hop wireless sensor networks (WSNs), which is an important application of 5G multi-hop wireless networks. Existing work on malicious link detection generally requires that the detection process being performed at the intermediate nodes, leading to considerable overhead in system design, as well as unstable detection accuracy due to limited resources and the uncertainty in the loyalty of the intermediate nodes themselves. We propose an efficient and robust malicious link detection scheme by exploiting the statistics of packet delivery rates only at the base stations. More specifically, first, we present a secure packet transmission protocol to ensure that except the base stations, any intermediate nodes on the route cannot access the contents and routing paths of the packets. Second, we design a malicious link detection algorithm that can effectively detect the irregular dropout at *every hop (or link)* along the routing path with guaranteed false alarm rate and low miss detection rate.

Dedicated to my family.

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my advisor, Dr. Tongtong Li, for her mentoring and support, as well as her thoughtfulness and kindness, throughout my PhD study at Michigan State University. This work would not have been possible without the help of Dr. Li. While working with Dr. Li, I learned a lot from not only her domain knowledge of research, but also her philosophy of life, which would be beneficial for my entire life.

I would like to thank Dr. Subir Biswas, Dr. Wen Li and Dr. Eric Torng for serving on my committee, and for their helpful comments and discussions. I would like to thank Dr. Jian Ren for his insightful suggestions on research.

Special thanks go to my labmates: Tianlong Song, Ahmed Alahmadi, Zhe Wang, Run Tian and Yu Zheng. It was their generous help in the past few years that made my PhD life much easier and more enjoyable.

I am blessed with a family that always supports and encourages me. I would like to express my profound gratitude to my mother for her endless love, patience, and support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

Introduction

The past few decades witnessed the evolution of mobile communication systems from the 1G analog system to the 4G Long Term Evolution (LTE) [1]. Each new generation of mobile communication brought about significant performance improvement to its predecessor. Right now, the 5G is around the corner: the standardization of 5G is expected to be completed by 2019 and the commercial deployment of 5G is planned to begin by 2020. The changes of 5G to the existing 4G LTE are not limited to a higher speed mobile access: 5G is envisaged to support a variety of different devices and communication environments, including ultra-reliable and low latency communications and massive machine type communications [2]. This versatility requirement makes the reliability under different application scenarios an essential concern in the design and evaluation of 5G systems. In this dissertation, we will consider reliable 5G system design in both the physical layer and the network layer.

1.1 Overview of 5G Systems

The main technical innovation of 5G at the physical layer and the network layer lies in the following three aspects: spectrum regulation, physical layer design and network deployment.

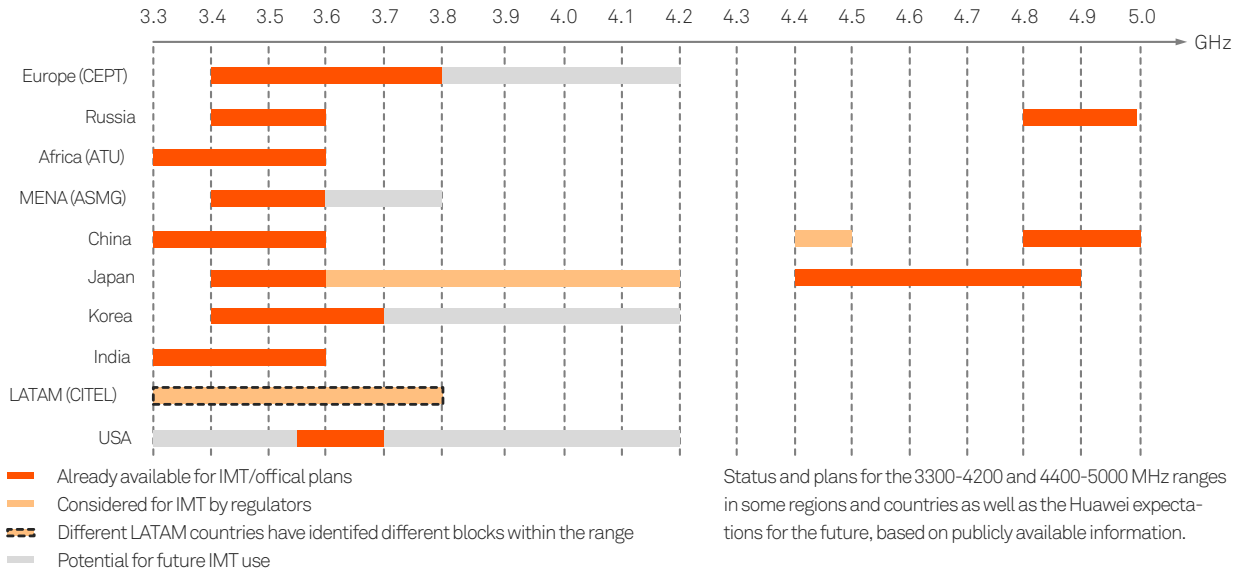


Figure 1.1: Global availability and planning of the C-band

1.1.1 Spectrum Regulation

To address the different use cases in the 5G era, three different layers of frequency bands will be utilized in the 5G systems: coverage and capacity layer, coverage layer and super data layer.

Coverage and capacity layer The coverage and capacity layer refers to the C-band, i.e., 3.3 - 4.2 and 4.4 - 5.5 GHz on the spectrum. C-band balances the coverage and capacity: compared to the higher frequency bands (e.g. millimeter-wave band), the C-band has better channel characteristics in terms of attenuation and penetration for a better coverage, while compared to the lower frequency bands in existing 4G mobile systems, C-band is able to provide wider bandwidth for a larger channel capacity. Therefore, in the introduction stage of 5G, the 3.3 - 3.8 GHz of C-band will be the primary frequency band. The global availability of C-band is shown in Figure 1.1.

Coverage layer The coverage layer utilizes low frequency bands below 2 GHz, coexisting with or reusing the frequency bands in the existing mobile communication systems. The coverage layer provides the wide-area and deep indoor coverage, which the higher frequency bands are inept at. In addition, the lower frequency bands are expected to function as the uplink channel of user equipment (UE) in 5G because of the lower data rate requirement for the uplink channel.

Super data layer The super data layer refers to the high frequency bands within the 24.25 - 86 GHz range, most of which lies in the millimeter-wave (mm-wave) band. The mm-wave bands will play a very important role in the 5G system because of the large spectrum resources they provide, which are essential for the 5G high data rate transmission. However, the mm-wave bands also pose new challenges to the system. Millimeter-wave channels experience different propagation characteristics from those in lower frequency bands. Millimeter-wave tends to be more susceptible to the attenuations from atmosphere, foliages and buildings. Meanwhile, mm-wave is not able to effectively penetrate, or diffract around different objects. All these factors greatly limit the coverage of mm-wave links, and lead to significant variations in the channels. Because of the advantages and the challenges, the mm-wave band is of special interest in the research and design of 5G systems. Among the high frequency bands, the 24.25-29.5 and 37-43.5 GHz ranges are the most promising frequencies for the early deployment of 5G mm-wave system. The availability of high frequency bands for 5G early mm-wave deployment in the leading markets is shown in Figure 1.2.

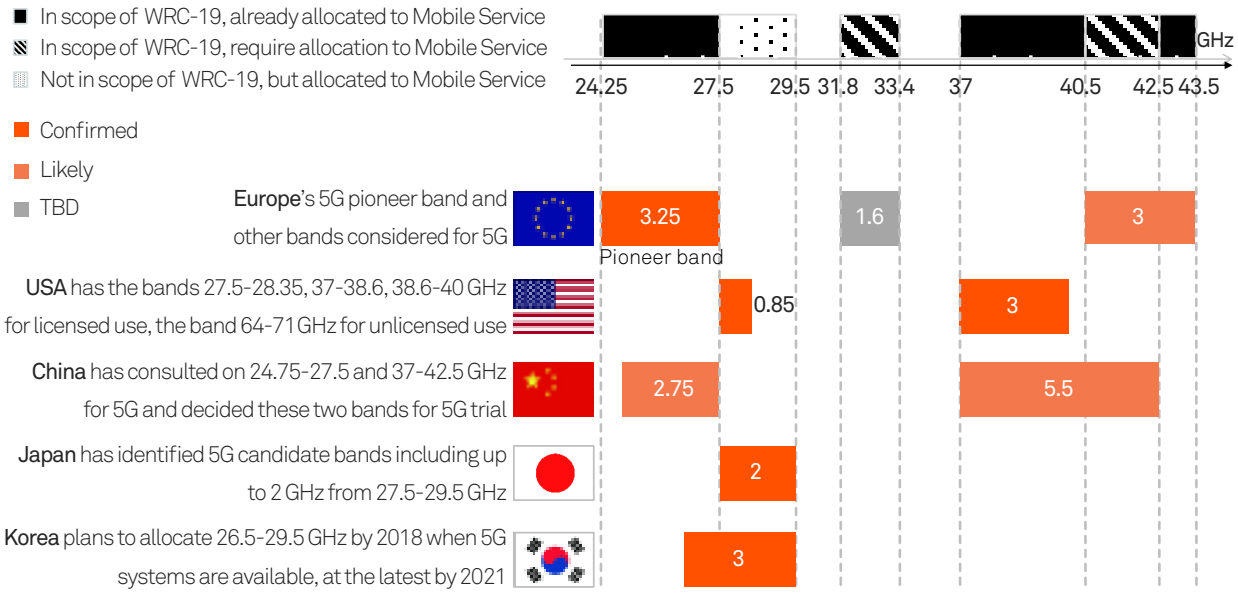


Figure 1.2: Frequency bands for early deployment of 5G mm-wave systems

Table 1.1: Physical layer specifications of selected 5G field trials

Vendor	Frequency	Bandwidth	Antenna Size	Waveform
Ericsson [3]	28 GHz	100 MHz	32*4 (BS), 8 (UE)	OFDM
Ericsson [4]	3.5 GHz	80 MHz	128 (BS), 1 (UE)	OFDM
Nokia [5]	73.5 GHz	1 GHz	64 (BS), horn antenna (UE)	OFDM
Mitsubishi	44 GHz	500 MHz	48*16 (BS), horn antenna (UE)	OFDM
NEC [6]	5.2 GHz	40 MHz	64 (BS), 2 (UE)	OFDM

1.1.2 Physical Layer Design

In the physical layer, 5G inherits the waveform of 4G system, i.e., orthogonal frequency division multiplexing (OFDM), and introduces the massive multi-input and multi-output (MIMO) techniques. The physical layer specifications of selected 5G field trials are listed in Table 1.1.

1.1.2.1 Waveforms – OFDM and others

For a wireless system, one of the most essential parts is the waveform design, which largely affects the efficiency and reliability of the proposed architecture. In the past few decades,

numerous waveform techniques were devised, while among them, orthogonal frequency division multiplexing (OFDM) emerges to be one of the most popular ones that are widely adopted in different standards, such as 4G LTE [1] and WiMAX [7]. By allowing the overlap between neighboring subcarriers, OFDM is able to provide much higher spectral efficiency than the conventional multicarrier schemes, while the orthogonality between subcarriers enables simple signal detection and receiver design. In addition, OFDM transceivers can be implemented with a low-complexity design [8], while being easily compatible with multi-input and multi-output (MIMO) techniques [9]. Considering all the advantages of OFDM, 3GPP chose OFDM as the waveform technique in the 5G new radio phase 1 standard [10].

With the aforementioned advantages, the versatility of OFDM has its own boundary. For example, OFDM relies on accurate time and frequency synchronizations between the transmitter and receiver to ensure the orthogonality between subcarriers. Such stringent requirements on synchronization may not be easily achievable for some random access applications considered in 5G [11]. In addition, OFDM signals tend to have strong side lobes on spectrum, which prohibits the application of carrier aggregation [12] in OFDM based systems. To address the limitations of OFDM, several alternative multicarrier waveforms have been proposed, such as quadrature amplitude modulation filter bank multicarrier (QAM-FBMC) [13], polar OFDM (P-OFDM) [14], Flexible Configured OFDM (FC-OFDM) [15], Universal Filtered OFDM (UF-OFDM) [16] and filtered OFDM (F-OFDM) [17]. A common ground among these newly proposed techniques is to apply certain pulse shaping filters so as to weaken the side lobes of the generated signals. However, each of these waveforms has its own limitations, such as the degradation on orthogonality or larger delay spread. Considering the different application scenarios in the 5G era, the final 5G standard should incorporate multiple waveforms to satisfy the demands in different services.

1.1.2.2 Massive MIMO

Even though mm-waves experience some unfavorable channel characteristics compared with lower frequency waves, the shorter wavelength makes it possible to deploy large scale antenna arrays at the base station, which can include hundreds of antennas. This is known as the massive MIMO system.

The large antenna array in massive MIMO provides a large spatial multiplexing gain by serving multiple users simultaneously in the same resource block. It is shown that, using massive MIMO, the channel capacity can be increased by more than 10 times over the existing systems [18], with a much higher power efficiency. Meanwhile, massive MIMO strengthens the system robustness against channel fading as it can exploit the favorable propagation property of the massive MIMO channels [19]. The beamforming techniques employed in massive MIMO not only boost the signal power at the intended user, but also weaken the possible interference to other users [18].

1.1.3 Network Deployment

5G is expected to have a much denser network deployment, e.g. more small cells, than the existing mobile communication systems. This is because of two reasons: first, an increased cell density is necessary to satisfy the demands from the increasing number of accessing devices in the 5G era, including smart sensors, smart home devices and other devices in the Internet of Things (IoT) networks; second, the limited coverage of mm-wave link requires a shorter distance between the user and base station. By offloading the traffic from macro cells to smaller cells or indoor hotspots, 5G is able to provide users with fast and seamless accesses. An illustration diagram of 5G heterogeneous network is shown in Figure 1.3.

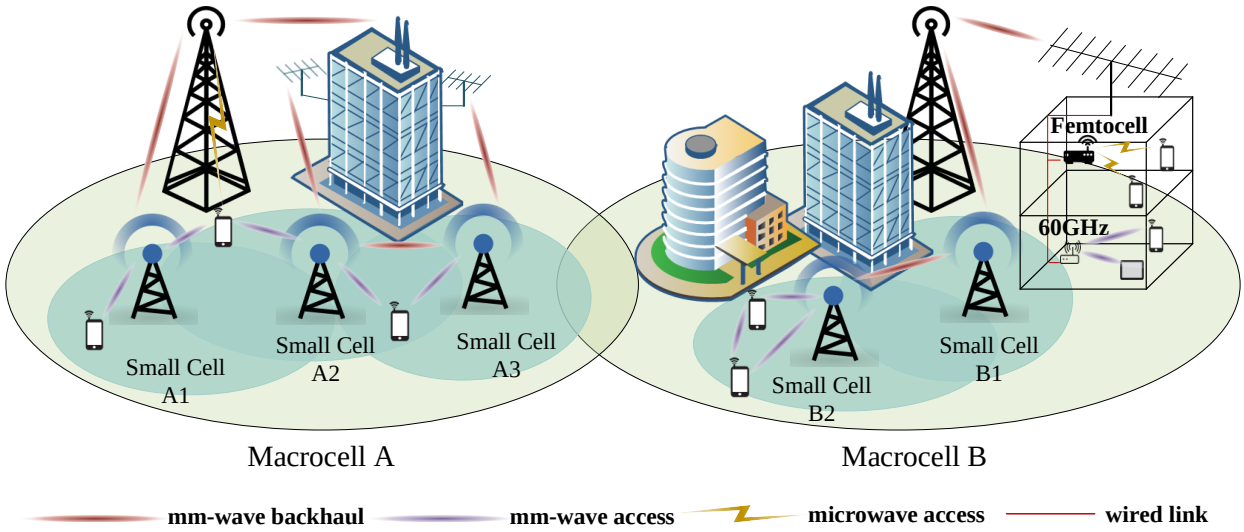


Figure 1.3: 5G heterogeneous network

The densified network structure also poses new challenges to 5G system, that is, the dense small cells will generate stronger inter-cell interference to each other. This issue can be partially alleviated by the attenuation of mm-wave signals as well as the beamforming techniques. Nevertheless, interference modeling and cancellation are still crucial problems in the design of 5G systems.

1.2 Challenges and Proposed Research Directions

1.2.1 Major Challenges in 5G System Design, Modeling and Operation

1.2.1.1 Vulnerability of OFDM under Disguised Jamming

In wireless systems, one of the most commonly used techniques for limiting the effectiveness of an opponent's communication is referred to as jamming, in which the authorized user's signal is deliberately interfered by the adversary. Along with the wide spread of various

wireless devices, especially with the advent of user configurable intelligent devices, jamming attack is no longer limited to battlefield or military related events, but has become an urgent and serious threat to civilian communications as well.

Existing jamming resistant systems mainly rely on the spread spectrum techniques [20], including both code division multiple access (CDMA) and frequency hopping (FH). Direct sequence spread spectrum, known as CDMA, spreads the transmitted signal into a large bandwidth so that the interference from jamming can be dispersed; in frequency hopping spread spectrum (FHSS), the transmitted signal hops across different frequency bands in a pseudo-random manner so that the jammer cannot locate the signal in the frequency domain. Both FH and CDMA systems gain anti-jamming features by exploiting the frequency diversity over large spectrum. However, for spectral efficiency, OFDM is unable to provide such spectral diversity to combat jamming attacks. Its very limited jamming resistance relies on the redundancy introduced by the channel coding [21–27].

In literature [28–31], jamming has widely been modeled as Gaussian interference. Based on the noise jamming model and the Shannon capacity formula, $C = B\log(1 + SNR)$, an intuitive impression is that jamming is really harmful only when the jamming power is much higher than the signal power. However, this is only partially true. More recently, it has been found that disguised jamming [32–35], where the jamming is highly correlated with the signal, and has a power level close or equal to the signal power, can be much more destructive than noise jamming; it can reduce the system capacity to zero even when the jamming power equals the signal power. Consider the following example:

$$R = S + J + N$$

where S is the authorized signal, J is the jamming interference, N is the noise independent of J and S, and R is the received signal. If the jammer is capable of eavesdropping on the symbol constellation and the codebook of the transmitter, it can simply replicate one of the sequences in the codebook of the legitimate transmitter, the receiver, then, would not be able to distinguish between the authorized sequence and the jamming sequence, resulting in a complete communication failure [36, ch 7.3].

In summary, as the major waveform in 5G systems, there is an ever increasing need on the development of secure and efficient OFDM systems that are reliable under hostile jamming, especially the destructive disguised jamming.

1.2.1.2 Spatial Randomness of Heterogeneous Networks

As we know, the densified heterogeneous networks will be the trend of 5G. Conventionally, the distribution of base stations in homogeneous networks is assumed to follow a hexagonal grid model. However, in a high density network, the nodes tend to follow a more irregular pattern considering the distribution of users and the possible geographical limitations.

In a high density network, interference level is a key factor in determining the quality of a wireless link, and the interference is largely affected by the spatial locations of neighboring nodes which transmit over the same frequency band. Considering the irregular and random spatial pattern of 5G network, the traditional hexagonal grid model can only provide a performance upper bound of the network [37]. An alternative way to measure the interference level is Monte Carlo simulation. However, simulation based method may be inefficient in practice considering the large amount of nodes in 5G network; meanwhile, it will be hard to derive an analytical relationship between different network parameters and performance metrics precisely, based solely on the simulation results.

On the other hand, considering the propagation characteristics of mm-wave and the power constraints of low-power devices, the coverage distance of wireless links will be limited in some application scenarios. Network densification provides a solution to some extent, however, it might not be cost effective to deploy dense cells in the areas where users are sparse. In addition, for the device-to-device (D2D) communication considered in 5G, end-to-end connections between devices can be established without base stations. Therefore, it is still necessary to provide long distance communications in 5G. A possible solution is multi-hop communication with relay assistance. Similar to the interference modeling, the spatial randomness of the relays will largely affect the quality of multi-hop links as it determines the distance of each hop.

In summary, for more accurate performance evaluation of heterogeneous networks, we need an effective and tractable model to characterize the spatial randomness of nodes.

1.2.1.3 Malicious Behavior Detection in Large Scale Multi-hop Wireless Networks

Large scale multi-hop wireless networks will become essential components in 5G system, e.g. smart sensor networks or IoT networks. However, compared to the single hop cellular networks, multi-hop wireless networks are more vulnerable to malicious node/link pollution, as one malicious link or node in the network can compromise the data flow passing through it originated from multiple nodes. To detect the malicious behaviors in multi-hop wireless networks, a variety of schemes and algorithms have been proposed in literature [38–43]. However, most existing detection methods require the nodes in the network either to implement extra verification in packet transmission and reception so as to prevent the occurrence of malicious behaviors, or to report additional information to the authority in the network

for malicious behavior localization. Considering the diversity and population of accessing devices in the 5G era, these methods would either increase the complexity and power consumption of the devices, or pose a significant burden on the network throughput. Hence, more efficient methods of malicious behavior detection are needed for the multi-hop wireless networks in the 5G era.

To guarantee the efficiency, the proposed malicious behavior detection method should have the following features: (i) Generality. That is, the proposed scheme should have a minimum dependency on the network deployment and the functionalities of nodes in the network. This ensures that the proposed method can be applicable to various networks. (ii) Centralized detection. That is, the detection process is mainly carried out by the authorities (e.g. the base stations) in the network. This feature minimizes the power consumption of the intermediate nodes, and reduces the communication overhead between intermediate nodes and authorities in the detection process. (iii) Non-transparency. That is, the identification process is not transparent to the intermediate nodes so that they are not aware of whether the network is detecting the malicious nodes/links or not. This feature is necessary to combat malicious nodes with intelligence, which might disguise themselves as normal nodes when they are aware of that the network is detecting the malicious nodes.

1.2.2 Proposed Research Directions

1.2.2.1 Secure OFDM System Design under Disguised Jamming

If we examine disguised jamming carefully, we can see that the main issue there is the symmetricity between the authorized signal and the jamming interference. Intuitively, to design the corresponding anti-jamming system, the main task is to break the symmetricity

between the authorized signal and the jamming interference, or make it impossible for the jammer to achieve this symmetricity. For this purpose, encryption or channel coding at the bit level will not really help, since the symmetricity actually appears at the symbol level. That is, instead of using a fixed symbol constellation, we have to introduce secure randomness to our constellation, and utilize a dynamic constellation scheme, such that the jammer can no longer mimic the authorized user's signal. At the same time, the authorized user does not have to sacrifice too much on the performance, efficiency and system complexity.

Motivated by the observations above and our previous research on anti-jamming system design [27,33–35,44], we propose a securely precoded OFDM (SP-OFDM) system for efficient and reliable transmission under disguised jamming. By integrating advanced cryptographic techniques into OFDM transceiver design, we design a dynamic constellation by introducing shared randomness between the legitimate transmitter and receiver, which breaks the symmetricity between the authorized signal and the jamming interference, and hence ensures reliable performance under disguised jamming. A remarkable feature of the proposed SP-OFDM scheme is that it achieves strong jamming resistance, but has the same high spectral efficiency as the traditional OFDM system. Moreover, the change to the physical layer transceivers is minimal, feasible and affordable.

1.2.2.2 The Worst Jamming Analysis and the Performance of SP-OFDM under the Worst Jamming

We can see that, without any secure precoding, disguised jamming is the worst jamming that can cause the deterministic coding capacity to be zero, while in the proposed SP-OFDM, disguised jamming is no longer able to nullify the communication because of the introduced secure precoding. Then an interesting question is: what would be the worst

jamming distribution that minimizes the channel capacity of SP-OFDM?

By exploiting tools in constrained functional optimization, we consider this problem in a practical wireless communication scenario, where the transmitted symbols are uniformly distributed over a finite alphabet, and the jamming interference is subject to an average power constraint, but may or may not have a peak power constraint. First, we prove the existence and uniqueness of the worst jamming distribution. Second, by analyzing the Kuhn-Tucker conditions for the worst jamming, we prove that the worst jamming distribution is discrete in amplitude with a finite number of mass points, either with or without peak power constraints. Numerical results are provided on the worst jamming distribution and the minimum channel capacity under disguised jamming. However, due to the inherent secure randomness in SP-OFDM, disguised jamming is no longer the worst jamming for SP-OFDM. In addition, SP-OFDM is able to achieve a non-zero channel capacity even under the worst jamming.

1.2.2.3 End-to-End Performance Analysis in Multi-Hop Wireless Networks using Stochastic Geometry

An effective tool to characterize the spatial randomness in wireless networks is stochastic geometry (SG), which is a very powerful mathematical and statistical framework for the modeling, analysis and design of wireless networks with random topologies and has been applied in ad hoc networks for several decades [45–49]. The basic idea is to model the nodes in network as Point Processes (PPs) and calculate the spatial averages of network performance characteristics by averaging over all potential geometrical patterns of the nodes. In [37], the authors compared the performance of a SG model with that of an actual deployed cellular network. It was shown that the theoretical results derived from SG model provide an

effective lower bound on the network performance, compared to the actual measurements.

Even though SG modeling has been widely used in literature [50], most of them were focused on the single hop performance [51, 52]. Most existing work on the multi-hop link analysis using SG either assumes a deterministic pattern of the relay nodes [53, 54] or lacks sufficient end-to-end performance analysis [55–58].

As an effort to further explore the effect of relay randomness on network performance, we investigate the end-to-end throughput of a general multi-hop route in a wireless network with randomly located relays. In contrast to most previous work in literature, we consider a two-fold spatial randomness of the multi-hop network, that is, the spatial randomness of the interferers as well as that of the relay nodes. More specifically, we model the relays as a linear Poisson PP (PPP) between the source and destination following the TDMA medium access control (MAC) protocol, and model the external interferers as an independent PPP over the whole plane, following the ALOHA MAC protocol. We focus on the end-to-end performance of the system.

For problem tractability, we start with a simple nearest neighbor routing protocol where each relay selects the nearest node along the direction to the destination as its next hop. We analyze the end-to-end throughput in a relatively *sparse* network so as to obtain a performance benchmark or lower bound. The throughput is evaluated under both conventional TDMA with fixed, uniform slot length, as well as TDMA with dynamic slot length or resource allocation; the optimal relay density is also discussed. Motivated by the observation that, while the ideal equal-distance routing generally provides the optimal network performance, it is not realizable due to the randomness in relay distribution, we propose a quasi-equal-distance (QED) routing protocol, derive the range for the optimal hop distance, and specify the selection of the optimal relays to formulate a quasi-equidistant deployment. We analyze

the end-to-end throughput of the proposed QED routing, both with and without intra-route resource reuse.

1.2.2.4 Malicious Link Detection in Wireless Sensor Networks

As we mentioned earlier, most existing methods for malicious behavior detection in multi-hop wireless networks may not be suitable for 5G networks in terms of complexity and efficiency. In this research, we develop an efficient malicious link detection scheme which is easy to implement, and causes minimum overhead on the network performance.

We consider the problem under the context of multi-hop wireless sensor networks (WSNs), which would be a major application of 5G multi-hop wireless networks. We propose a malicious link detection algorithm by exploiting the statistics of packet delivery rates at the base stations. More specifically, first, we present a secure packet transmission protocol to ensure that except the base stations, any intermediate nodes on the route cannot access the contents and routing paths of the packets. Second, we design a malicious link detection algorithm that can effectively detect the irregular dropout at *every hop (or link)* along the routing path with guaranteed false alarm rate and miss detection rate. Comparing to [59] which can detect whether a routing path is problematic, our detection method can be localized to every link. It should be pointed out that, illegal packet modification and injection of invalid packets, which essentially result in the dropout of legal packets, can be detected successfully as well. Simulation results are provided to validate the proposed approaches.

1.3 Overview of the Dissertation

This dissertation is organized as follows.

Chapter 2 proposes a securely precoded OFDM (SP-OFDM) system for efficient and reliable transmission under disguised jamming, where the jammer intentionally confuses the receiver by mimicking the characteristics of the authorized signal, and causes complete communication failure. More specifically, we bring off a dynamic constellation by introducing secure shared randomness between the legitimate transmitter and receiver, and hence break the symmetricity between the authorized signal and the disguised jamming. We analyze the channel capacities of both the traditional OFDM and SP-OFDM under hostile jamming using the arbitrarily varying channel (AVC) model. It is shown that the deterministic coding capacity of the traditional OFDM is zero under the worst disguised jamming. On the other hand, due to the secure randomness shared between the authorized transmitter and receiver, SP-OFDM can achieve a positive capacity under disguised jamming since the AVC channel corresponding to SP-OFDM is not symmetrizable. A remarkable feature of the proposed SP-OFDM scheme is that while achieving strong jamming resistance, it has the same high spectral efficiency as the traditional OFDM system. The robustness of the proposed SP-OFDM scheme under disguised jamming is demonstrated through both theoretic and numerical analyses.

Chapter 3 addresses the problem of finding the worst jamming distribution in terms of channel capacity for the proposed SP-OFDM system, so as to evaluate the performance of SP-OFDM under destructive hostile jamming. We consider a practical communication scenario, where the transmitting symbols are uniformly distributed over a discrete and finite alphabet, and the jamming interference is subject to an average power constraint, but may

or may not have a peak power constraint. By exploiting the tools in constrained functional optimization, first, we prove the existence and uniqueness of the worst jamming distribution. Second, by analyzing the Kuhn-Tucker conditions for the worst jamming, we prove that the worst jamming distribution is discrete in amplitude with a finite number of mass points, either with or without peak power constraints. We show that disguised jamming, which is the worst jamming in the traditional OFDM system, is no longer the worst jamming attack in the SP-OFDM system. In addition, with the inherent secure randomness, SP-OFDM is able to achieve a non-zero channel capacity even under the worst jamming attack. Numerical examples are provided under different scenarios to demonstrate our theoretical results.

Chapter 4 investigates the effect of relay randomness on the end-to-end throughput in multi-hop wireless networks using stochastic geometry. We model the nodes as Poisson Point Processes and calculate the spatial average of the throughput over all potential geometrical patterns of the nodes. More specifically, for problem tractability, we first start with the simple nearest neighbor (NN) routing protocol, and analyze the end-to-end throughput so as to obtain a performance benchmark. Next, note that the ideal equal-distance routing is generally not realizable due to the randomness in relay distribution, we propose a quasi-equal-distance (QED) routing protocol. We derive the range for the optimal hop distance, and select the relays to formulate a quasi-equidistant deployment. We analyze the end-to-end throughput both with and without intra-route resource reuse. Our analysis indicates that: (i) The throughput performance of the proposed QED routing can achieve a significant performance gain over that of the NN routing. As the relay intensity gets higher, the performance of QED routing converges to that of the equidistant routing. (ii) If the node intensity is a constant over the network, then intra-route resource reuse is always beneficial when the routing distance is sufficiently large. (iii) With randomly distributed relays, the

communication distance can generally be extended. However, due to the uncertainty in relay distribution, long distance communication is generally not feasible with random relays. This implies that the existence of a reasonably defined infrastructure is critical in effective long distance communication. Our analysis is demonstrated through numerical examples.

Chapter 5 considers malicious link detection in multi-hop wireless sensor networks (WSNs). Existing work on malicious link detection generally requires that the detection process being performed at the intermediate nodes, leading to considerable overhead in system design, as well as unstable detection accuracy due to limited resources and the uncertainty in the loyalty of the intermediate nodes themselves. In this chapter, we propose an efficient and robust malicious link detection scheme by exploiting the statistics of packet delivery rates only at the base stations. More specifically, first, we present a secure packet transmission protocol to ensure that except the base stations, any intermediate nodes on the route cannot access the contents and routing paths of the packets. Second, we design a malicious link detection algorithm that can effectively detect the irregular dropout at every hop (or link) along the routing path. We prove that the proposed algorithm has guaranteed false alarm rate and low miss detection rate. Simulation results are provided to validate the proposed approaches.

Chapter 6 summarizes the contributions and concludes the dissertation. An outline of future work is also provided.

Chapter 2

Secure OFDM System Design under Disguised Jamming

In this chapter, we propose a securely precoded OFDM (SP-OFDM) system for efficient and reliable transmission under disguised jamming, where the jammer intentionally confuses the receiver by mimicking the characteristics of the authorized signal, and causes complete communication failure. More specifically, we bring off a dynamic constellation by introducing secure randomness between the legitimate transmitter and receiver, and hence break the symmetricity between the authorized signal and the disguised jamming. We analyze the channel capacities of both the traditional OFDM and SP-OFDM under hostile jamming using the arbitrarily varying channel (AVC) model. It is shown that the deterministic coding capacity of the traditional OFDM is zero under the worst disguised jamming. On the other hand, due to the secure randomness shared between the authorized transmitter and receiver, SP-OFDM can achieve a positive capacity under disguised jamming since the AVC channel corresponding to SP-OFDM is not symmetrizable. A remarkable feature of the proposed SP-OFDM scheme is that while achieving strong jamming resistance, it has the same high spectral efficiency as the traditional OFDM system. The robustness of the proposed SP-OFDM scheme under disguised jamming is demonstrated through both theoretic and numerical analyses.

2.1 Introduction

Orthogonal frequency division multiplexing (OFDM), due to its high spectral efficiency and robustness under fading channels, has been widely used in modern high speed multimedia communication systems [9], such as LTE and WiMax. However, unlike the spread spectrum techniques [20], OFDM mainly relies on channel coding for communication reliability under hostile jamming, and has very limited built-in resilience against jamming attacks [21–27]. For example, in [21], the bit error rate (BER) performance of the traditional OFDM was explored under full-band and partial band Gaussian jamming, as well as multitone jamming. It was shown that OFDM is quite fragile under jamming, as BER can go above 10^{-1} when the jamming power is the same as the signal power. In [24–26], the jamming attacks aiming at the pilots in OFDM systems were studied. It was shown that when the system standard is public and no encryption is applied to the transmitted symbol sequence, pilot attacks can completely nullify the channel estimation and synchronization of OFDM, and hence result in complete communication failure. Most existing work [21, 22, 26] has been focused on the jamming attacks which damage OFDM by minimizing the signal-to-interference power ratio (SIR). In this chapter, we identify the threat to OFDM from the disguised jamming: when the jamming interference is also OFDM modulated, the receiver can easily be deceived into synchronizing with the jamming interference instead of the legitimate signal, hence paralyzing the legitimate transmission.

In [23], the anti-jamming performance of Frequency Hopped (FH) OFDM system was explored. Like the traditional FH system, this approach achieves jamming resistance through large frequency diversity and sacrifices the spectral efficiency of OFDM. In [27], a collision-free frequency hopping (CFFH) scheme was proposed, where the basic idea was to randomize

the jamming interference through frequency domain interleaving based on secure, collision-free frequency hopping. The most significant feature of CFFH based OFDM is that it is very effective under partial band jamming, and at the same time, has the same spectral efficiency as the original OFDM. However, CFFH based OFDM is still fragile under *disguised jamming* [33–35, 60].

To combat disguised jamming in OFDM systems, a precoding scheme was proposed in [35], where extra redundancy is introduced to achieve jamming resistance. However, lack of plasticity in the precoding scheme results in inadequate reliability under cognitive disguised jamming. As OFDM being identified as a major modulation technique for the 5G systems, there is an ever increasing need on the development of secure and efficient OFDM systems that are reliable under hostile jamming, especially the destructive disguised jamming.

In this chapter, we propose a securely precoded OFDM (SP-OFDM) system for efficient and reliable transmission under disguised jamming. By integrating advanced cryptographic techniques into OFDM transceiver design, we design a dynamic constellation by introducing shared randomness between the legitimate transmitter and receiver, which breaks the symmetricity between the authorized signal and the jamming interference, and hence ensures reliable performance under disguised jamming. More specifically, the main contributions of this chapter can be summarized as follows:

- We design a highly secure and efficient OFDM system under disguised jamming, named securely precoded OFDM (SP-OFDM), by exploiting secure symbol-level precoding basing on phase randomization. The basic idea is to randomize the phase of transmitted symbols using the secure PN sequences generated from the Advanced Encryption Standard (AES) algorithm. The security is guaranteed by the secret key shared only

between the legitimate transmitter and receiver. While SP-OFDM achieves strong jamming resistance, it does not introduce too much extra coding redundancy into the system and can achieve roughly the same spectral efficiency as the traditional OFDM system.

- We identify the vulnerability of the synchronization algorithm in the original OFDM system under disguised jamming, and propose a secure synchronization scheme for SP-OFDM which is robust against disguised jamming. In the proposed synchronization scheme, we design an encrypted cyclic prefix (CP) for SP-OFDM, and the synchronization algorithm utilizes the encrypted CP as well as the precoded pilot symbols to estimate time and frequency offsets in the presence of jamming.

- We analyze the channel capacity of the traditional OFDM and the proposed SP-OFDM under hostile jamming using the arbitrarily varying channel (AVC) model. It is shown that the deterministic coding capacity of the traditional OFDM is zero under the worst disguised jamming. At the same time, we prove that with the secure randomness shared between the authorized transmitter and receiver, the AVC channel corresponding to SP-OFDM is not symmetrizable, and hence SP-OFDM can achieve a positive capacity under disguised jamming. Note that the authorized user aims to maximize the capacity while the jammer aims to minimize the capacity, we show that the maximin capacity for SP-OFDM under hostile jamming is given by $C = \log\left(1 + \frac{P_S}{P_J + P_N}\right)$ bits/symbol, where P_s denotes the signal power, P_J the jamming power and P_N the noise power.

Numerical examples are provided to demonstrate the effectiveness of the proposed system under disguised jamming and channel fading. Potentially, SP-OFDM is a promising modulation scheme for high speed transmission under hostile environments. Moreover, it

should be pointed out that the secure precoding scheme proposed in this chapter can also be applied to modulation techniques other than OFDM.

The rest of this chapter is organized as follows. The design of the proposed SP-OFDM system is described in Section 2.2. The synchronization procedure of SP-OFDM is presented in Section 2.3. The symmetricity analysis and capacity evaluation of SP-OFDM are presented in Section 2.4. Numerical examples are provided in Section 2.5 and we conclude in Section 2.6.

2.2 Secure OFDM System Design under Disguised Jamming

In this section, we introduce the proposed anti-jamming OFDM system with secure precoding and decoding, named as securely procoded OFDM (SP-OFDM).

2.2.1 Transmitter Design with Secure Precoding

The block diagram of the proposed system is shown in Fig. 2.1. Let N_c be the number of subcarriers in the OFDM system and Φ the alphabet of transmitted symbols. For $i = 0, 1, \cdots, N_c - 1$ and $k \in \mathbb{Z}$, let $S_{k,i} \in \Phi$ denote the symbol transmitted on the i-th carrier of the k-th OFDM block[1]. We denote the symbol vector of the k-th OFDM block by $\boldsymbol{S}_k = [S_{k,0}, S_{k,1}, \cdots, S_{k,N_c-1}]^T$. The input data stream is first fed to the channel encoder, mapped to the symbol vector $\boldsymbol{S}_k$, and then fed to the proposed symbol-level secure precoder.

As pointed out in [34, 44, 61, 62], a key enabling factor for reliable communication under

[1]In literature, the term *OFDM symbol* is often used to denote the symbol block transmitted in one OFDM symbol period. In this chapter, to avoid the ambiguity with the data symbols transmitted at each subcarrier, we choose to use the term *OFDM block* instead.

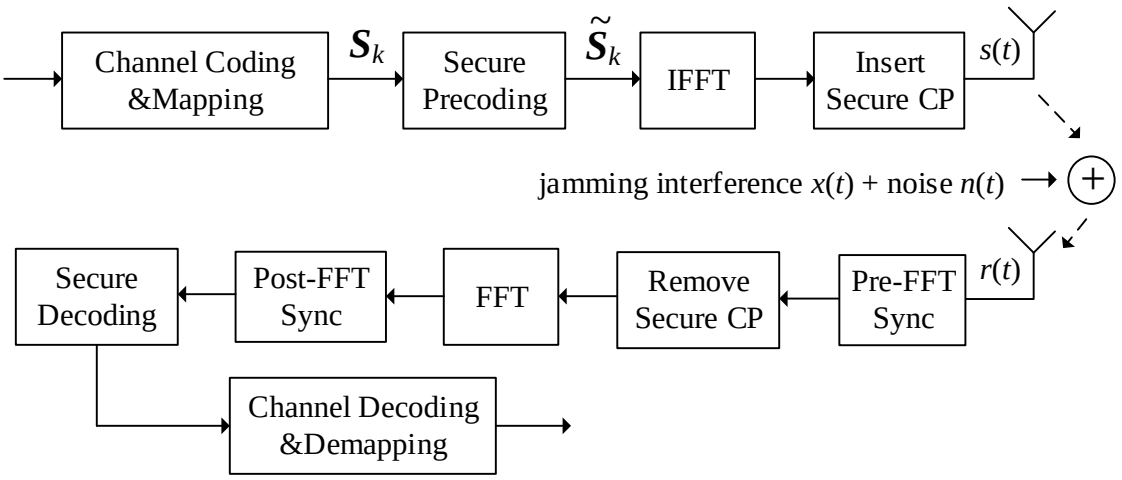


Figure 2.1: Anti-jamming OFDM design through secure precoding and decoding.

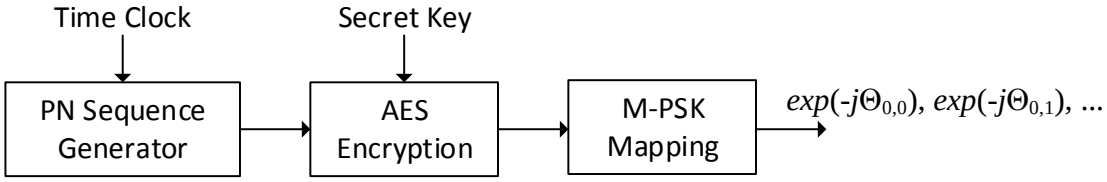


Figure 2.2: Secure phase shift generator

disguised jamming is to introduce shared randomness between the transmitter and receiver, such that the symmetry between the authorized signal and the jamming interference is broken. To maintain full spectral efficiency of the traditional OFDM system, the precoding is performed by multiplying an *invertible* $N_c \times N_c$ precoding matrix $\boldsymbol{P}_k$ to the symbol vector $\boldsymbol{S}_k$, i.e.,

$$\tilde{\boldsymbol{S}}_k = \boldsymbol{P}_k \mathbf{S}_k. \tag{2.1}$$

In this chapter, we design the precoding matrix $\boldsymbol{P}_k$ to be a diagonal matrix as

$$\boldsymbol{P}_k = diag(e^{-j\Theta_{k,0}}, e^{-j\Theta_{k,1}}, \cdots, e^{-j\Theta_{k,N_c-1}}). \tag{2.2}$$

That is, a random phase shift is applied to each transmitted symbol; more specifically, for

$i = 0, 1, \cdots, N_c - 1$ and $k \in \mathbb{Z}$, a random phase shift $-\Theta_{k,i}$ is applied to the symbol transmitted on the i-th carrier of the k-th OFDM block. The phase shift changes randomly and independently across sub-carriers and OFDM blocks, and is encrypted so that the jammer has no access to it. More specifically, $\{\Theta_{k,i}\}$ is generated through a secure phase shift generator as shown in Fig. 2.2. The secure phase shift generator consists of three parts: (i) a pseudo-noise (PN) sequence generator; (ii) an Advanced Encryption Standard (AES) [63] encryption module; and (iii) an M-PSK mapper.

The *PN sequence generator* generates a pseudo-random sequence, which is then encrypted with AES. The encrypted sequence is further converted to PSK symbols using an M-PSK mapper, where M is a power of 2, and every $\log_2 M$ bits are converted to a PSK symbol. To facilitate the synchronization process, the PN sequence generator is initialized in the following way: each party is equipped with a global time clock, and the PN sequence generators are reinitialized at fixed intervals. The new state for reinitialization, for example, can be the elapsed time after a specific reference epoch in seconds for the time being, which is public. As the initial state changes with each reinitialization, no repeated PN sequence will be generated. The security, as well as the randomness of the generated phase shift sequence, are guaranteed by the AES encryption algorithm [63], for which the secret encryption key is only shared between the authorized transmitter and receiver. Hence, the phase shift sequence is random and unaccessible for the jammer. The resulted symbol vector from the secure precoding, $\tilde{\boldsymbol{S}}_k$, is then used to generate the body of OFDM block through IFFT, whose duration is T_s.

In OFDM transceiver design, the synchronization module plays a crucial role: OFDM requires both accurate time and frequency synchronization to avoid inter-symbol interference (ISI) and inter-carrier interference (ICI). In SP-OFDM, we propose a cyclic prefix (CP) based

synchronization algorithm, as in traditional OFDM. However, SP-OFDM differs in that its CP is encrypted to ensure the security under disguised jamming.

2.2.2 Cyclic Prefix Design with Secure Precoding

In traditional OFDM, CP has three major functions: (i) eliminating the ISI between neighboring blocks; (ii) converting the linear convolution of OFDM block body with the channel impulse response into circular convolution under multi-path channel fading; and (iii) eliminating the ICI introduced by multipath propagation. As CP is a copy of the tail of OFDM block body, we can calculate the correlation between CP and the tail of OFDM block to estimate the starting point of each OFDM block [64] when disguised jamming is absent.

However, as to be shown in Section 2.3, the traditional CP based synchronization is fragile under disguised jamming. As shown in Fig. 2.3, to ensure the robustness of synchronization, in SP-OFDM, we apply a secure phase shift to part of the CP for each OFDM block. More specifically, the CP of each OFDM block is divided into two parts: for the first part, with a duration of $T_{CP,1}$, a secure phase shift is applied to the signal. We name this part of CP as CP1; while for the second part, which is of length $T_{CP,2}$, no special processing is applied. We name the second part as CP2. CP1 is used for effective synchronization under disguised jamming; CP2 maintains the functions of the original CP. To avoid ISI and ICI, both $T_{CP,1}$ and $T_{CP,2}$ are chosen to be longer than the maximum delay spread of the channel.

To ensure the security, the phase shift applied to CP1 is encrypted and varies for each OFDM block. The corresponding secure phase shift sequence can be generated using the same phase shift generator proposed in Fig. 2.2, with a much lower generation rate, since only one phase shift symbol is needed per OFDM block. Let $s_k(t)$ denote signal of the k-th OFDM block in the time domain by aligning the beginning of the OFDM block body at

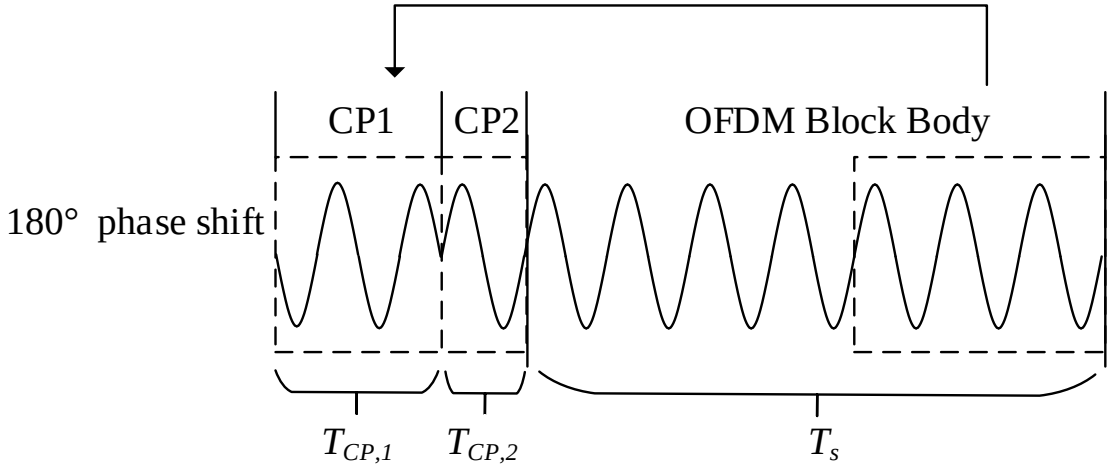


Figure 2.3: An OFDM waveform example with secure cyclic prefix, illustrated with a 180° phase shift on CP1.

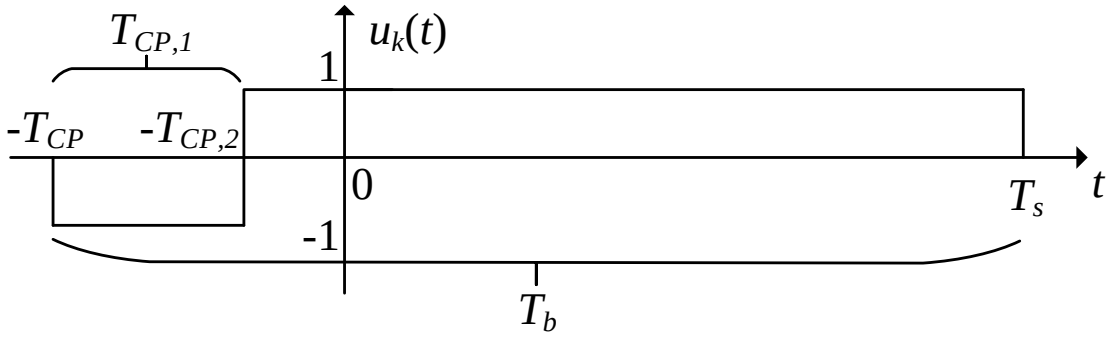


Figure 2.4: The waveform of $u_k(t)$ with $C_k = -1$.

$t = 0$, and C_k denote the phase shift symbol applied to its CP1; let $u(t)$ be the unit step function, $T_{CP} = T_{CP,1} + T_{CP,2}$ and T_s denote the duration of OFDM block body. Define function $u_k(t)$ as

$$u_k(t) \triangleq C_k[u(t + T_{CP}) - u(t + T_{CP,2})] + u(t + T_{CP,2}) - u(t - T_s). \tag{2.3}$$

An example of $u_k(t)$ with $C_k = -1$ is plotted in Fig. 2.4. For SP-OFDM with secure CP, $s_k(t)$ can be expressed as

$$s_k(t) = \frac{1}{N_c} \sum_{i=0}^{N_c-1} \tilde{S}_{k,i} e^{j\frac{2\pi i}{T_s}t} u_k(t), \tag{2.4}$$

where $\tilde{S}_{k,i} = S_{k,i} e^{-j\Theta_{k,i}}$. Let $T_b = T_s + T_{CP}$ denote the duration of an OFDM block. Then the entire OFDM signal in the time domain can be expressed as

$$s(t) = \sum_{k=-\infty}^{\infty} s_k(t - kT_b). \tag{2.5}$$

Even though the receiver can generate identical phase shift sequences used in CP1 generation from the design of Fig. 2.2, there will still be an offset between the two generated sequences considering the delays in communication and the mismatch between the time clocks. Let C_k and $\tilde{C}_k$ denote the phase shift symbols generated at the transmitter and receiver respectively, and we have

$$C_k = \tilde{C}_{k+k_0}, \forall k. \tag{2.6}$$

Since the phase shift sequences are generated from the global time clock, the offset k_0 is bounded. The offset k_0 can be estimated by the synchronization module at the receiver.

Note that synchronization is needed for the precoding matrix sequence $\boldsymbol{P}_k$ as well; for the ease of synchronization, we pair the CP phase shift symbol C_k with the precoding matrix $\boldsymbol{P}_k$ for each OFDM block k; that is, for each CP phase shift symbol generated, we generate N_c phase shift symbols in parallel as the sub-carrier phase shifts. In this way, the two phase shift sequences are synchronized, in the sense that once the synchronization on the CP phase shift sequence is obtained, the synchronization on the precoding matrices is achieved automatically.

2.2.3 Receiver Design with Secure Decoding

We consider an additive white Gaussian noise (AWGN) channel under hostile jamming. The transmitted OFDM signal is subject to an AWGN term, denoted by $n(t)$, and an additive jamming interference $x(t)$. The received OFDM signal can be expressed as

$$r(t) = s(t - t_0)e^{j(\omega_0 t + \phi_0)} + x(t) + n(t), \tag{2.7}$$

where t_0, ω_0 and ϕ_0 denote the time, frequency and phase offsets between the transmitter and receiver, respectively. Without loss of generality, we can assume that $t_0 \in [0, T_b)$.

As in the traditional OFDM system, the synchronization module of SP-OFDM consists of two stages: a *pre-FFT synchronization*, which makes use of the correlation between the secure CP and the OFDM body tail to roughly estimate the offsets, and a *post-FFT synchronization*, which makes use of the pilot symbols inserted to certain sub-carriers to obtain a fine estimation. The phase shift offset k_0 is also estimated in the pre-FFT stage. The detailed algorithm and analysis on the synchronization of SP-OFDM will be presented in Section 2.3.

The demodulation module at the receiver will crop the CP to obtain the body of each OFDM block, and apply FFT to obtain the frequency component at each sub-carrier. Under perfect synchronization, the received signal of the k-th OFDM block body can be expressed as

$$r_k(t) = s_k(t) + x_k(t) + n_k(t), \quad t \in [0, T_s), \tag{2.8}$$

where $x_k(t)$ and $n_k(t)$ are the jamming interference and noise overlaid on the k-th OFDM block, respectively. The frequency components of jamming and noise can be calculated as

$$J_{k,i} = \sum_{m=0}^{N_c-1} x_k(\frac{mT_s}{N_c}) e^{-j\frac{2\pi i}{N_c}m}, i = 0, 1, \cdots, N_c - 1, \tag{2.9}$$

$$\bar{N}_{k,i} = \sum_{m=0}^{N_c-1} n_k(\frac{mT_s}{N_c}) e^{-j\frac{2\pi i}{N_c}m}, i = 0, 1, \cdots, N_c - 1, \tag{2.10}$$

where $\frac{T_s}{N_c}$ is the sampling interval. For an AWGN channel, $\bar{N}_{k,i}$'s are i.i.d. circularly symmetric complex Gaussian random variables with variance σ^2. After applying FFT to the received signal, a symbol vector $\tilde{\boldsymbol{R}}_k = [\tilde{R}_{k,0}, \tilde{R}_{k,1}, \cdots, \tilde{R}_{k,N_c-1}]^T$ is obtained for the k-th transmitted OFDM block. That is,

$$\tilde{\boldsymbol{R}}_k = \boldsymbol{P}_k \boldsymbol{S}_k + \boldsymbol{J}_k + \bar{\boldsymbol{N}}_k. \tag{2.11}$$

where

$$\boldsymbol{J}_k = [J_{k,0}, J_{k,1}, \cdots, J_{k,N_c-1}]^T, \tag{2.12}$$

and

$$\bar{\boldsymbol{N}}_k = [\bar{N}_{k,0}, \bar{N}_{k,1}, \cdots, \bar{N}_{k,N_c-1}]^T. \tag{2.13}$$

The secure decoding module multiplies the inverse matrix of $\boldsymbol{P}_k$ to $\tilde{\boldsymbol{R}}_k$, which results in the symbol vector

$$\boldsymbol{R}_k = \boldsymbol{S}_k + \boldsymbol{P}_k^{-1}\boldsymbol{J}_k + \boldsymbol{P}_k^{-1}\bar{\boldsymbol{N}}_k, \tag{2.14}$$

where $\boldsymbol{R}_k = [R_{k,0}, R_{k,1}, \cdots, R_{k,N_c-1}]^T$, with

$$R_{k,i} = S_{k,i} + e^{j\Theta_{k,i}} J_{k,i} + N_{k,i}, \tag{2.15}$$

where $N_{k,i} = e^{j\Theta_{k,i}}\bar{N}_{k,i}$, and $\Theta_{k,i}$ is uniformly distributed over $\{\frac{2\pi i}{M} \mid i = 0, 1, \cdots, M-1\}$. Note that for any circularly symmetric Gaussian random variable N, $e^{j\theta}N$ and N have the same distribution for any angle θ [65, p66]; that is, $N_{k,i}$ is still a circular symmetric complex Gaussian random variable of zero-mean and variance σ^2. Taking the delay in the communication system into consideration, in this chapter, we assume that the authorized user and the jammer do not have pre-knowledge on the sequence of each other.

2.3 Synchronization in SP-OFDM under Disguised Jamming

In this section, first, we show the vulnerability of the synchronization process in tradition OFDM under disguised jamming attacks; then we propose the synchronization algorithm of SP-OFDM and prove its effectiveness under hostile jamming.

In modern OFDM systems, there are generally two kinds of approaches to achieve signal synchronization: (i) making use of the correlation between the CP and the tail of each OFDM block [64]; or (ii) inserting certain training symbols in every OFDM frame [66].

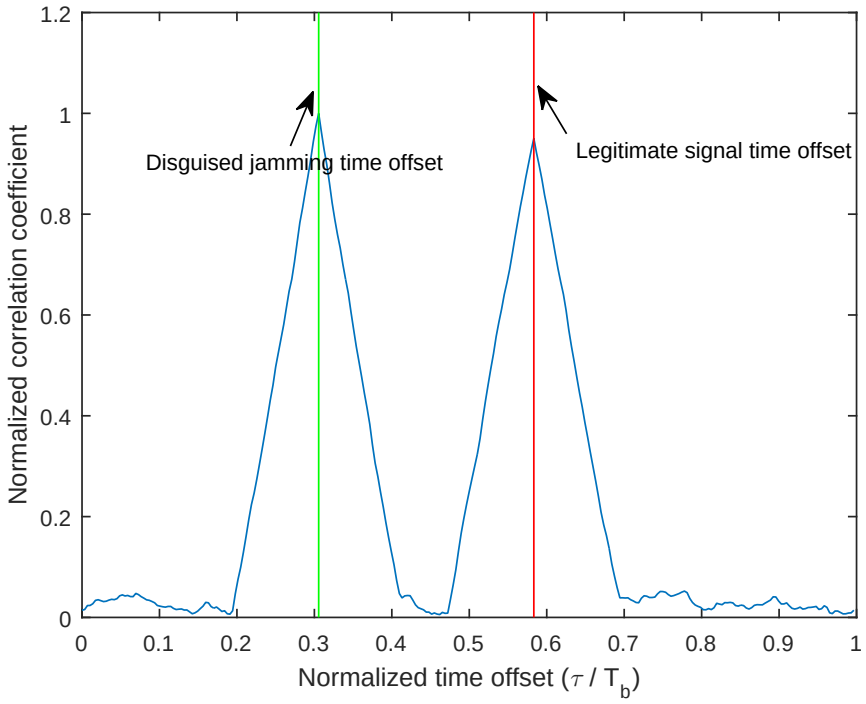


Figure 2.5: Correlation coefficients of the original OFDM under disguised jamming.

However, neither of these two approaches is robust under malicious jamming, especially disguised jamming, where the jammer modulates the inference with OFDM and deceive the receiver into synchronizing with the disguised jamming instead of the legitimate signal. For the training sequence based synchronization approach, even if the training sequence is not public, there is still a chance for the jammer to eavesdrop on the training sequence, and then generate the OFDM modulated disguised jamming with the true training sequence.

Synchronization of traditional OFDM under disguised jamming: To demonstrate the damage of disguised jamming, we calculate the CP based correlation coefficients of the traditional OFDM signal at different time offsets in the AWGN channel under an OFDM modulated disguised jamming. We average the correlation coefficients over multiple OFDM blocks, and the result is shown in Fig. 2.5. *Without proper encryption applied to the signal, the legitimate signal and the jamming interference are completely symmetric; we can*

observe peaks of the correlation coefficients at two different time offsets, one corresponding to that of the legitimate signal and the other corresponding to that of the disguised jamming. If the jamming power is the same as the signal power, then the probability that the receiver chooses to synchronize with jamming is 50%. Obviously, a complete communication failure occurs when the receiver chooses to synchronize with the disguised jamming instead of the legitimate signal.

To address this problem, in the synchronization algorithm of SP-OFDM, we apply encrypted phase shifts to the sub-carriers and CP. For the ease of analysis, in the following, we consider an AWGN channel model; the effectiveness of the proposed algorithm in multi-path fading channels will be verified through numerical analysis in Section 2.5. Even though our goal is to guarantee the robustness of SP-OFDM under disguised jamming, in the following analysis, we do not assume any specific form on the jamming interference $x(t)$, that is, we prove the robustness of our algorithm under any form of jamming attacks. Without loss of generality, we denote the combined term of jamming and noise as $z(t) = x(t) + n(t)$, and the received signal can be expressed as

$$r(t) = s(t - t_0)e^{j(\omega_0 t + \phi_0)} + z(t). \tag{2.16}$$

2.3.1 Pre-FFT Synchronization

In the pre-FFT stage, we estimate the encrypted phase shift sequence offset k_0, time offset t_0 and the fractional part of $w_0 T_s/2\pi$ for frequency offset w_0. Since the phase shift sequence C_k is generated from the global time clock, the receiver has rough bounds on k_0 relative to the arrival time of the signal. We denote the finite candidate set of offset k_0 by $\mathcal{K}$.

In the traditional OFDM system, the CP correlation based synchronization algorithm is derived from the maximum-likelihood (ML) rule [64, 67]. However, since the jamming distribution is unspecified in our case, the ML rule is not applicable. Instead, we prove the robustness of the synchronization algorithm of SP-OFDM using the Chebychev inequality [68, Theorem 5.11].

In the pre-FFT stage, the receiver calculates the following correlation coefficient

$$Y_k(\tau, d) \triangleq \int_{\tau - T_{CP} + kT_b}^{\tau - T_{CP,2} + kT_b} r(t) r^*(t + T_s) \tilde{C}_{k+d}^* \mathrm{d}t, \ k \in \mathbb{Z}^*, \tag{2.17}$$

for $\tau \in [0, T_b), d \in \mathcal{K}$. We have the following proposition on $Y_k(\tau, d)$, whose proof is given in Appendix A.

Proposition 2.1 *If the fourth moment of $z(t)$ is bounded for any time instant t, i.e., $\mathbb{E}\{|z(t)|^4\} < \infty, \forall t \in \mathbb{R}$, then as $K \to +\infty$, we have*

$$\frac{1}{K} \sum_{k=0}^{K-1} Y_k(\tau, d) = \begin{cases} \frac{P_S}{N_c} v(\tau + T_b - t_0) e^{-j\omega_0 T_s}, & d = k_0 - 1, \\ \frac{P_S}{N_c} v(\tau - t_0) e^{-j\omega_0 T_s}, & d = k_0, \\ \frac{P_S}{N_c} v(\tau - T_b - t_0) e^{-j\omega_0 T_s}, & d = k_0 + 1, \\ 0, & \textit{otherwise}, \end{cases} \tag{2.18}$$

almost surely (a.s.), where

$$v(\tau) \triangleq \begin{cases} \tau + T_{CP,1}, & -T_{CP,1} \le \tau < 0, \\ T_{CP,1} - \tau, & 0 \le \tau < T_{CP,1}, \\ 0, & \textit{otherwise}, \end{cases} \tag{2.19}$$

and P_S is the average symbol power of constellation Φ.

Basing on Proposition 2.1, to estimate t_0 and k_0, we search for τ and d which can

maximize $|\frac{1}{K}\sum_{k=0}^{K-1} Y_k(\tau, d)|$ for some K. Meanwhile, after we obtain t_0 and k_0, the phase of the average correlation coefficient $\frac{1}{K}\sum_{k=0}^{K-1} Y_k(t_0, k_0)$ is

$$-w_0 T_s \mod 2\pi, \tag{2.20}$$

where we can estimate the fractional part of $w_0 T_s/2\pi$ as well. In practice, the jamming interference should be peak power bounded considering the constraints in RF, so we can ensure that the fourth moment of $z(t)$ is bounded. The selection of K depends on the power and the form of the jamming interference. In Section 2.5, we will show that under a disguised jamming, SP-OFDM is able to obtain relatively accurate estimation results with 25 to 30 OFDM blocks.

As in the traditional OFDM, the CP based synchronization is only able to provide a coarse estimation of time offset t_0, especially under multi-path fading, and it requires a fine estimation on the time offset at the post-FFT stage. In addition, from (2.21), it can be seen that even for a very minor estimation error on the carrier frequency, there still may be an essential phase offset. As long as the range of the time estimation error is smaller than the duration of CP2, without loss of generality, we can model the signal after pre-FFT synchronization as

$$r'(t) = s(t - t'_0)e^{j(\frac{2\pi(n_0+\zeta_0)}{T_s}t+\phi_0)} + z'(t), \tag{2.21}$$

where $z'(t)$ is the jamming interference after pre-FFT synchronization, $t'_0 \in [0, T_{CP,2})$ is the remaining time offset, $2\pi(n_0 + \zeta_0)/T_s$ is the remaining frequency offset, n_0 is an integer and $|\zeta_0| \ll 1$.

2.3.2 Post-FFT Synchronization

In this stage, we first estimate $n_0 + \zeta_0$ after demodulating the synchronized signal $r'(t)$ in (2.21) using FFT. Suppose n_0 satisfies

$$N_l \leq n_0 \leq N_u, \tag{2.22}$$

where integers N_l and N_u are determined by the maximal frequency offset between the transmitter and receiver. Basing on (2.21), to demodulate the k-th OFDM block, the receiver applies FFT to signal $r'(t)$ within interval $[kT_b, kT_b+T_s)$. The received signal of k-th OFDM block after alignment can be expressed as

$$r'_k(t) = s_k(t - t'_0)e^{j(\frac{2\pi(n_0+\zeta_0)}{T_s}t+\phi_k)} + z'_k(t), \quad t \in [0, T_s), \tag{2.23}$$

where

$$\phi_k = \phi_0 + \frac{2\pi(n_0 + \zeta_0)T_b}{T_s}k, \tag{2.24}$$

and

$$z'_k(t) = z'(t + kT_b). \tag{2.25}$$

Considering the frequency offset n_0, the receiver samples the received signal with a sampling frequency $\frac{N_c+N_u-N_l}{T_s}$. Let $N'_c \triangleq N_c + N_u - N_l$. For $0 \leq i < N'_c$, the FFT applied to

$r'_k(t)$ can be expressed as

$$\begin{aligned} R_k(i) &= \sum_{m=0}^{N'_c-1} r'_k(\frac{mT_s}{N'_c}) e^{-j\frac{2\pi i}{N'_c}m} \\ &= \frac{e^{j\phi_k}}{N_c} \sum_{i'=0}^{N'_c-1} \tilde{S}_{k,i'} \frac{e^{-j\frac{2\pi t'_0}{Ts}i'}(1-e^{j2\pi\zeta_0})}{1-e^{j\frac{2\pi(n_0+\zeta_0+i'-i)}{N'_c}}} + Z'_k(i), \end{aligned} \tag{2.26}$$

where

$$Z'_k(i) = \sum_{m=0}^{N'_c-1} z'_k(\frac{mT_s}{N'_c}) e^{-j\frac{2\pi i}{N'_c}m} \quad . \tag{2.27}$$

Since we assume $|\zeta_0| \ll 1$, for $0 \le i < N'_c$, we can neglect the ICI in (2.26) and approximate $R_k(i)$ as

$$R_k(i) = \frac{N'_c}{N_c} e^{j\phi_k} e^{-j\frac{2\pi t'_0}{Ts}[(i-n_0) \mod N'_c]} \tilde{S}'_{k,i-n_0} + Z'_k(i), \tag{2.28}$$

where

$$\tilde{S}'_{k,i} = \begin{cases} \tilde{S}_{k,\ (i \mod N'_c)}, & 0 \le i \mod N'_c < N_c, \\ 0, & \text{otherwise.} \end{cases} \tag{2.29}$$

The post-FFT synchronization generally utilizes the pilot symbols inserted at certain sub-carriers. For the ease of analysis, we assume a pilot symbol $\boldsymbol{p}$ is placed at sub-carrier i_p of each OFDM block. Note that, as the precoding matrix sequence is synchronized with the CP phase shift sequence, the precoding matrix sequence is synchronized at the receiver after pre-FFT synchronization. We calculate the following correlation coefficients for each OFDM block k:

$$\Gamma_k(i) \stackrel{\triangle}{=} R_k(i) R^*_{k+1}(i) e^{j(\Theta_{k,i_p} - \Theta_{k+1,i_p})}. \tag{2.30}$$

We have the following proposition on $\Gamma_k(i)$.

Proposition 2.2 *If the fourth moment of $z(t)$ is bounded for any time t, then as $K \to +\infty$, we have*

$$\begin{aligned}
&\frac{1}{K}\sum_{k=0}^{K-1}\Gamma_k(i) \\
&= \begin{cases} \left(\frac{N_c'}{N_c}\right)^2 e^{j\frac{2\pi(n_0+\zeta_0)T_b}{T_s}}|\boldsymbol{p}|^2, & i = n_0 + i_p \bmod N_c' \\ 0, & \textit{otherwise}, \end{cases} \quad a.s..
\end{aligned} \tag{2.31}$$

Proof: Note that $\Gamma_k(i)$ can be derived as

$$\begin{aligned}
\Gamma_k(i) &= [\left(N_c'/N_c\right)^2 e^{j\frac{2\pi(n_0+\zeta_0)T_b}{T_s}}\tilde{S}'_{k,i-n_0}\tilde{S}'^*_{k+1,i-n_0} \\
&+ \frac{N_c'}{N_c}e^{j\phi_k}\tilde{S}'_{k,i-n_0}Z'^*_{k+1}(i) + \frac{N_c'}{N_c}e^{j\phi_{k+1}}\tilde{S}'^*_{k+1,i-n_0}Z'_k(i) \\
&+ Z'_k(i)Z'^*_{k+1}(i)]e^{j(\Theta_{k,i_p}-\Theta_{k+1,i_p})}.
\end{aligned} \tag{2.32}$$

Since the phase shifts $\Theta_{k,i}$'s are independent across the sub-carriers, following the approach in the pre-FFT analysis, we have

$$\mathbb{E}\{\Gamma_k(i)\} = \begin{cases} \left(\frac{N_c'}{N_c}\right)^2 e^{j\frac{2\pi(n_0+\zeta_0)T_b}{T_s}}|\boldsymbol{p}|^2, & i = n_0+i_p \bmod N_c', \\ 0, & \text{otherwise.} \end{cases} \tag{2.33}$$

while the variance of $\frac{1}{K}\sum_{k=0}^{K-1}\Gamma_k(i)$ converges to 0 as $K \to +\infty$. Therefore (2.31) is obtained accordingly. We skip the details here for brevity. □

Following Proposition 2.2, n_0 can be estimated by finding the i which maximizes $\frac{1}{K}\sum_{k=0}^{K-1}\Gamma_k(i)$. With the n_0 obtained, we can further estimate the frequency estimation

error ζ_0 in the pre-FFT stage by evaluating the phase of $\frac{1}{K}\sum_{k=0}^{K-1}\Gamma_k((n_0+i_p) \bmod N_c')$.

After n_0 is estimated, without loss of generality, we can assume $n_0 = 0$ in the following derivation. In terms of the time offset t_0', given two pilot symbols $\boldsymbol{p}_1$ and $\boldsymbol{p}_2$ located at sub-carriers i_{p_1} and i_{p_2}, respectively, we evaluate the following correlation coefficient for each OFDM block k:

$$\Upsilon_k(i_{p_1}, i_{p_2}) = R_k(i_{p_1})R_k^*(i_{p_2})\boldsymbol{p}_1^*\boldsymbol{p}_2 e^{j(\Theta_{k,ip_1}-\Theta_{k,ip_2})}, \tag{2.34}$$

and we have the following proposition.

Proposition 2.3 *If the fourth moment of $z(t)$ is bounded for any time t, then as $K \to +\infty$, we have*

$$\frac{1}{K}\sum_{k=0}^{K-1}\Upsilon_k(i_{p_1}, i_{p_2}) = \left(\frac{N_c'}{N_c}\right)^2 e^{-j\frac{2\pi t_0'}{T_s}(i_{p_1}-i_{p_2})}|\boldsymbol{p}_1|^2|\boldsymbol{p}_2|^2, \tag{2.35}$$

a.s.

The proof of Proposition 2.3 follows a similar approach as Proposition 2.1, and we skip it for brevity. Note that $t_0' \in [0, T_{CP,2})$, so t_0' can be estimated from the phase of $\frac{1}{K}\sum_{k=0}^{K-1}\Upsilon_k(i_{p_1}, i_{p_2})$. Likewise, the phase offset ϕ_0 can be estimated by averaging $R_k(i_p)e^{j\Theta_{k,ip}}$ after compensating for the frequency offset.

Discussions Note that under disguised jamming, the estimator averages multiple OFDM blocks to make use of the encrypted signal for an accurate synchronization. In practice, estimation errors always exist in synchronization, so the receiver has to keep track of all the offsets, which can be implemented by the moving average approach.

The pre-FFT synchronization exploits the correlation between secure CP and the OFDM body tail. The data-aided synchronization approach, i.e., inserting independent training

sequence in each OFDM frame, is still an option under disguised jamming if encryption is applied to the training sequence. However, the CP based approach experiences less delay in synchronization. By inserting secure CP for each OFDM block, it is easier to keep track of the time offset continuously.

In the post-FFT stage, inserting more pilots can accelerate the synchronization process; meanwhile, under fading channels, the channel estimation process necessitates pilot symbols over different sub-carrier locations. Channel estimation can be implemented by averaging the received pilot symbols at each sub-carrier location following the approach in synchronization. However, an important point here is that for time varying channels, the duration of the OFDM blocks used for averaging should be smaller than the coherence time so that the channel does not change significantly during each estimation. This is guaranteed in practical systems where the whole OFDM frame duration is shorter than the channel coherence time [66].

2.4 Symmetricity and Capacity Analysis using the AVC Model

In this section, we analyze the symmetricity and capacity of the proposed SP-OFDM system using the arbitrarily varying channel (AVC) model. Recall that from Section 2.2, under perfect synchronization, the equivalent channel model of SP-OFDM can be expressed as

$$R = S + e^{j\Theta}J + N, \tag{2.36}$$

where $S \in \Phi$, $J \in \mathbb{C}$, $N \sim \mathcal{CN}(0, \sigma^2 I)$, Θ is uniformly distributed over $\{\frac{2\pi i}{M} \mid i = 0, 1, ..., M-1\}$, and $\mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$ denotes a circularly symmetric complex Gaussian distribution with mean $\boldsymbol{\mu}$ and variance $\boldsymbol{\Sigma}$. For generality, in this section, we do not assume any *a priori* information on the jamming J, except a finite average power constraint of P_J, i.e., $\mathbb{E}\{|J|^2\} \leq P_J$. We will show that the AVC corresponding to SP-OFDM is nonsymmetrizable, and hence the AVC capacity of SP-OFDM is positive under disguised jamming.

2.4.1 AVC Symmetricity Analysis

The arbitrarily varying channel (AVC) model, first introduced in [62], characterizes the communication channels with unknown states which may vary in arbitrary manners across time. For the jamming channel (2.36) of interest, the jamming symbol J can be viewed as the state of the channel under consideration. The channel capacity of AVC evaluates the data rate of the channel under the most adverse jamming interference among all the possibilities [69]. Note that unlike the jamming free model where the channel noise sequence is independent of the authorized signal and is independent and identically distributed (i.i.d.), the AVC model considers the possible correlation between the authorized signal and the jamming, as well as the possible temporal correlation among the jamming symbols, which may cause much worse damages to the communication.

To prove the effectiveness of the proposed SP-OFDM under disguised jamming, we need to introduce some basic concepts and properties of the AVC model. First we revisit the definition of symmetrizable AVC channel.

Definition 2.1 *[69] [70] Let $W(\boldsymbol{r} \mid \boldsymbol{s}, \boldsymbol{x})$ denote the conditional PDF of the received signal R given the transmitted symbol $\boldsymbol{s} \in \Phi$ and the jamming symbol $\boldsymbol{x} \in \mathbb{C}$. The AVC channel*

(2.36) is symmetrizable iff for some auxiliary channel $\pi : \Phi \to \mathbb{C}$, $\forall \boldsymbol{s}, \boldsymbol{s}' \in \Phi, \boldsymbol{r} \in \mathbb{C}$, *we have*

$$\int_{\mathbb{C}} W(\boldsymbol{r} \mid \boldsymbol{s}, \boldsymbol{x}) dF_{\pi}(\boldsymbol{x}|\boldsymbol{s}') = \int_{\mathbb{C}} W(\boldsymbol{r} \mid \boldsymbol{s}', \boldsymbol{x}) dF_{\pi}(\boldsymbol{x}|\boldsymbol{s}), \tag{2.37}$$

where $F_{\pi}(\cdot|\cdot)$ *is the probability measure of the output of channel* π *given the input, i.e., the conditional CDF*

$$F_{\pi}(\boldsymbol{x}|\boldsymbol{s}) = \Pr\{Re(\pi(\boldsymbol{s})) \leq Re(\boldsymbol{x}), Im(\pi(\boldsymbol{s})) \leq Im(\boldsymbol{x})\}, \tag{2.38}$$

for $\boldsymbol{x} \in \mathbb{C}, \boldsymbol{s} \in \Phi$, *where* $\pi(\boldsymbol{s})$ *denotes the output of channel* π *given input symbol* $\boldsymbol{s}$.

We denote the set of all the auxiliary channels, π's, that can symmetrize channel (2.36) by Π, that is,

$$\Pi = \left\{ \pi \mid \text{ Eq. (2.37) is satisfied w.r.t. } \pi \ \forall \boldsymbol{s}, \boldsymbol{s}' \in \Phi, \boldsymbol{r} \in \mathbb{C} \right\}. \tag{2.39}$$

With the average jamming power constraint considered in this chapter, we further introduce the definition of l-symmetrizable channel.

Definition 2.2 *[70] The AVC channel (2.36) is called* l*-symmetrizable under average jamming power constraint iff there exists a* $\pi \in \Pi$ *such that*

$$\int_{\mathbb{C}} |\boldsymbol{x}|^2 dF_{\pi}(\boldsymbol{x}|\boldsymbol{s}) < \infty, \quad \forall \boldsymbol{s} \in \Phi. \tag{2.40}$$

In [70], it was shown that reliable communication can be achieved as long as the AVC channel is not l-symmetrizable.

Lemma 2.1 *[70, Corollary 2] The deterministic coding capacity*[2] *of AVC channel (2.36)*

[2]The deterministic coding capacity is defined by the capacity that can be achieved by a communication

is positive under any hostile jamming with finite average power constraint iff the AVC is not l-symmetrizable. Furthermore, given a specific average jamming power constraint P_J, the channel capacity C in this case equals

$$\begin{aligned} C &= \max_{\mathcal{P}_S} \min_{F_J} I(S,R), \\ s.t. \quad & \int_{\mathbb{C}} |\boldsymbol{x}|^2 dF_J(\boldsymbol{x}) \leq P_J, \end{aligned} \tag{2.41}$$

where $I(S,R)$ denotes the mutual information (MI) between the R and S in (2.36), $\mathcal{P}_S$ denotes the probability distribution of S over Φ and $F_J(\cdot)$ the CDF of J.

First, we show that the traditional OFDM system is l-symmetrizable under disguised jamming.

Theorem 2.1 *The traditional OFDM system is l-symmetrizable. Therefore, the deterministic coding capacity is zero under the worst disguised jamming with finite average jamming power.*

Proof: The AVC model of the traditional OFDM system is

$$R = S + J + N. \tag{2.42}$$

We will show that when S and J have the same constellation Φ, hence the same finite average power, the AVC channel is l-symmetrizable. It follows from (2.42) that

$$W(\boldsymbol{r} \mid \boldsymbol{s}, \boldsymbol{s'}) = W(\boldsymbol{r} \mid \boldsymbol{s'}, \boldsymbol{s}),\ \forall \boldsymbol{s}, \boldsymbol{s'} \in \Phi, \boldsymbol{r} \in \mathbb{C}. \tag{2.43}$$

system, when it applies only one code pattern during the information transmission. In other words, the coding scheme is deterministic and can be readily repeated by other users [71].

Since Φ has finite average power, the average power constraint (2.40) is satisfied by disguised jamming. Hence, channel (2.42) is l-symmetrizable. From Lemma 2.1, a necessary condition for a positive AVC deterministic coding capacity is that the channel is not l-symmetrizable. So the traditional OFDM system has zero deterministic coding capacity under disguised jamming with finite average jamming power. □

Next, we show that with the proposed secure precoding, it is impossible to l-symmetrize the AVC channel (2.36) corresponding to the SP-OFDM system.

Theorem 2.2 *The AVC channel corresponding to the proposed SP-OFDM is not l-symmetrizable.*

Proof: We prove this result by contradiction. Suppose that there exists a channel $\pi \in \Pi$ such that the AVC channel is l-symmetrizable. Denote the output of channel π given input $\boldsymbol{x}$ by $\pi(\boldsymbol{x})$, and define the corresponding AVC channel output for inputs $\boldsymbol{s}$ and $\boldsymbol{s'}$ as

$$\hat{R}(\boldsymbol{s}, \boldsymbol{s'}) = \boldsymbol{s} + \pi(\boldsymbol{s'})e^{j\Theta} + N, \tag{2.44}$$

where $\hat{R}(\boldsymbol{s}, \boldsymbol{s'})$ denotes the channel output. Following (2.37), $\hat{R}(\boldsymbol{s}, \boldsymbol{s'})$ and $\hat{R}(\boldsymbol{s'}, \boldsymbol{s})$ have the same distribution. Let $\varphi_X(\omega_1, \omega_2)$ denote the characteristic function (CF) of a complex random variable X. So we have

$$\varphi_{\hat{R}(\boldsymbol{s},\boldsymbol{s'})}(\omega_1, \omega_2) \equiv \varphi_{\hat{R}(\boldsymbol{s'},\boldsymbol{s})}(\omega_1, \omega_2), \tag{2.45}$$

and

$$\varphi_{\hat{R}(\boldsymbol{s},\boldsymbol{s'})}(\omega_1, \omega_2) = \varphi_{[\boldsymbol{s}+\pi(\boldsymbol{s'})e^{j\Theta}]}(\omega_1, \omega_2)\ \varphi_N(\omega_1, \omega_2), \tag{2.46}$$

where, for the complex Gaussian noise N, we have

$$\varphi_N(\omega_1,\omega_2) = e^{-\frac{\sigma^2}{4}(w_1^2+w_2^2)}, \quad \omega_1,\omega_2 \in (-\infty,+\infty), \tag{2.47}$$

which is non-zero over $\mathbb{R}^2$. Thus by eliminating the characteristic functions of the Gaussian noises on both sides of equation (2.45), we have

$$\varphi_{[\boldsymbol{s}+\pi(\boldsymbol{s'})e^{j\Theta}]}(\omega_1,\omega_2) = \varphi_{[\boldsymbol{s'}+\pi(\boldsymbol{s})e^{j\Theta}]}(\omega_1,\omega_2). \tag{2.48}$$

for $\omega_1,\omega_2 \in (-\infty,+\infty)$. Let $\boldsymbol{s} = s_1 + js_2$, we can then express $\varphi_{[\boldsymbol{s}+\pi(\boldsymbol{s'})e^{j\Theta}]}(\omega_1,\omega_2)$ as

$$\varphi_{[\boldsymbol{s}+\pi(\boldsymbol{s'})e^{j\Theta}]}(\omega_1,\omega_2) = e^{js_1\omega_1+js_2\omega_2}\varphi_{[\pi(\boldsymbol{s'})e^{j\Theta}]}(\omega_1,\omega_2), \tag{2.49}$$

and

$$\begin{aligned} & \varphi_{[\pi(\boldsymbol{s'})e^{j\Theta}]}(\omega_1,\omega_2) \\ = \; & \mathbb{E}\{e^{j\omega_1 Re(\pi(\boldsymbol{s'})e^{j\Theta})+j\omega_2 Im(\pi(\boldsymbol{s'})e^{j\Theta})}\} \\ = \; & \int_{\mathbb{C}} \mathbb{E}\{e^{j\omega_1 Re(\boldsymbol{x}e^{j\Theta})+j\omega_2 Im(\boldsymbol{x}e^{j\Theta})}\}\mathrm{d}F_\pi(\boldsymbol{x}|\boldsymbol{s'}). \end{aligned} \tag{2.50}$$

Recall that under the proposed secure precoding scheme, Θ is uniformly distributed over

$\{\frac{2\pi i}{M} \mid i = 0, 1, ..., M-1\}$, where M is a power of 2. We have

$$\begin{aligned}
&\mathbb{E}\{e^{j\omega_1 Re(\boldsymbol{x}e^{j\Theta})+j\omega_2 Im(\boldsymbol{x}e^{j\Theta})}\} \\
=&\frac{1}{M}\sum_{i=0}^{M-1} e^{j\omega_1|\boldsymbol{x}|\cos(\frac{2\pi i}{M}+\arg(\boldsymbol{x}))+j\omega_2|\boldsymbol{x}|\sin(\frac{2\pi i}{M}+\arg(\boldsymbol{x}))} \\
=&\frac{2}{M}\sum_{i=0}^{M/2-1} \cos\{\omega_1|\boldsymbol{x}|\cos[2\pi i/M+\arg(\boldsymbol{x})] \\
&\qquad +\omega_2|\boldsymbol{x}|\sin[2\pi i/M+\arg(\boldsymbol{x})]\}, \qquad (2.51)
\end{aligned}$$

which is of real value for $\omega_1, \omega_2 \in (-\infty, +\infty)$. So $\varphi_{[\pi(\boldsymbol{s}')e^{j\Theta}]}(\omega_1, \omega_2)$ and $\varphi_{[\pi(\boldsymbol{s})e^{j\Theta}]}(\omega_1, \omega_2)$ are also real-valued over $\mathbb{R}^2$. For $\boldsymbol{s} \neq \boldsymbol{s}'$ and $\boldsymbol{s}' = s_1' + js_2'$, $e^{j[(s_1-s_1')\omega_1+(s_2-s_2')\omega_2]}$ has non-zero imaginary part for $(s_1 - s_1')\omega_1 + (s_2 - s_2')\omega_2 \neq n\pi$, $n \in \mathbb{Z}$. Without loss of generality, we assume $s_1 \neq s_1'$. From (2.48), (2.49) and (2.51), for $\omega_1 + \frac{s_2-s_2'}{s_1-s_1'}\omega_2 \neq \frac{n\pi}{s_1-s_1'}, \forall n \in \mathbb{Z}$, we have

$$\varphi_{[\pi(\boldsymbol{s})e^{j\Theta}]}(\omega_1, \omega_2) = 0. \qquad (2.52)$$

On the other hand, the characteristic function of an RV should be uniformly continuous in the real domain [68, Theorem 15.21]. So for any fixed $\omega_2 \in (-\infty, \infty)$, we should have

$$\begin{aligned}
&\varphi_{[\pi(\boldsymbol{s})e^{j\Theta}]}(\frac{n\pi-(s_2-s_2')\omega_2}{s_1-s_1'}, \omega_2) \\
=&\lim_{\omega_1 \to \frac{n\pi-(s_2-s_2')\omega_2}{s_1-s_1'}} \varphi_{[\pi(\boldsymbol{s})e^{j\Theta}]}(\omega_1, \omega_2), \ \forall n \in \mathbb{Z}. \qquad (2.53)
\end{aligned}$$

For $\omega_1 \in \left(\frac{(n-1)\pi-(s_2-s_2')\omega_2}{s_1-s_1'}, \frac{n\pi-(s_2-s_2')\omega_2}{s_1-s_1'}\right) \cup \left(\frac{n\pi-(s_2-s_2')\omega_2}{s_1-s_1'}, \frac{(n+1)\pi-(s_2-s_2')\omega_2}{s_1-s_1'}\right)$,

$\varphi_{[\pi(\boldsymbol{s})e^{j\Theta}]}(\omega_1, \omega_2) \equiv 0$, so

$$\varphi_{[\pi(\boldsymbol{s})e^{j\Theta}]}(\frac{n\pi - (s_2 - s_2')\omega_2}{s_1 - s_1'}, \omega_2) = 0, \ \forall n \in \mathbb{Z}. \tag{2.54}$$

Combining (2.52) and (2.54), we have

$$\varphi_{[\pi(\boldsymbol{s})e^{j\Theta}]}(\omega_1, \omega_2) = 0, \quad \forall \omega_1, \omega_2 \in (-\infty, \infty). \tag{2.55}$$

However, (2.55) cannot be a valid characteristic function for any RV. Therefore, the auxiliary channel π does not exist, and Π is empty. Hence, the AVC channel is not l-symmerizable. □

Following Lemma 2.1, the result in Theorem 2.2 implies that the proposed SP-OFDM will always have positive capacity under any hostile jamming with finite average power constraint. The next subsection is focused on how to calculate the channel capacity of SP-OFDM under hostile jamming.

2.4.2 Capacity Analysis

From Lemma 2.1, the capacity of channel $R = S + e^{j\Theta}J + N$ is given by

$$C = \max_{\mathcal{P}_S} \min_{F_J} I(S, R),$$

$$s.t. \quad \int_{\mathbb{C}} |\boldsymbol{x}|^2 \mathrm{d}F_J(\boldsymbol{x}) \leq P_J.$$

It is hard to obtain a closed form solution of the channel capacity for a general discrete transmission alphabet Φ. However, if we relax the distribution of the transmitted symbol S from the discrete set Φ to the entire complex plane $\mathbb{C}$ under an average power constraint,

we are able to obtain the following result on channel capacity.

Theorem 2.3 *The deterministic coding capacity of SP-OFDM is positive under any hostile jamming. More specifically, let the alphabet* $\Phi = \mathbb{C}$ *and the average power of* S *being upper bounded by* P_S*, then the maximin channel capacity in (2.41) under average jamming power constraint* P_J *and noise power* $P_N = \sigma^2$ *is given by*

$$C = \log\left(1 + \frac{P_S}{P_J + P_N}\right). \tag{2.56}$$

The capacity is achieved at input distribution $\mathcal{CN}(0, P_S)$ *and jamming distribution* $\mathcal{CN}(0, P_J)$.

To prove Theorem 2.3, we need the following lemma [70, Lemma 4].

Lemma 2.2 *Mutual information* $I(S, R)$ *is concave with respect to the input distribution* $F_S(\cdot)$ *and convex with respect to the jamming distribution* $F_J(\cdot)$.

Proof: [Proof of Theorem 2.3] First, following Lemma 2.1 and Theorem 2.2, we can get that the deterministic coding capacity of SP-OFDM is positive under any hostile jamming.

Second, we will evaluate the channel capacity of SP-OFDM under hostile jamming. When the support of S is $\Phi = \mathbb{C}$, the whole complex plane, following Lemma 2.1, the channel capacity in (2.41) equals

$$C = \max_{F_S} \min_{F_J} I(S, R), \tag{2.57}$$

$$s.t. \quad \int_{\mathbb{C}} |\boldsymbol{x}|^2 \mathrm{d}F_S(\boldsymbol{x}) \leq P_S, \tag{2.58}$$

$$\int_{\mathbb{C}} |\boldsymbol{x}|^2 \mathrm{d}F_J(\boldsymbol{x}) \leq P_J, \tag{2.59}$$

where $F_S(\cdot)$ denotes the CDF function of S defined on $\mathbb{C}$, and (2.58) and (2.59) denote the average power constraints on the input and the jamming, respectively.

We denote the $I(S,R)$ w.r.t the input distribution $F_S(\cdot)$ and the jamming distribution $F_J(\cdot)$ by $\phi(F_S, F_J)$. Following Lemma 2.2, $\phi(F_S, F_J)$ is concave w.r.t. $F_S(\cdot)$ and convex w.r.t. $F_J(\cdot)$. As shown in [72], if we can find the input distribution F_S^* and the jamming distribution F_J^* such that

$$\phi(F_S, F_J^*) \leq \phi(F_S^*, F_J^*) \leq \phi(F_S^*, F_J), \tag{2.60}$$

for any F_S and F_J satisfying the average power constraints (2.58) and (2.59), respectively, then

$$\phi(F_S^*, F_J^*) = C. \tag{2.61}$$

That is, the pair (F_S^*, F_J^*) is the saddle point of the max-min problem in equation (2.57) [73].

Assume the jamming interference is circularly symmetric complex Gaussian with average power P_J, that is, $F_J^* = \mathcal{CN}(0, P_J)$. Note that the phase shift would not change the distribution of a complex Gaussian RV, and the fact that the jamming J and the noise N are independent, hence the jammed channel in this case is equivalent to a complex AWGN channel with noise power $P_J + P_N$, where the capacity achieving input distribution is also a complex Gaussian with power P_S, that is, $F_S^* = \mathcal{CN}(0, P_S)$. It follows that for any input distribution F_S satisfying the power constraint P_S,

$$\phi(F_S, \mathcal{CN}(0, P_J)) \leq \phi(\mathcal{CN}(0, P_S), \mathcal{CN}(0, P_J)). \tag{2.62}$$

On the other hand, when the input distribution is $F_S^* = \mathcal{CN}(0, P_S)$, the worst noise in

Table 2.1: SP-OFDM parameters in numerical results (T_s: duration of OFDM body)

Carrier number N_c	128	CP1 duration $T_{CP,1}$	$T_s/8$
Phase shift constellation size M	16	CP2 duration $T_{CP,2}$	$T_s/16$
Number of candidate phase shift offset $\|\mathcal{K}\|$	50	Signal-to-noise ratio (dB)	15

terms of capacity for Gaussian input is Gaussian [36]. Since $e^{j\Theta}J + N$ is complex Gaussian with power $P_J + P_N$ if $F_J^* = \mathcal{CN}(0, P_J)$, then for any jamming distribution F_J satisfying the power constraint P_J,

$$\phi(\mathcal{CN}(0, P_S), \mathcal{CN}(0, P_J)) \leq \phi(\mathcal{CN}(0, P_S), F_J). \tag{2.63}$$

So the saddle point (F_S^*, F_J^*) is achieved at $(\mathcal{CN}(0, P_S),\ \mathcal{CN}(0, P_J))$, where the corresponding channel capacity is

$$C = \log\left(1 + \frac{P_S}{P_J + P_N}\right), \tag{2.64}$$

which completes the proof. □

2.5 Numerical Results

In this section, we evaluate the synchronization and bit error rate (BER) performances of the proposed SP-OFDM system under disguised jamming attacks through numerical examples. Throughout this section, we consider the case where the malicious user generates disguised jamming using OFDM, with the same format and power level as that of the legitimate signal.

Example 1: Synchronization performance under disguised jamming in AWGN channels: In this example, we verify the robustness of SP-OFDM under disguised jamming

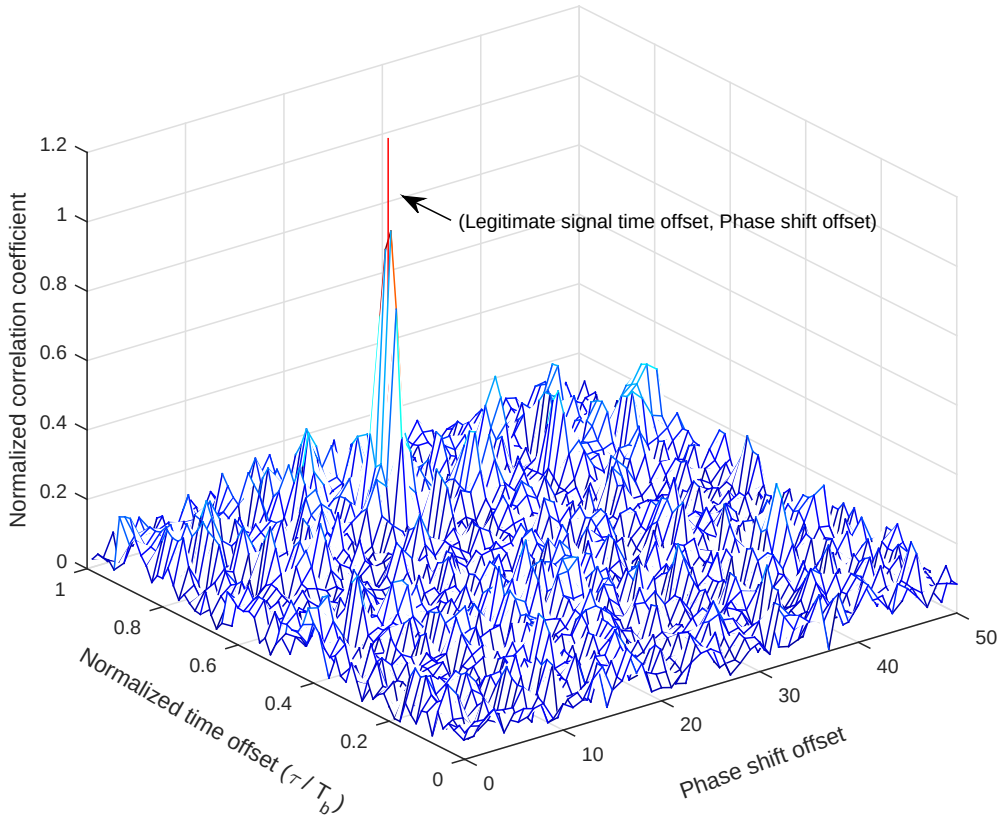


Figure 2.6: Correlation coefficients of SP-OFDM at different time and phase shift sequence offsets under disguised jamming.

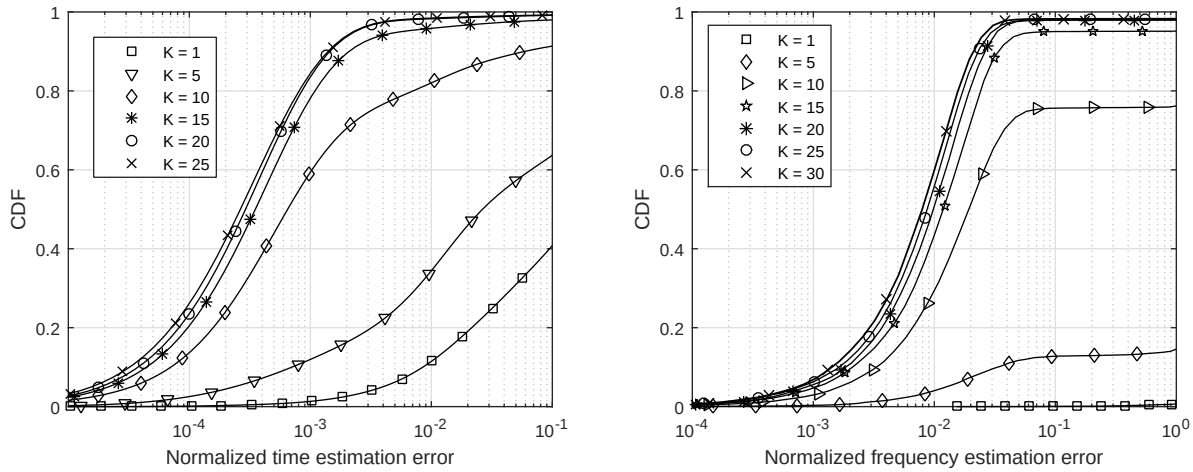


Figure 2.7: The synchronization error distribution under AWGN channels with disguised jamming attack.

in terms of synchronization for AWGN channels. The system parameters are listed in Table 2.1. We first compute the average correlation coefficients at different time offsets and phase shift sequence offsets for the received signal as in (2.17), and the result is plotted in Fig. 2.6 for $K = 40$[3]. Here, K denotes the number of OFDM blocks used for estimation. It shows that with the secure precoding scheme, even under disguised jamming, the receiver is able to correctly estimate the time offset as well as the phase shift sequence offset of the legitimate signal. Then we simulate the synchronization accuracy of SP-OFDM by calculating the cumulative distribution functions (CDFs) of the estimation errors with different numbers of OFDM blocks K to average the correlation coefficients. We normalize the time offset by the duration of one OFDM block T_b and the frequency offset by the sub-carrier spacing $1/T_s$, and the results are shown in Fig. 2.7. It can be observed that under the given setup, with 25 OFDM blocks to compute the correlation coefficients, the synchronization algorithm is robust under disguised jamming, where 99% cases have less than 0.01 *normalized* time offset estimation errors and 98% cases have less than 0.04 *normalized* frequency offset estimation errors.

Example 2: Synchronization performance under disguised jamming in multi-path fading channels: In this example, we simulate the synchronization accuracy of SP-OFDM under disguised jamming in static and time varying multi-path fading channels, which are modeled as 4 paths fading channels with a maximum delay spread of $3T_s/256$. Fig. 2.8 shows the estimation error distribution in the static channel. A slight performance loss is observed compared with the AWGN case, where 98% cases have less than 0.02 *normalized* time offset estimation errors and 96.5% cases have less than 0.04 *normalized* frequency offset

[3]In the 802.11a WLAN [66], 40 OFDM blocks correspond to 1440 data bytes with 64QAM mapping, while the OFDM frame length can be as large as 2312 bytes.

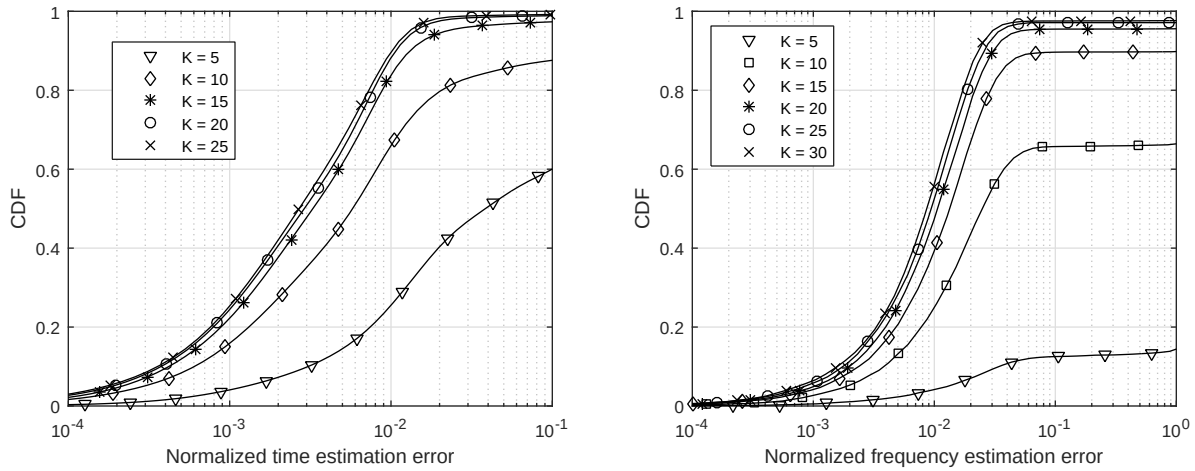


Figure 2.8: The synchronization error distribution under static multi-path fading channels with disguised jamming attack.

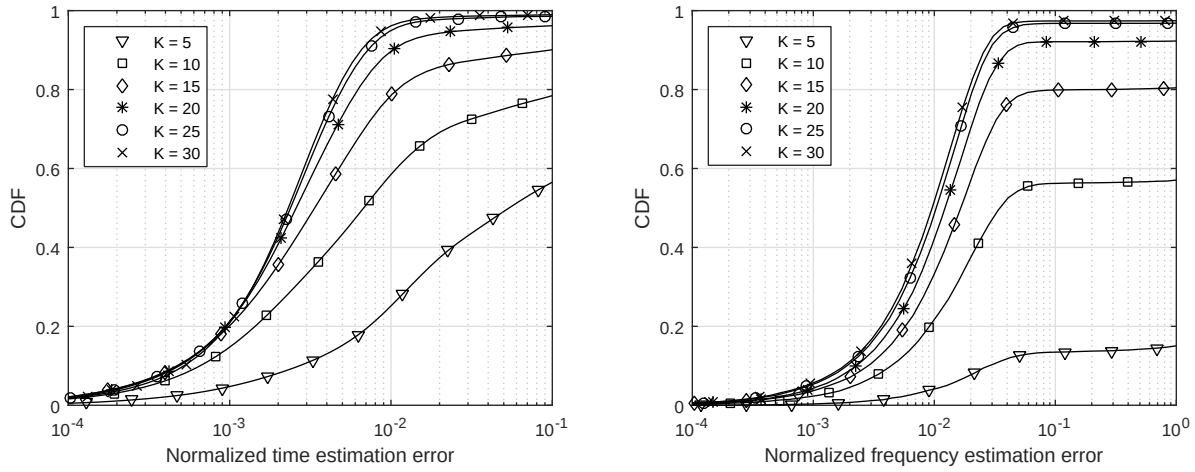


Figure 2.9: The synchronization error distribution under time varying multi-path fading channels with disguised jamming attack.

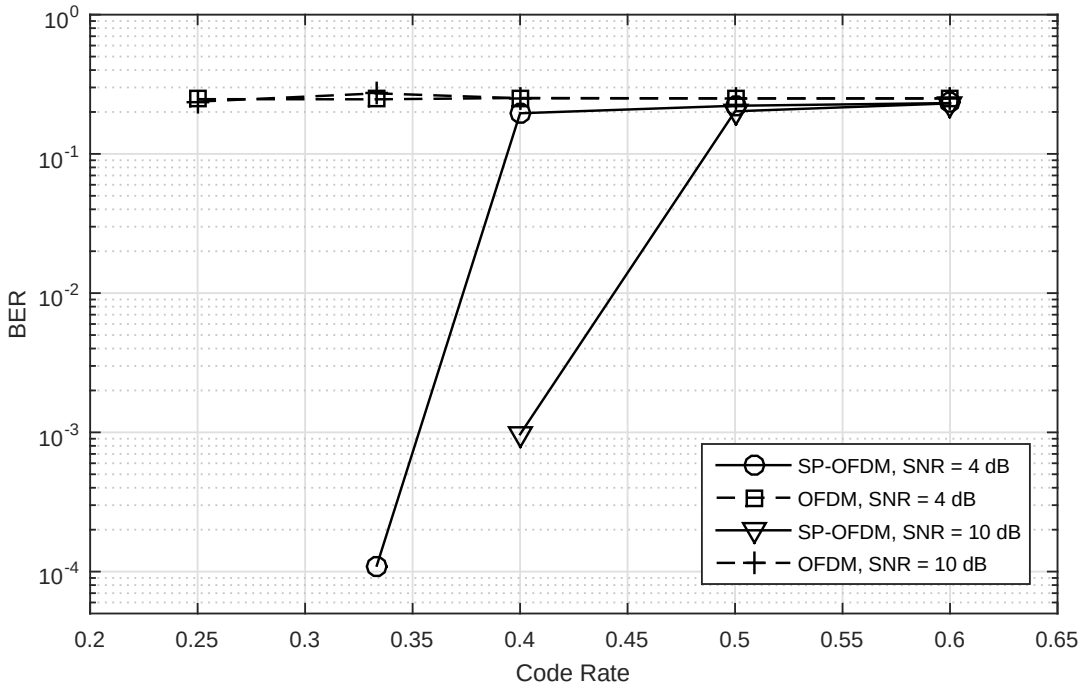


Figure 2.10: BER performance comparison under disguised jamming in AWGN channels: SP-OFDM versus the traditional OFDM system, signal to jamming power ratio (SJR) = 0 dB.

estimation errors using 25 OFDM blocks in estimation. To demonstrate the effectiveness of the synchronization algorithm under slow time varying channels, we introduce a Doppler shift to each path with a maximum value of 2% sub-carrier spacing ($0.02/T_s$) in the multi-path fading channel. Fig. 2.9 shows the estimation error distribution under the time-varying multi-path fading channel, where around 98% cases have less than 0.02 normalized time offset estimation errors and 96.5% cases have less than 0.04 normalized frequency offset estimation errors using 30 OFDM blocks in estimation. The simulation results illustrate the robustness of SP-OFDM against disguised jamming attacks under various channel conditions.

Example 3: BER performance under disguised jamming in AWGN channels: In this example, we analyze the bit error rate (BER) of the proposed system under disguised jamming in AWGN channels. Perfect synchronization is assumed. We use the low density

parity check (LDPC) codes for channel coding, and adopt the parity check matrices from the DVB-S.2 standard [74]. The coded bits are mapped into QPSK symbols. The random phase shifts in the proposed secure precoding are approximated as i.i.d. continuous RVs uniformly distributed over $[0, 2\pi)$. We observe that such an approximation has negligible difference on BER performance compared with a sufficiently large M. The jammer randomly selects one of the codewords in the LDPC codebook and sends it to the receiver after the mapping and modulation. On the receiver side, we use a soft decoder for the LDPC codes, where the belief propagation (BP) algorithm [75] is employed. The likelihood information in the BP algorithm is calculated using the likelihood function of a general Gaussian channel, where the noise power is set to $1 + \sigma^2$ considering the existence of the disguised jamming, and σ^2 is the noise power. That is, the signal to jamming power ratio (SJR) is set to be 0 dB. It should be noted that for more complicated jamming distributions or mapping schemes, customized likelihood functions basing on the jamming distribution will be needed for the optimal performance. Fig. 2.10 compares the BERs of the communication system studied with and without the proposed secure precoding under different code rates and SNRs. It can be observed that: (i) under the disguised jamming, in the traditional OFDM system, the BER cannot really be reduced by decreasing the code rate or the noise power, which indicates that without appropriate anti-jamming procedures, the traditional OFDM cannot achieve reliable communications under disguised jamming; (ii) with the proposed SP-OFDM scheme, when the code rates are below certain thresholds, the BER can be significantly reduced with the decrease of code rates using the proposed secure precoding. This demonstrates that the proposed SP-OFDM system can achieve a positive deterministic channel coding capacity under disguised jamming.

Example 4: BER performance under disguised jamming in Rician channels:

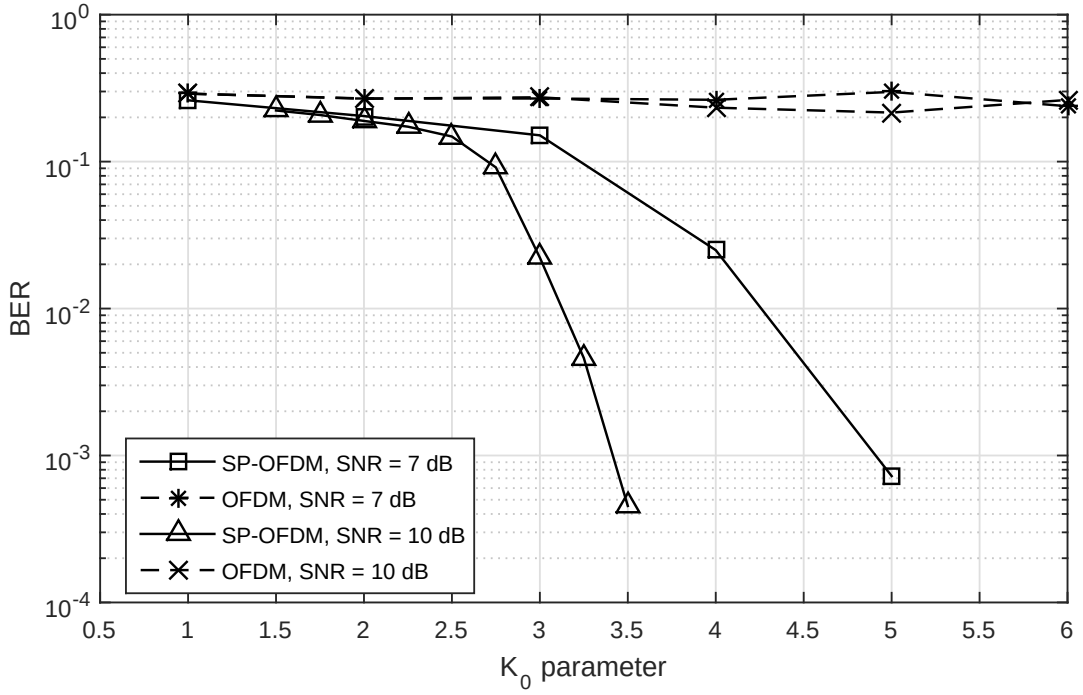


Figure 2.11: BER performance comparison under disguised jamming in Rician channels: code rate = 1/3, SJR = 0 dB. Here the K_0 parameter refers to the power ratio between the direct path and the scattered path.

In this example, we verify the effectiveness of the proposed system in fading channels. We consider a Rician channel, where the multipath interference is introduced and a strong line of sight (LOS) signal exists [76]. The fading effect is slow enough so that the channel remains unchanged for one OFDM symbol duration. In the simulation, we set the power of the direct path of Rician channel to be 1 and vary the K_0 parameter, which is the ratio between the power of the direct path and that of the scattered path. Fig. 2.11 shows the BERs for LDPC code rate 1/3 under disguised jamming. It can be observed that the proposed system is still effective under the fading channel with a sufficient large K_0 parameter. For a small K_0 parameter, i.e., when the fading is severe, channel estimation and equalization will be needed to guarantee a reliable communication.

2.6 Summary

In this chapter, we designed a highly secure and efficient OFDM system under disguised jamming, named securely precoded OFDM (SP-OFDM), by exploiting secure symbol-level precoding basing on phase randomization. We demonstrated the destructive effect of disguised jamming on the traditional OFDM system, and proved the robustness of SP-OFDM against disguised jamming in terms of synchronization and channel capacity. First, we showed that the traditional OFDM cannot distinguish between the legitimate signal and disguised jamming in the synchronization process, while SP-OFDM, with the secure CP, can achieve accurate synchronization under disguised jamming. Second, we analyzed the channel capacity of the traditional OFDM and the proposed SP-OFDM under hostile jamming using the arbitrarily varying channel (AVC) model. It was shown that the deterministic coding capacity of the traditional OFDM is zero under the worst disguised jamming; on the other hand, with the secure randomness shared between the authorized transmitter and receiver, the AVC channel corresponding to SP-OFDM is not symmetrizable, and hence SP-OFDM can achieve a positive capacity under disguised jamming. Both our theoretical and numerical results demonstrated that SP-OFDM is robust under disguised jamming and frequency selective fading. Potentially, SP-OFDM is a promising modulation scheme for high speed transmission under hostile environments, and the secure precoding scheme proposed in this chapter can also be applied to modulation techniques other than OFDM.

Chapter 3

The Worst Jamming Analysis and the Performance of SP-OFDM under the Worst Jamming

In Chapter 2, we saw that without secure precoding, disguised jamming is the worst jamming that can cause the deterministic channel capacity to be zero, while SP-OFDM is still robust against disguised jamming. An interesting question is: when secure precoding is applied, what would be the worst jamming distribution that minimizes the channel capacity of SP-OFDM?

In this chapter, by exploiting tools in constrained functional optimization, we explore the worst jamming distribution that minimizes the channel capacity of SP-OFDM under practical assumptions, where the transmitted symbols are uniformly distributed over a finite alphabet, and the jamming interference is subject to an average power constraint, but may or may not have a peak power constraint. First, we prove the existence and uniqueness of the worst jamming distribution. Second, by analyzing the Kuhn-Tucker conditions for the worst jamming, we prove that the worst jamming distribution is discrete in amplitude with a finite number of mass points, either with or without peak power constraints. Numerical results are provided on the worst jamming distribution and the minimum channel capacity

under disguised jamming. However, due to the inherent secure randomness in SP-OFDM, disguised jamming is no longer the worst jamming for SP-OFDM.

3.1 Introduction

The channel capacity evaluation of SP-OFDM under additive jamming is formulated as a minimax optimization problem, where the legitimate transmitter aims to maximize the mutual information (MI) between the transmitted signal and received signal while the jammer aims to minimize it. It was shown in Chapter 2 that, given the average power constraints for both the legitimate transmitter and jammer, the minimax problem exists a saddle point solution, that is, the minimax capacity is achieved when both the legitimate signal and the jamming interference follow the Gaussian distribution. The underlying argument is that assuming a Gaussian input distribution for SP-OFDM, then the worst jamming distribution should also be Gaussian. However, such a result might not be applicable to practical communication systems, where (i) the input distribution is generally a uniform distribution over a finite constellation, and (ii) practical RF amplifiers will exert certain peak power constraints on the transmitted signals. Taking these two constraints into consideration, in this chapter, we discuss the worst jamming distribution which minimizes the channel capacity of SP-OFDM under practical communication scenarios, and aim to provide a more in-depth understanding on the performance lower bound of SP-OFDM under jamming.

We formulate the worst jamming problem as a constrained functional optimization process [77] following the literature on the capacity-achieving input distributions under different channel constraints. In [78, 79], the capacity-achieving input distribution in Gaussian channels under average and peak power constraints were studied. The capacity-achieving input

distributions in Rayleigh-fading and Rician-fading channels were analyzed in [80] and [81], respectively. In [82], the optimal input distribution was analyzed under non-coherent Gaussian channels, where random phase shifts were applied to the transmitted signals. A good summary in this line of research was provided in [83]. More recently, the capacity-achieving input distributions were explored for Gaussian MAC channels with peak power constraints [84], Gaussian Mixture Noise channels [85], Gaussian MIMO channels with peak power constraints [86] and signal-dependent noise channels [87]. One common result among the existing work is that, the capacity-achieving input distributions for these channels are often discretely distributed in amplitude [88].

In this chapter, applying the constrained functional optimization to the channel capacity of SP-OFDM, we show that the worst jamming distribution for SP-OFDM should be discrete in amplitude with a finite number of mass points. More specifically,

- We prove the existence, uniqueness and the Kuhn-Tucker conditions of the worst jamming distribution for SP-OFDM, either with or without a peak power constraint on jamming. The major challenge in the analysis lies in the derivation of the tight bounds on the distribution function of the channel output for any given jamming distribution. We obtain both the upper and lower bounds by exploiting some inequalities involving the modified Bessel functions from literature [89–91].

- We prove the discreteness of the worst jamming distribution for SP-OFDM, either with or without peak power constraints, and show that the worst jamming distribution has a finite number of mass points. More specifically, we first derive a lower bound of the Kuhn-Tucker function for the worst jamming distribution. Second, by applying the identity theorem, we show that any non-discrete jamming distribution cannot satisfy

the Kuhn-Tucker conditions of the worst jamming distribution under a finite peak power constraint. Finally, by further exploiting the derived lower bound on the Kuhn-Tucker function, we show that when the peak power constraint is sufficiently large, the worst jamming under the peak power constraint is identical with the worst jamming without peak power constraint. We further discuss the maximal amplitude of the worst jamming distribution in different cases, and show that the worst jamming distribution always has a mass point at the peak power constraint when the average power constraint is inactive.

- Numerical results are provided on the worst jamming distribution and the minimal channel capacity under disguised jamming. The numerical results are consistent with the theoretical analysis, that is, the worst jamming is discrete in amplitude with a finite number of mass points; the minimal channel capacity of SP-OFDM is guaranteed to be positive under disguised jamming, which demonstrates the robustness of SP-OFDM under disguised jamming. We further study the impact of the power constraints. It is shown that the worst jamming distribution tends to have more mass points as the peak jamming power increases, while with the decrease of average jamming power, there is a larger chance for the jammer to keep silent for energy saving and the best jamming effect.

We would like to point out that in functional optimization of channel capacity, the analysis is generally more complex without the peak power constraint, compared to that with a finite peak power constraint [83]. Existing work on optimal input distribution analysis without peak power constraint generally involves complicated integral transforms (such as the Hankel transform) [82,85]. To overcome this obstacle, in this chapter, our analysis on worst jamming

distribution is decomposed into two steps: first, we prove the discreteness of the worst jamming distribution under finite peak power constraints; second, we generalize the result to the case without peak power constraint. Through this two-step approach, the analysis can be conducted without the integral transforms, and hence be significantly simplified.

3.2 Problem Formulation

From our previous discussions in Chapter 2, we can see that: *for an AWGN channel $R = S + J + N$, when (i) the constellation of the authorized signal, Φ, is fixed; (ii) S is uniformly distributed over Φ; and (iii) no secure symbol-level precoding is involved, then the worst jamming is the disguised jamming that has an identical distribution with S. In this case, the deterministic coding capacity is zero. That is, the traditional OFDM has zero deterministic coding capacity under disguised jamming.*

However, in this chapter, we will show that for systems with secure precoding, i.e.,

$$R = S + e^{j\Theta} J + N, \tag{3.1}$$

disguised jamming is no longer the worst jamming in terms of channel capacity.

From Lemma 2.1, with the AES-based phase randomization, the channel capacity equals the maximin mutual information between S and R, $I(S, R)$. In this section, we consider the maximin problem,

$$\begin{aligned} C &= \max_{\mathcal{P}_S} \min_{F_J} I(S, R), \\ s.t. \quad & \textstyle\int_{\mathbb{C}} |\boldsymbol{x}|^2 \mathrm{d}F_J(\boldsymbol{x}) \leq P_J, \end{aligned} \tag{3.2}$$

in practical communication systems, by considering (i) the transmitted symbol is uniformly

distributed in the alphabet, and (ii) there *might* exist a constraint on the peak power of the jamming interference.

Let the transmitting alphabet $\Phi = \{\boldsymbol{s}_1, \boldsymbol{s}_2, ..., \boldsymbol{s}_{M_\Phi}\}$. The size of Φ is $|\Phi| = M_\Phi$. In realistic communication systems, S is uniformly distributed over Φ , i.e.,

$$\Pr\{S = \boldsymbol{s}_i\} = \frac{1}{M_\Phi}, \quad i \in \{1, 2, ..., M_\Phi\}. \tag{3.3}$$

Hence, the calculation of the capacity in (3.2) is reduced to finding the CDF F_J of the jamming interference that minimizes the MI $I(S, R)$, under an average power constraint of P_J, with a possible peak power constraint. .

The phase shift Θ is controlled by the authorized user, and is uniformly distributed over $\{\frac{2\pi l}{M} \mid l = 0, 1, ..., M-1\}$. When M is sufficiently large (e.g., $M \gg \frac{2\pi}{\sigma_\Theta^2}$, where σ_Θ^2 is the variance of the phase noise existing in practical communication systems), taking the noise effect into consideration, we can approximately model Θ as a continuous RV uniformly distributed over $[0, 2\pi)$, and independent of J. In this way, the phase item within J can be completely absorbed into Θ. As a result, we only need to find the CDF of $|J|$ that minimizes the MI in (3.2). Without loss of generality, in the following, J is degraded to a RV over $\mathbb{R}$.

Let $\mathcal{F}_a$ be the set of all the possible CDFs $F_J(\cdot)$ of $J \in \mathbb{R}$, where the peak amplitude is bounded by a, and $a \in (0, \infty)$ or $a = \infty$. For $a \in (0, \infty)$, the peak jamming power is bounded by a^2, and $\mathcal{F}_a$ is defined as

$$\begin{aligned}\mathcal{F}_a = &\{F(\cdot) \mid F(0^-) = 0, F(a) = 1, \\ &F(x) \text{ is nondecreasing and right-continuous}\}.\end{aligned}$$

For the special case $a = \infty$, the jamming interference is not peak power limited, where

$$\begin{aligned}\mathcal{F}_\infty =&\{F(\cdot) \mid F(0^-) = 0, \lim_{x\to\infty} F(x) = 1,\\ &F(x) \text{ is nondecreasing and right-continuous}\}.\end{aligned}$$

In both cases, $\mathcal{F}_a$ is a convex set. For any $a \in (0, \infty)$, $\mathcal{F}_a \subset \mathcal{F}_\infty$. Unless otherwise specified, the following analysis of this chapter applies to both cases of $\mathcal{F}_a$.

Note that the MI $I(S, R) = H(S) - H(S|R)$ and S is uniformly distributed over Φ. Define functional $G(\cdot)$ as

$$G(F_J) \stackrel{\Delta}{=} -H(S|R). \tag{3.4}$$

Given that S is uniformly distributed over Φ, the maximin problem (3.2) can be reduced to

$$\begin{aligned}&\min_{F_J(\cdot)\in\mathcal{F}_a} G(F_J)\\ s.t.\quad &\int_0^\infty x^2 \mathrm{d}F_J(x) \le P_J\end{aligned} \tag{3.5}$$

The optimal solution to (3.5) is the worst jamming distribution that results in the minimal capacity from the information theoretic point of view. In the following, we will discuss the worst jamming distribution F_J to (3.5). The main result is that the worst jamming distribution should be discrete in amplitude with a finite number of mass points.

3.3 Preliminary Results

In this section, to pave the way for a thorough analysis on the optimization problem in (3.5), we first derive the specific expression of functional $G(\cdot)$; then we derive several important

inequalities involving the modified Bessel function of the first kind. These results are essential for the analysis on the worst jamming distribution in Sections 3.4 and 3.5.

The conditional distribution of the received signal R is provided the following lemma.

Lemma 3.1 *For noise power σ^2, the conditional PDF of R given S and J is given by*

$$f_{R|S,J}(\boldsymbol{r} \mid \boldsymbol{s}_i, x) = u(|\boldsymbol{r} - \boldsymbol{s}_i|, x), \boldsymbol{r} \in \mathbb{C}, \boldsymbol{s}_i \in \Phi, x \geq 0 \tag{3.6}$$

where

$$u(x, y) \triangleq \frac{1}{\pi\sigma^2} e^{-\frac{x^2+y^2}{\sigma^2}} I_0(\frac{2xy}{\sigma^2}),\ x \geq 0, y \geq 0, \tag{3.7}$$

and $I_0(\cdot)$ is the modified Bessel function of the first kind with order 0.

Proof: Please refer to Appendix B. □

Following Lemma 3.1,

$$f_R(\boldsymbol{r}) = \frac{\sum_i f_{R|S}(\boldsymbol{r} \,|\, \boldsymbol{s}_i)}{M_\Phi} = \frac{\sum_i \int_0^\infty u(|\boldsymbol{r} - \boldsymbol{s}_i|, x) \mathrm{d}F_J(x)}{M_\Phi}, \tag{3.8}$$

$$\Pr\{S = \boldsymbol{s}_i \mid R = \boldsymbol{r}\} = \frac{\int_0^\infty u(|\boldsymbol{r} - \boldsymbol{s}_i|, x) \mathrm{d}F_J(x)}{M_\Phi \cdot f_R(\boldsymbol{r})}. \tag{3.9}$$

For notation simplicity, define functionals $Q_i(\boldsymbol{r}, F)$ and $L_i(\boldsymbol{r}, F)$ over $\mathbb{C} \times \mathcal{F}_a$ as

$$Q_i(\boldsymbol{r}, F) = \int_0^\infty u(|\boldsymbol{r} - \boldsymbol{s}_i|, x) \mathrm{d}F(x),\ \boldsymbol{r} \in \mathbb{C}, F \in \mathcal{F}_a. \tag{3.10}$$

$$L_i(\boldsymbol{r}, F) = \log\left(\frac{Q_i(\boldsymbol{r}, F)}{\sum_k Q_k(\boldsymbol{r}, F)}\right),\ \boldsymbol{r} \in \mathbb{C}, F \in \mathcal{F}_a. \tag{3.11}$$

Therefore $G(F_J)$ can be expressed as

$$G(F_J) = \frac{1}{M_\Phi} \sum_i \int_{\mathbb{C}} Q_i(\boldsymbol{r}, F_J) L_i(\boldsymbol{r}, F_J) \mathrm{d}\boldsymbol{r}. \tag{3.12}$$

Moreover, $I(S, R)$ is a convex function w.r.t. $F_J(\cdot)$, so is $G(\cdot)$. That is, $G((1-\lambda)F_1 + \lambda F_2) \leq (1-\lambda)G(F_1) + \lambda G(F_2)$ for any $\lambda \in [0, 1]$ and $F_1, F_2 \in \mathcal{F}_a$.

For any $P \geq 0$, define functional $K_P(\cdot)$ as:

$$K_P(F) \triangleq \int_0^\infty x^2 \mathrm{d}F(x) - P. \tag{3.13}$$

Let $P = P_J$, the average jamming power constraint, and define

$$\Omega(a, P_J) \triangleq \{F(\cdot) \mid F(\cdot) \in \mathcal{F}_a, K_{P_J}(F) \leq 0\}. \tag{3.14}$$

The optimization problem (3.5) can be expressed equivalently as

$$\min_{F \in \Omega(a, P_J)} G(F). \tag{3.15}$$

In the following, the subscript J in the distribution function and the average power constraint is discarded for brevity. For notation simplicity, we use Ω to denote $\Omega(a, P)$ when the peak amplitude constraint a and average power constraint P of jamming interference are fixed in the context.

We derive an upper and lower bound on the integral $\int_0^\infty u(x, y) \mathrm{d}F(y)$ in the following lemma.

Lemma 3.2 *For any CDF $F(\cdot) \in \Omega$, integral $\int_0^\infty u(x, y) dF(y)$ has the following upper and*

lower bound:

- ***Upper Bound****: there exists some constant $c_0 \in (0, \infty)$ independent of $F(\cdot)$ such that for any sufficiently large $x \in [0, \infty)$,*

$$\int_0^\infty u(x, y)\, dF(y) \leq \frac{c_0}{x^{2.5}}. \tag{3.16}$$

- ***Lower Bound****: there exists some constant $c_0' \in (0, \infty)$ independent of $F(\cdot)$ such that*

$$\int_0^\infty u(x, y)\, dF(y) \geq \begin{cases} c_0', & 0 \leq x \leq \sigma, \\ \dfrac{I_0(\frac{4x^2}{\sigma^2})\left(1 - \frac{P}{4x^2}\right)}{\pi\sigma^2 e^{5x^2/\sigma^2}}, & x > \sigma. \end{cases} \tag{3.17}$$

Proof: Please refer to Appendix C. □

In addition, we derive an upper bound for the ratio of $\int_0^\infty u(x_1, y)\mathrm{d}F(y) / \int_0^\infty u(x_2, y)\mathrm{d}F(y)$ when the jamming interference is peak power constrained, which is stated in the following lemma.

Lemma 3.3 *If the peak amplitude $a \in (0, \infty)$, for any CDF $F(\cdot) \in \Omega$, and $x_1 > x_2 > 0$, we have*

$$\frac{\int_0^a u(x_1, y)\, dF(y)}{\int_0^a u(x_2, y)\, dF(y)} < e^{\frac{x_2^2 - x_1^2 + 2(x_1 - x_2)a}{\sigma^2}}. \tag{3.18}$$

Proof: Please refer to Appendix D. □

3.4 Existence of the Worst Jamming Distribution

In this section, we verify the existence of the worst jamming distribution and derive the necessary and sufficient conditions for the worst jamming distribution from the Kuhn-Tucker (KT) theorem.

We first show that the minimum of functional $G(F)$ over Ω is achievable. More specifically, we have:

Theorem 3.1 *Given $\Omega = \{F(\cdot) \mid F(\cdot) \in \mathcal{F}_a, K_P(F) \leq 0\}$, where P is the average jamming power constraint, and $G(F) = -H(S \mid R)$ on set Ω. The real-valued functional $G(\cdot)$ can achieve its minimum on Ω.*

The proof of Theorem 3.1 is based on the following lemma, which makes use of the weak* topology on the set of CDFs over $\mathbb{R}$.

Lemma 3.4 *[80] If G is a real-valued, weak* continuous functional [1] [77] on a weak* compact set [2] [77] Ω, then G achieves its minimum on Ω.*

Proof: [Proof of Theorem 3.1] Please refer to Appendix E. □

Having proved the existence of the worst jamming distribution over Ω, we will further show that the worst jamming distribution is also unique.

Corollary 3.1 *The jamming distribution $F^* \in \Omega$ that minimizes functional $G(\cdot)$ is unique.*

Proof: Please refer to Appendix F. □

[1] A functional G defined on X^* is weak* continuous iff for each $x^* \in X^*$ and each neighborhood V of $f(x^*)$, there is a neighborhood U of x^* such that $f(U) \subset V$. Here, X^* denotes the set of CDFs over $\mathbb{R}$.

[2] A set $K \subset X^*$ is said to be weak* compact if every finite sequence from K contains a weak* convergent subsequence.

As we are solving a constrained optimization problem, following the Kuhn-Tucker Theorem [77] [80], we can obtain the Lemma below.

Lemma 3.5 *For a convex subset $\mathcal{D}$ of a linear vector space, let f and g be two real-valued convex functionals defined on $\mathcal{D}$. Suppose there exits an $F_1(\cdot) \in \mathcal{D}$ such that $g(F_1) < 0$, and*

$$C = \inf_{F(\cdot)\in\mathcal{D}, g(F)\leq 0} f(F), \tag{3.19}$$

where C is finite, then there exists a $\gamma \geq 0$, such that

$$C = \inf_{F(\cdot)\in\mathcal{D}} \{f(F) + \gamma g(F)\}. \tag{3.20}$$

Furthermore, if the infimum in (3.19) is achieved at $F_0(\cdot) \in \{F \mid F \in \mathcal{D}, g(F) \leq 0\}$, then the infimum in (3.20) is also achieved at F_0, and $\gamma g(F_0) = 0$.

For our problem of interest, let $\mathcal{D}$ be $\mathcal{F}_a$ and $g(\cdot)$ be $K_P(\cdot)$. It is obvious that for any average power constraint $P > 0$, there always exists an $F \in \mathcal{F}_a$ such that $K_P(F) < 0$. Combining Lemma 3.4 and Lemma 3.5, we can obtain the following result.

Theorem 3.2 *There exists a unique solution to the constrained convex optimization problem (3.5) on Ω. If $F_0(\cdot) \in \Omega$ is the solution to (3.5), then there exists a $\gamma \geq 0$ such that $F_0(\cdot)$ is also the solution to the Lagrangian dual problem*

$$\min_{F\in\mathcal{F}_a} G(F) + \gamma K_P(F) \tag{3.21}$$

and $\gamma K_P(F_0) = 0$.

It should be noted that when $a = \infty$, the Lagrangian multiplier $\gamma > 0$. To see this,

consider the case $\gamma = 0$. Following (3.3), the value of the target function in (3.21) can be arbitrarily close to $-\log M_\Phi$. This indicates the worst jamming could render a zero channel capacity, that is, the distribution of R is independent of S, which is impossible under the average power constraint considering the fact that the characteristic function (CF) of R is a product of those of S, $Je^{j\Theta}$ and N.

Next we analyze the necessary and sufficient conditions satisfied by the minima in the dual problem. Before that, the definition of the weak differentiability is introduced.

Definition 3.1 *[78] Let f be a functional on a convex set $\mathcal{D}$. Let $F_0 \in \mathcal{D}$ and $\theta \in [0,1]$. Suppose that there exists a map defined as*

$$f'(F_0, F) = \lim_{\theta \to 0, \theta > 0} \frac{f((1-\theta)F_0 + \theta F) - f(F_0)}{\theta}, \quad \forall F \in \mathcal{D}, \tag{3.22}$$

then f is said to be weakly differentiable at F_0, and $f'(F_0, \cdot)$ is called its weak derivative at F_0. If f is weakly differentiable for every $F_0 \in \mathcal{D}$, f is said to be weakly differentiable over $\mathcal{D}$.

The weak derivatives of functional $G(\cdot)$ and $K_P(\cdot)$ are provided in the following Lemma.

Lemma 3.6 *Define functional $g(\cdot\ ;\ \cdot)$ over $[0,\infty) \times \Omega$ as*

$$g(x; F) \triangleq \frac{\sum_i \int_{\mathbb{C}} u(|\boldsymbol{r} - \boldsymbol{s}_i|, x) L_i(\boldsymbol{r}, F) d\boldsymbol{r}}{M_\Phi}, \quad x \geq 0, F \in \Omega. \tag{3.23}$$

The weak derivatives of $G(\cdot)$ and $K_P(\cdot)$ at any $F_0 \in \Omega$ are given by

$$G'(F_0, F) = \int_0^\infty g(x; F_0) dF(x) - G(F_0), F \in \Omega, \tag{3.24}$$

$$K'_P(F_0, F) = \int_0^\infty x^2 d(F(x) - F_0(x)), F \in \Omega. \tag{3.25}$$

Proof: The weak derivative of $G(\cdot)$ is derived in Appendix G. The weak derivative of $K_P(\cdot)$ was given in [80]. □

The following lemma states the conditions satisfied by the optima for a weakly differentiable target functional.

Lemma 3.7 *[78, 80] Assume a weakly differentiable functional f over a convex set $\mathcal{D}$.*

1. *If f achieves its minimum at F_0, then $f'(F_0, F) \geq 0, \forall F \in \mathcal{D}$.*
2. *If f is convex, then $f'(F_0, F) \geq 0, \forall F \in \mathcal{D}$, implies that f achieves its minimum at F_0.*

From Lemma 3.6, the target functional in the dual problem (3.21) is weakly differentiable over $\mathcal{F}_a$. Applying Lemma 3.7 to the dual problem, the following result can be obtained.

Theorem 3.3 *A necessary and sufficient condition for $F_0(\cdot) \in \Omega$ to be the minima of the dual problem (3.21) is, $\forall F(\cdot) \in \Omega$,*

$$\int_0^\infty [g(x; F_0) + \gamma x^2] dF(x) \geq G(F_0) + \gamma \int_0^\infty x^2 dF_0(x). \tag{3.26}$$

Moreover, if γ satisfies $\gamma K_P(F_0) = 0$, then F_0 is also the minima of the primal problem (3.5).

Proof: The result follows directly from Lemma 3.6 and Lemma 3.7, and the fact that $G(\cdot)$ and $K_P(\cdot)$ are convex functionals over the convex set $\mathcal{F}_a$. □

Furthermore, the following conditions on the worst jamming distribution can be derived from (3.26) following the approach in [80].

Corollary 3.2 *Let $E_0 \subseteq [0, +\infty)$ be the set of points of increase* [3] *of a distribution function $F_0(\cdot) \in \Omega$.*

$$\int_0^\infty [g(x; F_0) + \gamma x^2] dF(x) \geq G(F_0) + \gamma \int_0^\infty x^2 dF_0(x), \forall F(\cdot) \in \Omega, \tag{3.27}$$

iff

$$g(x; F_0) + \gamma x^2 \geq G(F_0) + \gamma \int_0^\infty t^2 dF_0(t),$$
$$\forall x \in \begin{cases} [0, a], & a \in (0, \infty) \\ [0, \infty), & a = \infty \end{cases}, \tag{3.28}$$

and

$$g(x; F_0) + \gamma x^2 = G(F_0) + \gamma \int_0^\infty t^2 dF_0(t), \quad \forall x \in E_0. \tag{3.29}$$

In the following, we refer to (3.28) and (3.29) as the *KT conditions*.

3.5 Discreteness of the Worst Jamming Distribution

In this section, we first prove that when the jamming interference is peak power limited, i.e., $a \in (0, \infty)$, in order for the optimal CDF function to satisfy (3.28) and (3.29), the corresponding optimal jamming distribution should be discrete in amplitude with a finite number of mass points; then we conduct the analysis for the case of $a = \infty$ and obtain a

[3] A point $x_0 \in [0, a]$ is said to be a point of increase of the CDF function $F_0(\cdot)$ iff $\exists \delta > 0$, such that $\forall 0 < \varepsilon \leq \delta$, $\int_{x_0-\varepsilon}^{x_0+\varepsilon} \mathrm{d}F_0(x) > 0$

consistent result; at last, we discuss the maximal amplitude of the worst jamming distribution in different cases.

The proof of discreteness makes use of the facts in complex analysis, i.e., the identity theorem [92], to show that condition (3.29) cannot be satisfied over an infinite number of points within any bounded interval. To facilitate the application of the identity theorem, we first prove the following Lemma.

Lemma 3.8 *The function in Corollary 3.2*

$$g(z;F)+\gamma z^2 \tag{3.30}$$

is an analytic function w.r.t. $z\in\mathbb{C}$ *for any CDF function* $F(\cdot)\in\Omega$.

Proof: Please refer to Appendix H. □

Next, we derive a closed form lower bound of $g(x;F)$ on $x\in\mathbb{R}$ when the jamming interference is peak power constrained.

Proposition 3.1 *Suppose the jamming interference is peak power constrained, i.e.,* $a\in(0,\infty)$. *For any* $F(\cdot)\in\mathcal{F}_a$, $g(x;F)$ *is lower bounded by*

$$g(x;F)\geq\kappa(a)-\frac{4\bar{s}}{\sigma}\Gamma(\frac{3}{2})\frac{M(\frac{3}{2},1;\frac{x^2}{\sigma^2})}{e^{x^2/\sigma^2}}, \tag{3.31}$$

where $\bar{s}=\max_k|\boldsymbol{s}_k|$, $\kappa(a)\overset{\Delta}{=}-\log M_\Phi-4\bar{s}(\bar{s}+a)/\sigma^2$, $\Gamma(\cdot)$ *denotes the gamma function and* $M(\cdot,\cdot;\cdot)$ *the Kummer's M function. For any* $\zeta\in(0,\infty)$, *we further have*

$$g(x;F)\geq\kappa(a)-\frac{4\bar{s}x}{\sigma^2}\Gamma(\frac{3}{2})\frac{M(\frac{3}{2},1;\zeta)}{\sqrt{\zeta}e^{\zeta}},\ x\in[\sigma\sqrt{\zeta},\infty). \tag{3.32}$$

Proof: Since $L_i(\boldsymbol{r}, F) < 0$, a lower bound of $L_i(\boldsymbol{r}, F)$ is

$$L_i(\boldsymbol{r}, F) \geq -\max_k \left\{ \log \frac{M_\Phi Q_k(\boldsymbol{r}, F)}{Q_i(\boldsymbol{r}, F)} \right\}. \tag{3.33}$$

With Lemma 3.3, an upper bound of $\frac{Q_k(\boldsymbol{r},F)}{Q_i(\boldsymbol{r},F)}$ is

$$\begin{aligned} \frac{Q_k(\boldsymbol{r}, F)}{Q_i(\boldsymbol{r}, F)} &\leq \exp\left(\frac{|\boldsymbol{r} - s_i|^2 - |\boldsymbol{r} - s_k|^2 + 2(|\boldsymbol{s}_k - \boldsymbol{s}_i|)a}{\sigma^2} \right) \\ &\leq \exp\left(\frac{4\bar{s}[|\boldsymbol{r} - \boldsymbol{s}_i| + \bar{s} + a]}{\sigma^2} \right). \end{aligned} \tag{3.34}$$

The lower bound of $L_i(\boldsymbol{r}, F)$ can be further derived as

$$L_i(\boldsymbol{r}, F) \geq -\log M_\Phi - \frac{4\bar{s}[|\boldsymbol{r} - \boldsymbol{s}_i| + \bar{s} + a]}{\sigma^2}. \tag{3.35}$$

We can derive a lower bound of $g(x; F)$ as

$$\begin{aligned} g(x; F) &= \frac{1}{M_\Phi} \sum_i \int_{\mathbb{C}} u(|\boldsymbol{r} - \boldsymbol{s}_i|, x) L_i(\boldsymbol{r}, F) \mathrm{d}\boldsymbol{r} \\ &\geq \int_{\mathbb{C}} u(|\boldsymbol{r}|, x) \left(\kappa(a) - \frac{4\bar{s}}{\sigma^2} |\boldsymbol{r}| \right) \mathrm{d}\boldsymbol{r}. \end{aligned} \tag{3.36}$$

Moreover, for any constant $v \in \mathbb{R}$,

$$\int_{\mathbb{C}} u(|\boldsymbol{r}|, x) |\boldsymbol{r}|^\nu \mathrm{d}\boldsymbol{r} = \frac{e^{-\frac{x^2}{\sigma^2}}}{\sigma^2} \int_0^\infty \frac{\rho^{\nu/2}}{e^{\rho/\sigma^2}} I_0\left(\frac{2x\sqrt{\rho}}{\sigma^2}\right) \mathrm{d}\rho. \tag{3.37}$$

From [93, 6.643], for any $Re(\mu + \frac{1}{2}) > 0$, we have

$$\int_0^\infty \frac{x^{\mu-\frac{1}{2}}}{e^{\alpha x}} I_0(2\beta\sqrt{x})\mathrm{d}x = \frac{\Gamma(\mu+\frac{1}{2})}{\beta}\alpha^{-\mu}e^{\frac{\beta^2}{2\alpha}}\mathcal{M}_{-\mu,0}(\frac{\beta^2}{\alpha}), \tag{3.38}$$

where $\mathcal{M}_{\cdot,\cdot}(\cdot)$ is the Whittaker M function. For the special case of $\mu = \frac{1}{2}$, we have $\mathcal{M}_{-\frac{1}{2},0}(x) = \sqrt{x}e^{\frac{x}{2}}$.

Therefore, the lower bound (3.36) can be further derived as

$$g(x;F) \geq \kappa(a) - 4\bar{s}\Gamma(\frac{3}{2})\frac{\mathcal{M}_{-1,0}(\frac{x^2}{\sigma^2})}{xe^{x^2/2\sigma^2}}, \tag{3.39}$$

which is equivalent to (3.31) as $\mathcal{M}_{-1,0}(x) = \sqrt{x}e^{-\frac{x}{2}}M(\frac{3}{2},1;x)$. Note that the second term on the R.H.S. of (3.31) is independent of a. We next show that $M(\frac{3}{2},1;x)/(\sqrt{x}e^x)$ is a decreasing function over $x \in (0,\infty)$.

By calculating the derivative of $M(\frac{3}{2},1;x)/(\sqrt{x}e^x)$ over $x \in (0,\infty)$, we can see that the sign of the derivative is the same as that of

$$2x\left[\frac{\mathrm{d}M(3/2,1,x)}{\mathrm{d}x} - M(3/2,1,x)\right] - M(3/2,1,x), \tag{3.40}$$

where

$$2x\left[\frac{\mathrm{d}M(3/2,1,x)}{\mathrm{d}x} - M(3/2,1,x)\right] = \sum_{n=1}^{\infty}\frac{n}{n+1/2}\frac{(3/2)_n}{(n!)^2}x^n, \tag{3.41}$$

which is less than $M(3/2,1,x)$. $M(\frac{3}{2},1;x)/(\sqrt{x}e^x)$ is hence a decreasing function over $x \in (0,\infty)$. So for any $\zeta \in (0,\infty)$,

$$\frac{M(\frac{3}{2},1;x)}{e^x} \leq \sqrt{x}\frac{M(\frac{3}{2},1;\zeta)}{\sqrt{\zeta}e^\zeta}, x \in [\zeta,\infty), \tag{3.42}$$

This completes the proof. □

In the following, we define

$$F_{a,P}^{*} \overset{\Delta}{=} \arg \min_{F \in \Omega(a,P)} G(F) \tag{3.43}$$

With Lemma 3.8 and Proposition 3.1, we are able to prove that the "optimal" (i.e., the worst) jamming distribution $F_{a,P}^{*}$ should be discrete with a finite number of mass points. However, instead of proving the general result directly, we first study the case when the jamming interference is peak power constrained.

Theorem 3.4 *Let $E_{a,P}^{*}$ denote the set of points of increase for the optimal jamming distribution $F_{a,P}^{*}$, then $E_{a,P}^{*}$ has a finite number of elements when $a \in (0, \infty)$.*

Proof:

We prove by contradiction that $|E_{a,P}^{*}| = \infty$ is impossible. First we show that if $|E_{a,P}^{*}| = \infty$, then for the worst jamming distribution $F_{a,P}^{*}$,

$$g(x; F_{a,P}^{*}) + \gamma x^2 \equiv G(F_{a,P}^{*}) + \gamma \int_0^{\infty} t^2 \mathrm{d}F_{a,P}^{*}(t), \quad \forall x \in \mathbb{R}. \tag{3.44}$$

In fact, since each point in $E_{a,P}^{*}$ is bounded on $[0, a]$, using the Bolzano-Weierstrass theorem, we can find an infinite sequence $x_n, n = 1, 2, ..., \infty$ in $E_{a,P}^{*}$ which has a limit point x^*, i.e.,

$$\lim_{n \to \infty} x_n = x^*, \text{and } x^* \in [0, a]. \tag{3.45}$$

From Corollary 3.2, we have $g(x_n; F_{a,P}^{*}) + \gamma x_n^2 \equiv G(F_{a,P}^{*}) + \gamma \int_0^{\infty} t^2 \mathrm{d}F_{a,P}^{*}(t), \forall x_n$. Since function $g(z; F_{a,P}^{*}) + \gamma z^2$ is analytic on $\mathbb{C}$ from Lemma 3.8, this implies its continuity on

$[0, a]$, where

$$g(x^*; F^*_{a,P}) + \gamma(x^*)^2 = G(F^*_{a,P}) + \gamma \int_0^\infty t^2 \mathrm{d}F^*_{a,P}(t). \tag{3.46}$$

From the Identity Theorem [92], if two analytic functions are identical on a infinite set of points (sequence x_n) in a region along with their limit points (x^*), these two functions are identical in the entire region. Therefore, we have

$$g(x; F^*_{a,P}) + \gamma x^2 - G(F^*_{a,P}) - \gamma \int_0^\infty t^2 \mathrm{d}F^*_{a,P}(t) \equiv 0, \forall x \in \mathbb{R}. \tag{3.47}$$

which is equivalent to (3.44).

Next we consider two cases: (1) $\gamma > 0$, and (2) $\gamma = 0$. We show that (3.44) cannot hold in either cases.

For $\gamma > 0$, from Proposition 3.1, for any given $\zeta \in (0, \infty)$, $x \geq \sigma\sqrt{\zeta}$, a lower bound of $g(x; F^*_{a,P}) + \gamma x^2$ is

$$g(x; F^*_{a,P}) + \gamma x^2 \geq \gamma x^2 - \frac{4\bar{s}x}{\sigma^2}\Gamma(\frac{3}{2})\frac{M(\frac{3}{2}, 1; \zeta)}{\sqrt{\zeta}e^\zeta} + \kappa(a), \tag{3.48}$$

which scales quadratically with x as $x \to \infty$. That is, when x is sufficiently large, $g(x; F^*_{a,P}) + \gamma x^2 - G(F^*_{a,P}) - \gamma \int_0^\infty t^2 \mathrm{d}F^*_{a,P}(t) > 0$, which contradicts with (3.47). So $|E^*_{a,P}| = \infty$ is impossible.

For $\gamma = 0$, the average power constraint is inactive, that is, the optimal jamming distribution obtained in this case equals that obtained with $P = \infty$. If for some a_0, $|E^*_{a_0,\infty}| = \infty$, it follows from (3.47) that

$$g(x; F^*_{a_0,\infty}) - G({F_{a_0,\infty}}^*) \equiv 0, \forall x \in \mathbb{R}. \tag{3.49}$$

This implies that for any $a \geq a_0$, $F^*_{a,\infty} = F^*_{a_0,\infty}$. As the channel capacity approaches 0 as $a \to \infty$ with no average power constraint, we must have $G(F^*_{a_0,\infty}) = -\log M_\Phi$ (please refer to [94]). This indicates R is independent of S under jamming distribution $F^*_{a_0,\infty}$, which is impossible.

As (3.44) cannot hold for any $\gamma \geq 0$, it implies that $|E^*_{a,P}| = \infty$ cannot hold for $a \in (0, \infty)$. This completes the proof.

□

Next, we extend the result of Theorem 3.4 to the case of $a = \infty$.

Theorem 3.5 *$E^*_{\infty,P}$ has a finite number of elements.*

Proof: As is noted in Theorem 3.2, $F^*_{\infty,P}$ should minimize $G(F) + \gamma K_P(F)$ over $\mathcal{F}_\infty$ for some $\gamma > 0$. Fixing the γ, we optimize the dual problem (3.21) again over $\mathcal{F}_{a_0}$ for some sufficiently large $a_0 \in (0, \infty)$. Denote the obtained optimal distribution by $\tilde{F}^*_{a_0,\gamma}$. Note that

$$G(\tilde{F}^*_{a_0,\gamma}) + \gamma \int_0^\infty t^2 \mathrm{d}\tilde{F}^*_{a_0,\gamma}(t) \leq -H(S|R, J = 0) < 0. \tag{3.50}$$

According to Theorem 3.4, $\tilde{F}^*_{a_0,\gamma}$ has a finite number of points of increase. From (3.48), by selecting $a_0 \geq \max\left\{\sigma\sqrt{\zeta}, \Gamma(\frac{3}{2})\frac{2\bar{s}M(\frac{3}{2},1;\zeta)}{\gamma\sigma^2\sqrt{\zeta}e^\zeta}\right\}$ for some $\zeta \in (0, \infty)$, we have $\forall x \in (a_0, \infty)$

$$g(x;\tilde{F}^*_{a_0,\gamma}) + \gamma x^2 \geq \gamma a_0^2 - \frac{4\bar{s}a_0}{\sigma^2}\Gamma(\frac{3}{2})\frac{M(\frac{3}{2},1;\zeta)}{\sqrt{\zeta}e^\zeta} + \kappa(a_0), \tag{3.51}$$

where the R.H.S. can be made arbitrarily large by increasing a_0. Combining (3.50) and

(3.51), we can obtain $\forall x \in (a_0, \infty)$,

$$g(x; \tilde{F}^*_{a_0,\gamma}) + \gamma x^2 \geq G(\tilde{F}^*_{a_0,\gamma}) + \gamma \int_0^\infty t^2 \mathrm{d}\tilde{F}^*_{a_0,\gamma}(t). \tag{3.52}$$

Basing on Corollary 3.2, this implies that $\tilde{F}^*_{a_0,\gamma}$ is also the optimal solution to the dual problem over $\mathcal{F}_\infty$. Since the worst jamming distribution is unique, we have $F^*_{\infty,P} = \tilde{F}^*_{a_0,\gamma}$. Therefore, $F^*_{\infty,P}$ has a finite number of points of increase. This completes the proof. □

The underlying argument of Theorem 3.5 is that the worst jamming distribution under no peak power constraint can be obtained equivalently under some sufficiently large peak power constraint. The following corollary provides an upper bound on the amplitude of the worst jamming distribution.

Corollary 3.3 *For $\gamma > 0$, the amplitude of the worst jamming distribution to the dual problem (3.21) is upper bounded by $\sigma\sqrt{\zeta^*}$, where ζ^* is the root of equation*

$$\gamma\sigma^2\sqrt{\zeta} - \frac{\log M_\Phi + 4\bar{s}^2/\sigma^2}{\sqrt{\zeta}} - \frac{4\bar{s}}{\sigma} = \frac{4\bar{s}}{\sigma}\Gamma(\frac{3}{2})\frac{M(\frac{3}{2}, 1; \zeta)}{\sqrt{\zeta}e^\zeta}. \tag{3.53}$$

Proof: Following (3.51), if $a_0 \geq \max\left\{\sigma\sqrt{\zeta}, \Gamma(\frac{3}{2})\frac{2\bar{s}M(\frac{3}{2},1;\zeta)}{\gamma\sigma^2\sqrt{\zeta}e^\zeta}\right\}$ for some $\zeta \in (0, \infty)$ satisfying

$$\gamma a_0^2 - \frac{4\bar{s}a_0}{\sigma^2}\Gamma(\frac{3}{2})\frac{M(\frac{3}{2}, 1; \zeta)}{\sqrt{\zeta}e^\zeta} + \kappa(a_0) \geq 0, \tag{3.54}$$

then the amplitude of the worst jamming distribution should be upper bound by a_0. We denote the minimum of such a_0 by a_m.

For a_m, there exists some $\zeta_m \in (0, \infty)$, such that $a_m \geq \max\left\{\sigma\sqrt{\zeta_m}, \Gamma(\frac{3}{2})\frac{2\bar{s}M(\frac{3}{2},1;\zeta_m)}{\gamma\sigma^2\sqrt{\zeta_m}e^{\zeta_m}}\right\}$

and (3.54) is satisfied. This implies that $a_m = \sigma\sqrt{\zeta_m} \geq \Gamma(\frac{3}{2})\frac{2\bar{s}M(\frac{3}{2},1;\zeta_m)}{\gamma\sigma^2\sqrt{\zeta_m}e^{\zeta_m}}$. To see this, consider the case either $a_m > \sigma\sqrt{\zeta_m}$ or $\sigma\sqrt{\zeta_m} < \Gamma(\frac{3}{2})\frac{2\bar{s}M(\frac{3}{2},1;\zeta_m)}{\gamma\sigma^2\sqrt{\zeta_m}e^{\zeta_m}}$. Since $\frac{2\bar{s}M(\frac{3}{2},1;\zeta)}{\gamma\sigma^2\sqrt{\zeta}e^{\zeta}}$ is a decreasing function w.r.t. ζ, we can find some $\zeta' > \zeta_m$ such that $a_m > \max\left\{\sigma\sqrt{\zeta'}, \Gamma(\frac{3}{2})\frac{2\bar{s}M(\frac{3}{2},1;\zeta')}{\gamma\sigma^2\sqrt{\zeta'}e^{\zeta'}}\right\}$, and

$$\gamma a_m^2 - \frac{4\bar{s}a_m}{\sigma^2}\Gamma(\frac{3}{2})\frac{M(\frac{3}{2},1;\zeta')}{\sqrt{\zeta'}e^{\zeta'}} + \kappa(a_m) > 0. \tag{3.55}$$

This contradicts with the fact that a_m is the minimum of a_0 satisfying (3.54). Hence ζ_m is the minimum solution satisfying equations

$$\sigma\sqrt{\zeta} \geq \Gamma(\frac{3}{2})\frac{2\bar{s}M(\frac{3}{2},1;\zeta)}{\gamma\sigma^2\sqrt{\zeta}e^{\zeta}}, \tag{3.56}$$

$$\gamma\sigma^2\zeta - \frac{4\bar{s}\sqrt{\zeta}}{\sigma}\Gamma(\frac{3}{2})\frac{M(\frac{3}{2},1;\zeta)}{\sqrt{\zeta}e^{\zeta}} + \kappa(\sigma\sqrt{\zeta}) \geq 0. \tag{3.57}$$

Eq. (3.57) can be rewritten as

$$\gamma\sigma^2\sqrt{\zeta} - \frac{\log M_\Phi + 4\bar{s}^2/\sigma^2}{\sqrt{\zeta}} - \frac{4\bar{s}}{\sigma} \geq \frac{4\bar{s}}{\sigma}\Gamma(\frac{3}{2})\frac{M(\frac{3}{2},1;\zeta)}{\sqrt{\zeta}e^{\zeta}}. \tag{3.58}$$

where the L.H.S. is an increasing function of ζ and the R.H.S. is a decreasing one, implying a unique root of (3.58) over $(0,\infty)$ when the equality holds. Let ζ_1^* and ζ_2^* denote the root of (3.56) and (3.58) when the equalities hold, respectively. It follows that $\zeta_1^* < \zeta_2^*$ by letting $\sigma\sqrt{\zeta} = \Gamma(\frac{3}{2})\frac{2\bar{s}M(\frac{3}{2},1;\zeta)}{\gamma\sigma^2\sqrt{\zeta}e^{\zeta}}$ in (3.58). Therefore, we have $\zeta_m = \zeta_2^*$. This completes the proof. □

The upper bound above on the jamming amplitude applies to the case where the average

power constraint is active, i.e., $\gamma > 0$. For the case of $\gamma = 0$, the worst jamming distribution must have a mass point at the peak amplitude $a \in (0, \infty)$. To obtain this result, we first prove the following lemma.

Lemma 3.9 *When the average power constraint is inactive, the channel capacity under the worst jamming is strictly decreasing w.r.t. the peak jamming amplitude a. That is, for any $0 < a_1 < a_2$, we have $G(F^*_{a_1,\infty}) > G(F^*_{a_2,\infty})$.*

Proof: Please refer to Appendix I. □

With Lemma 3.9, we have the following theorem on the worst jamming distribution.

Theorem 3.6 *When the average power constraint is inactive, the worst jamming distribution under peak power constraint $a \in (0, \infty)$ must have a mass point at $J = a$.*

Proof: Suppose the largest mass point of the worst jamming distribution $F^*_{a,\infty}$ is a_0. If $a_0 < a$, then $F^*_{a,\infty} \in \mathcal{F}_{a_0,\infty}$, and $G(F^*_{a_0,\infty}) = G(F^*_{a,\infty})$, which contradicts with Lemma 3.9. This completes the proof. □

Even though we have proved the discreteness of the worst jamming distribution, it is still very difficult to obtain its closed form expression. Therefore, we resort to numerical methods to evaluate the worst jamming distribution in Section 3.6.

3.6 Numerical Results

In this subsection, we compute the worst jamming distribution through numerical methods.

The KT conditions in Corollary 3.2 provide the gradients in the optimization problem [80], and the convexity of functional $G(\cdot)$ guarantees the convergence to the global optimal in optimization. However, as we are optimizing the distribution function of J, which is infinite dimensional, we are not able to obtain the value of the KT condition for every possible point on a continuous interval through numerical calculation. Even though we can discretize the distribution function into finite dimensions, it is still computational expensive to evaluate the KT conditions at all the selected points in each round of optimization because of the double integral in the evaluation of functional $g(\cdot;\cdot)$.

Since we have proved the worst jamming distribution is discrete with a finite number of mass points, we adopt an optimization strategy similar to that in [85]. Instead of optimizing the dual problem over the infinite dimensional space $\mathcal{F}_a$, we first fix a set of mass points $\mathcal{M} = \{m_1, m_2, ..., m_n\}$ arbitrarily and optimize their probabilities $\{p_{m_1}, p_{m_2}, ..., p_{m_n}\}$ for the dual problem. Once the local optima is achieved on $\mathcal{M}$, we examine the KT conditions in Corollary 3.2. If the KT conditions are satisfied, then set $\mathcal{M}$ and the corresponding probabilities will be the global optima. If not, we select a point in $[0, a]$ where the KT condition is not satisfied, add it to $\mathcal{M}$ and repeat the process. The mass points whose probabilities are zero in the local optima will be removed from $\mathcal{M}$ in the next round to reduce unnecessary computations.

Discreteness of the worst jamming: We first verify the discreteness of the worst jamming. In the numerical results, the average power of the legitimate signal is normalized to 1 and noise power $\sigma^2 = 0.25$. Figures 3.1 and 3.2 plot the worst jamming distributions and the KT functions[4] with different parameters in the dual problem. Note that for the

[4]In the numerical results, we refer to KT function as $g(x; F) + \gamma x^2 - G(F) - \gamma \int_0^\infty t^2 \mathrm{d}F_0(t)$ given a jamming distribution F, where x is the jamming amplitude.

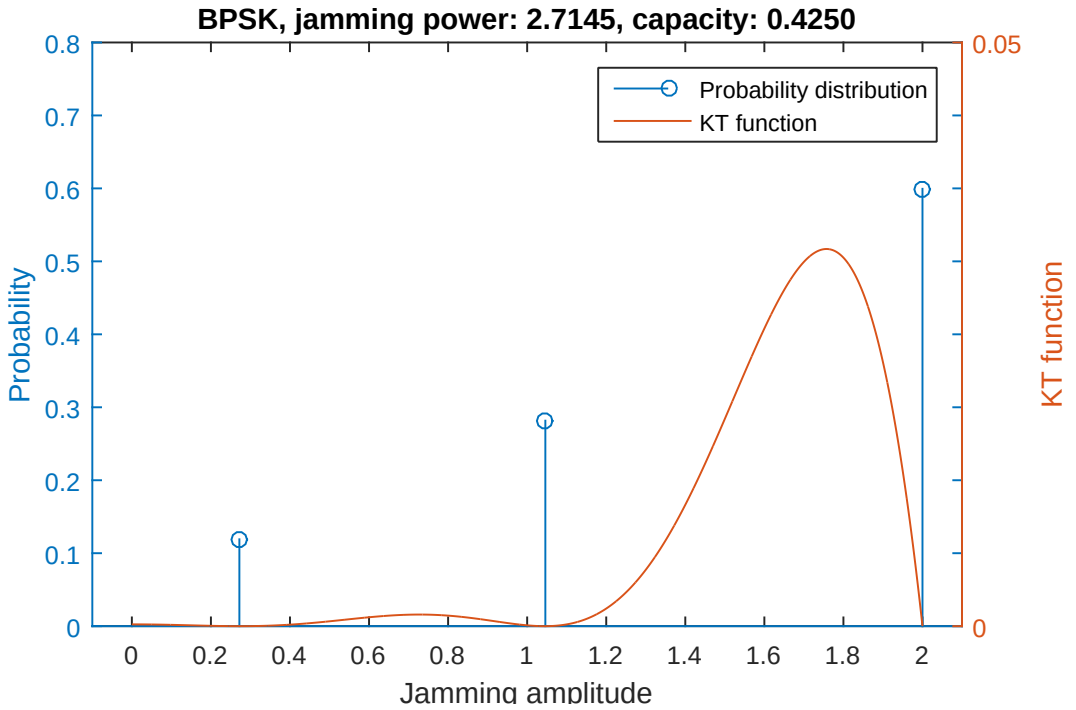


Figure 3.1: The worst jamming distribution and KT conditions for $a = 2, \gamma = 0$, BPSK alphabet.

case without peak power constraint in Fig. 3.2, to limit the peak jamming amplitude, we set a large γ in the dual problem, which results in a small average jamming power. The numerical results demonstrate the theoretical results, where the worst jamming distributions are discrete with finite mass points. The corresponding KT conditions satisfy Corollary 3.2, which indicate that the obtained jamming distributions are indeed globally optimal.

The impact of the power constraints: We study the effect of peak and average power constraints on the worst jamming. The worst jamming distributions with different peak amplitude a's are plotted in Fig. 3.3, where γ is set to 0 in the dual problem, that is, the average power constraint is inactive. In Fig. 3.3, *the points on the same y-coordinate are the set of mass points in the worst jamming under the corresponding peak power constraint; the x-coordinate of each point is the amplitude of the mass point while the annotated value is the probability.* It is shown that given the average jamming power constraint inactive, the

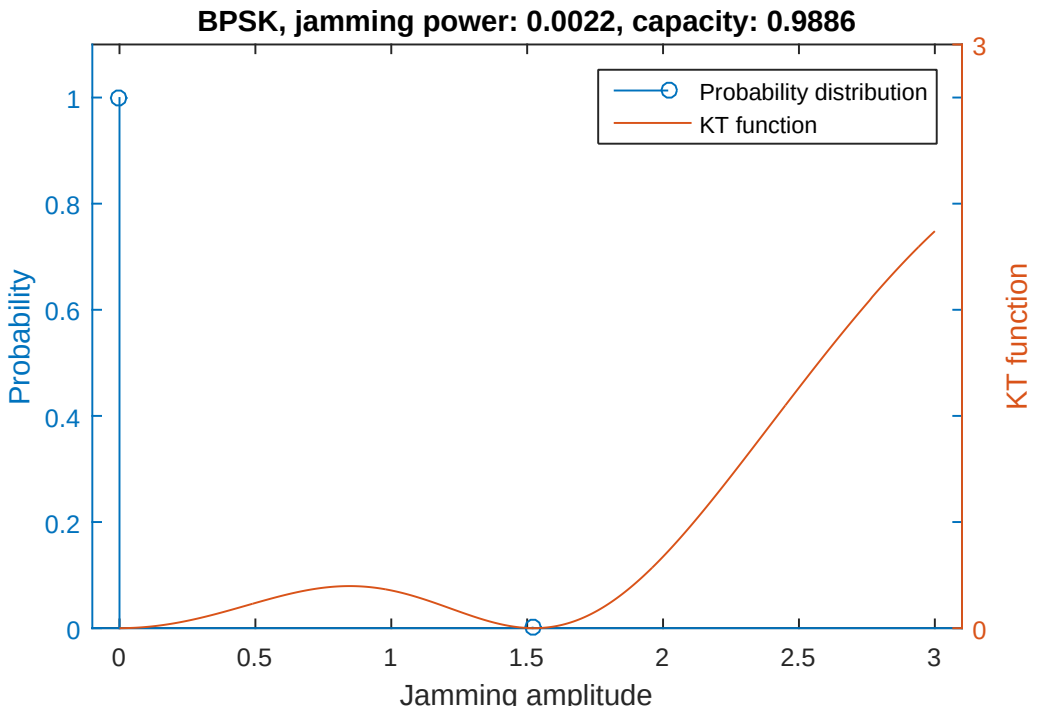


Figure 3.2: The worst jamming distribution and KT conditions for $a = \infty, \gamma = 0.8$, BPSK alphabet.

worst jamming intends to have more mass points as the peak power constraint increases; the worst jamming has a mass point at the given peak amplitude, which verifies Theorem 3.6. The worst jamming distributions with different Lagrangian multiplier γ's are plotted in Fig. 3.4, where the peak amplitude constraint $a = 2$. In Fig. 3.4, the points on the same y-coordinate are the set of mass points in the worst jamming obtained with the corresponding Lagrangian multiplier. Recall that the average jamming power is actually controlled by γ in the dual problem, where a larger γ indicates a lower average power. It is shown that for a low average jamming power, the worst jamming has a mass point at 0, whose probability increases as the average power decreases. This implies that with a limited average power, the optimal strategy for the jammer is to launch jamming with a higher overall power level during a proportional of time and then keep silent during the other time intervals.

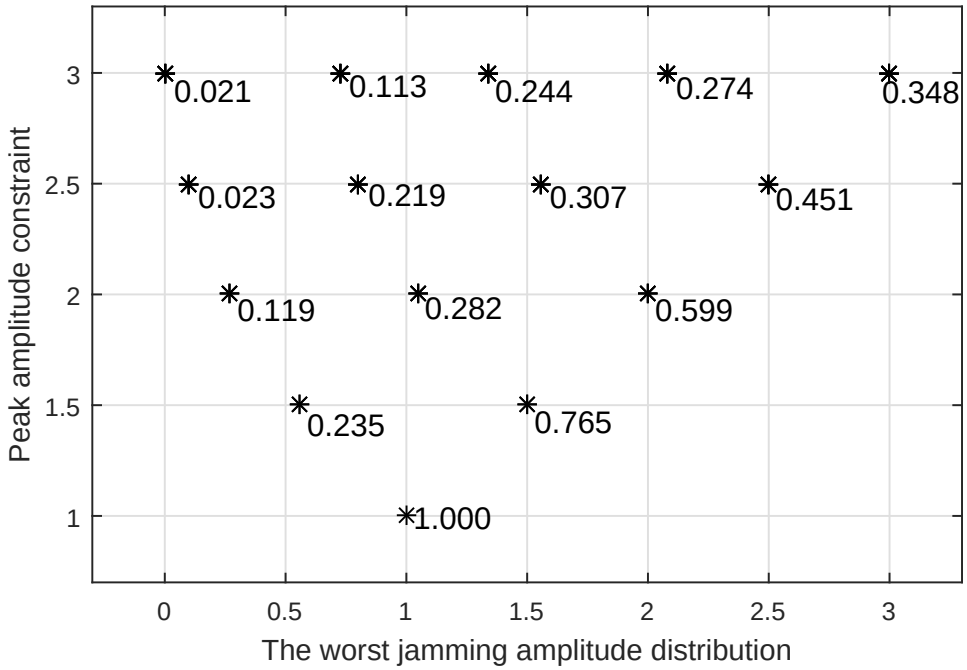


Figure 3.3: The worst jamming distribution versus peak power constraint, $\gamma = 0$, $\sigma^2 = 0.25$, BPSK alphabet.

3.7 Summary

In this chapter, we studied the problem of finding the worst jamming distribution that minimizes the channel capacity of the SP-OFDM system. The problem was formulated as a constrained functional optimization process under practical conditions, where each transmitted symbol is uniformly distributed over an alphabet, and the jamming interference may or may not be subjected to a finite peak power constraint. In this chapter, first, we proved the existence and the uniqueness of the worst jamming distribution. Second, by analyzing the KT conditions for the worst jamming, we proved that the worst jamming distribution should be discrete in amplitude with a finite number of mass points, either with or without peak power constraints. Numerical results demonstrated the discreteness of the worst jamming, which validated our theoretical analysis. Moreover, it was shown that under lim-

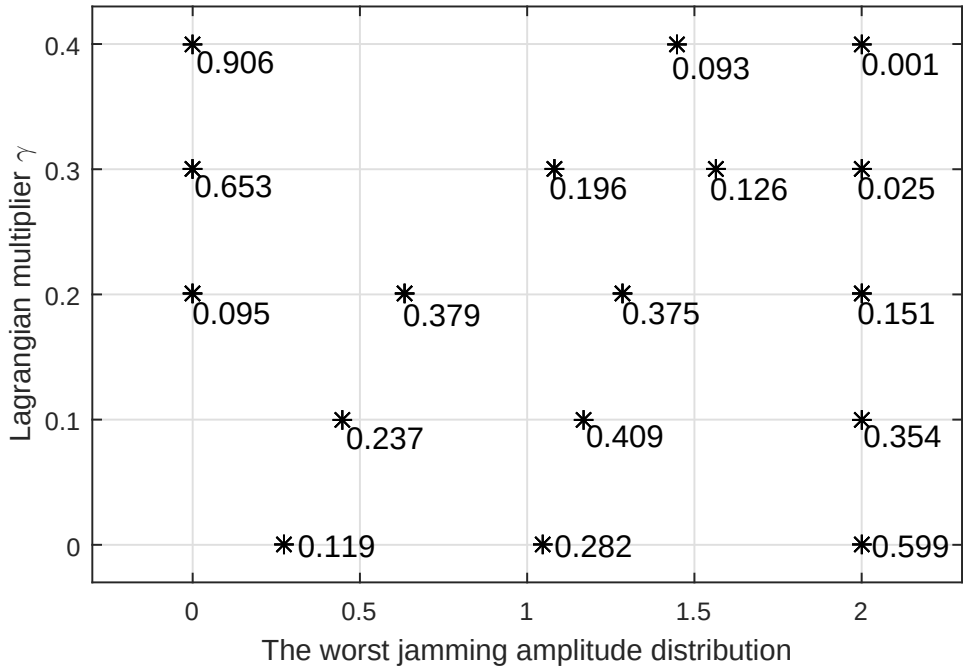


Figure 3.4: The worst jamming distribution versus Lagrangian multiplier γ, $a = 2$, $\sigma^2 = 0.25$, BPSK alphabet.

ited average jamming power constraint, for best jamming effect, the optimal strategy for the jammer is to launch partial-time jamming that concentrates more at the high power mass points. The in-depth analysis on the worst jamming distribution carried out hereby demonstrated the robustness of SP-OFDM and also revealed its performance lower bound under disguised jamming. Finally, we would like to point out that our theoretical approach in finding the worst jamming distribution got around the complicated integral transforms, which were often involved in existing work on optimal input distribution analysis.

Chapter 4

End-to-End Throughput in Multi-Hop Wireless Networks With Random Relay Deployment

This chapter investigates the effect of relay randomness on the end-to-end throughput in multi-hop wireless networks using stochastic geometry. We model the nodes as Poisson Point Processes and calculate the spatial average of the throughput over all potential geometrical patterns of the nodes. More specifically, for problem tractability, we first start with the simple nearest neighbor (NN) routing protocol, and analyze the end-to-end throughput so as to obtain a performance benchmark. Next, note that the ideal equal-distance routing is generally not realizable due to the randomness in relay distribution, we propose a quasi-equal-distance (QED) routing protocol. We derive the range for the optimal hop distance, and select the relays to formulate a quasi-equidistant deployment. We analyze the end-to-end throughput both with and without intra-route resource reuse. Our analysis indicates that: (i) The throughput performance of the proposed QED routing can achieve a significant performance gain over that of the NN routing. As the relay intensity gets higher, the performance of QED routing converges to that of the equidistant routing. (ii) If the node intensity is a constant over the network, then intra-route resource reuse is always beneficial

when the routing distance is sufficiently large. (iii) With randomly distributed relays, the communication distance can generally be extended. However, due to the uncertainty in relay distribution, long distance communication is generally not feasible with random relays. This implies that the existence of a reasonably defined infrastructure is critical in effective long distance communication. Our analysis is demonstrated through numerical examples.

4.1 Introduction

Multi-hop communication with relay assistance has become a prominent scheme in today's hybrid network design. The main reason is that it can extend the communication distance in wireless networks without the deployment of wired backhaul facilities. In wireless networks, the geometric locations of the nodes play a key role in determining the signal to interference and noise ratio (SINR), and hence the probability of successful transmission. In large scale multi-hop wireless networks, the node locations, including the relay locations, are generally random. The spatial randomness in node locations raises significant challenges in network performance analysis.

An effective tool to characterize the spatial randomness in wireless networks is stochastic geometry, for which the basic idea is to model the nodes as Poisson Point Processes (PPPs) and calculate the spatial averages of network performance characteristics by averaging over all potential geometrical patterns of the nodes [45, 46, 50, 95, 96].

In literature, stochastic geometry modeling has been utilized to study multi-hop wireless networks. In [53, 97], the random access transport capacity, which was defined as the spatially normalized end-to-end data rate obtained by multi-hop relays, was evaluated and optimized with respect to hop number. In [98], the transport capacity was evaluated un-

der delay constraints. In [54, 99–101], the end-to-end delay of multi-hop wireless networks was characterized and optimized. In [102], the dependence of interference among the relays along a multi-hop route was discussed. It was shown that spatially and temporally correlated interference would increase both the mean and variance of the end-to-end delay. In most of these approaches, the source nodes were modeled as PPPs, however, the relay locations were assumed to be *deterministic and known*, and were often approximated as *equidistant*. Note that in large scale wireless networks, it is impractical to optimize the relay locations for each source destination pair as equidistant, and the overall relay distribution is generally random rather than deterministic, hence, for more reasonable performance evaluation, the relay randomness needs to be taken into account more accurately.

Assuming random relay distribution, in [51, 52], different hopping strategies were compared in terms of aggregate multi-hop information efficiency. These approaches focused on the efficiency of each individual hop in a multi-hop network, and the end-to-end performance of the network needs to be further exploited. Similarly, in [55–58], the performance analysis was also focused on individual hops. In [103], the cost of routing selection was evaluated under opportunistic geographic routing strategies in a Poisson network. In [104], the end-to-end delay was simulated in a Poisson multi-hop wireless network using the time-space opportunistic routing. In [105], limited random deviations of relays from their ideal locations in the equidistant deployment were introduced. This model was more practical than the equidistant one, but it required the relays to be deployed within a small range around the equidistant locations. In [106], the theoretical upper bounds were derived for the throughput that could be achieved by any routing algorithm assisted by dynamic routing selection. In [107], the relays were modeled as a linear PPP along the route, and the end-to-end delay was evaluated. While the randomness of relays was taken into account in [107], there was no

the consideration on node stability or traffic overflow, and the end-to-end throughput was not explicitly evaluated. In addition, the results there only applied to the cases where the routing distances were sufficiently long so that asymptotic analysis could be utilized.

As an effort to further explore the effect of relay randomness on network performance, in this chapter, we analyze the end-to-end throughput of a general multi-hop route in a wireless network with randomly located relays. In our analysis, we model the relays as a linear PPP between the source and destination following the TDMA medium access control (MAC) protocol, and model the external interferers as an independent PPP over the whole plane, following the ALOHA MAC protocol. We assume that multi-hop transmissions are performed under an interference limiting scenario, where the interference power is much more significant than the noise power.

More specifically, in this chapter, *first*, for problem tractability, we start with a simple nearest neighbor routing protocol where each relay will select the nearest node along the direction to the destination as its next hop. We analyze the end-to-end throughput in a relatively *sparse* network so as to obtain a performance benchmark or lower bound. The throughput is evaluated under both conventional TDMA with fixed, uniform slot length, as well as TDMA with dynamic slot length or resource allocation; the optimal relay density is also discussed. *Next*, motivated by the observation that, while the ideal equal-distance routing generally provides the optimal network performance, it is not realizable due to the randomness in relay distribution, we propose a quasi-equal-distance (QED) routing protocol, where we derive the range for the optimal hop distance, and select the relays to formulate a quasi-equidistant deployment. We analyze the end-to-end throughput both with and without intra-route resource reuse. Our analysis indicates that, compared with the optimal end-to-end throughput of NN routing, the proposed QED routing obtains a significant performance

improvement under the same relay intensity and routing distance.

The main contributions of this chapter can be summarized as follows:

- First, to pave the way for throughput analysis, we derive the distribution of the longest hop distance L_m under NN routing for any given routing distance r. We formulate the distribution of L_m as a continuous auto-regression system, and solve it using the Laplace transform. It is shown that the mean of L_m scales with $\mathcal{O}(\ln r)$ as the routing distance $r \to \infty$, and the variance of L_m is bounded. This implies that the throughput vanishes as $r \to \infty$, hence multi-hop relaying with random relays is infeasible for long distance communication.

- Second, we derive the average end-to-end throughput of a multi-hop route under NN routing and TDMA MAC with both fixed and flexible slot length. By expressing the average end-to-end throughput as a function of the routing distance r, we obtain the Laplace transform of the throughput function. Under conventional TDMA with fixed slot length, we obtain a closed-form expression for the lower bound of the throughput, and derive the range for the optimal relay intensity. We maximize the throughput under TDMA, and show that the optimal slot length varies from hop to hop and is determined by the coverage probability of every hop. That is, TDMA with flexible, properly selected slot length can increase the system efficiency and lead to optimal throughput.

- Third, we propose a quasi-equal-distance (QED) routing protocol for throughput optimization with random relays. Under the proposed QED routing and conventional TDMA, we analyze the average end-to-end throughput with and without intra-route resource reuse, respectively. Note that accurate expression of the throughput is hard

to derive, as an alternative, we obtain close approximations of the throughput under different scenarios. The optimal number of time slots is also analyzed when there is intra-route resource reuse. It is shown that the proposed QED routing protocol achieves a significant performance gain over NN routing. It is also observed that the effect of intra-route resource reuse depends on the network setup. If the node intensity is a constant over the network, then as expected, intra-route resource reuse is always beneficial when the routing distance r is sufficiently large (i.e. , as $r \to \infty$). However, if the source-destination pair density remains unchanged as the routing distance increases, then intra-route resource reuse is no longer beneficial for throughput improvement even if the routing distance $r \to \infty$.

Our results are demonstrated through numerical examples. Overall, our numerical results, together with the theoretical analysis, show that: (i) The throughput performance of the proposed QED routing can achieve a significant performance gain over that of the NN routing. For network with sparse random relays, compared with the ideal equidistant routing, the performance loss of QED routing due to relay randomness is not negligible. However, as the relay intensity gets higher, the performance of QED routing converges to that of the equidistant routing. (ii) If the node intensity is a constant over the network, then intra-route resource reuse can increase the network throughput when the routing distance r is sufficiently large. (iii) With randomly distributed relays, the communication distance can generally be extended. However, due to the uncertainty in relay distribution, long distance communication is generally not feasible with random relays. This implies that the existence of a reasonably defined infrastructure is critical for effective long distance communication. The results in this chapter also echo our previous observations in [108–110] that

future network design would reflect the convergence of centralized and ad hoc networks.

4.2 System Description

4.2.1 Network Model

We consider a source node $\boldsymbol{S}$, and a destination node $\boldsymbol{D}$ located at a distance of R. A linear relay pattern is studied, where the candidate relay nodes are distributed randomly along the line segment between $\boldsymbol{S}$ and $\boldsymbol{D}$. Without loss of generality, we assume $\boldsymbol{S}$ is at the origin and $\boldsymbol{D}$ is located at $(R, 0)$. Thus the candidate relay nodes formulate a 1D point process $\Phi = \{\boldsymbol{X}_i, i = 1, 2, ..., N\}$, where N is the random variable (RV) denoting the number of relays, and $\boldsymbol{X}_i$ is the location of the i-th relay along the line segment between $(0, 0)$ and $(R, 0)$. In the remaining part of this chapter, we model Φ as a 1D homogeneous PPP (HPPP) of intensity λ. That is, for $i = 1, 2, ..., N$ and letting $\boldsymbol{X}_0 = \boldsymbol{S}$, the distances between successive nodes, $L_i = |\boldsymbol{X}_i - \boldsymbol{X}_{i-1}|$, are exponentially distributed independent RVs of mean $1/\lambda$ [107]. The locations of the relays would keep static during packet delivery. Considering a backlogged source $\boldsymbol{S}$ which has infinite packets to transmit, *we define the end-to-end throughput from* $\boldsymbol{S}$ *to* $\boldsymbol{D}$ *as the number of packets initiated from source* $\boldsymbol{S}$ *that are successfully received at destination* $\boldsymbol{D}$ *per time slot.*

The route selects a subset $\Phi' = \{\boldsymbol{X}'_1, \boldsymbol{X}'_2, ..., \boldsymbol{X}'_{N'}\} \subseteq \Phi$ as the actual relays to be used, following a specific routing protocol, where $\boldsymbol{X}'_i$ denotes the location of the i-th selected relay and N' the number of relays selected. Relay node $\boldsymbol{X}'_i$ transmits the packets originated from the source $\boldsymbol{S}$ to the next relay $\boldsymbol{X}'_{i+1}$ along the direction to $\boldsymbol{D}$ in a *decode-and-forward* manner. For tractable analysis, we assume that each relay node has an infinite transmission buffer, and each packet relayed is served in a first-in first-out fashion. The packet that fails

in one transmission would go back to the head of the transmission queue, waiting for the opportunity of next transmission. The nodes on the route follow the TDMA MAC protocol, where each node will be assigned with at least one time slot in a TDMA cycle and is allowed to transmit signals only at the designated time slots.

We apply the *decoupling* technique in [107] to our network model, where all the other nodes that are not along the $\boldsymbol{S}$-$\boldsymbol{D}$ path are modeled as an independent 2D point process Ψ over $\mathbb{R}^2$ from Φ. Potentially, these nodes can be the external interferers to the relays we study when they transmit over the same spectrum and time slot. For the remaining part of this chapter, we model Ψ as a 2D HPPP of intensity μ. We assume that the transmissions of the nodes in Ψ follow the ALOHA protocol, where each node would transmit at each time slot independently with a probability of p_a.

As can be seen, the network model adopted here is actually a combination of the models in [100] and [107]. More specifically, we combine the random relay model in [107] with the TDMA/ALOHA multi-hop network model in [100]. For the tractability of the problem, in this chapter, we mainly consider the case where relays are deployed along the line segment between $\boldsymbol{S}$ and $\boldsymbol{D}$. However, the results obtained here actually provide an upper bound on the more practical scenario where relays are modeled as a 2D HPPP over an area surrounding segment $\boldsymbol{S}-\boldsymbol{D}$. For example, in Fig. 4.1, the relays are deployed randomly in a $R \times W$ rectangle $\mathcal{R}$ whose widths intersect $\boldsymbol{S}$ and $\boldsymbol{D}$. A simple routing protocol is that each relay would transmit to its nearest neighbor along the direction to $\boldsymbol{D}$ (the x-coordinate). By projecting the relays to the x-coordinate, we can find that the hop distances in the 2D case are lower bounded by those in the 1D case. Thus, the throughput in 1D case is an upper bound of that in 2D case.

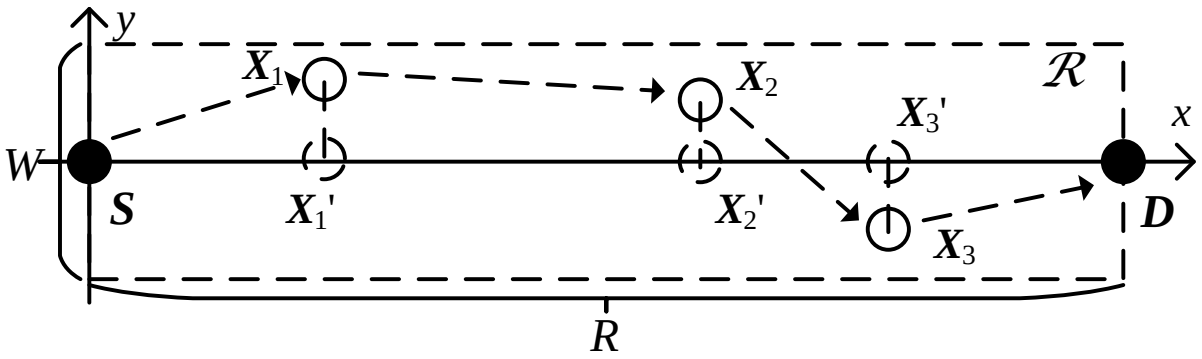


Figure 4.1: An illustration of relays randomly deployed over a 2D area

4.2.2 Channel Model

Both large-scale path-loss and small-scale fading are considered. The received power of a signal transmitted at a distance of x meters with transmit power P_T is [46]

$$P_R(x) = \frac{P_T \cdot H}{c \cdot x^{\beta}} \ , \tag{4.1}$$

where H denotes channel gain, β the path-loss exponent, and c a constant determined by the antenna gains and signal wavelength. H is an exponentially distributed random variable with mean 1, i.e., Rayleigh fading is considered. Independent small scale fading is assumed for different transmitter-receiver pairs in different time slots. The small scale fading from location $\boldsymbol{x}_1$ to $\boldsymbol{x}_2$ at time slot k is represented by $H^k_{\boldsymbol{x}_1,\boldsymbol{x}_2}$.

4.2.3 Routing Protocol

In this chapter, we investigate two routing protocols: the nearest neighbor (NN) routing protocol and the proposed quasi-equal-distance (QED) routing protocol.

Nearest Neighbor Routing

For problem tractability, we start with the simple NN routing protocol to obtain a performance lower bound. In NN routing [51], each relay will select the nearest node in Φ along the direction to the destination D as its next hop. In this case, the selected relay set is the same as the candidate relay set, i.e., $\Phi' = \Phi$. So in the NN routing, we use Φ' and Φ interchangeably unless otherwise clarified.

The nearest neighbor routing protocol aims to guarantee the link quality of each single hop by utilizing all the available relays in Φ and minimizing the hop distances. When the node intensity λ is large, nearest neighbor routing will degrade the end-to-end throughput because of the extra delay and bandwidth it takes. A simple variation of the NN routing is to choose Φ' by independently thinning [47, Proposition 1.3.5] the original relay set Φ, which can generate an HPPP of intensity $\lambda^* < \lambda$. The throughput analysis in this case is the same as that of the original NN routing by replacing λ with λ^*.

Quasi-Equal-Distance (QED) Routing

As is well known [54,111], equal-distance routing provides the optimal network performance. However, limited by the randomness in relay distribution, the ideal equal-distance routing generally cannot be realized in practical systems. Therefore, in this chapter, we propose a QED routing protocol where we select the relays Φ' to be close to a equidistant relay deployment. In the QED protocol, given a selected relay, instead of choosing the nearest neighbor as the next hop, it will select the next hop to be the first node which is at least l_0 away along the direction to the destination, where l_0 is a parameter that can be tuned in the protocol. That is, the QED routing aims to make the hop distance of each hop close to l_0. In this case, except for the last hop, the hop distances should be at least l_0. Note that

if l_0 is set to be 0, the QED routing will be reduced to the NN routing. The optimal value of l_0 can be obtained by optimizing the end-to-end throughput, which will be discussed in Section 4.6 of this chapter.

As the relay intensity $\lambda \to +\infty$, the distribution of the selected relays will converge to an equidistant deployment, and the performance of QED will converge to that of equidistant relays.

4.3 Problem Formulation

A fixed rate coding scheme is assumed in the physical layer, where a packet can be successfully received if and only if the received signal to interference and noise ratio (SINR) is above a given threshold $\theta > 0$. We consider an interference-limiting scenario, where the noise power is negligible compared with the interference power, so we use signal to interference ratio (SIR) and SINR interchangeably. Without loss of generality, we assume that each node in the network transmits with unit power. Let binary RV $B(\boldsymbol{X}'_{i-1}, k)$ indicate whether relay $\boldsymbol{X}'_{i-1}$ is allowed by the MAC protocol to transmit signals at time slot k. For $i = 1, 2, ..., N' + 1$ and let $\boldsymbol{X}'_{N'+1} = \boldsymbol{D}$, given $B(\boldsymbol{X}'_{i-1}, k) = 1$, the received SIR at relay $\boldsymbol{X}'_i$ on time slot k can be expressed as

$$\mathrm{SIR}(\boldsymbol{X}'_i, k) = \frac{H^k_{\boldsymbol{X}'_{i-1}, \boldsymbol{X}'_i} |\boldsymbol{X}'_i - \boldsymbol{X}'_{i-1}|^{-\beta}}{I_o(\boldsymbol{X}'_i, k) + I_{in}(\boldsymbol{X}'_i, k)} \ , \tag{4.2}$$

where $I_o(\boldsymbol{X}'_i, k)$ denotes the interference that the active external interferers in Ψ generates on relay $\boldsymbol{X}'_i$ at time slot k, and $I_{in}(\boldsymbol{X}'_i, k)$ denotes the intra-route interference generated by other relays in Φ' transmitting over time slot k.

Let $\mathbb{1}\{\mathcal{A}\}$ denote the indicator variable of event $\mathcal{A}$. So the local throughput of link

$\boldsymbol{X}'_{i-1} \to \boldsymbol{X}'_i$ can be expressed as

$$T_{\text{local}}(\boldsymbol{X}'_i) = \lim_{K\to\infty} \frac{1}{K} \sum_{k=0}^{K-1} B(\boldsymbol{X}'_{i-1}, k) \mathbb{1}\{\text{SIR}(\boldsymbol{X}'_i, k) > \theta\} \ . \tag{4.3}$$

According to the stability analysis in queuing theory, the end-to-end throughput is determined by the hop with the lowest throughput [112]. So the end-to-end throughput can be expressed as

$$T_{\text{end}} = \min_{\boldsymbol{X}'_i \in \Phi' \cup \{\boldsymbol{D}\}} T_{\text{local}}(\boldsymbol{X}'_i) \ . \tag{4.4}$$

Our goal is to calculate the expectation of T_{end} over all the possible realizations of the relay distribution Φ' for any given routing distance $R = r$, $\mathbb{E}\{T_{end} \mid R = r\}$.

In general, the external interference $I_o(\boldsymbol{X}'_i, k)$ can be represented as

$$I_o(\boldsymbol{X}'_i, k) = \sum_{\boldsymbol{Y}_j \in \Psi} B(\boldsymbol{Y}_j, k) H^k_{\boldsymbol{Y}_j, \boldsymbol{X}'_i} |\boldsymbol{Y}_j - \boldsymbol{X}'_i|^{-\beta} \ , \tag{4.5}$$

where for any $\boldsymbol{Y}_j \in \Psi$, the binary RV $B(\boldsymbol{Y}_j, k)$ indicates whether the "external" node $\boldsymbol{Y}_j$ would transmit at time slot k. Under the ALOHA protocol, the distribution of external interferers in any given time slot can be viewed as an independent thinning of Ψ with a retention probability of p_a, i.e., an HPPP with intensity $\mu' = p_a \mu$. Following the same assumption in [100], we make the following approximation.

Approximation 1 *The distribution of external interferers are approximated as independent across different time slots.*

With the approximation above, for a given deployment of relays Φ', the distribution of $I_o(\boldsymbol{X}'_i, k)$ is independent of time slot k. So we discard the time index k for the external interference.

Given R and Φ', $B(\boldsymbol{X}'_{i-1}, k)$ and $I_{in}(\boldsymbol{X}'_i, k)$ will depend on the resource allocation scheme in the TDMA protocol. Here, we discuss the NN and the QED routing respectively.

4.3.1 NN Routing

For the NN routing, we assume that each time slot in a TDMA cycle will be allocated to at most one relay in Φ' (Φ). That is, no intra-route resource reuse is allowed in the NN routing and $I_{in}(\boldsymbol{X}'_i, k) = 0$ for all the possible i and k. This is because in the NN routing, relays can be quite close to each other, where a strong intra-route interference will possibly be generated. In this case, $\mathrm{SIR}(\boldsymbol{X}'_i, k)$ is independent of time slot k given $B(\boldsymbol{X}'_{i-1}, k) = 1$. So we discard the time index k and let $\mathrm{SIR}(\boldsymbol{X}'_i)$ denote the SIR at $\boldsymbol{X}'_i$ for an arbitrary time slot where $\boldsymbol{X}'_{i-1}$ is allowed to transmit signals.

Define $A_i \stackrel{\triangle}{=} \lim\limits_{K\to\infty} \frac{1}{K} \sum_{k=0}^{K-1} B(\boldsymbol{X}'_{i-1}, k)$ as the normalized slot length allocated to link $\boldsymbol{X}'_{i-1} \to \boldsymbol{X}'_i$. So the local throughput $T_{\mathrm{local}}(\boldsymbol{X}'_i)$ can be rewritten as

$$T_{\mathrm{local}}(\boldsymbol{X}'_i) = \lim_{K\to\infty} \frac{\sum\limits_{k=0}^{K-1} B(\boldsymbol{X}'_{i-1}, k)}{K} \frac{\sum\limits_{B(\boldsymbol{X}'_{i-1},k)=1} \mathbb{1}\{\mathrm{SIR}(\boldsymbol{X}'_i, k) > \theta\}}{\sum_{k=0}^{K-1} B(\boldsymbol{X}'_{i-1}, k)}. \tag{4.6}$$

From ergodicity, given the routing distance R and the relay set Φ', the local throughput

$$T_{\mathrm{local}}(\boldsymbol{X}'_i) = A_i \Pr\{\mathrm{SIR}(\boldsymbol{X}'_i) > \theta \mid R, \Phi'\} \ . \tag{4.7}$$

From the stationarity of HPPP, the distribution of $I_o(\boldsymbol{X}'_i)$ will be independent of the location of $\boldsymbol{X}'_i$. If we assume that the distribution of the small scale fading $H_{\boldsymbol{X}'_{i-1},\boldsymbol{X}'_i}$ is independent of the location of $\boldsymbol{X}'_{i-1}$ and $\boldsymbol{X}'_i$, then it follows from (4.2) that the conditional probability $\Pr\left\{\mathrm{SIR}(\boldsymbol{X}'_i) > \theta \mid R, \Phi'\right\}$ is a function of hop distance $|\boldsymbol{X}'_i - \boldsymbol{X}'_{i-1}|$. Define the

coverage probability of a hop distance of l with only external interference as

$$P_s(l) \stackrel{\triangle}{=} \Pr\left\{Hl^{-\beta}/I_o > \theta\right\} \ , \tag{4.8}$$

where I_o denotes the external interference at an arbitrary location. So we have

$$\Pr\left\{\mathrm{SIR}(\boldsymbol{X}_i') > \theta \mid R, \Phi'\right\} = P_s(|\boldsymbol{X}_i' - \boldsymbol{X}_{i-1}'|) \ . \tag{4.9}$$

The coverage probability $P_s(l)$ can be calculated using the following lemma.

Lemma 4.1 *Given a hop distance l, the coverage probability for the hop is*

$$P_s(l) = \exp(-\kappa l^2) \ , \tag{4.10}$$

where $\kappa = 2\pi\mu' \frac{\pi}{\beta \sin(2\pi/\beta)} \theta^{2/\beta}$.

Proof: See [55]. □

So the end-to-end throughput can be expressed as

$$T_{\mathrm{end}} = \min_{\boldsymbol{X}_i' \in \Phi' \cup \{\boldsymbol{D}\}} A_i P_s(|\boldsymbol{X}_i' - \boldsymbol{X}_{i-1}'|) \ . \tag{4.11}$$

4.3.2 QED Routing

In the QED routing, we analyze the throughput both with and without intra-route resource reuse.

For the case without intra-route resource reuse, the analysis follows that of the NN case,

where the expression of the end-to-end throughput is the same as (4.11).

Next, we consider the case with intra-route resource reuse. Assuming a TDMA scheme where the TDMA cycle consists of M time slots, indexed from 0 to $M-1$, the source node will be assigned with slot 0, and relay i will be assigned with slot $i \mod M$. The nodes assigned with the same time slot will transmit concurrently at the specified time slot, thus the nodes will be subject to the intra-route interference generated. The intra-route interference experienced by relay $\boldsymbol{X}_i'$ at time slot k, $I_{in}(\boldsymbol{X}_i', k)$, can be expressed as

$$I_{in}(\boldsymbol{X}_i', k) = \sum_{\boldsymbol{X}_m \in \Phi',\ m \neq i} B(\boldsymbol{X}_m, k) H^k_{\boldsymbol{X}_m, \boldsymbol{X}_i'} |\boldsymbol{X}_m - \boldsymbol{X}_i'|^{-\beta} \ . \tag{4.12}$$

Here, without loss of generality, we assume that each relay will always transmit signals at its designated time slots. Note that, given $B(\boldsymbol{X}_{i-1}, k) = 1$, $B(\boldsymbol{X}_m, k) = 1$ iff. $m = i - 1 + jM$ for some integer $j \neq 0$. So the intra-route interference is independent of time index k, which can be expressed as

$$I_{in}(\boldsymbol{X}_i') = \sum_{\substack{j \in \mathbb{Z} \setminus 0, \\ \boldsymbol{X}'_{i-1+jM} \in \Phi'}} H_{\boldsymbol{X}'_{i-1+jM}, \boldsymbol{X}_i'} |\boldsymbol{X}'_{i-1+jM} - \boldsymbol{X}_i'|^{-\beta}. \tag{4.13}$$

Similar to the NN case, we use $\mathrm{SIR}(\boldsymbol{X}_i')$ to denote the SIR at $\boldsymbol{X}_i'$ for an arbitrary time slot.

The introduction of intra-route resource reuse greatly complicates the throughput analysis because that: (i) the intra-route interference is correlated with the distribution of the relays; and (ii) the temporal correlation of intra-route interference results in the correlation of transmission success probability across time [113]. To make the problem tractable, we assume

$M \geq 2$ and approximate the intra-route interference at $\boldsymbol{X}'_i$ as

$$\tilde{I}_{in}(\boldsymbol{X}'_i) = \sum_{j\in\mathbb{Z}^-} H_j|jMl_0 + L'_i|^{-\beta} + \sum_{j\in\mathbb{Z}^+} H_j|(jM-1)l_0|^{-\beta} \ , \tag{4.14}$$

where $L'_i = |\boldsymbol{X}'_i - \boldsymbol{X}'_{i-1}|$ and H_j, $j = \pm1, \pm2, ...$, are independent exponential RVs of mean 1. As hop distance is lower bounded by l_0 except for the last hop in the QED routing, it follows that $\Pr\{\tilde{I}_{in}(\boldsymbol{X}'_i) \geq x \mid \Phi'\} \geq \Pr\{I_{in}(\boldsymbol{X}'_i) \geq x \mid \Phi'\}$ for any x.

Define the corresponding lower bound of $\mathrm{SIR}(\boldsymbol{X}'_i)$ as

$$\widetilde{\mathrm{SIR}}(\boldsymbol{X}'_i) = \frac{H_{\boldsymbol{X}'_{i-1},\boldsymbol{X}'_i}|\boldsymbol{X}'_i - \boldsymbol{X}'_{i-1}|^{-\beta}}{I_o(\boldsymbol{X}'_i) + \tilde{I}_{in}(\boldsymbol{X}'_i)}. \tag{4.15}$$

We use $\widetilde{\mathrm{SIR}}(\boldsymbol{X}'_i)$ instead of $\mathrm{SIR}(\boldsymbol{X}'_i)$ in the throughput analysis under intra-route resource reuse. Assuming M time slots per TDMA cycle, we have $A_i = \lim\limits_{K\to\infty} \frac{1}{K}\sum_{k=0}^{K-1} B(\boldsymbol{X}'_{i-1}, k) = 1/M$. Given the routing distance R and the relay set Φ', the local throughput of link $\boldsymbol{X}'_{i-1} \to \boldsymbol{X}'_i$ is

$$T_{\mathrm{local}}(\boldsymbol{X}'_i) = \frac{1}{M}\Pr\left\{\widetilde{\mathrm{SIR}}(\boldsymbol{X}'_i) > \theta \mid R, \Phi'\right\} \ . \tag{4.16}$$

Except for the hop distance L'_i of link $\boldsymbol{X}'_{i-1} \to \boldsymbol{X}'_i$, $\tilde{I}_{in}(\boldsymbol{X}'_i)$ is independent of the distribution of other relays in Φ. So following the definition of (4.8), we define the coverage probability of a hop distance l with intra-route resource reuse as

$$P'_s(l) \stackrel{\triangle}{=} \Pr\left\{Hl^{-\beta}/(I_o + \tilde{I}_{in}(l)) > \theta\right\} \ , \tag{4.17}$$

where

$$\tilde{I}_{in}(l) = \sum_{j\in\mathbb{Z}^-} H_j|jMl_0 + l|^{-\beta} + \sum_{j\in\mathbb{Z}^+} H_j|(jM-1)l_0|^{-\beta} \ . \tag{4.18}$$

Let function $\mathcal{L}_{I_o}(s)$ denote the Laplace transform of the PDF of the external interference I_o, and $\mathcal{L}_{\tilde{I}_{in}(l)}(s)$ the Laplace transform of the PDF of the intra-route inference $\tilde{I}_{in}(l)$. We have

$$P_s'(l) = \mathcal{L}_{I_o}(\theta l^\beta)\mathcal{L}_{\tilde{I}_{in}(l)}(\theta l^\beta) \ . \tag{4.19}$$

Since we assume that the locations of the active external interferers are independent across time, it follows that $\mathcal{L}_{I_o}(\theta l^\beta) = P_s(l) = \exp(-\kappa l^2)$ as defined in *Lemma 4.1.* $\mathcal{L}_{\tilde{I}_{in}(l)}(s)$ can be calculated as [114]

$$\prod_{k\in\mathbb{Z}^+} \frac{1}{s(kMl_0 + l)^{-\beta} + 1} \cdot \frac{1}{s[(kM-1)l_0]^{-\beta} + 1} \ . \tag{4.20}$$

Combining (4.19) and (4.20), we have the following lemma on the local throughput.

Lemma 4.2 *Define function $P_{in}(l)$ as*

$$P_{in}(l) \stackrel{\triangle}{=} \prod_{k\in\mathbb{Z}^+} \frac{1}{\theta(kM\frac{l_0}{l} + 1)^{-\beta} + 1} \cdot \frac{1}{\theta[(kM-1)\frac{l_0}{l}]^{-\beta} + 1} \ . \tag{4.21}$$

In the QED routing with intra-route resource reuse, for a hop distance of l, the coverage probability is

$$P_s'(l) = P_s(l)P_{in}(l) \ , \tag{4.22}$$

where $P_s(l)$ is defined in Lemma 4.1. *A closed form lower bound of $P_{in}(l)$ can be calculated*

as

$$
\begin{aligned}
P_{in}(l) \geq \exp\{ & -\frac{l}{Ml_0\theta^{-\frac{1}{\beta}}}\mathcal{B}(\frac{1}{\theta^{-1}(M\frac{l_0}{l}+1)^{\beta}+1};1-\frac{1}{\beta},\frac{1}{\beta}) \\
& -\left(2+\frac{l}{Ml_0}\right)\ln\left(\theta(M\frac{l_0}{l}+1)^{-\beta}+1\right) \\
& -\frac{l}{Ml_0\theta^{-\frac{1}{\beta}}}\mathcal{B}(\frac{1}{\theta^{-1}[(M-1)\frac{l_0}{l}]^{\beta}+1};1-\frac{1}{\beta},\frac{1}{\beta}) \\
& -(2-\frac{1}{M})\ln\left(\theta[(M-1)\frac{l_0}{l}]^{-\beta}+1\right)\} \ , \qquad (4.23)
\end{aligned}
$$

where $\mathcal{B}(\cdot;\cdot,\cdot)$ *is the incomplete beta function.*

Proof: Note that $\ln P_{in}(l)$ can be expressed as

$$
-\sum_{k=1}^{\infty}\ln\left(\theta(kM\frac{l_0}{l}+1)^{-\beta}+1\right)+\ln\left(\theta[(kM-1)\frac{l_0}{l}]^{-\beta}+1\right).
$$

Since $\ln\left(\theta(kM\frac{l_0}{l}+1)^{-\beta}+1\right)$ and $\ln(\theta[(kM-1)\frac{l_0}{l}]^{-\beta}+1)$ are both decreasing functions with respect to k for $k \geq 1$, (4.23) can be obtained by approximating the summation of series with the integral of the corresponding function. □

So the end-to-end throughput can be expressed as

$$
T_{\text{end}} = \min_{\boldsymbol{X}'_i \in \Phi' \cup \{\boldsymbol{D}\}} \frac{1}{M} P'_s(|\boldsymbol{X}'_i - \boldsymbol{X}'_{i-1}|) \ . \qquad (4.24)
$$

In the rest of this chapter, we first derive the average end-to-end throughput of the NN routing, followed by the case of the QED routing.

4.4 Stochastic Analysis on Hop-Distance under NN Routing

As a preparation for further throughput analysis, in this section, we analyze the distribution of the longest hop distance in the NN routing, denoted by L_m.

The longest hop distance L_m of Φ is of special interest for two reasons. First, consider a simple TDMA where the relays in Φ are assigned with a fixed slot length, i.e., $A_i = 1/(N+1)$ for $i = 0, 1, ..., N$, with N being the number of relays. In this case, as the coverage probability $P_s(l)$ is a non-increasing function with respect to the hop distance l, the end-to-end throughput will be the local throughput of the hop with the longest hop distance. Second, for any MAC protocol or resource allocation scheme employed, the end-to-end throughput cannot exceed the coverage probability of the longest hop distance, $P_s(L_m)$. Thus, the stochastic analysis of L_m sheds light on the theoretical upper bound of the end-to-end throughput.

We have the following theorem on the distribution of L_m.

Theorem 4.1 *Given the routing distance between source and destination $R = r$, we have:*

1. *The conditional CDF of L_m, $\Pr\{L_m \leq l | R = r\} = 1$ for $l \geq r$. Moreover, $\Pr\{L_m = r | R = r\} = e^{-\lambda r}$ and $\Pr\{L_m < r | R = r\} = 1 - e^{-\lambda r}$.*

2. *Define $g(l, r) \stackrel{\triangle}{=} \Pr\{L_m \leq l | R = r\}$ and denote the Laplace transform (LT) of $g(l, r)$ with respect to r by $G(l, s)$, then*

$$G(l, s) = \frac{1 - e^{-(\lambda+s)l}}{s + \lambda e^{-(\lambda+s)l}} \ . \tag{4.25}$$

Proof:

1) This part follows directly from the properties of PPP.

2) For $0 < l < r$, consider the conditional probability of L_m given that the first relay $\boldsymbol{X}_1$ is located at $(x, 0)$, $\Pr\{L_m \leq l | R = r, |\boldsymbol{X}_1| = x\}$. Since the distribution of the points of Φ in disjoint intervals are independent, basing on the Palm theory of PPP[1], given $|\boldsymbol{X}_1| = x$, the remaining relay nodes within the interval (x, r) is still a 1D PPP of intensity λ. The distribution of the longest hop distance for the relays within (x, r) should be the same as that for $R = r - x$. Since $|\boldsymbol{X}_1|$ is exponentially distributed for $x < r$, we have

$$\begin{aligned} \Pr\{L_m \leq l | R = r\} &= \int_0^l f_{|\boldsymbol{X}_1|}(x) \Pr\{L_m \leq l | R = r, |\boldsymbol{X}_1| = x\} \mathrm{d}x \\ &= \int_0^l \lambda e^{-\lambda x} \Pr\{L_m \leq l | R = r - x\} \mathrm{d}x \ . \end{aligned} \tag{4.26}$$

Consider the following integral

$$\begin{aligned} & \int_l^{+\infty} \Pr\{L_m \leq l | R = r\} e^{-sr} \mathrm{d}r \\ = & \int_l^{+\infty} \int_0^l \lambda e^{-\lambda x} \Pr\{L_m \leq l | R = r - x\} e^{-sr} \mathrm{d}x \mathrm{d}r \\ = & \int_0^l \lambda e^{-\lambda x} \left(\int_l^{l+x} \Pr\{L_m \leq l | R = r - x\} e^{-sr} \mathrm{d}r \right. \\ & \left. + \int_{l+x}^{+\infty} \Pr\{L_m \leq l | R = r - x\} e^{-sr} \mathrm{d}r \right) \mathrm{d}x \\ = & \frac{e^{-sl}}{s}(1 - e^{-\lambda l}) - \frac{\lambda e^{-sl}}{s(\lambda + s)}(1 - e^{-(\lambda+s)l}) \\ & + \frac{\lambda}{\lambda + s}(1 - e^{-(\lambda+s)l})[G(l, s) - \frac{1 - e^{-sl}}{s}] \ . \end{aligned} \tag{4.27}$$

[1]For a PPP, given that one node is located at a particular point, the conditional distribution of all other nodes is still a PPP, which is known as Slivnyak-Mecke Theorem [47, Theorem 1.4.5].

Note that we also have

$$\int_{l}^{+\infty} \Pr\{L_m \leq l | R = r\} e^{-sr} \mathrm{d}r = G(l,s) - \frac{1 - e^{-sl}}{s} \ . \tag{4.28}$$

Following (4.27) and (4.28), we get $G(l,s) = \frac{1-e^{-(\lambda+s)l}}{s+\lambda e^{-(\lambda+s)l}}$. □

Moreover, we have the following result about the region of convergence (ROC) of $G(l,s)$.

Corollary 4.1 *The ROC of $G(l,s)$ includes the imaginary axis. More specifically, $g(l,r)$ is absolutely integrable, i.e.,*

$$\int_{-\infty}^{+\infty} |g(l,r)| dr < +\infty \ . \tag{4.29}$$

Proof: Please refer to Appendix J. □

Following *Theorem 4.1* and *Corollary 4.1*, the conditional CDF of L_m given $R = r$ can be computed numerically by calculating the inverse Fourier Transform (FT) of $G(l, j\omega)$.

To obtain a closed form expression for the CDF of L_m, instead of fixing the routing distance $R = r$, we can model R as an exponentially distributed RV of mean $\frac{1}{\nu}$. Basing on *Theorem 4.1*, the CDF of L_m can be calculated as

$$\Pr\{L_m \leq l\} = \frac{\nu(1 - e^{-(\lambda+\nu)l})}{\nu + \lambda e^{-(\lambda+\nu)l}} \ , \quad \forall l \geq 0 \ . \tag{4.30}$$

Basing on *Theorem 4.1*, we can also evaluate the mean and variance of L_m with respect to the routing distance.

Theorem 4.2 *For a fixed relay intensity λ, as r approaches $+\infty$, $\mathbb{E}\{L_m \mid R = r\} \sim$*

$\mathcal{O}(\ln(r))$. *More specifically, for* $r > 0$, *let* $m_{L_m}(r) \stackrel{\triangle}{=} \mathbb{E}\{L_m \mid R = r\}$, *we have*

$$m_{L_m}(r) = \int_0^r \frac{1 - e^{-\lambda x}}{\lambda x} dx \ , \tag{4.31}$$

whose LT is

$$M_{L_m}(s) = \frac{1}{s\lambda} \ln(\frac{\lambda}{s} + 1) \ . \tag{4.32}$$

Moreover, for any given λ, *the conditional variance of* L_m *under* $R = r$, $\mathbb{D}\{L_m \mid R = r\}$, *satisfies*

$$\lim_{r \to \infty} \mathbb{D}\{L_m \mid R = r\} = \frac{\pi^2}{6\lambda^2} \ . \tag{4.33}$$

Proof: Please refer to Appendix K. □

Remark 4.1 *From* Theorem 4.2, *we can see that for a fixed relay intensity* λ, *the conditional mean of the longest hop distance* $\mathbb{E}\{L_m \mid R = r\} \sim \mathcal{O}(\ln(r))$ *as the routing distance* $r \to +\infty$, *and its variance is bounded. Unlike the case with evenly deployed relays where the per hop distance stays constant with respect to the routing distance, for randomly distributed relays, the longest hop distance would go to infinity as the routing distance approaches infinity, i.e., the throughput of the worst hop would approach zero. This shows that long distance communication is not feasible in randomly deployed networks.*

4.5 The Average End-to-End Throughput under NN routing

In this section, we derive the average end-to-end throughput under NN routing over all the possible realizations of relays Φ. We discuss two different resource allocation schemes: a conventional TDMA scheme with fixed slot length and a dynamic TDMA scheme with flexible slot length.

4.5.1 Throughput Analysis under NN Routing with fixed slot length

We consider a conventional TDMA resource allocation scheme where a TDMA cycle would consist of $N+1$ time slots, each of which would be allocated to one relay node or the source node. Following (4.11), the end-to-end throughput can be expressed as

$$T_{\text{end}} = \min_{\boldsymbol{X}_i' \in \Phi' \cup \{\boldsymbol{D}\}} \frac{P_s(|\boldsymbol{X}_i' - \boldsymbol{X}_{i-1}'|)}{N+1} = \frac{P_s(L_m)}{N+1} \ , \tag{4.34}$$

where the second equation follows from the fact that $P_s(\cdot)$ is a non-increasing function.

Given the coverage probability function $P_s(\cdot)$, the average coverage probability of the longest hop, $\mathbb{E}\{P_s(L_m)\}$, should depend on the intensity of the relays, λ, and the routing distance R. For this reason, we define $p(x,r) \stackrel{\triangle}{=} \mathbb{E}\{P_s(L_m) \mid \lambda = x, R = r\}$. Then, we have the following theorem on the end-to-end throughput.

Theorem 4.3 *For a relay intensity λ, given the routing distance R, the average end-to-end*

throughput is given by

$$\mathbb{E}\{T_{end} \mid R\} = \frac{e^{-\lambda R}}{\lambda} \int_0^{\lambda} e^{Rx}\ p(x,R)dx\ . \tag{4.35}$$

Proof: Please refer to Appendix L. □

Note that the function $p(x,r)$ can be computed numerically, which only depends on the marginal distribution of L_m. Following *Theorem 4.3*, we can calculate $\mathbb{E}\{T_{\text{end}} \mid R\}$ without deriving the joint *probability density function* (PDF) of N and L_m explicitly. With the following Lemma, we can further reduce the computational complexity by calculating the Laplace transform of $\mathbb{E}\{T_{\text{end}} \mid R = r\}$ with respect to r.

Lemma 4.3 *Taking the relay intensity Λ as a random variable and let $f_{L_m|\Lambda,R}(l \mid x,r)$ denote the conditional PDF of the longest hop distance L_m given the relay intensity $\Lambda = x$ and routing distance $R = r$. Define*

$$q(l,\lambda,r) \stackrel{\triangle}{=} \frac{e^{-\lambda r}}{\lambda} \int_0^{\lambda} e^{rx}\ f_{L_m|\Lambda,R}(l \mid x,r)\ dx\ , \tag{4.36}$$

then the Laplace transform of $q(l,\lambda,r)$ with respect to r is

$$Q(l,\lambda,s) = \frac{(s+\lambda)}{\lambda + e^{(s+\lambda)l}s}\ . \tag{4.37}$$

This lemma follows directly from the Laplace transform of $f_{L_m|\Lambda,R}(l \mid x,r)$ and we skip the proof for brevity. Basing on *Lemma 4.3*, we have the following result on $\mathbb{E}\{T_{\text{end}} \mid R = r\}$.

Proposition 4.1 *For a fixed relay intensity λ, define $T_{end}(r) \stackrel{\triangle}{=} \mathbb{E}\{T_{end}|R = r\}$ as the average end-to-end throughput given routing distance $R = r$. The Laplace transform of*

$T_{end}(r)$, $\mathcal{T}_{end}(s)$, can be calculated as

$$\mathcal{T}_{end}(s) = \int_0^{+\infty} P_s(l) \ \frac{s+\lambda}{\lambda + e^{(s+\lambda)l}s} \ dl \ . \tag{4.38}$$

Proof: Recall that $p(x,r) = \mathbb{E}\{P_s(L_m) \mid \lambda = x, R = r\}$, where $P_s(L_m)$ is the coverage probability of the longest hop, then $p(x,r)$ can be calculated as

$$p(x,r) = \int_0^{+\infty} P_s(l) \ f_{L_m|\Lambda,R}(l \mid x,r)\mathrm{d}l \ . \tag{4.39}$$

So $T_{\text{end}}(r)$ can be expressed as

$$\begin{aligned} T_{\text{end}}(r) \ &= \ \frac{e^{-\lambda r}}{\lambda} \int_0^{\lambda} e^{rx} \int_0^{+\infty} P_s(l) \ f_{L_m|\Lambda,R}(l \mid x,r)\mathrm{d}l\mathrm{d}x \\ &= \int_0^{+\infty} P_s(l) \ q(l,\lambda,r) \ \mathrm{d}l \ . \end{aligned} \tag{4.40}$$

Basing on *Lemma 4.3*, (4.38) can be obtained accordingly. □

Following *Proposition 4.1* and *Corollary 4.1*, the mean of the throughput can be computed numerically through the inverse Fourier transform of $T_{\text{end}}(j\omega)$.

As shown in *Proposition 4.1*, a closed-form expression of the end-to-end throughput is hard to derive. In order to further analyze the impacts of different network parameters on the network performance, we derive the following lower bound on end-to-end throughput.

Proposition 4.2 *For a given relay intensity λ and routing distance r, the end-to-end*

throughput $T_{end}(r)$ is lower bounded by $T_{end,L}(r)$, i.e., $T_{end}(r) \geq T_{end,L}(r)$, where

$$T_{end,L}(r) = \frac{1-e^{-\lambda r}}{\lambda r} \exp(-\frac{\kappa\lambda^{-2}}{1-e^{-\lambda r}}[\ln^2(\lambda r)+2B(\lambda r)\ln(\lambda r) \\ +2C(\lambda r)+c-e^{-\lambda r}\left(A(\lambda r)^2+(2+c)\lambda r+c\right)]), \tag{4.41}$$

with $c = \max\limits_{t\in(0,1)} \left[\frac{\ln^2 t}{(1-t)^2} - \ln^2 t\right] \approx 1.51$, $A \triangleq \int_0^{+\infty} \frac{l^2 e^{-l}}{1-e^{-l}} dl \approx 2.404$, $B(x) \triangleq \int_0^1 \frac{1-e^{-u}}{u} du - \int_1^x \frac{e^{-u}}{u} du$, $C(x) \triangleq \int_1^x \ln u \frac{e^{-u}}{u} du - \int_0^1 \ln u \frac{1-e^{-u}}{u} du$.

For $\lambda r \gg 1$, the lower bound $T_{end,L}(r)$ approximates

$$T_{end,L}(r) \approx \frac{1}{\lambda r} \exp\left(-\kappa\lambda^{-2}[\ln^2(\lambda r)+2B\ln(\lambda r)+2C+c]\right), \tag{4.42}$$

where $B = \lim\limits_{x\to+\infty} B(x) \approx 0.577$, $C = \lim\limits_{x\to+\infty} C(x) \approx 0.989$.

Proof: Please refer to Appendix M. □

In the following, we consider to optimize the lower bound $T_{\text{end,L}}(r)$ with respect to the relay intensity λ.

Corollary 4.2 *For $\lambda r \gg 1$, the optimal relay intensity λ^* that maximizes $T_{end,L}(r)$ should satisfy $\lambda_1 < \lambda^* < \lambda_2$, where*

$$\lambda_1 = \frac{1}{r} \exp\left(\frac{1}{r\sqrt{2\kappa}} \exp\left(-W_{-1}(-\frac{1}{r\sqrt{2\kappa}})\right)\right), \tag{4.43}$$

$$\lambda_2 = \frac{1}{r} \exp\left(\frac{e^{-\sqrt{2C+c-B}}}{r\sqrt{2\kappa}} \exp\left(-W_{-1}(-\frac{e^{-\sqrt{2C+c-B}}}{r\sqrt{2\kappa}})\right)\right), \tag{4.44}$$

and $W_{-1}(\cdot)$ is the real branch of Lambert W function over $(-\infty,-1)$ [115].

Proof: Please refer to Appendix N. □

4.5.2 Throughput Analysis under NN Routing with flexible slot length

In TDMA, it may be unwise to allocate equal time slots to each hop since the time resources may be wasted at the relay nodes whose arrival rates are much lower than their service rates. Recall that A_i denotes the normalized slot length allocated to hop i and L_i denotes its hop distance. Given the relay deployment Φ, we can formulate the resource allocation problem as

$$\begin{aligned} \text{Maximize} \quad & \min_i (A_i P_s(L_i)) \\ \text{s.t.} \quad & \sum_i A_i = 1 \ . \end{aligned} \tag{4.45}$$

It follows that the optimal $A_i = 1/\left[P_s(L_i)\sum_j 1/P_s(L_j)\right]$, and the optimized throughput is

$$T_{\text{end}} = 1/\left(\sum_i 1/P_s(L_i)\right) \ . \tag{4.46}$$

Note that the end-to-end throughput (4.46) is a function of hop distances L_i for $i = 1, 2, ..., N+1$. Our goal is to evaluate the mean of (4.46) with respect to the distribution of Φ.

Define the RVs Y_i and Y as

$$Y_i \stackrel{\triangle}{=} 1/P_s(L_i) \ , \quad Y \stackrel{\triangle}{=} \sum_i Y_i = 1/T_{\text{end}} \ . \tag{4.47}$$

We first derive the distribution of Y and then calculate the mean of its reciprocal, i.e., the average end-to-end throughput.

Define function $g_Y(y,r) \stackrel{\triangle}{=} f_{Y|R}(y|r)$, the conditional PDF of Y given routing distance $R = r$. For a given location of the first relay, following a similar derivation as in the proof of *Theorem 4.1*, we have

$$\begin{aligned} f_{Y|R}(y|r) = {} & \Pr\{|\Phi| = 0\}\ f_{Y_1|L_1}(y \mid r) \\ & + \int_0^r f_{L_1}(x) \int_0^y f_{Y_1|L_1}(\tau \mid x) f_{Y|R}(y-\tau|r-x) \mathrm{d}\tau \mathrm{d}x \ . \end{aligned} \tag{4.48}$$

Since Y_i is a deterministic function of L_i, we have $f_{Y_1|L_1}(y \mid x) = \delta(y - 1/P_s(x))$. The 2D Laplace transform of $g_Y(y,r)$ can be expressed as

$$G_Y(s_1,s_2) = \frac{F_{Y_1,L_1}(s_1,s_2)}{\lambda(1 - F_{Y_1,L_1}(s_1,s_2))} \ , \tag{4.49}$$

where

$$F_{Y_1,L_1}(s_1,s_2) = \int_0^{+\infty} \lambda e^{-(\lambda+s_2)r} e^{-\frac{s_1}{P_s(r)}} \mathrm{d}r \ , \tag{4.50}$$

is the 2D Laplace transform of $f_{Y_1,L_1}(y,x)$. We have the following theorem on the average end-to-end throughput:

Theorem 4.4 *Denote the average throughput with dynamic resource allocation given routing distance r, $\mathbb{E}\{T_{end} \mid R = r\}$, by function $T_{end}(r)$. The Laplace transform of $T_{end}(r)$ is*

$$\mathcal{T}_{end}(s) = \int_0^{+\infty} G_Y(u,s)\, du \ , \tag{4.51}$$

where $G_Y(u,s)$ is defined in (4.49).

This theorem follows directly from the property of Laplace transform.

4.6 The Average End-to-End Throughput under QED Routing

In this section, we evaluate the average end-to-end throughput of the proposed QED routing under fixed-length TDMA, both with and without intra-route resource reuse.

4.6.1 Throughput Analysis under QED Routing without Intra-Route Resource Reuse

In this scheme, each relay in Φ' is allocated with a time slot of fixed length. Let L'_m denote the longest hop distance in the relay set Φ'. Following (4.34), the end-to-end throughput can be expressed by

$$T_{\text{end}} = \frac{1}{N'+1} P_s(L'_m) \ . \tag{4.52}$$

where N' is the number of relays in Φ'. Unfortunately, as Φ' is not a PPP anymore, it is hard to derive an accurate expression of the end-to-end throughput for QED routing as we did for the NN routing. In order to make the end-to-end throughput analysis tractable, the following approximation is made.

Approximation 2 *Given routing distance $R = r$, the average end-to-end throughput is approximated by*

$$\mathbb{E}\{T_{end} \mid R = r\} = \frac{P_s(\mathbb{E}\{L'_m \mid R = r\})}{\mathbb{E}\{N' \mid R = r\} + 1} \ . \tag{4.53}$$

The validity of this approximation is verified by simulation, as shown in Section 4.7. In

addition, we make the following approximation on $\mathbb{E}\{N' \mid R = r\}$.

Approximation 3 *Given routing distance $R = r$, the average number of relays selected by QED routing, $N' = |\Phi'|$ is approximated by*

$$\mathbb{E}\{N' \mid R = r\} = \frac{r}{l_0 + 1/\lambda} \ . \tag{4.54}$$

The reason behind this approximation is that, if an infinite routing distance is assumed, the average routing distance per hop under QED routing is $l_0 + 1/\lambda$. Also, according to the ergodicity, N' will approach its mean almost surely as $r \to +\infty$.

We have the following theorem on the distribution of the longest hop distance L'_m for Φ'.

Theorem 4.5 *Define $g'(l, r) \stackrel{\triangle}{=} \Pr\{L'_m \leq l \mid R = r\}$ as the condition CDF of L'_m given routing distance $R = r$. Denote its Laplace transform with respect to r by $G'(l, s) = \int_0^{+\infty} g'(l, r)e^{-sr}\,dr$ for $l > l_0$, we have*

$$G'(l, s) = \frac{1}{s} - \frac{(\lambda + s)e^{-(s+\lambda)\cdot l + \lambda l_0}}{s\{\lambda \cdot [1 + e^{-(s+\lambda)\cdot l + \lambda l_0} - e^{-s\cdot l_0}] + s\}} \ . \tag{4.55}$$

As $r \to +\infty$, the conditional mean of L'_m given routing distance $R = r$, $\mathbb{E}\{L'_m \mid R = r\}$, satisfies

$$\lim_{r \to +\infty} \mathbb{E}\{L'_m \mid R = r\} - \left[\frac{1}{\lambda}\left(\ln \frac{\lambda r}{\lambda l_0 + 1} + B\right) + l_0\right] = 0 \ . \tag{4.56}$$

where constant $B \approx 0.577$ is defined the same as Proposition 4.2.

Proof: Please refer to Appendix O. □

Basing on *Theorem 4.5*, we can make the following approximation on L'_m.

Approximation 4 *Then conditional mean of L'_m given $R = r \gg l_0$ is approximated by*

$$\mathbb{E}\{L'_m \mid R = r\} \approx \frac{1}{\lambda}\left(\ln \frac{\lambda r}{\lambda l_0 + 1} + B\right) + l_0 \ . \tag{4.57}$$

Basing on the approximations above, we have the following theorem on the end-to-end throughput of QED routing.

Theorem 4.6 *The average end-to-end throughput of QED routing for routing distance $r \gg l_0$, $\mathbb{E}\{T_{end} \mid R = r\}$, can be approximated by*

$$\frac{l_0 + 1/\lambda}{r + l_0 + 1/\lambda} \exp\left\{-\kappa \left[\frac{1}{\lambda}\left(\ln \frac{\lambda r}{\lambda l_0 + 1} + B\right) + l_0\right]^2\right\}. \tag{4.58}$$

Routing parameter l_0 can be optimized to maximize the end-to-end throughput (4.58) by calculating its derivative, by which the following Corollary is obtained.

Corollary 4.3 *For a routing distance $r \gg \max(l_0, 1/\lambda)$, the optimal l_0 satisfies $\underline{l_0} < l_0^* < \overline{l_0}$, where*

$$\underline{l_0} = \frac{\sqrt{(\ln \lambda r + B)^2 + \frac{2\lambda^2}{\kappa}} - (\ln \lambda r + B)}{2\lambda} , \tag{4.59}$$

$$\overline{l_0} = \frac{\sqrt{B^2 + \frac{2\lambda^2}{\kappa}} - B}{2\lambda} . \tag{4.60}$$

4.6.2 Throughput Analysis under QED Routing with Intra-Route Resource Reuse

Recall that in *Lemma 4.2*, we derived the coverage probability function $P_s'(l)$ for the intra-route resource reuse, which is a non-increasing function with respect to the hop distance l. Following (4.24), the end-to-end throughput of QED routing with the intra-route resource reuse can be expressed as

$$T_{\text{end}} = \min_{\boldsymbol{X}_i' \in \Phi' \cup \{\boldsymbol{D}\}} \frac{1}{M} P_s'(|\boldsymbol{X}_i' - \boldsymbol{X}_{i-1}'|) = \frac{1}{M} P_s'(L_m') , \tag{4.61}$$

where M is the number of time slots in a TDMA cycle. Following *Approximation 2* where the RV L'_m is replaced by its mean, we have the following theorem on the average end-to-end throughput.

Theorem 4.7 *Given the routing distance r, the average end-to-end throughput of QED routing with intra-route resource reuse can be approximated by*

$$\mathbb{E}\{T_{end} \mid R = r\} = \frac{1}{M} P'_s(\mathbb{E}\{L'_m \mid R = r\}) \ , \tag{4.62}$$

where $\mathbb{E}\{L'_m \mid R = r\}$ is given in Approximation 4.

The effect of slot number M on the network performance is two fold. First, a smaller M allows a larger number of concurrent transmissions on the route, by which a larger equivalent bandwidth can be obtained, whereas a stronger intra-route interference is introduced. Second, consider a large scale wireless network which consists of a number of multi-hop links, the increase of concurrent transmissions on each route, which results from the decrease of M, will also generate a stronger inter-route interference on other routes. That is, the selection of M also affects the intensity of the active external interferers. Since the number of concurrent transmissions on a route is linearly proportional to $1/M$, we assume that the intensity of active external interferers μ' satisfies $\mu' = \mu'_1/M$, where μ'_1 denotes the intensity of active interferers for $M = 1$. For a given μ'_1, we discuss the selection of M for different routing distance r under two scenarios: 1) the node intensity is constant; and 2) the source-destination pair intensity is constant.

4.6.2.1 Constant node intensity

In this case, μ_1' is assumed to be constant for different r, denoted by $\mu_1' = \bar{\mu}$ for a constant $\bar{\mu}$. Then we have the following corollary on the optimal number of time slots M.

Corollary 4.4 *As the routing distance $r \to \infty$, the optimal number of time slots $M^*(r)$ for routing distance r that maximizes the end-to-end throughput scales with*

$$M^*(r) \sim \mathcal{O}(\bar{\kappa}\mathbb{E}^2\{L_m' \mid R = r\}) \ , \tag{4.63}$$

where $\bar{\kappa} = 2\pi\bar{\mu}\frac{\pi}{\beta\sin(2\pi/\beta)}\theta^{2/\beta}$.

Proof: Please refer to Appendix P. □

4.6.2.2 Constant source-destination pair intensity

In this case, we consider a multi-hop wireless network formed by multiple source-destination pairs, where the intensity of the source-destination pairs is assumed to be a constant and their routing distances are the same as r. So for a given r, μ_1' will be linearly proportional to the average hop number per route, $\mathbb{E}\{N' + 1 \mid R = r\}$, which is linearly proportional to r as shown in *Approximation 3*. For simplicity, with other parameters being fixed, we assume that $\mu_1' = \bar{\mu}r$ for a constant $\bar{\mu}$. So the intensity of the active external interferers can be denoted by $\mu' = \bar{\mu}r/M$.

Corollary 4.4 still holds for this case by replacing $\bar{\kappa}$ with $\bar{\kappa}r$, i.e., $M^*(r) \sim \mathcal{O}(\bar{\kappa}r\mathbb{E}^2\{L_m' \mid R = r\})$. However, since the average hop number $\mathbb{E}\{N' + 1 \mid R = r\}$ is linearly proportional to r, for $r \to +\infty$, we have

. (4.64)

That is, *the number of time slots in a TDMA cycle is greater than the number hops on the route,* which implies that each time slot will be allocated to at most one hop on the same route. Thus, we have the following corollary.

Corollary 4.5 *In a network with random relays and a finite relay intensity λ, for a fixed source-destination pair intensity, as the routing distance $r \to +\infty$, the intra-route resource reuse should not be adopted for the end-to-end throughput optimization.*

Remark 4.2 *It is interesting to note that when the relay intensity $\lambda = \infty$, the intra-route resource reuse would still be beneficial even for fixed source-destination pair intensity. In fact, when $\lambda = \infty$, the relays selected by the QED routing converge to a equidistant deployment with a hop distance of l_0. From* Corollary 4.4 *and the discussions above, the optimal number of time slots for the equidistant relays scales with $\mathcal{O}(\bar{\kappa} r l_0^2)$ as the routing distance $r \to +\infty$. Since the hop number of the equidistant relays is r/l_0, as long as $r/l_0 \gg \bar{\kappa} r l_0^2$, i.e., $\bar{\kappa} l_0^3 \ll 1$, the intra-route resource reuse is still beneficial. Comparing with the result in* Corollary 4.5*, we can see that this is another difference between equidistant relays and random relays.*

4.7 Numerical Results

In this section, we evaluate the end-to-end throughput performance with random relay deployment through numerical results. Unless otherwise clarified, we will use the following parameters: the interferer intensity $\mu = 5 \times 10^{-4}$ $/m^2$, the ALOHA access probability $p_a = 0.1$, the path-loss exponent $\beta = 4$, the SINR threshold for successful transmission $\theta = 10$ dB. We first start with the case of NN routing and then simulate the performance of QED routing.

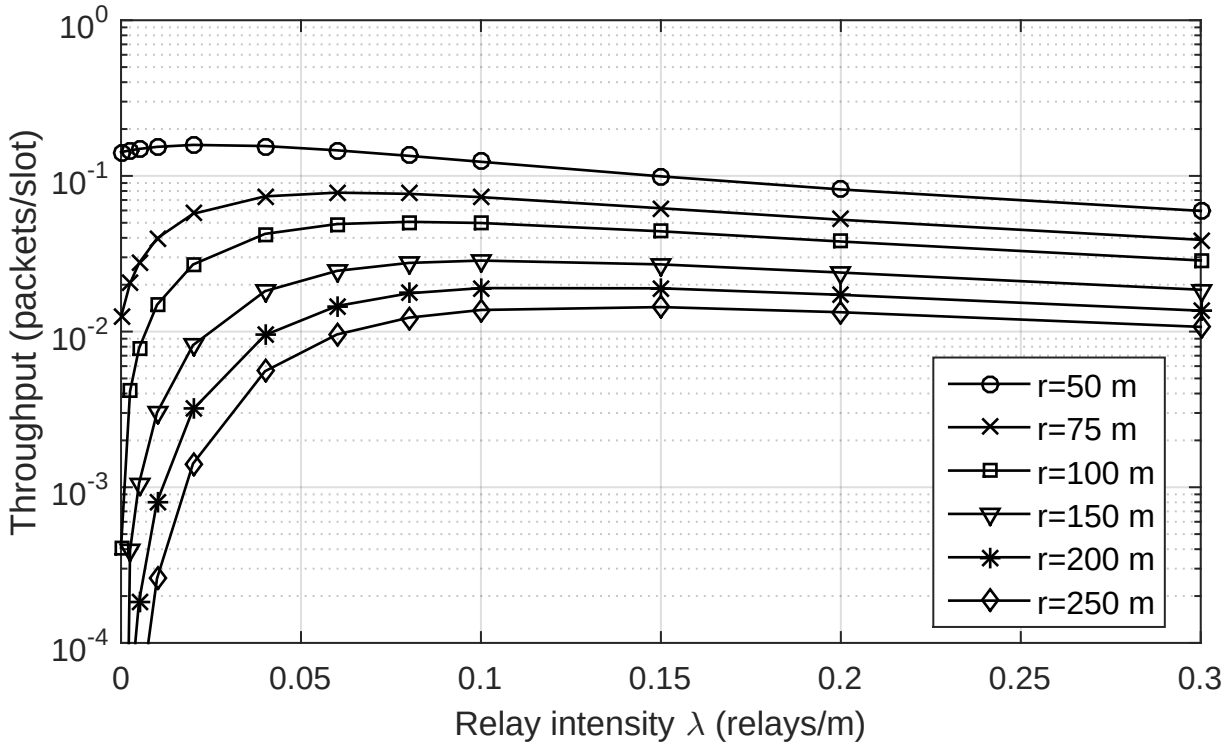


Figure 4.2: Average end-to-end throughput versus relay intensity under NN routing with fixed slot length.

4.7.1 Numerical Results of NN Routing

Example 1: End-to-end throughput of NN routing with fixed slot length In this example, we evaluate the end-to-end throughput with random relays using NN routing and fixed slot length. Fig. 4.2 shows the average end-to-end throughput versus relay intensity λ for different routing distance r. It can be observed that: even without an optimized deployment of relays, the end-to-end throughput can still be obviously improved compared with the case of direct connection. For example, if a minimum end-to-end throughput of 1×10^{-2} packets/slot is required, the maximum communication range is around 75 m without the relays, while the communication range expands to more than 250 m with multi-hop relays. It can be observed that the optimal relay intensity λ increases as r increases, on the contrary

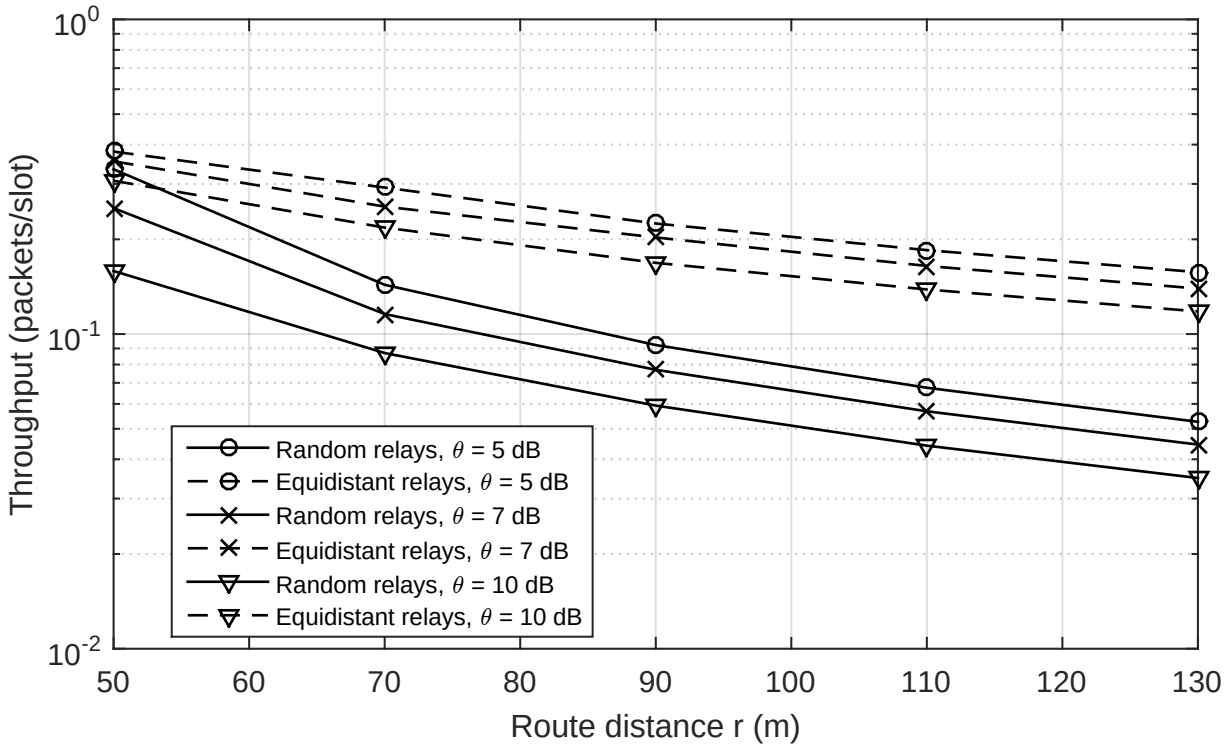


Figure 4.3: Throughput comparison with fixed slot length: random relays under NN routing versus equidistant relays

to the equidistant relays where the optimal relay distance stays constant[2].

Example 2: Performance comparison with equidistant relays In this example, we compare the end-to-end throughput between equidistant and random relays using NN routing with fixed slot length. Fig. 4.3 shows the optimal end-to-end throughput of random relay deployment and that of equidistant relays under different routing distance r and SINR threshold θ. The relay intensity λ is optimized for each routing distance. The random relay deployment suffers a significant performance loss compared to the ideal case. For instance, with a SINR threshold θ of 10 dB under the network configuration, there is a 48% throughput loss at $r = 50$ m and a 70% performance loss at $r = 130$ m, which are not negligible for system evaluation.

[2]Here, we refer to the upper bound of end-to-end throughput for equidistant relays, $\frac{d}{r}P_{cov}(d)$, where d is the per hop distance, and the optimal d is independent of r.

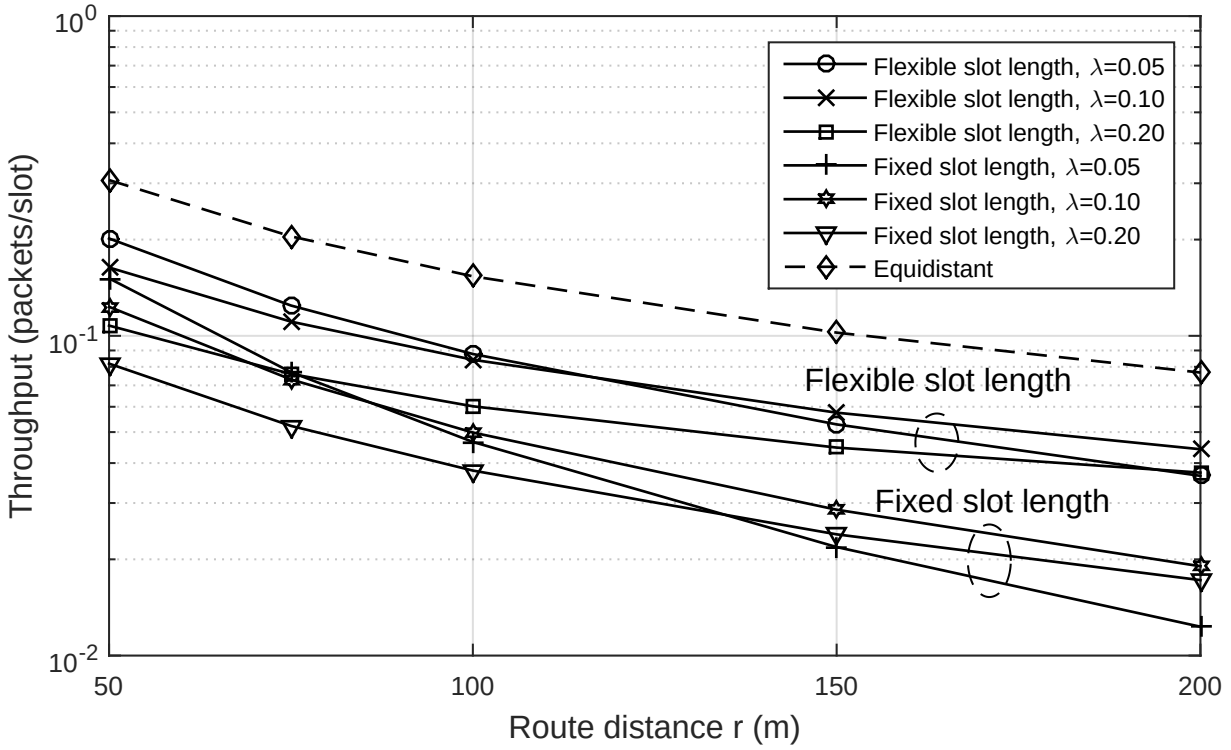


Figure 4.4: Throughput comparison under NN routing: fixed slot length versus flexible slot length

Example 3: End-to-end throughput with flexible slot length In this example, we test the end-to-end throughput with flexible slot length in NN routing. Fig. 4.4 shows the end-to-end throughputs of different schemes under different relay intensities and routing distances. We can observe that a significant performance improvement is achieved by dynamic resource allocation compared with the fixed slot length. Using a flexible slot length, the performance loss from the equidistant case also degrades much slower than the case of fixed slot length with the increase of routing distance.

4.7.2 Numerical Results of QED routing

Example 4: End-to-end throughput under QED routing without intra-route resource reuse In this example, we evaluate the average end-to-end throughput of the QED routing without intra-route resource reuse, and compare it with that of the NN routing as well as that of the equidistant relays. Fig. 4.5 shows the average end-to-end throughputs of the QED routing and the NN routing for different routing distances. For each routing distance, the relay intensity λ is the same for both the NN and the QED routing, which is optimized with respect to the average end-to-end throughput of the NN routing. In terms of the selection of parameter l_0 in the QED routing, we choose $l_0 = (\overline{l_0} + \underline{l_0})/2$ as defined in Corollary 4.3. First, it can be observed that the average end-to-end throughput derived in Theorem 4.6 provides a very close approximation to the simulation results, substantiating the validity of the approximations we made. In addition, a significant performance improvement can be achieved by the QED routing, compared with the NN routing. However, there is still a non-negligible performance loss compared with the equidistant relays for the selected relay intensities.

Example 5: End-to-end throughput under QED routing with intra-route re-

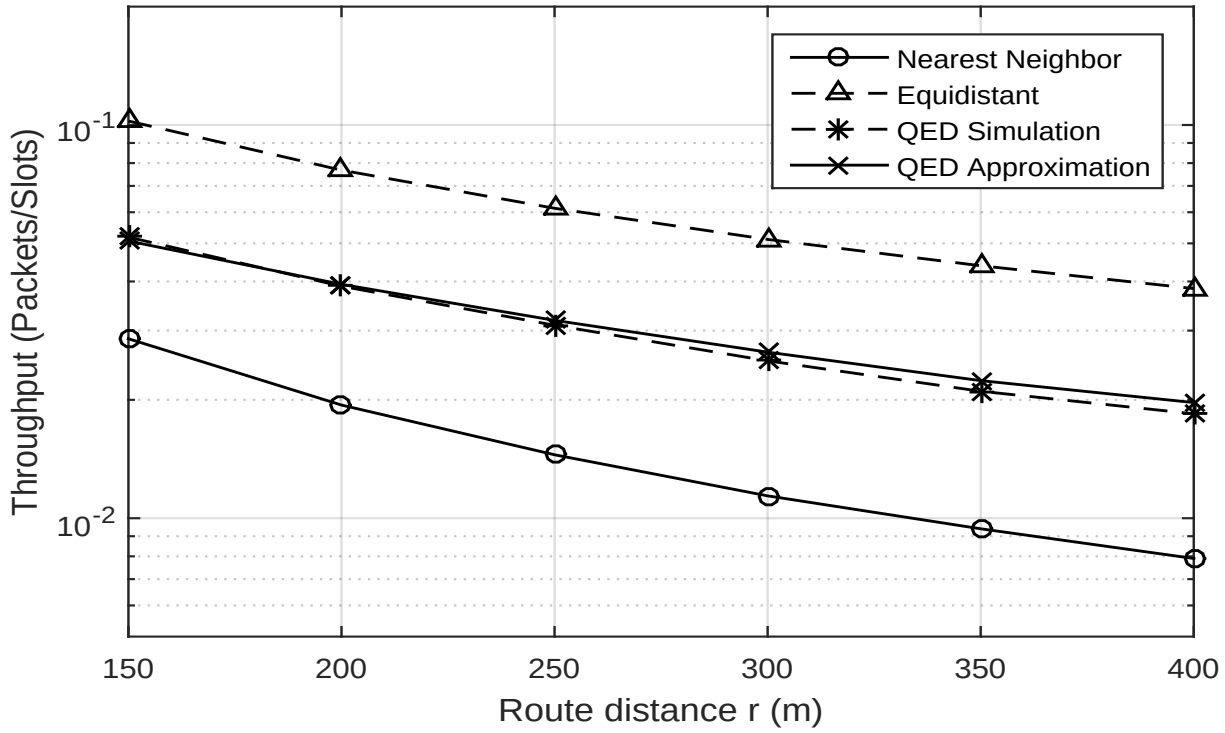


Figure 4.5: Throughput comparison: QED versus NN

source reuse In this example, we evaluate the end-to-end throughput with the intra-route resource reuse for the QED routing. We set $l_0 = 15$ m and $\lambda = 0.2$ /m. As is discussed in the previous section, we consider both the case of constant node intensity and that of constant source-destination pair intensity. We use $\bar{\mu} = 5 \times 10^{-4}$ for the constant node intensity and $\bar{\mu} = 3 \times 10^{-6}$ for the constant source-destination pair intensity. The results are compared with the end-to-end throughput of the QED routing without the intra-route resource reuse, where we set the intensity of the interferers the same as the case of $M = \mathbb{E}\{N' + 1 \mid R = r\}$. The numerical results of the two cases are shown in Fig. 4.6 and Fig. 4.7 respectively. First, it can be observed that there is a gap between the end-to-end throughput derived in *Theorem 4.7* and the simulation results for small M's. This is because we approximate the intra-route interference by a very conservative upper bound of it. However, as M becomes larger and the intra-route interference becomes less significant, the approximation values become very

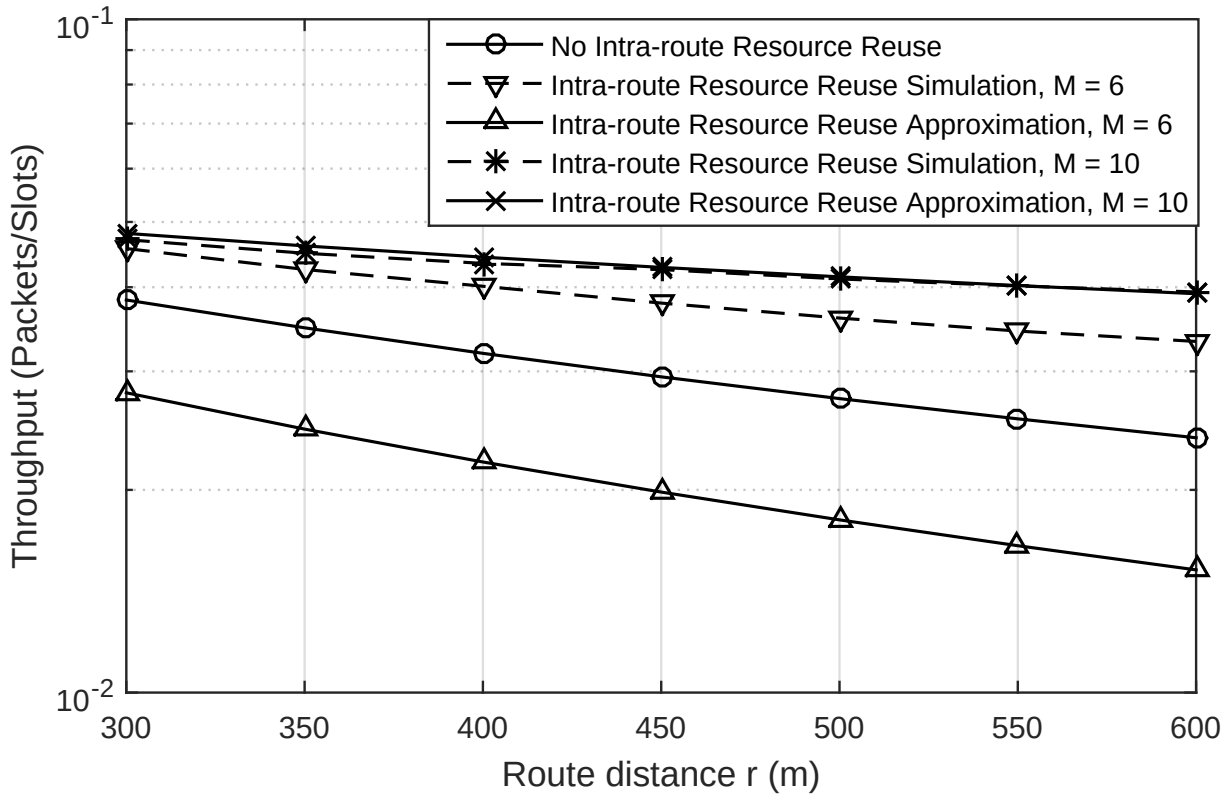


Figure 4.6: The average end-to-end throughput under QED routing with the intra-route resource reuse for constant node intensity

close to the simulation results. Second, the numerical results verify our theoretical analysis on the effect of intra-route resource reuse. That is, generally, intra-route resource reuse can lead to an increase in the throughput; however, if the source-destination pair density is approximately time-invariant or does not change significantly, then it is not beneficial to apply intra-route resource reuse for long distance routing.

4.8 Conclusions & Discussions

In this chapter, we investigated the effect of relay randomness on the end-to-end throughput in multi-hop wireless networks using stochastic geometry. We modeled the relays as a linear Poisson Point Process between the source and destination, and the external interferers as an

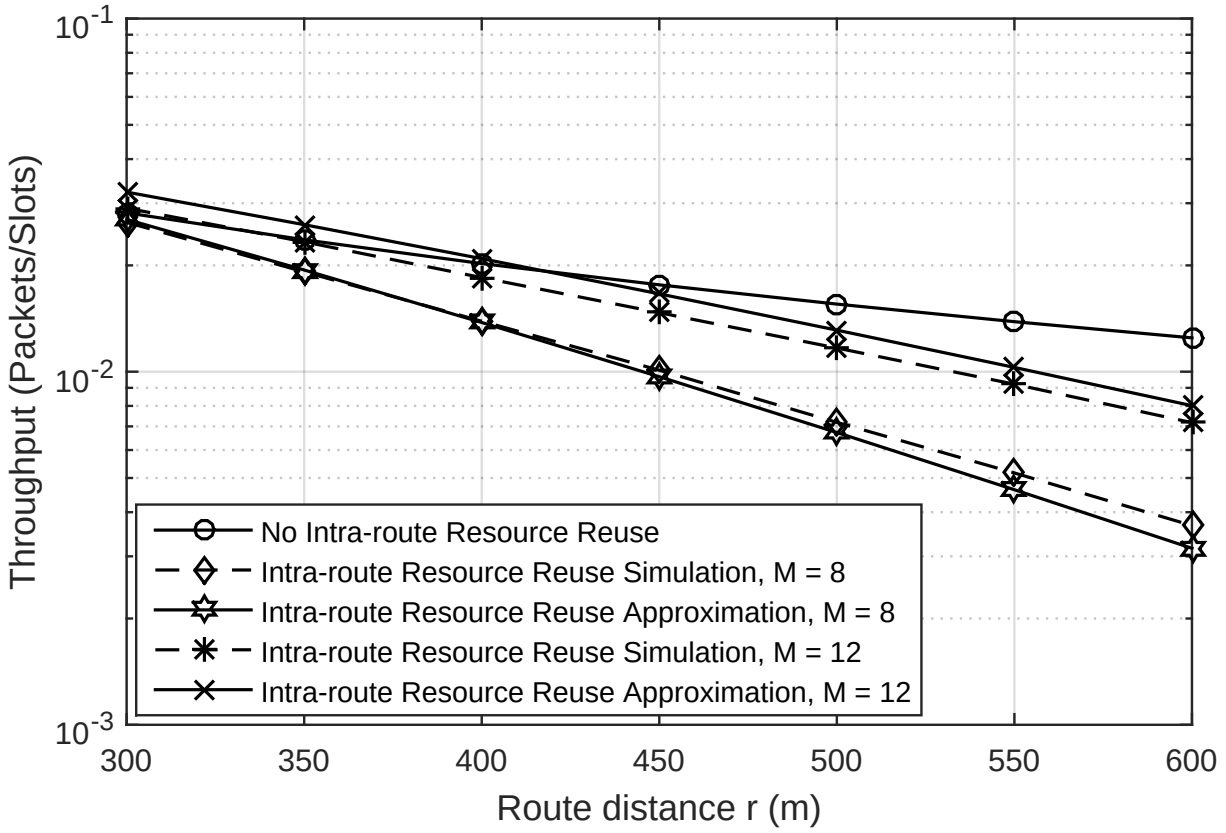


Figure 4.7: The average end-to-end throughput under QED routing with the intra-route resource reuse for constant source-destination pair intensity

independent Poisson Point Process. We first evaluated the end-to-end throughputs under nearest neighbor routing and TDMA MAC with fixed and flexible slot length, respectively. Then we proposed a quasi-equal-distance (QED) routing protocol, and analyzed its end-to-end throughputs with and without intra-route resource reuse. The optimal number of time slots was also analyzed for intra-route resource reuse. The analysis was further demonstrated through numerical examples. Both the theoretic and numerical results indicated that: (i) The throughput performance of the proposed QED routing can achieve a significant performance gain over that of the NN routing. For network with sparse random relays, compared with the ideal equidistant routing, the performance loss of QED routing due to relay randomness is not negligible. However, as the relay intensity gets higher, the performance of QED routing converges to that of the equidistant relays; (ii) The effect of intra-route resource reuse depends on the network setup. If the node intensity is a constant over the network, then as expected, intra-route resource reuse is always beneficial when the routing distance r is sufficiently large. (iii) With randomly distributed relays, the communication distance can generally be extended. However, due to the uncertainty in relay distribution, long distance communication is generally not feasible with random relays. This implies that the existence of a reasonably defined infrastructure needs to be ensured for effective long distance communication. The results in this chapter also echoed our previous observation in [108–110] that future network design would reflect the convergence of centralized and ad hoc networks.

Chapter 5

Malicious Link Detection in Multi-Hop Wireless Sensor Networks

This chapter considers malicious link detection in multi-hop wireless sensor networks (WSNs). Existing work on malicious link detection generally requires that the detection process being performed at the intermediate nodes, leading to considerable overhead in system design, as well as unstable detection accuracy due to limited resources and the uncertainty in the loyalty of the intermediate nodes themselves. In this chapter, we propose an efficient and robust malicious link detection scheme by exploiting the statistics of packet delivery rates only at the base station. More specifically, first, we present a secure packet transmission protocol to ensure that except the base station, any intermediate nodes on the route cannot access the contents and routing paths of the packets. Second, we design a malicious link detection algorithm that can effectively detect the irregular dropout at every hop (or link) along the routing path. We prove that the proposed algorithm has guaranteed false alarm rate and low miss detection rate. Simulation results are provided to validate the proposed approaches.

5.1 Introduction

Wireless sensor networks (WSNs) are often multi-hop networks where individual sensor nodes need to function as relays to forward the data flow originated from their peers to the sink. Such a distributed network organization makes WSNs especially vulnerable to various attacks, such as wireless jamming, spoofing attacks and internal attacks [116], in a sense that one malicious link or node in the network can compromise the data flow passing through it from multiple nodes. In this chapter, we consider the detection of malicious links in WSNs.

The detection of malicious behaviors in WSNs, or more generally, the multi-hop wireless networks, has been broadly discussed in literature. In [38, 117], audit based schemes were proposed for malicious node identification. In [39], the security of disruption tolerant networks (DTN) was studied. In [40], an heuristic method was proposed to identify the failed nodes by re-organizing the network topology. In [41], a 2ACK scheme was proposed to detect the nodes that intentionally drop packets. In [118], the blackhole and grayhole attacks were investigated. In [42], the malicious node detection was explained under the context of network coding. Making use of the open medium in wireless communications, an overhearing scheme was proposed to monitor the behaviors of the neighboring nodes in [43].

A major limitation with most existing methods on malicious behavior detection is that the nodes are required to implement additional verification process in packet delivery, or report additional information to the authority in the network, leading to considerable overhead on system complexity, energy consumption and network throughput. In this chapter, as an effort to improve the efficiency and minimize the system complexity, we propose a malicious link detection algorithm by exploiting the statistics of packet delivery rates at the base stations. More specifically, first, we present a secure packet transmission protocol to ensure

that except the base stations, any intermediate nodes on the route cannot access the contents and routing paths of the packets. Second, we design a malicious link detection algorithm that can effectively detect the irregular dropout at *every hop (or link)* along the routing path with guaranteed false alarm rate and miss detection rate. Comparing to [59] which can detect whether a routing path is problematic, our detection method can be localized to every link. It should be pointed out that, illegal packet modification and injection of invalid packets, which essentially result in the dropout of legal packets, can be detected successfully as well. Simulation results are provided to validate the proposed approaches.

It should be noted that the proposed scheme is focused on the security of the network layer or below, that is, ensuring the secure delivery of packets from source to destination. Malicious behaviors may also exist in the application layer, such as in the case where the sensors may send packets with false contents to the sink. The detection of such malicious behaviors mainly relies on the data analysis in the application layer, and may vary from application to application [119]; hence it is out of the scope of the proposed scheme.

5.2 Network Model

In this chapter, we consider a single unit of a multi-hop WSN. The unit is governed by an authority, the sink or the base station (BS), which is responsible for collecting data from the nodes in the unit, and issuing control messages. Each node can be either a regular sensor or the aggregator of several sensors. In this chapter, we model the WSN unit using the N-hop framework [120], as shown in Fig. 5.1, where the nodes are sorted basing on the hop distance from each node to the BS. The nodes on layer i are the set of nodes i hops away from the BS; each node at layer $i+1$ forwards the packets it generates and receives from higher layers

to one or several nodes at layer i until the BS (layer 0). The proposed scheme can be readily scalable to WSNs with multiple BSs.

In a WSN, the major data flow is from the sensors to the base station, i.e., the uplink. Therefore, in this chapter, we focus on the uplink data flow of the WSN. Since we consider an environment where the reliability of the links cannot be guaranteed, we employ multi-path routing [121] in the network, to enhance the diversity and robustness of routing. For each packet to be delivered to the BS, a node randomly selects one of the candidate nodes in the lower layer as the next hop with certain probability according to the routing table; the routing table is determined by the BS and assigned to each node through the control message. The topology and the routing table of the network can be determined either statically or dynamically. In the static case, the topology and routing paths are essentially fixed during network operation. In the dynamic case, the routing table can be determined by utilizing the ad-hoc on-demand distance vector (AODV) routing [122] protocol, where the BS sorts the route request (RREQ) messages and selects the next hops accordingly for each node in the unit. Since the major focus of this chapter is on the malicious link detection process, in the following, we assume that the routing table has been established and fixed during detection.

The malicious behaviors considered in this chapter include (i) irregular dropout of packets, (ii) illegal modification of packets, and (iii) injection of invalid packets. The reasons for the malicious behaviors may be the degradation of wireless channels, attacks from external jammers or corrupted internal nodes, etc. Note that the above malicious behaviors committed by an internal node can be equivalently converted to those happen on its incidental links; therefore, without loss of generality we focus on malicious link detection. A node can be considered as malicious if a certain amount of its incidental links are identified as malicious.

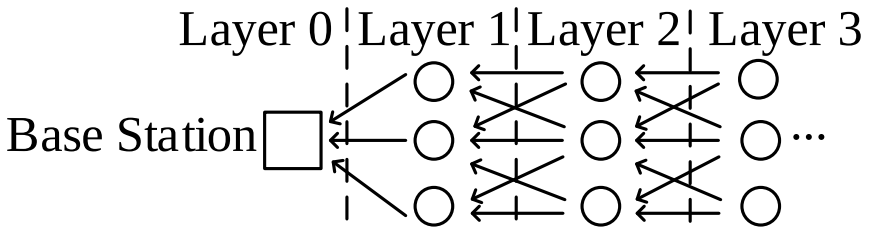


Figure 5.1: Hierarchical structure of a WSN.

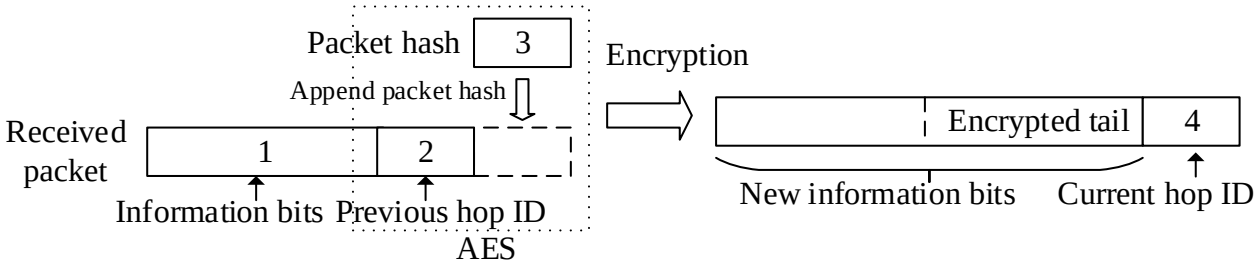


Figure 5.2: The packet encoding process at intermediate node.

We will further show in Section 5.3 that the detection of packet modification and packet injection can both be converted to that of packet dropout.

Notations We let N_i denote the number of node of layer i. Following the notation in graph theory, the nodes of layer i are denoted by $v_{i,0}, v_{i,1}, ..., v_{i,N_i-1}$, and $v_{0,0}$ denotes the BS; e_{i,j_1,j_2} denotes the link/edge $v_{i,j_1} \rightarrow v_{i-1,j_2}$. $G_{i,j}$ denotes the self generated packet rate of node $v_{i,j}$, $p_d(i, j_1, j_2)$ the dropout rate of link e_{i,j_1,j_2}, $p_t(i, j_1, j_2)$ the probability that v_{i,j_1} selects v_{i-1,j_2} as its next hop in the multi-path routing. $\mathbb{F}_q^n$ denotes the Galois Field (q^n). We use bold capital letters, e.g., $\boldsymbol{X}$, to denote random vectors, and bold lower case letters, e.g., $\boldsymbol{x}$, to denote their values.

5.3 Packet Transmission Protocol

In this section, we design the packet transmission protocol for the WSN. In order to combat packet content attacks, we encrypt the transmitted packets so that except the BS, any intermediate nodes on the route cannot access the contents and the paths of the packets. However, it should be noted that the proposed protocol is not necessary in malicious link detection if the malicious party does not launch attacks basing on the packet contents.

5.3.1 Protocol Description

5.3.1.1 Packet Encoding

Each node in the WSN shares a distinct secret key with the BS for packet encryption. Each packet received at a node contains two parts: the information bits and the ID of the previous hop. Let the length of the node ID be L_n bits. In addition to the content generated from the source, the information bits also contain the history of the previous hops the packet passed through, however, that information is encrypted by each previous hop so it is not accessible by the current node. The encoding process in packet forwarding includes the following steps:

- Generate a packet hash and append it to the packet. The hash is calculated using the entire packet based on a secure hash algorithm [123]. The secure hash is inserted to provide integrity check of the packet. For efficiency, the generated hash sequence may be truncated before attached to the packet. Let the length of the hash sequence be L_h bits.

- Encrypt the tail part of the packet, including the previous hop ID and packet hash. In general, the verification of a packet is implemented by certain asymmetric encryption

algorithms [123]. However, since only the BS, rather than the intermediate nodes, is required to check the integrity of the received packet; hence a symmetric block cipher, i.e., AES algorithm, is sufficient in the proposed scheme. In practice, if the length of the tail, $L_t = L_n + L_h$, is less than, or not a multiple of the block size of AES cipher, we can include the tail of the information bits in the plain text.

- Append the node ID to the packet and transmit it to the next hop.

The encoding process is demonstrated in Fig. 5.2. The proposed packet relaying protocol ensures that each packet is not traceable in delivery. Therefore, the malicious party is unable to launch attacks to packets based on the routing history.

5.3.1.2 Packet Decoding at the BS

At the reception of a packet, the BS applies the inverse of the encoding process successively. Suppose the BS has recovered the packet received at node v_{i-1,j_2}, and found that the previous hop is v_{i,j_1} basing on the tail of the packet. Then by decrypting the tail part of the information bits, the BS obtains the packet hash, as well as the packet received by node v_{i,j_1}. Since the BS stores the secret keys of all the nodes in the network, it is able to recover the packet version received by each intermediate node on the route if no malicious link exists.

5.3.1.3 Protocol Implementation and Efficiency

The proposed protocol is implemented between the existing network layer and transmission layer of the WSN. This implementation has two advantages: first, it facilitates easy integration into any existing systems; second, the packet length in the proposed protocol is not limited by the network layer design. Therefore, the loss of throughput from the appended tails at the intermediate nodes can be leveraged by the increased packet length.

5.3.2 Security Analysis

In this subsection, we first discuss the security of the packet transmission scheme under illegal packet modification, then we show that both the detection of packet modification and injection can be converted to that of the packet dropout.

Suppose e_{i,j_1,j_2} is a malicious link in the network and the secret key of v_{i,j_1} is unknown to the malicious party. For an arbitrary packet passing through e_{i,j_1,j_2}, let $\boldsymbol{X}_{i,j_1,j_2} \in \mathbb{F}_2^L$ denote the vector of its information bits and $\boldsymbol{E}_{i,j_1,j_2} \in \mathbb{F}_2^L$ the error pattern applied on it, where L is the length of the information bits. To modify the packet without being detected, the malicious link seeks an error pattern $\boldsymbol{E}_{i,j_1,j_2} \neq \boldsymbol{0}$ such that $\boldsymbol{Y}_{i,j_1,j_2} = \boldsymbol{X}_{i,j_1,j_2} + \boldsymbol{E}_{i,j_1,j_2}$ is a valid output of v_{i,j_1}. We have the following proposition on the security.

Proposition 5.1 *Assuming an ideal cipher (random oracle), the probability that the malicious link generates an unseen $\boldsymbol{Y}_{i,j_1,j_2}$ that is valid is negligible if it is infeasible for the malicious party to succeed in the preimage attack to the hash function.*

Proof: Let $f(\cdot)$ denote the encryption function, which is an bijective mapping defined on $\mathbb{F}_2^{L_t} \mapsto \mathbb{F}_2^{L_t}$. For the random oracle, if the secret key is unknown, for any integer $1 \leq m \leq 2^{L_t}$ and $\boldsymbol{x} \in \mathbb{F}_2^{L_t}$, we have

$$\begin{aligned} &\Pr\{f(\boldsymbol{x}) = \boldsymbol{y} \mid f(\boldsymbol{x}_k) = \boldsymbol{y}_k, 1 \leq k \leq m\} \\ &= \begin{cases} \frac{1}{2^{L_t} - m}, \ \boldsymbol{y} \in \mathbb{F}_2^{L_t}, \ \boldsymbol{y} \notin \{\boldsymbol{y}_k \mid 1 \leq k \leq m\}, \\ \quad 0, \text{ otherwise.} \end{cases} \end{aligned} \tag{5.1}$$

where for $1 \leq k \leq m$, $\boldsymbol{x}_k \in \mathbb{F}_2^{L_t}$ and $\boldsymbol{x} \neq \boldsymbol{x}_k$. That is, the cipher text of an unseen plain text is uniformly distributed over all the unseen cipher texts, and vice versa. For the encrypted tail with error $\boldsymbol{Y}_{i,j_1,j_2}(L - L_t :)$, we consider two cases:

First, if $\boldsymbol{Y}_{i,j_1,j_2}(L-L_t:)$ has been seen, i.e., the malicious link uses the encrypted tail of another packet to replace the current packet; let $f(\boldsymbol{X'}) = \boldsymbol{Y}_{i,j_1,j_2}(L-L_t:)$, then the target of the malicious party is to find a vector $\boldsymbol{Y}_{i,j_1,j_2}(:L-L_t)$, combined with $\boldsymbol{X'}(:L_t-L_h)$, such that its hash value is $\boldsymbol{X'}(L_t-L_h:)$. This is the preimage attack to the hash function.

Second, if $\boldsymbol{Y}_{i,j_1,j_2}(L-L_t:)$ has not been seen before, then for the malicious party, the plain text of $\boldsymbol{Y}_{i,j_1,j_2}(L-L_t:)$ is uniformly distributed over all the unseen plain texts. For any given prefix vector $\boldsymbol{Y}_{i,j_1,j_2}(:L-L_t)$, there are $2^{L_t-L_h}$ possible tails since the hash value is determined by the content; so given m observed plain and cipher texts for $f(\cdot)$, the probability that $\boldsymbol{Y}_{i,j_1,j_2}$ is valid is $\frac{2^{L_t-L_h}}{2^{L_t-m}} \approx \frac{1}{2^{L_h}}$, which is negligible for a large L_h. □

A secure hash function which is believed to be resistant against preimage attacks generally requires L_h to be more than 256 bits [124]. However, considering the efficiency, such hash value might be too long since each hop attaches a hash to the packet in relaying. So we employ two different policies depending on the power of malicious party:

Case I If the malicious party is unable to attack the hash function at each hop, then we believe $\boldsymbol{E}_{i,j_1,j_2} = \boldsymbol{0}$ if $\boldsymbol{Y}_{i,j_1,j_2}$ passes the verification. In this case, for each packet, we are able to locate the last misbehaved link on the route if any.

Case II If the malicious party is able to attack the hash function at each hop, then $\boldsymbol{E}_{i,j_1,j_2}$ might be non-zero even if $\boldsymbol{Y}_{i,j_1,j_2}$ passes the verification. However, while the BS is unable to locate the misbehaved link, it is still able to detect an error by checking the integrity of the packet content. In this case, the BS drops the packet.

For generality, in the following analysis, we focus on case II, where the hash can be quite short to achieve higher efficiency. However, case I provides a quick identification of malicious

links for illegal packet modification, when the malicious party is less powerful.

Next, we show that the detection of packet modification and injection can be converted to that of legitimate packet dropout.

Packet Modification As is noted in case II, the modified packets can be detected by checking the packet contents at the BS. This requires the encryption and verification on the higher layers, e.g., the application layer, which has less effect on the efficiency as they are applied only by the source node. The modified packets will be dropped by the BS, which is equivalent to the packet dropout on the malicious link.

Packet Injection To prevent the injection of invalid packets in the WSN, e.g., the denial of service (DoS) attacks, we apply flow control at each node for each incoming link. Because of the flow control, the invalid packets will occupy the resources of the legitimate packets on the same link, and again, the legitimate packets will be dropped on the malicious link.

5.4 The Proposed Malicious Link Detection Algorithm

In this section, we present the proposed malicious link detection algorithm. As shown in Section 5.3, the malicious behaviors considered in this chapter can be converted to the irregular packet dropout on the malicious links. The proposed algorithm hence detects links with higher dropout rates than a predefined baseline, denoted by p_0. Our algorithm relies solely on the statistics of packet delivery at the BS to identify the malicious links, and does not require any additional information collected from the nodes. Therefore, the system complexity and overhead can be kept minimum.

We will analyze the packet delivery ratio of each node in the WSN during an observation

window. We assume the duration of the observation window is T. $K_{i,j}$ denotes number of received packets at BS generated by $v_{i,j}$ during the observation window, while K_{i,j_1,j_2} denotes number of received packets generated by v_{i,j_1} and passing through e_{i,j_1,j_2} during the observation window.

In the following, we first consider the simplistic case of a 1-hop network, then we discuss the 2-hop network, and further generalize the algorithm to the N-hop network. Finally, we analyze the misdetection rate of the proposed algorithm.

5.4.1 1-Hop Network

The nodes in 1-hop network connect to the BS directly. Verifying the dropout rate of link $e_{1,j,0}$ can be formulated as a one-tailed hypothesis testing on a Bernoulli random variable (RV) as

$$\text{Null hypothesis } H_0 : p_d(1,j,0) \leq p_0.$$

$$\text{Alternative hypothesis } H_1 : p_d(1,j,0) > p_0.$$

During the observation window of the algorithm, the number of packets generated from $v_{1,j}$ can be approximated by $\lfloor TG_{1,j} \rfloor$. $K_{1,j}$ should follow a binomial distribution $B(\lfloor TG_{1,j} \rfloor, 1 - p_d(1,j,0))$. Conventionally, by allowing a probability of α to reject a true hypothesis (type I error or false alarm), define threshold $\theta(\alpha, n, p)$ as

$$\theta(\alpha, n, p) \triangleq \max \left\{ \theta \mid \sum_{k=0}^{\theta} \binom{n}{k} (1-p)^k p^{n-k} \leq \alpha \right\}. \tag{5.2}$$

Then we reject hypothesis H_0 if $K_{1,j} < \theta(\alpha, \lfloor TG_{1,j} \rfloor, p_0)$ in the observation window, i.e., link $e_{1,j,0}$ is identified as malicious.

5.4.2 2-Hop Network

In a 2-hop network, all the links incidental to the BS can be tested as in the 1-hop network. Here we focus on the links between layer 2 and layer 1, e.g., e_{2,j_1,j_2}. We test the following hypothesis:

$$\text{Null hypothesis } H_0 : p_d(2, j_1, j_2) \leq p_0. \tag{5.3}$$

$$\text{Alternative hypothesis } H_1 : p_d(2, j_1, j_2) > p_0. \tag{5.4}$$

With multi-path routing, the data rate on e_{2,j_1,j_2} is $p_t(2, j_1, j_2)G_{2,j_1}$. Since the contents and path information of each packet are encrypted, all the packets generated by v_{2,j_1} and received by v_{1,j_2} should be treated equivalently as the packets generated by v_{1,j_2} after leaving v_{1,j_2}[1]. Let $p_d(1, j_2)$ denote the dropout rate of the combined path from v_{1,j_2} to BS. Hence, K_{2,j_1,j_2} follows a binomial distribution $B(\lfloor Tp_t(2, j_1, j_2)G_{2,j_1} \rfloor, (1-p_d(2, j_1, j_2))(1-p_d(1, j_2)))$, while K_{1,j_2} follows a binomial distribution $B(\lfloor TG_{1,j_2} \rfloor, (1-p_d(1, j_2)))$. However, we are unable to apply the algorithm in the 1-hop network directly to testing link e_{2,j_1,j_2} as $p_d(1, j_2)$ is unknown. Even if we can obtain an estimate of $p_d(1, j_2)$ from the value of K_{1,j_2}, the estimation error would render the false alarm rate unbounded, as will be shown in Section 5.5.

We solve the problem by exploiting the joint distribution of K_{2,j_1,j_2} and K_{1,j_2}, where we derive a bounded false alarm in testing e_{2,j_1,j_2}. The result is generalized in the following proposition.

[1]It is possible that v_{1,j_2} treats the packets it relays and those it generates differently, however, since the malicious node behavior can be considered as that of its incidental links, i.e., e_{2,j_1,j_2}, this will not void the results of the detection algorithm.

Proposition 5.2 *Consider i.i.d RVs* $X_i \sim Bernoulli(p), i = 1, ..., n_1$ *and* $Y_i \sim Bernoulli(pq), i = 1, ..., n_2$, $p \in (0,1), q \in (0,1)$. *Let* $X = \sum_i X_i$ *and* $Y = \sum_i Y_i$ *follow binomial distribution* $B(n_1, p)$ *and* $B(n_2, pq)$, *respectively, and* $\Phi(x; n, \rho)$ *denote the distribution function of binomial distribution* $B(n, \rho)$, *i.e.*

$$\Pr\{X = x\} = \Phi(x; n_1, p), \quad \Pr\{Y = y\} = \Phi(y; n_2, pq). \tag{5.5}$$

For any $\alpha \in (0,1)$, $n \in \mathbb{Z}^+$ *and* $x \in (0, \infty)$, *define* $\rho(\alpha, n, x)$ *as*

$$\rho(\alpha, n, x) \stackrel{\triangle}{=} \max\{\rho \mid \sum_{k=\lceil x \rceil}^{n} \Phi(k; n, \rho) \leq \alpha, \rho \in [0,1]\}, \tag{5.6}$$

and define $\theta(\alpha, m, n, q, x) \in \mathbb{Z}^+$ *as*

$$\theta(\alpha, m, n, q, x) \stackrel{\triangle}{=} \max\{\theta \mid \sum_{k=0}^{\theta} \Phi(k; n, \rho(\alpha, m, x)q) \leq \alpha\}, \tag{5.7}$$

then for $\alpha \in (0,1)$ *we have*

$$P_{false} = \Pr\{Y \leq \theta(\alpha, n_1, n_2, q, X)\} \leq 2\alpha. \tag{5.8}$$

Proof: For $\rho \in [0,1]$, $n \in \mathbb{Z}^+, \alpha \in (0,1)$, we define function

$$x(n, \rho, \alpha) = \min\{x \mid \sum_{k=x}^{n} \Phi(k; n, \rho) \leq \alpha, x \in \mathbb{Z}^+\}, \tag{5.9}$$

e.g. $\Pr\{X \geq x(n_1, p, \alpha)\} \leq \alpha$ and $\Pr\{X \geq x(n_1, p, \alpha) - 1\} > \alpha$. Note that for any fixed $x \in (0, \infty)$ and $n \in \mathbb{Z}^+$, function $\sum_{k=\lceil x \rceil}^{n} \Phi(k; n, \rho)$ is non-decreasing w.r.t. $\rho \in [0,1]$. Then we have

$$\rho(\alpha, n, x(n, \rho_0, \alpha) - 1) < \rho_0, \ \rho_0 \in (0,1). \tag{5.10}$$

which can be obtained from the fact that

$$\sum_{k=x(n,\rho_0,\alpha)-1}^{n} \Phi(k; n, \rho_0) > \alpha. \tag{5.11}$$

From the monotonicity of $\sum_{k=\lceil x \rceil}^{n} \Phi(k; n, \rho)$, we have

$$\sum_{k=0}^{\theta(\alpha,m,n,q,x(m,\rho_0,\alpha)-1)} \Phi(k; n, \rho_0 q) \leq \alpha. \tag{5.12}$$

Also note that for any fixed $\alpha \in (0,1)$ and $n \in \mathbb{Z}^+$, $\rho(\alpha, n, x)$ is non-decreasing w.r.t. $x \in (0, \infty)$. Again, using the monotonicity of $\sum_{k=\lceil x \rceil}^{n} \Phi(k; n, \rho)$, $\theta(\alpha, m, n, q, x)$ is non-decreasing w.r.t. $x \in (0, \infty)$ with other parameters being fixed. According to (5.9) and (5.12) and the fact that X and Y are independent, we have

$$\begin{aligned} P_{false} =& \sum_{x=0}^{n_1} \Pr\{X = x\} \Pr\{Y \leq \theta(\alpha, n_1, n_2, q, x)\} \\ \leq& \alpha + \Pr\{Y \leq \theta(\alpha, n_1, n_2, q, x(n_1, p, \alpha) - 1)\}, \end{aligned} \tag{5.13}$$

where $\Pr\{Y \leq \theta(\alpha, n_1, n_2, q, x(n_1, p, \alpha) - 1)\}$ equals

$$\sum_{k=0}^{\theta(\alpha,n_1,n_2,q,x(n_1,p,\alpha)-1)} \Phi(k; n_2, pq) \leq \alpha. \tag{5.14}$$

which completes the proof. □

The underlying argument of Proposition 5.2 is that, even through parameter p is unknown, we can still obtain a region of X and Y with bounded probability. According to Proposition 5.2, by setting the threshold of K_{2,j_1,j_2} as $\theta(\alpha, \lfloor TG_{1,j_2} \rfloor, \lfloor Tp_t(2, j_1, j_2)G_{2,j_1} \rfloor, 1 - p_0, K_{1,j_2})$, the false alarm rate in testing is upper bounded by 2α. In this way, all the links can be tested.

5.4.3 N-Hop Network

We further generalize the algorithm to the N-hop network. Consider link $e_{i,j_1,j_2}, i > 1$ in the network. The input data rate originated from v_{i,j_1} on e_{i,j_1,j_2} is $p_t(i, j_1, j_2)G_{i,j_1}$; after

being received by v_{i-1,j_2}, these packets should have the same routing distribution as those originated from v_{i-1,j_2} if v_{i-1,j_2} behaves normally. Let $p_d(i-1,j_2)$ denote the dropout rate from v_{i-1,j_2} to BS. Then both K_{i,j_1,j_2} and K_{i-1,j_2} follow binomial distributions. According to Proposition 5.2, if $K_{i,j_1,j_2} \leq \theta(\alpha, \lfloor TG_{i-1,j_2} \rfloor, \lfloor Tp_t(i,j_1,j_2)G_{i,j_1} \rfloor, 1-p_0, K_{i-1,j_2})$, we identify e_{i,j_1,j_2} as malicious, whose false alarm rate is bounded by 2α.

It is possible that v_{i-1,j_2} may treat the packets it relays differently from those it generates, e.g., dropping the incoming packets or forwarding them disobeying the routing table. These malicious behaviors can be decomposed as either the dropout on the incoming links or the injection to the outgoing links, which can both be detected by the proposed algorithm as noted in Section 5.3. Therefore, the misbehavior of v_{i-1,j_2} will not void the generality of the proposed algorithm.

5.4.4 Misdetection Rate Analysis

In this subsection, we show that in the proposed algorithm, if the dropout rate from the end node to the BS is less than 1, the misdetection rate on a link converges to 0 as $T \to \infty$.

Misdetection happens on link e_{i,j_1,j_2} if its dropout rate $p_d(i,j_1,j_2)$ is greater than the base line p_0 while K_{i,j_1,j_2} and K_{i-1,j_2} satisfy $K_{i,j_1,j_2} > \theta(\alpha, \lfloor TG_{i-1,j_2} \rfloor, \lfloor Tp_t(i,j_1,j_2)G_{i,j_1} \rfloor, 1-p_0, K_{i-1,j_2})$. The analysis on the probability is summarized in the following proposition.

Proposition 5.3 *Consider i.i.d RVs $X_i \sim Bernoulli(p), i = 1,...,n_1$ and $Y_i \sim Bernoulli(pq), i = 1,...,n_2$, $p \in (0,1], q \in (0,1)$. Let $X = \sum_i X_i$ and $Y = \sum_i Y_i$ follow binomial distribution $B(n_1,p)$ and $B(n_2,pq)$, respectively, and suppose $n_2/n_1 = \kappa$ being fixed. For some $\hat{q} > q$, the probability that $Y > \theta(\alpha, n_1, n_2, \hat{q}, X)$ converges to 0 as $n_2 \to +\infty$.*

More specifically, as $n_2 \to +\infty$, the miss detection rate $P_{miss} = \Pr\{Y > \theta(\alpha, n_1, n_2, \hat{q}, X)\}$ satisfies

$$P_{miss} \leq \left[\frac{e^{(1-\delta)\hat{q}/q - 1}}{[(1-\delta)\hat{q}/q]^{(1-\delta)\hat{q}/q}} + o(1) \right]^{n_2 pq} + e^{-\frac{\delta}{2} n_1 p}, \tag{5.15}$$

for any $\delta \in (0,1)$ and $(1-\delta)\hat{q}/q > 1$.

Proof: Note that X and Y are independent, so are $\theta(\alpha, n_1, n_2, \hat{q}, X)$ and Y. Therefore, the misdetection rate can be expressed as

$$P_{miss} = \sum_{x=0}^{n_1} \Phi(x; n_1, p) \sum_{y=\theta(\alpha, n_1, n_2, \hat{q}, x)+1}^{n_2} \Phi(y; n_2, pq). \tag{5.16}$$

One Chernoff bound of the binomial distribution $B(n, \rho)$ is

$$\sum_{k=\lceil x \rceil}^{n} \Phi(k; n, \rho) \leq \frac{(n\rho)^x e^{x - n\rho}}{x^x}. \tag{5.17}$$

for $x \geq n\rho$. This implies a lower bound of $\rho(\alpha, n, x)$ is

$$\rho(\alpha, n, x) \geq -\frac{x}{n} W_0(-\frac{\alpha^{\frac{1}{x}}}{e}). \tag{5.18}$$

where $W_0(\cdot)$ is the principle branch of the Lambert W function.

Another Chernoff bound of the binomial distribution is

$$\sum_{k=0}^{\theta} \Phi(k; n, \rho) \leq e^{-\frac{(n\rho - \theta)^2}{2n\rho}}, \tag{5.19}$$

for $\theta \leq n\rho$, from which we have a lower bound of (5.2) as

$$\theta(\alpha, n, \rho) \geq n\rho - \sqrt{-2n\rho \log \alpha}. \tag{5.20}$$

Note that $\sum_{k=0}^{\theta} \Phi(k; n, \rho)$ is non-increasing w.r.t. ρ with other parameters being fixed. From (5.18), we obtain a lower bound of $\theta(\alpha, m, n, q, x)$ as

$$-\frac{n}{m} x W_0(-\frac{\alpha^{\frac{1}{x}}}{e}) q - \sqrt{2\frac{n}{m} x W_0(-\frac{\alpha^{\frac{1}{x}}}{e}) q \log \alpha}, \tag{5.21}$$

where we denote (5.21) by $\tilde{\theta}(\alpha, m, n, q, x)$.

Since $\theta(\alpha, m, n, q, x)$ is non-decreasing w.r.t. x, for any $x_0 \in [0, n_1]$, an upper bound of P_{miss} is given by

$$P_{miss} \leq \Pr\{X \leq x_0\} + \Pr\{Y \geq \theta(\alpha, n_1, n_2, \hat{q}, x_0)\}. \tag{5.22}$$

Let $x_0 = (1-\delta)n_1 p$ for some $\delta \in (0,1)$ and $n_2/n_1 = \kappa$ being fixed, then we have

$$\lim_{n_1 \to +\infty} \frac{\tilde{\theta}(\alpha, n_1, n_2, \hat{q}, x_0)}{n_1} = (1-\delta)\kappa p \hat{q}, \tag{5.23}$$

i.e., $\tilde{\theta}(\alpha, n_1, n_2, \hat{q}, x_0) = (1-\delta)n_2 p\hat{q} + o(n_1)$. Since $q < \hat{q}$, by setting δ such that $1-\delta > q/\hat{q}$, we can derive an upper bound of $\Pr\{Y \geq \theta(\alpha, n_1, n_2, \hat{q}, x_0)\}$ from (5.17) and (5.21) as

$$\left[\frac{e^{(1-\delta)\hat{q}/q - 1 + o(n_1)/n_2}}{[(1-\delta)\hat{q}/q + o(n_1)/n_2]^{(1-\delta)\hat{q}/q + o(n_1)/n_2}} \right]^{n_2 pq}. \tag{5.24}$$

As $n_2 \to +\infty$, the (5.24) can be rewritten as

$$\left[\frac{e^{(1-\delta)\hat{q}/q - 1}}{[(1-\delta)\hat{q}/q]^{(1-\delta)\hat{q}/q}} + o(1) \right]^{n_2 pq}, \tag{5.25}$$

where $\frac{e^{(1-\delta)\hat{q}/q-1}}{[(1-\delta)\hat{q}/q]^{(1-\delta)\hat{q}/q}} \in (\frac{e^{\hat{q}/q-1}}{(\hat{q}/q)^{\hat{q}/q}}, 1)$. Furthermore, from (5.19),

$$\Pr\{X \leq x_0\} \leq e^{-\frac{\delta}{2} n_1 p}. \tag{5.26}$$

Then (5.16) follows from (5.22), (5.25) and (5.26), which completes the proof. □

5.5 Simulation

In this section, we validate the the proposed malicious link detection algorithm through numerical examples.

We consider an arbitrary link e_{i,j_1,j_2} during an observation window of duration T. To demonstrate the performance of the proposed algorithm under different network settings, we vary the data rates G_{i,j_1} and G_{i-1,j_2}, the dropout rates $p_d(i,j_1,j_2)$ and $p_d(i-1,j_2)$, in the numerical results.

Baseline Algorithm: Since the difficulty of the malicious link detection lies in that the dropout rate $p_d(i-1,j_2)$ is unknown at the BS, we consider a baseline algorithm which first estimates $p_d(i-1,j_2)$ by

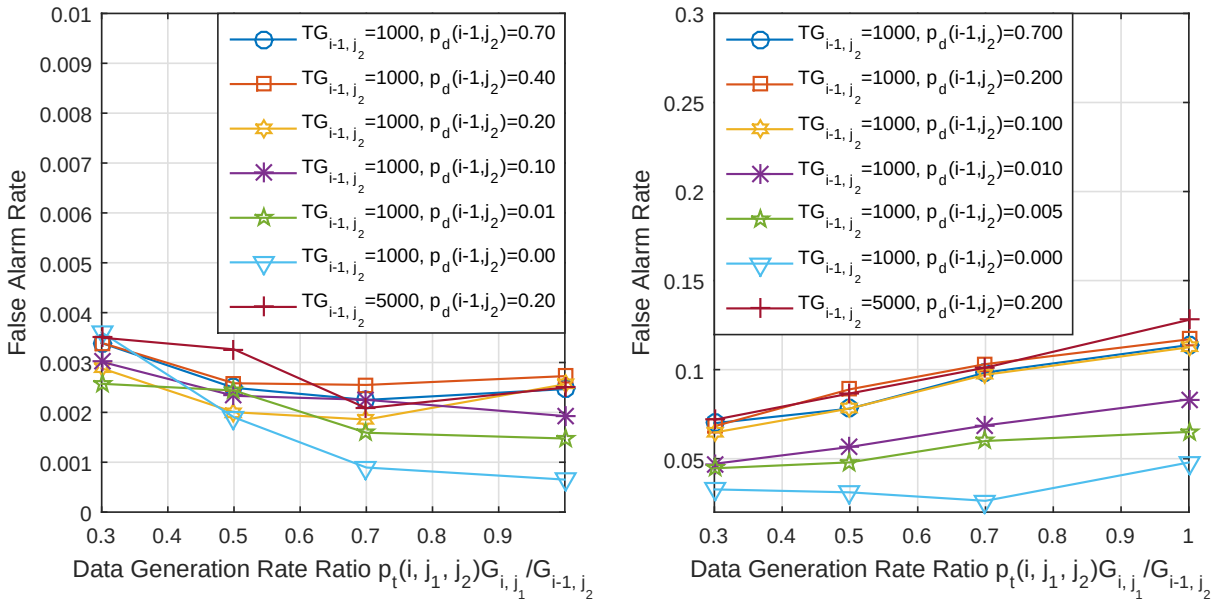
$$\tilde{p}_d = K_{i-1,j_2}/(TG_{i-1,j_2}). \tag{5.27}$$

Then for a baseline dropout rate p_0, it calculates the threshold in the hypothesis test following the traditional method by

$$\theta(\alpha, Tp_t(i,j_1,j_2)G_{i,j_1}, (1-\tilde{p}_d)(1-p_0)), \tag{5.28}$$

for an allowed false alarm rate of α. However, we will see that its actual false alarm rate cannot be bounded by α.

False alarm rate comparison between the proposed algorithm and the baseline algorithm: In this example, we set the allowed false alarm rate $\alpha_0 = 0.05$ and the baseline dropout rate as $p_0 = p_d(i,j_1,j_2) = 0.01$. The results are plotted in Fig. 5.3a and Fig. 5.3b, respectively. For the proposed algorithm, it is shown the actual false alarm rate is much lower than the required bound α_0. On the other hand, because of the error in $p_d(i-1,j_2)$ estimation, the



(a) Proposed algorithm

(b) Baseline algorithm

Figure 5.3: The false alarm rates versus the data generation rate ratio $p_t(i, j_1, j_2)G_{i,j_1}/G_{i-1,j_2}$.

baseline algorithm cannot bound the false alarm rate in detection unless the dropout rate $p_d(i-1, j_2)$ is very close to 0. It is also shown that the actual false alarm rate increases with the increase of ratio $\frac{p_t(i,j_1,j_2)G_{i,j_1}}{G_{i-1,j_2}}$. One interesting fact here is that even though the estimation error of $p_d(i-1, j_2)$ becomes smaller by increasing the observation window duration T, it cannot reduce the false alarm rate as shown in Fig. 5.3b; this is because with the increase of T, the variance of K_{i,j_1,j_2} also becomes smaller, hence requiring a even more accurate estimation of $p_d(i-1, j_2)$, which the baseline algorithm is inept at.

Misdetection rate of the proposed algorithm: In this example, we evaluate the misdetection rate of the proposed algorithm when e_{i,j_1,j_2} is a malicious link. We keep the baseline dropout rate $p_0 = 0.01$ and false alarm rate upper bound $\alpha_0 = 0.05$, and set $p_t(i, j_1, j_2)G_{i,j_1}/G_{i-1,j_2} = 1$ and $p_d(i-1, j_2) = 0.2$. The results are plotted in Fig. 5.4. The numerical results are consistent with the theoretical analysis, i.e., the misdetection

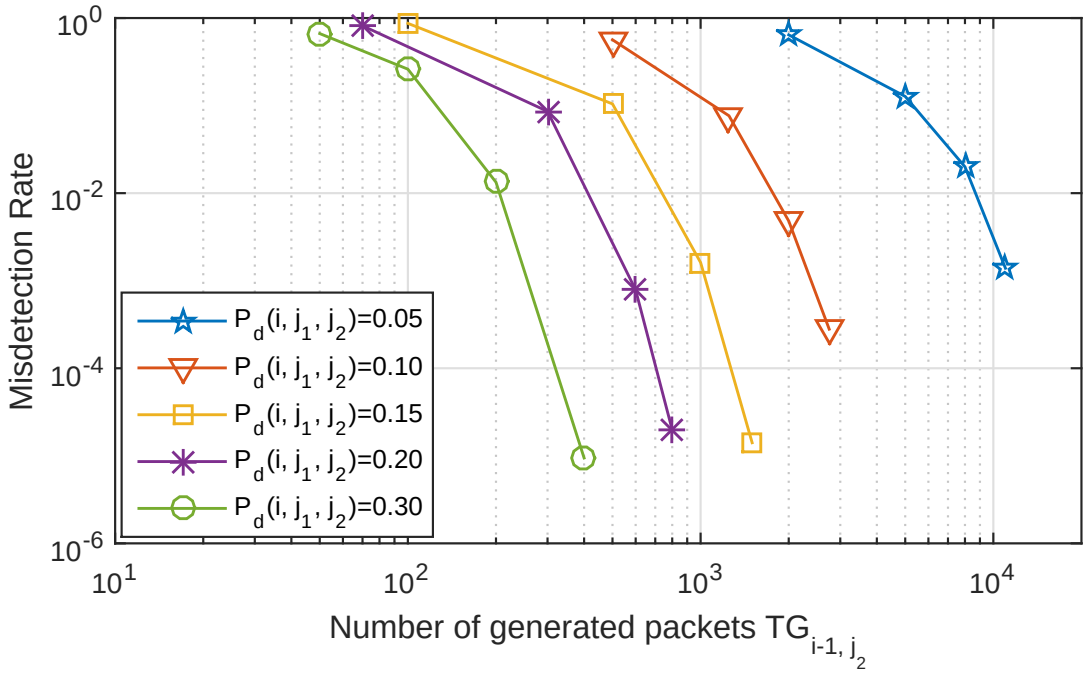


Figure 5.4: The misdetection rate of the proposed algorithm versus the number of generated packets in the observation window TG_{i-1,j_2} for $p_d(i-1,j_2) = 0.2$ and $\frac{p_t(i,j_1,j_2)G_{i,j_1}}{G_{i-1,j_2}} = 1$.

rate becomes arbitrarily small as the observation window duration T increases. However, the number of packets needed for an accurate detection varies significantly with the actual dropout rate $p_d(i, j_1, j_2)$.

5.6 Conclusion

In this chapter, we proposed an efficient and robust malicious link detection scheme for multi-hop WSNs. Comparing with existing approaches that rely on the intermediate nodes to carry out the detection process, in the proposed scheme, malicious link detection was only performed at the base stations by exploiting the statistics of packet delivery rates. As a result, the proposed scheme could effectively detect the irregular dropout at every hop (or link) along the routing paths with significantly higher accuracy, and at the same time,

reducing system overhead and improving the efficiency. The effectiveness of the proposed scheme was demonstrated through both theoretical analysis and simulation results.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

The main contributions of this dissertation lie in the design and evaluation of robust 5G systems under both benign and malicious environments, with considerations on both the physical layer and higher layers. For the physical layer, to improve the robustness of OFDM systems against disguised jamming, we proposed a securely precoded OFDM (SP-OFDM) system by introducing a dynamic and encrypted constellation into the system. Basing on the channel model of SP-OFDM, we further studied the worst jamming distribution against it. For the higher layers, we first studied the modeling of 5G high-density heterogeneous networks using stochastic geometry; we designed effective routing protocols and evaluated the performance of multi-hop 5G networks under various protocols. Then, for the multi-hop wireless sensor networks (WSNs), we proposed an efficient and robust malicious link detection scheme by exploiting the statistics of packet delivery rates at the base station. More specifically, the main conclusions are summarized in the following:

On the physical layer OFDM transceiver design:

- We designed a highly secure and efficient OFDM system under disguised jamming, named securely precoded OFDM (SP-OFDM), by exploiting secure symbol-level precoding basing on phase randomization. The basic idea is to randomize the phase

of transmitted symbols using the secure PN sequences generated from the Advanced Encryption Standard (AES) algorithm. The security is guaranteed by the secret key shared only between the legitimate transmitter and receiver. While SP-OFDM achieves strong jamming resistance, it does not introduce significant redundancy into the system and can achieve almost the same spectral efficiency as the traditional OFDM system.

- We identified the vulnerability of the synchronization algorithm in the original OFDM system under disguised jamming, and proposed a secure synchronization scheme for SP-OFDM which is robust against disguised jamming. In the proposed synchronization scheme, we designed an encrypted cyclic prefix (CP) for SP-OFDM, and the synchronization algorithm utilized the encrypted CP as well as the precoded pilot symbols to estimate time and frequency offsets in the presence of jamming.

- We analyzed the channel capacity of the traditional OFDM and the proposed SP-OFDM under hostile jamming using the arbitrarily varying channel (AVC) model. It was shown that the deterministic coding capacity of the traditional OFDM is zero under the worst disguised jamming. At the same time, we proved that with the secure randomness shared between the authorized transmitter and receiver, the AVC channel corresponding to SP-OFDM is not symmetrizable, and hence SP-OFDM can achieve a positive capacity under disguised jamming. Note that the authorized user aims to maximize the capacity while the jammer aims to minimize the capacity, we showed that the maximin capacity for SP-OFDM under hostile jamming is given by $C = \log\left(1 + \frac{P_S}{P_J + P_N}\right)$ bits per symbol, where P_s denotes the signal power, P_J the jamming power and P_N the noise power.

- We discussed the worst jamming distribution problem for SP-OFDM given a finite

input constellation. We proved the existence, uniqueness and the Kuhn-Tucker conditions of the worst jamming distribution for SP-OFDM, either with or without a peak power constraint on jamming. The major challenge in the analysis lay in the derivation of the tight bounds on the distribution function of the channel output for any given jamming distribution. We obtained both the upper and lower bounds by exploiting the properties of the modified Bessel functions.

- We proved the discreteness of the worst jamming distribution for SP-OFDM, either with or without peak power constraints, and showed that the worst jamming distribution has a finite number of mass points. More specifically, we first derived a lower bound of the Kuhn-Tucker function for the worst jamming distribution. Second, by applying the identity theorem, we showed that any non-discrete jamming distribution cannot satisfy the Kuhn-Tucker conditions of the worst jamming distribution under a finite peak power constraint. Finally, by further exploiting the derived lower bound on the Kuhn-Tucker function, we showed that when the peak power constraint is sufficiently large, the worst jamming under the peak power constraint is identical with the worst jamming without peak power constraint. We further discussed the maximal amplitude of the worst jamming distribution in different cases, and showed that the worst jamming distribution always has a mass point at the peak power constraint when the average power constraint is inactive.

- Numerical results were provided on the worst jamming distribution and the minimal channel capacity under disguised jamming. The numerical results were consistent with the theoretical analysis, that is, the worst jamming is discrete in amplitude with a finite number of mass points; the minimal channel capacity of SP-OFDM is guaranteed to be

positive under disguised jamming, which demonstrated the robustness of SP-OFDM under disguised jamming. We further studied the impact of the power constraints. It was shown that the worst jamming distribution tends to have more mass points as the peak jamming power increases, while with the decrease of average jamming power, there is a larger chance for the jammer to keep silent for energy saving and the best jamming effect.

On the higher layers protocol design and performance evaluation of 5G multi-hop wireless networks:

- We modeled the node distribution of 5G high-density heterogeneous networks using stochastic geometry. A remarkable feature of 5G is network densification, which makes the node distribution in 5G less organized and more random than existing mobile networks. We characterized the spatial randomness of 5G heterogeneous networks using the effective tools of stochastic geometry. We modeled the nodes as Poisson Point Processes and calculated the spatial average of network performance over all potential geometrical patterns of the nodes. We investigated the effect of relay randomness on the end-to-end throughput in multi-hop wireless networks.

- We designed effective routing protocols for the 5G heterogeneous multi-hop networks. Motivated by the observation that, while the ideal equal-distance routing generally provides the optimal network performance, it is not realizable due to the randomness in relay distribution, we proposed a quasi-equal-distance (QED) routing protocol, derived the range for the optimal hop distance, and specified the selection of the optimal relays to formulate a quasi-equidistant deployment.

- We developed the tools for performance evaluation of multi-hop networks with random

relay deployment. To evaluate the end-to-end throughput of the multi-hop route in 5G wireless networks with randomly located relays, first, we derived the distribution of the longest hop distance for any given routing distance. We showed that multi-hop relaying with random relays is infeasible for long distance communications. Second, to obtain a performance benchmark, we derived the average end-to-end throughput of a multi-hop route under the simple nearest neighbor (NN) routing and TDMA MAC with both fixed and flexible slot length. We maximized the throughput under TDMA, and showed that the optimal slot length varies from hop to hop and is determined by the coverage probability of every hop. Third, under the proposed QED routing and conventional TDMA, we analyzed the average end-to-end throughput with and without intra-route resource reuse, respectively. It was shown that the proposed QED routing protocol achieves a significant performance gain over NN routing.

On the malicious behavior detection in large scale multi-hop wireless networks:

- We proposed an efficient and robust malicious link detection scheme for multi-hop wireless sensor networks (WSNs). Existing work on malicious link detection generally required that the detection process being performed at the intermediate nodes, leading to considerable overhead in system design, as well as unstable detection accuracy due to limited resources and the uncertainty in the loyalty of the intermediate nodes themselves. As an effort to improve the efficiency and minimize the system complexity, in the proposed scheme, malicious link detection was only performed at the base stations, by exploiting the statistics of packet delivery rates.

- We presented a secure packet transmission protocol in the proposed scheme to ensure that except the base stations, any intermediate nodes on the route could not access the

contents and routing paths of the packets. We then designed a malicious link detection algorithm that could effectively detect the irregular dropout at *every hop (or link)* along the routing path with guaranteed false alarm rate and low miss detection rate. It should be pointed out that, illegal packet modification and injection of invalid packets, which essentially resulted in the dropout of legal packets, could be detected successfully as well. Simulation results were provided to validate the proposed approaches.

6.2 Future Work

The future research will be focused on the 5G network performance evaluation under malicious attacks, and the security problems in the 5G massive MIMO transceiver design.

6.2.1 Network Performance Evaluation under Malicious Attacks

In this research direction, we will study and evaluate the 5G network performance, in terms of throughput, delay and energy efficiency under various malicious attacks. We will look into the performance impact of the percentage of malicious nodes/links and the network size. It is anticipated that under the same malicious nodes to benign nodes ratio, the malicious node/link detection accuracy will increase significantly as the network size increases. The underlying argument is that the estimation accuracy of the corresponding statistics will increase significantly as the network size increases. Moreover, each node in the network has a different level of node significance. Higher level of security should be assured for nodes with a higher level of significance. Appropriate mathematic models and tools will be developed for more in-depth and comprehensive network performance evaluation under various malicious attacks.

6.2.2 Anti-jamming Massive MIMO Transceiver Design

Traditionally, the signal design in wireless communications mainly lies in two dimensions: time and frequency. By making use of the diversity in the frequency domain, spread spectrum techniques, for example, are able to provide built-in resilience against jamming attacks.

With the development of MIMO techniques, an extra dimension of signal is introduced in the new generation communication systems: the space. For a point-to-point MIMO communication, the received signal vectors lie in the linear space spanned by the channel vectors. Therefore, the spatial diversity in MIMO system provides another degree of freedom in anti-jamming system design. For example, in analogy to spread spectrum, we can limit the received signal vectors to a smaller subspace of the received space using beamforming techniques, so as to alleviate the interference from jamming.

In this research direction, we will design anti-jamming massive MIMO transceivers by making use of the spatial diversity, and evaluate their feasibility in real world channel scenarios.

APPENDICES

APPENDIX A

Proof of Proposition 2.1

Note that $r(t)r^*(t+T_s)$ can be calculated as

$$\begin{aligned} r(t)r^*(t+T_s) &= s(t-t_0)s^*(t+T_s-t_0)e^{-j\omega_0 T_s} \\ &+ z(t)s^*(t+T_s-t_0)e^{-j(\omega_0 t+\omega_0 T_s+\phi_0)} \\ &+ s(t-t_0)e^{j(\omega_0 t+\phi_0)}z^*(t+T_s) + z(t)z^*(t+T_s). \end{aligned} \tag{A.1}$$

In the following we analyze the four terms on the right-hand-side (RHS) of (A.1) respectively.

First, define

$$Y_{k,1}(\tau) \triangleq \int_{\tau-T_{CP}+kT_b}^{\tau-T_{CP,2}+kT_b} s(t-t_0)s^*(t+T_s-t_0)\mathrm{d}t, \tag{A.2}$$

for $k \in \mathbb{Z}^*, \tau \in [0, T_b)$. We evaluate the expectation of $Y_{k,1}(\tau)\tilde{C}^*_{k+d}$ for $d \in \mathcal{K}$. Note that for $t \in [\tau - T_{CP} + kT_b, \tau - T_{CP,2} + kT_b]$, where $\tau \in [0, T_b)$, we have

$$s(t-t_0) = \sum_{l=k-1}^{k+1} s_l(t-t_0-lT_b), \tag{A.3}$$

$$s(t+T_s-t_0) = \sum_{l=k-1}^{k+1} s_l(t+T_s-t_0-lT_b). \tag{A.4}$$

Note that since the OFDM blocks are zero-mean and independent, for $k_1 \neq k_2$, we have

$$\mathbb{E}\left\{s_{k_1}(t_1)s_{k_2}^*(t_2)\right\} = 0, \forall t_1, t_2 \in \mathbb{R}. \tag{A.5}$$

So we focus on

$$\begin{aligned}
&\int_{\tau-T_{CP,2}+kT_b}^{\tau-T_{CP}+kT_b} \sum_{l=k-1}^{k+1} s_l(t-t_0-lT_b)s_l^*(t+T_s-t_0-lT_b)\ \mathrm{d}t \\
=&\frac{1}{N_c^2}\sum_{l=-1}^{1}\int_{\tau-lT_b-t_0-T_{CP}}^{\tau-lT_b-t_0-T_{CP,2}} \sum_{i_1=0}^{N_c-1} \tilde{S}_{l+k,i_1} e^{j\frac{2\pi i_1}{T_s}t} u_{l+k}(t) \\
&\qquad\qquad \sum_{i_2=0}^{N_c-1} \tilde{S}_{l+k,i_2}^* e^{-j\frac{2\pi i_2}{T_s}t} u_{l+k}^*(t+T_s)\ \mathrm{d}t.
\end{aligned} \tag{A.6}$$

Since for $i_1 \neq i_2$, $\mathbb{E}\{\tilde{S}_{k,i_1}\tilde{S}_{k,i_2}^*\} = 0$, we further focus on

$$\frac{1}{N_c^2}\sum_{l=-1}^{1}\sum_{i=0}^{N_c-1}|\tilde{S}_{l+k,i}|^2 \int_{\tau-lT_b-t_0-T_{CP}}^{\tau-lT_b-t_0-T_{CP,2}} u_{l+k}(t)u_{l+k}^*(t+T_s)\ \mathrm{d}t. \tag{A.7}$$

Define function $v_k(\tau)$ as

$$\begin{aligned}
v_k(\tau) &\triangleq \int_{\tau-T_{CP}}^{\tau-T_{CP,2}} u_k(t)u_k^*(t+T_s)\mathrm{d}t \\
&= \begin{cases}
(\tau+T_{CP,1})C_k, & -T_{CP,1} \leq \tau < 0, \\
\tau + (T_{CP,1}-\tau)C_k, & 0 \leq \tau < T_{CP,2}, \\
T_{CP,2} + (T_{CP,1}-\tau)C_k, & T_{CP,2} \leq \tau < T_{CP,1}, \\
T_{CP}-\tau, & T_{CP,1} \leq \tau < T_{CP}, \\
0, & otherwise.
\end{cases}
\end{aligned} \tag{A.8}$$

So (A.7) can be expressed as

$$\frac{1}{N_c^2}\sum_{l=-1}^{1}\sum_{i=0}^{N_c-1}|\tilde{S}_{l+k,i}|^2 v_{l+k}(\tau - lT_b - t_0). \tag{A.9}$$

In addition, since the phase shift symbols are zero-mean and independent, for $\tau \in \mathbb{R}$, we have

$$\mathbb{E}\{v_{k_1}(\tau)C_{k_2}^*\} = \begin{cases} v(\tau),\ k_1 = k_2, \\ 0,\ k_1 \neq k_2. \end{cases} \tag{A.10}$$

So the expectation of $Y_{k,1}(\tau)\tilde{C}_{k+d}^*$ is

$$\mathbb{E}\{Y_{k,1}(\tau)\tilde{C}_{k+d}^*\} = \begin{cases} \frac{P_S}{N_c}v(\tau + T_b - t_0),\ d = k_0 - 1, \\ \frac{P_S}{N_c}v(\tau - t_0),\ d = k_0, \\ \frac{P_S}{N_c}v(\tau - T_b - t_0),\ d = k_0 + 1, \\ 0,\ otherwise. \end{cases} \tag{A.11}$$

whose maximum is achieved at $\tau = t_0$ and $d = k_0$. In addition, since constellation Φ is a finite set, the variance of $Y_{k,1}(\tau)\tilde{C}_{k+d}^*$ is bounded for any possible k, τ and d, while given τ and d,

$$\mathbb{E}\{Y_{k_1,1}(\tau)\tilde{C}_{k_1+d}^* Y_{k_2,1}(\tau)\tilde{C}_{k_2+d}^*\} = 0,\ \text{for } |k_1 - k_2| > 1. \tag{A.12}$$

So as $K \to \infty$, the variance of $\frac{1}{K}\sum_{k=0}^{K-1} Y_{k,1}(t_0)\tilde{C}_{k+k_0}^*$ converges to 0, and using the Chebychev inequality, we have

$$\frac{1}{K}\sum_{k=0}^{K-1} Y_{k,1}(t_0)\tilde{C}_{k+k_0}^* = \frac{P_S T_{CP,1}}{N_c}, a.s.. \tag{A.13}$$

Second, define

$$Y_{k,2}(\tau) \triangleq \int_{\tau-T_{CP}+kT_b}^{\tau-T_{CP,2}+kT_b} z(t)s^*(t+T_s-t_0)e^{-j(\omega_0 t+\omega_0 T_s+\phi_0)}\mathrm{d}t, \tag{A.14}$$

and

$$Z_{k,l}(\omega,\tau,t_0) \triangleq \int_{\tau-T_{CP}}^{\tau-T_{CP,2}} z(t+kT_b)e^{j\omega t}u_l(t-lT_b+T_s-t_0)\mathrm{d}t. \tag{A.15}$$

It can be derived that

$$Y_{k,2}(\tau) = \sum_{l=-1}^{1}\sum_{i=0}^{N_c-1} \frac{e^{j\frac{2\pi i}{T_s}[-lT_b-t_0]}\tilde{S}_{k+l,i}Z_{k,l}(\frac{2\pi i}{T_s}-\omega_0,\tau,t_0)}{N_c e^{j(k\omega_0 T_b+\omega_0 T_s+\phi_0)}}. \tag{A.16}$$

Considering the delay in signal processing, we assume the jamming term $Z_{k,l}(\frac{2\pi i}{T_s}-\omega_0,\tau,t_0)$ is independent of the transmitted symbol $\tilde{S}_{k+l,i}$ in (A.16). Therefore, we have

$$\mathbb{E}\{Y_{k,2}(\tau)\tilde{C}^*_{k+d}\} = 0, \forall k \in \mathbb{Z}^*, \tau \in [0,T_b), d \in \mathcal{K}. \tag{A.17}$$

Note that the fourth moment of jamming interference $z(t)$ is bounded, so are the variances of $z(t)$ of $Y_{k,2}(\tau)\tilde{C}^*_{k+d}$. In addition, for $\tau \in [0,T_b), d \in \mathcal{K}$, we have

$$\mathbb{E}\{Y_{k_1,2}(\tau)\tilde{C}^*_{k_1+d}Y^*_{k_2,2}(\tau)\tilde{C}_{k_2+d}\} = 0, \forall |k_1-k_2|>1. \tag{A.18}$$

Therefore,

$$\frac{1}{K}\sum_{k=0}^{K-1} Y_{k,2}(\tau)\tilde{C}^*_{k+d} = 0, \forall \tau \in [0,T_b), d \in \mathcal{K}, a.s.. \tag{A.19}$$

Third, define

$$Y_{k,3}(\tau) \triangleq \int_{\tau-T_{CP}+kT_b}^{\tau-T_{CP,2}+kT_b} s(t-t_0)e^{j(\omega_0 t+\phi_0)}z^*(t+T_s)\mathrm{d}t.$$

Following the same argument as in the derivation of (A.19) on $Y_{k,2}(\tau)$, we have

$$\frac{1}{K}\sum_{k=0}^{K-1} Y_{k,3}(\tau)\tilde{C}_{k+d}^{*} = 0, \forall \tau \in [0, T_b), d \in \mathcal{K}, a.s.. \tag{A.20}$$

At last, we define

$$Y_{k,4}(\tau) \triangleq \int_{\tau - T_{CP} + kT_b}^{\tau - T_{CP,2} + kT_b} z(t) z^{*}(t + T_s) \mathrm{d}t.$$

Considering the security of phase shift sequence C_k and the delay in signal processing, we assume that for $t \leq (k+1)T_b + T_s - T_{CP,2}$, the jammer is unable to recover $\tilde{C}_{k+d}, \forall d \in \mathcal{K}$. Since the fourth moment of $z(t)$ is bounded, we can have

$$\frac{1}{K}\sum_{k=0}^{K-1} Y_{k,4}(\tau)\tilde{C}_{k+d}^{*} = 0, \forall \tau \in [0, T_b), d \in \mathcal{K}, a.s.. \tag{A.21}$$

In conclusion, by averaging the correlation coefficients $Y_k(\tau, d)$ over multiple OFDM blocks, (2.18) can be obtained.

APPENDIX B

Conditional PDF of R given S and J

Here we calculate the conditional PDF of R given S and J. Recall that $R = R_1 + jR_2$, where R_1, R_2 denote the real and imaginary parts respectively.

$$\begin{aligned} & f(r_1, r_2 \mid S = \boldsymbol{s}_i, J = x) \\ =& \frac{1}{2\pi} \int_0^{2\pi} \frac{1}{\pi\sigma^2} e^{-\frac{(r_1 - s_{i,1} - x\cos\theta)^2}{\sigma^2}} e^{-\frac{(r_2 - s_{i,2} - x\sin\theta)^2}{\sigma^2}} \mathrm{d}\theta \\ =& \frac{1}{2\pi^2\sigma^2} e^{-\frac{|\boldsymbol{r} - \boldsymbol{s}_i|^2 + x^2}{\sigma^2}} \int_0^{2\pi} e^{\frac{2x|\boldsymbol{r} - \boldsymbol{s}_i|}{\sigma^2}\cos\theta} \mathrm{d}\theta. \end{aligned} \tag{B.1}$$

where $Re(\boldsymbol{s}_i) = s_{i,1}, Im(\boldsymbol{s}_i) = s_{i,2}$. Then we have

$$f(r_1, r_2 \mid S = \boldsymbol{s}_i, J = x) = \frac{1}{\pi\sigma^2} e^{-\frac{|\boldsymbol{r} - \boldsymbol{s}_i|^2 + x^2}{\sigma^2}} I_0\left(\frac{2x|\boldsymbol{r} - \boldsymbol{s}_i|}{\sigma^2}\right), \tag{B.2}$$

where $I_0(\cdot)$ is the modified Bessel function of the first kind with order 0.

APPENDIX C

The Proof of Lemma 3.2

Upper Bound

Since the second raw moment of distribution function $F(\cdot)$ is bounded by P, the integral can be expressed by

$$\begin{aligned}\int_0^\infty u(x,y)\mathrm{d}F(y) &= \int_0^\infty \frac{u(x,y)}{y^2+1}(y^2+1)\mathrm{d}F(y) \\ &\leq \max_y \left\{\frac{u(x,y)}{y^2+1}\right\}(P+1). \end{aligned} \tag{C.1}$$

We next analyze the maximum of $u(x,y)/(y^2+1)$ over $y \in [0,\infty)$.

Take the partial derivative of $\ln[u(x,y)/(y^2+1)]$ w.r.t. y,

$$\frac{\partial \ln \frac{u(x,y)}{(y^2+1)}}{\partial y} = \frac{2x^2 y}{\sigma^4}\left[2\frac{I_1(\frac{2xy}{\sigma^2})}{I_0(\frac{2xy}{\sigma^2})}\frac{\sigma^2}{2xy} - \frac{\sigma^2}{x^2}\left(1+\frac{\sigma^2}{y^2+1}\right)\right]. \tag{C.2}$$

We focus on the sign of the expression in the bracket of (C.2). In [89], it was shown that function $W_0(t) \stackrel{\Delta}{=} tI_0(t)/I_1(t)$ is strictly increasing and convex for $t \in (0,\infty)$, with $\lim_{t\to 0} W_0(t) = 2$. Therefore, given a fixed x, $\partial \ln \frac{u(x,y)}{(y^2+1)}/\partial y$ is negative for y sufficiently large. The maximum of $u(x,y)/(y^2+1)$ is hence located at either (i) $y=0$, or (ii) $\partial \ln \frac{u(x,y)}{(y^2+1)}/\partial y = 0$. Note that for $x > \sigma\sqrt{1+\sigma^2}$, $\left(\partial \ln \frac{u(x,y)}{(y^2+1)}/\partial y\right)|_{y=0} > 0$, therefore case (ii) holds for $x > \sigma\sqrt{1+\sigma^2}$.

For $x > \sigma\sqrt{1+\sigma^2}$, denote the maximum location of y by $y^*(x)$, where

$$W_0\left(\frac{2xy^*(x)}{\sigma^2}\right) = \frac{2x^2}{\sigma^2\left(1+\frac{\sigma^2}{y^*(x)^2+1}\right)}. \tag{C.3}$$

We have

$$\frac{2x^2}{\sigma^2(1+\sigma^2)} \leq W_0\left(\frac{2xy^*(x)}{\sigma^2}\right) \leq \frac{2x^2}{\sigma^2}. \tag{C.4}$$

In [91], it was shown that $W_0(\cdot)$ satisfies

$$W_0(t)^2 - W_0(t) - t^2 < 2, \quad W_0(t)^2 - t^2 > 4. \tag{C.5}$$

The corresponding bound of $y^*(x)$ satisfies

$$\frac{x}{1+\sigma^2} - \epsilon < y^*(x) < \sqrt{x^2 - \frac{\sigma^4}{x^2}}, \tag{C.6}$$

for some constant $\epsilon \in (0, \infty)$, from which we have

$$\frac{2x^2}{\sigma^2\left(1+\frac{\sigma^2}{(\frac{x}{1+\sigma^2}-\epsilon)^2+1}\right)} \leq W_0\left(\frac{2xy^*(x)}{\sigma^2}\right). \tag{C.7}$$

Note that (C.6) and (C.7) together show that

$$\lim_{x\to\infty}[y^*(x) - x] = 0. \tag{C.8}$$

For the modified Bessel function of the first kind with order 0, $I_0(x)$, we have

$\lim_{x\to\infty} \frac{I_0(x)}{e^x/\sqrt{2\pi x}} = 1$. This indicates that

$$\lim_{x\to\infty} \frac{u(x, y^*(x))}{y^*(x)^2 + 1} x^2 \sqrt{2\pi x} = \frac{1}{\pi\sigma^2}. \tag{C.9}$$

Hence, for x sufficiently large, there exists some constant $c_0 \in (0, \infty)$ such that

$$\int_0^\infty u(x, y) \mathrm{d}F(y) \leq \frac{c_0}{x^{2.5}}. \tag{C.10}$$

Note that compared with the result presented in [82], we provide a more precise upper bound on $\int_0^\infty u(x, y)\mathrm{d}F(y)$.

Lower Bound

The partial derivative of $\ln u(x, y)$ is

$$\frac{\partial \ln u(x, y)}{\partial y} = \frac{2x^2 y}{\sigma^4} \left[2 \frac{I_1(\frac{2xy}{\sigma^2})}{I_0(\frac{2xy}{\sigma^2})} \frac{\sigma^2}{2xy} - \frac{\sigma^2}{x^2} \right]. \tag{C.11}$$

For $x \leq \sigma$, $u(x, y)$ is decreasing w.r.t $y \in (0, \infty)$. For any $y_0 \in (0, \infty)$, $\int_0^\infty u(x, y)\mathrm{d}F(y)$ is lower bounded by

$$\int_0^\infty u(x, y)\mathrm{d}F(y) \geq u(x, y_0)F(y_0) \geq u(x, y_0)(1 - P/y_0^2). \tag{C.12}$$

Since function $u(x, y)$ is symmetric for x and y, for $y_0 \leq \sigma$, we have $u(x, y_0) \geq u(\sigma, y_0)$ and

$$\int_0^\infty u(x, y)\mathrm{d}F(y) \geq u(\sigma, y_0)(1 - P/y_0^2), \quad \forall y_0 \in (0, \sigma]. \tag{C.13}$$

Therefore, there exists some constant $c_0' > 0$ such that $\int_0^\infty u(x,y)\mathrm{d}F(y) \geq c_0'$ for $x \leq \sigma$.

For $x > \sigma$, $u(x,y)$ is increasing over $y \in (0, \tilde{y}^*(x))$ and decreasing over $y \in (\tilde{y}^*(x), \infty)$, where the maxima $\tilde{y}^*(x)$ satisfies

$$\sqrt{x^2 - \frac{\sigma^2}{2} - \frac{\sigma^4}{2x^2}} < \tilde{y}^*(x) < \sqrt{x^2 - \frac{\sigma^4}{x^2}}. \tag{C.14}$$

Note that

$$u(x,2x) = \frac{1}{\pi\sigma^2} e^{-\frac{5x^2}{\sigma^2}} I_0(\frac{4x^2}{\sigma^2}) \leq u(x,0), \tag{C.15}$$

which indicates $u(x,y) \geq u(x,2x)$ for $y \in [0,2x]$. Therefore, $u(x,y)$ is lower bounded by

$$\int_0^\infty u(x,y)\mathrm{d}F(y) \geq u(x,2x)F(2x) \geq \frac{I_0(\frac{4x^2}{\sigma^2})\left(1 - \frac{P}{4x^2}\right)}{\pi\sigma^2 e^{5x^2/\sigma^2}}. \tag{C.16}$$

This completes the proof.

APPENDIX D

The Proof of Lemma 3.3

Since the peak amplitude $a \in (0, \infty)$, given $x_1, x_2 \in [0, \infty)$, both functions $u(x_1, y)$ and $u(x_2, y)$ are positive and continuous over $y \in [0, a]$, so is the ratio function $u(x_1, y)/u(x_2, y)$. Applying the mean value theorem, we have

$$\begin{aligned}\int_0^a u(x_1, y)\mathrm{d}F(y) =& \int_0^a \frac{u(x_1, y)}{u(x_2, y)} u(x_2, y)\mathrm{d}F(y) \\ =& \frac{u(x_1, y_0)}{u(x_2, y_0)} \int_0^a u(x_2, y)\mathrm{d}F(y), \end{aligned} \tag{D.1}$$

for some $y_0 \in [0, a]$. This suggests that

$$\frac{\int_0^a u(x_1, y)\mathrm{d}F(y)}{\int_0^a u(x_2, y)\mathrm{d}F(y)} = \frac{u(x_1, y_0)}{u(x_2, y_0)} = e^{\frac{x_2^2 - x_1^2}{\sigma^2}} \frac{I_0(2x_1y_0/\sigma^2)}{I_0(2x_2y_0/\sigma^2)}. \tag{D.2}$$

In [125], it was shown that for any $0 < x < y$, $\frac{I_0(x)}{I_0(y)} > e^{x-y}$, from which we obtain that

$$\frac{I_0(2x_1y_0/\sigma^2)}{I_0(2x_2y_0/\sigma^2)} < e^{2(x_1 - x_2)y_0/\sigma^2} \leq e^{2(x_1 - x_2)a/\sigma^2}. \tag{D.3}$$

for $x_1 > x_2$. This completes the proof.

APPENDIX E

The Proof of Theorem 3.1

Following Lemma 3.4, it is sufficient to prove that Ω is weak* compact and $G(\cdot)$ is weak* continuous. The weak* compactness of Ω has been proved in [80]. Next, we prove that function $G(\cdot)$ is weak* continuous over Ω.

Since the weak topology on distribution functions is metrizable [78], the weak* continuity of the functional $G(\cdot)$ is equivalent to, for a sequence F_n defined on Ω,

$$\lim_{n\to\infty} F_n \overset{w^*}{=} F \Rightarrow \lim_{n\to\infty} G(F_n) = G(F), \tag{E.1}$$

where w^* represents the weak* convergence [77] of sequence F_n. We have

$$\lim_{n\to\infty} G(F_n) = \lim_{n\to\infty} \frac{1}{M_\Phi} \sum_i \int_{\mathbb{C}} Q_i(\boldsymbol{r}, F_n) L_i(\boldsymbol{r}, F_n) \mathrm{d}\boldsymbol{r}. \tag{E.2}$$

In order to apply the Lebesgue dominated convergence theorem, we first show that the integrand is bounded by an integrable function over $\mathbb{C}$.

Following (3.10), $Q_i(\boldsymbol{r}, F_n) > 0$ and we have

$$\begin{aligned} |Q_i(\boldsymbol{r}, F_n) L_i(\boldsymbol{r}, F_n)| \leq\ & Q_i(\boldsymbol{r}, F_n) \log \sum_k Q_k(\boldsymbol{r}, F_n) \\ & + |Q_i(\boldsymbol{r}, F_n) \log Q_i(\boldsymbol{r}, F_n)|. \end{aligned} \tag{E.3}$$

It is straightforward that $Q_i(\boldsymbol{r}, F_n) \in (0, \frac{1}{\pi\sigma^2})$ for any $\boldsymbol{r} \in \mathbb{C}$ and $F_n \in \Omega$. In addition, from Lemma 3.2, we are able to find some constants $c_0, \rho_0 \in (0, \infty)$ such that

$$Q_i(\boldsymbol{r}, F_n) \leq \frac{c_0}{|\boldsymbol{r} - \boldsymbol{s}_i|^{2.5}}, \ \forall |\boldsymbol{r} - \boldsymbol{s}_i| > \rho_0, \forall F_n \in \Omega. \tag{E.4}$$

Since function $|x \log x|$ is increasing for $x \in (0, 1/e)$, without loss of generality, we can set $c_0/\rho_0^{2.5} < 1/e$ such that

$$|Q_i(\boldsymbol{r}, F_n) \log Q_i(\boldsymbol{r}, F_n)| \leq \bar{Q}_i(\boldsymbol{r}), \tag{E.5}$$

where

$$\bar{Q}_i(\boldsymbol{r}) \triangleq \begin{cases} c_1, |\boldsymbol{r} - \boldsymbol{s}_i| \leq \rho_0 \\ \frac{c_2 \log |\boldsymbol{r} - \boldsymbol{s}_i| + c_3}{|\boldsymbol{r} - \boldsymbol{s}_i|^{2.5}}, |\boldsymbol{r} - \boldsymbol{s}_i| > \rho_0 \end{cases}. \tag{E.6}$$

for some constants $c_1, c_2, c_3 \in (0, \infty)$. $\bar{Q}_i(\boldsymbol{r})$ is absolutely integrable over $\mathbb{C}$.

In addition, we have $Q_i(\boldsymbol{r}, F_n) \log \sum_k Q_k(\boldsymbol{r}, F_n) \leq Q_i(\boldsymbol{r}, F_n) \log \frac{M_\Phi}{\pi\sigma^2}$, which is also integrable over $\mathbb{C}$. Therefore, $|Q_i(\boldsymbol{r}, F_n) L_i(\boldsymbol{r}, F_n)|$ is upper bounded by an absolutely integrable function over $\mathbb{C}$ for all $F_n \in \Omega$. Applying the Lebesgue dominated convergence theorem, we have

$$\lim_{n\to\infty} G(F_n) = \frac{1}{M_\Phi} \sum_i \int_{\mathbb{C}} \lim_{n\to\infty} Q_i(\boldsymbol{r}, F_n) L_i(\boldsymbol{r}, F_n) \mathrm{d}\boldsymbol{r}. \tag{E.7}$$

By the definition of $Q_i(\boldsymbol{r}, F_n)$ and the weak topology [80], we can get

$$\lim_{n\to\infty} Q_i(\boldsymbol{r}, F_n) = Q_i(\boldsymbol{r}, F). \tag{E.8}$$

Since x and $\log x$ are both continuous over $(0, \infty)$, we have $\lim_{n\to\infty} G(F_n) = G(F)$, which completes the proof.

APPENDIX F

The Proof of Corollary 3.1

Suppose there exists two jamming distributions $F_0^*, F_1^* \in \Omega$ that minimize $G(\cdot)$ equally, where the minimal $G(\cdot)$ over Ω is denoted by G^*. We define a auxiliary binary RV D denoting the state of J such that

$$\begin{aligned} D = 0 &: J \text{ follows distribution } F_0^*, \\ D = 1 &: J \text{ follows distribution } F_1^*, \end{aligned} \tag{F.1}$$

and $\Pr\{D = 0\} = 1 - \Pr\{D = 1\} = p \in (0, 1)$. It follows that $H(S \mid R, D) = -G^*$.

From the inequality of conditional entropy, we have

$$H(S \mid R, D) \leq H(S \mid R), \tag{F.2}$$

Since $G^* = \min_{F \in \Omega} -H(S \mid R)$, the equality in (F.2) holds. Following [126, Theorem 2.6.3], this indicates that S and D are independent given R, which implies that,

$$\frac{\int_0^\infty u(|\boldsymbol{r} - \boldsymbol{s}_i|, x) \mathrm{d}F_0^*(x)}{\int_0^\infty u(|\boldsymbol{r} - \boldsymbol{s}_i|, x) \mathrm{d}F_1^*(x)}, \tag{F.3}$$

should be invariant to i for any given $\boldsymbol{r} \in \mathbb{C}$, which further implies that

$$\int_0^\infty u(|\boldsymbol{r} - \boldsymbol{s}_i|, x) \mathrm{d}F_0^*(x) \equiv \int_0^\infty u(|\boldsymbol{r} - \boldsymbol{s}_i|, x) \mathrm{d}F_1^*(x). \tag{F.4}$$

Hence, F_0^* and F_1^* render the same conditional distribution of R given S. Note that the characteristic function (CF) of complex Gaussian noise N is non-zero over $\mathbb{R}^2$, therefore the characteristic functions of distribution F_0^* and F_1^* are equal, i.e., $F_0^* = F_1^*$. This proves that the worst jamming distribution $F^* \in \Omega$ is unique.

APPENDIX G

The weak derivative of $G(\cdot)$

First for the given distribution functions F_0 and F, we define

$$F_\theta = (1-\theta)F_0 + \theta F, \tag{G.1}$$

which is also a valid distribution function over Ω. Then

$$Q_i(\boldsymbol{r}, F_\theta) = Q_i(\boldsymbol{r}, F_0) + \theta \left[Q_i(\boldsymbol{r}, F) - Q_i(\boldsymbol{r}, F_0) \right]. \tag{G.2}$$

Following the proof of theorem 3.1, $|Q_i(\boldsymbol{r}, F_\theta)L_i(\boldsymbol{r}, F_\theta) - Q_i(\boldsymbol{r}, F_0)L_i(\boldsymbol{r}, F_0)|$ is absolutely integrable over $\mathbb{C}$. Applying the Lebesgue dominated convergence theorem, we have

$$\begin{aligned} \lim_{\theta \to 0^+} \frac{G(F_\theta) - G(F_0)}{\theta} &= \frac{1}{M_\Phi} \int_{\mathbb{C}} \sum_i \\ &\lim_{\theta \to 0^+} \left[\frac{Q_i(\boldsymbol{r}, F_\theta)L_i(\boldsymbol{r}, F_\theta) - Q_i(\boldsymbol{r}, F_0)L_i(\boldsymbol{r}, F_0)}{\theta} \right] \mathrm{d}\boldsymbol{r}, \end{aligned} \tag{G.3}$$

where

$$\begin{aligned} &\sum_i \lim_{\theta \to 0^+} \left[\frac{Q_i(\boldsymbol{r}, F_\theta)L_i(\boldsymbol{r}, F_\theta) - Q_i(\boldsymbol{r}, F_0)L_i(\boldsymbol{r}, F_0)}{\theta} \right] \\ &= \sum_i \left[Q_i(\boldsymbol{r}, F) - Q_i(\boldsymbol{r}, F_0) \right] \log \frac{Q_i(\boldsymbol{r}, F_\theta)}{\sum_k Q_k(\boldsymbol{r}, F_\theta)}, \end{aligned} \tag{G.4}$$

which completes the proof.

APPENDIX H

The Proof of Lemma 3.8

Since γz^2 is analytic on $\mathbb{C}$ for any finite constant γ, it is sufficient to prove that $g(z;F)$ is analytic. Recall from (3.23) that $g(z;F)$ can be expressed as

$$g(z;F) = \frac{1}{M_\Phi} \sum_i \int_{\mathbb{C}} u(|\boldsymbol{r} - \boldsymbol{s}_i|, z) L_i(\boldsymbol{r}, F) \mathrm{d}\boldsymbol{r}, \tag{H.1}$$

where $u(\rho, z) = \frac{1}{\pi\sigma^2} e^{-\frac{\rho^2+z^2}{\sigma^2}} I_0(\frac{2z\rho}{\sigma^2})$ is an analytic function w.r.t. z over $\mathbb{C}$ for any $\rho \in [0, \infty)$. Note that for any $\boldsymbol{r} \in \mathbb{C}$ and $F(\cdot) \in \Omega$, $Q_i(\boldsymbol{r}, F) > 0$, hence $L_i(\boldsymbol{r}, F) < 0$ and

$$u(|\boldsymbol{r} - \boldsymbol{s}_i|, z) L_i(\boldsymbol{r}, F) \text{ is analytic w.r.t. } z \in \mathbb{C}. \tag{H.2}$$

To prove that $g(z;F)$ is analytic w.r.t. z over $\mathbb{C}$, it is sufficient to prove that [81]

$$\int_{\mathbb{C}} |u(|\boldsymbol{r} - \boldsymbol{s}_i|, z) L_i(\boldsymbol{r}, F)| \mathrm{d}\boldsymbol{r} < \infty, \ \forall z \in \mathbb{C}. \tag{H.3}$$

Following the same argument as in the proof of Theorem 3.1, for any $\boldsymbol{r} \in \mathbb{C}$, we have $|u(|\boldsymbol{r} - \boldsymbol{s}_i|, z) L_i(\boldsymbol{r}, F)|$ being upper bounded by

$$|u(|\boldsymbol{r} - \boldsymbol{s}_i|, z)| \left[\log \frac{M_\Phi}{\pi\sigma^2} + |\log Q_i(\boldsymbol{r}, F)| \right], \tag{H.4}$$

where for $\rho \in [0, \infty)$, $|u(\rho, z)|$ is upper bounded by

$$|u(\rho, z)| \leq \frac{1}{\pi\sigma^2} e^{-\frac{(\rho-|z|)^2}{\sigma^2}+\frac{2|z|^2}{\sigma^2}}. \tag{H.5}$$

This indicates $\int_{\mathbb{C}} |u(|\boldsymbol{r} - \boldsymbol{s}_i|, z)| \mathrm{d}\boldsymbol{r}$ is integrable for $\forall z \in \mathbb{C}$.

Basing on Lemma 3.2, for any closed set $\mathcal{S} \subset \mathbb{C}$, $Q_i(\boldsymbol{r}, F)$ is bounded by some non-zero constants. Therefore, to prove (H.3), it is sufficient to show that for some $\rho_0 > 0$, such that

$$\int_{|\boldsymbol{r}-\boldsymbol{s}_i|\geq\rho_0} |u(|\boldsymbol{r} - \boldsymbol{s}_i|, z)||\log Q_i(\boldsymbol{r}, F)| \mathrm{d}\boldsymbol{r} < \infty, \ \forall z \in \mathbb{C}. \tag{H.6}$$

Note that for sufficiently large x, the lower bound (3.17) of $\int_0^\infty u(x, y)\mathrm{d}y$ is further lower bounded by $e^{-\frac{5x^2}{\sigma^2}}$, while the upper bound (3.16) is less than 1. We have

$$\int_{|\boldsymbol{r}-\boldsymbol{s}_i|\geq\rho_0} |u(|\boldsymbol{r} - \boldsymbol{s}_i|, z)||\log Q_i(\boldsymbol{r}, F)| \mathrm{d}\boldsymbol{r} \leq c \int_{\rho_0}^\infty \rho^3 |u(\rho, z)| \mathrm{d}\rho. \tag{H.7}$$

for some constant c, which is also integrable for $z \in \mathbb{C}$. Hence $u(|\boldsymbol{r} - \boldsymbol{s}_i|, z)L_i(\boldsymbol{r}, F)$ is absolutely integrable over $\boldsymbol{r} \in \mathbb{C}$. This proves that $g(z, F)$ is an analytical function w.r.t. $z \in \mathbb{C}$ for any CDF $F(\cdot) \in \Omega$.

APPENDIX I

The Proof of Lemma 3.9

Let a_1, a_2 be an arbitrary pair such that $0 < a_1 < a_2$. Let the jamming interference J be

$$J = |J_1 + J_2 e^{j\Theta_0}| \tag{I.1}$$

where the CDF function of $J_1 \in \mathbb{R}$ is $F^*_{a_1,\infty}$, $J_2 \in \mathbb{R}$ follows an arbitrary distribution under peak power constraint $a_2 - a_1$ such that $\Pr\{J_2 = 0\} < 1$, and Θ_0 is uniformly distributed over $[0, 2\pi)$. The equivalent channel model (3.1) in this case is

$$R = S + J_1 e^{j\Theta_1} + J_2 e^{j\Theta_2} + N, \tag{I.2}$$

where Θ_1 and Θ_2 are two independent RVs uniformly distributed over $[0, 2\pi)$. Since J satisfies the peak power constraint of a_2, we have $-H(S \mid R) \geq G(F^*_{a_2,\infty})$. Meanwhile, we have

$$-H(S \mid R, J_2 = 0) = G(F^*_{a_1,\infty}). \tag{I.3}$$

Next, we show that *for* $0 < a_3 \leq a_2 - a_1$, $H(S \mid R, J_2 = 0) < H(S \mid R, J_2 = a_3)$.

First, given J_2 and Θ_2, we can obtain $R - J_2 e^{j\Theta_2} = S + J_1 e^{j\Theta_1} + N$. Therefore,

$$H(S|R,J_2=a_3) \geq H(S|R,J_2=a_3,\Theta_2) = -G(F^*_{a_1,\infty}), \tag{I.4}$$

where the first equality holds iff the following assumption is true:

$$\text{Given } R \text{ and } J_2 = a_3,\ S \text{ and } \Theta_2 \text{ are independent.} \tag{I.5}$$

Suppose (I.5) holds. Then the ratio

$$\frac{\Pr\{S = \boldsymbol{s}_i \mid R = \boldsymbol{r}, J_2 = a_3, \Theta_2 = \theta\}}{\Pr\{S = \boldsymbol{s}_k \mid R = \boldsymbol{r}, J_2 = a_3, \Theta_2 = \theta\}}, \tag{I.6}$$

is invariant to θ. This implies that the ratio of (I.6) is constant over $\boldsymbol{r} \in \mathbb{C}$, which further indicates the distribution of R is invariant w.r.t. S, which is impossible. So (I.5) cannot hold. Therefore, for any $a_3 > 0$, $H(S|R, J_2 = a_3) > H(S|R, J_2 = 0)$, and

$$-G(F^*_{a_2,\infty}) \geq H(S|R, J_2) > H(S|R, J_2{=}0) = -G(F^*_{a_1,\infty}). \tag{I.7}$$

This completes the proof.

APPENDIX J

Proof of Corollary 4.1

We denote the number of relays within interval (a, b) by $\Phi(a, b)$. It follows that event

$$\bigcap_{i=0}^{\lfloor \frac{r}{l+\varepsilon} \rfloor - 1} (\Phi(i(l+\varepsilon), (i+1)(l+\varepsilon)) > 0) \neq \emptyset$$

is a necessary condition for $L_m \leq l$ given $R = r > l + \varepsilon$, where ε is a sufficiently small real value. So we have

$$\begin{aligned}
\Pr\{L_m \leq l \mid R = r\} &\leq \Pr\{ \bigcap_{i=0}^{\lfloor \frac{r}{l+\varepsilon} \rfloor - 1} (\Phi(i(l+\varepsilon), (i+1)(l+\varepsilon)) > 0) \mid R = r\} \\
&= \prod_{i=0}^{\lfloor \frac{r}{l+\varepsilon} \rfloor - 1} \Pr\{\Phi(i(l+\varepsilon), (i+1)(l+\varepsilon)) > 0 \mid R = r\} \qquad \text{(J.1)} \\
&= (1 - e^{-\lambda(l+\varepsilon)})^{\lfloor \frac{r}{l+\varepsilon} \rfloor} \leq (1 - e^{-\lambda(l+\varepsilon)})^{\frac{r}{l+\varepsilon} - 1} ,
\end{aligned}$$

where equality (J.1) follows from PPP's property that the distributions of points in disjoint sets are independent. For a fixed l, it can be proved that

$$\begin{aligned}
\int_{-\infty}^{+\infty} |g(l, r)| \mathrm{d}r &= l + \int_{l}^{+\infty} g(l, r) \mathrm{d}r \\
&\leq l + \varepsilon + \int_{d+\varepsilon}^{+\infty} (1 - e^{-\lambda(l+\varepsilon)})^{\frac{r}{l+\varepsilon} - 1} \mathrm{d}r \\
&= l + \varepsilon - \frac{l + \varepsilon}{\ln(1 - e^{-\lambda(l+\varepsilon)})} < +\infty ,
\end{aligned}$$

which completes the proof.

APPENDIX K

Proof of Theorem 4.2

The mean of L_m

Denote the PDF of L_m given $R = r$ by $f_{L_m|R}(l|r)$, so we have $\frac{\partial g(l,r)}{\partial l} = f_{L_m|R}(l|r)$. As $G(l,s)$ is defined as the LT of $g(l,r)$ with respect to r, the partial derivative of $G(l,s)$ with respect to l can be expressed as

$$\frac{\partial G(l,r)}{\partial l} = \int_0^\infty \frac{\partial g(l,r)}{\partial l} e^{-sr} \mathrm{d}r = \int_0^\infty f_{D_m|R}(l|r) e^{-sr} \mathrm{d}r. \tag{K.1}$$

Following (4.25), we have

$$\frac{\partial G(l,s)}{\partial l} = \frac{(\lambda+s)^2 e^{(\lambda+s)l}}{[e^{(\lambda+s)l}s + \lambda]^2}. \tag{K.2}$$

By definition, the mean of L_m given $R = r$ is

$$m_{L_m}(r) = \int_0^{+\infty} l \; f_{L_m|R}(l|r) \mathrm{d}l \quad \text{for} \quad r > 0 \; .$$

Its Laplace transform, $M_{L_m}(s)$, can be calculated as

$$\begin{aligned}
&\int_0^{+\infty}\int_0^{+\infty} l\ f_{L_m|R}(l|r)e^{-sr}\mathrm{d}l\mathrm{d}r \\
\overset{(a)}{=}& \int_0^{+\infty} l\frac{(\lambda+s)^2e^{(\lambda+s)l}}{[e^{(\lambda+s)l}s+\lambda]^2}\mathrm{d}l = \int_0^{+\infty} x\frac{e^x}{[e^x s+\lambda]^2}\mathrm{d}x \\
=& -\frac{1}{s^2}\int_0^{+\infty} x\ \mathrm{d}\frac{1}{e^x+\frac{\lambda}{s}} = \frac{1}{s\lambda}\ln(\frac{\lambda}{s}+1),
\end{aligned}$$

where (a) is obtained from (K.2). Note that

$$\mathcal{L}\left(\frac{1-e^{-\lambda r}}{\lambda r}u(r)\right) = \frac{1}{\lambda}\ln(\frac{\lambda}{s}+1)\ ,$$

and (4.31) can be obtained accordingly.

The variance of L_m

We prove that the variance of L_m is bounded. Denote $\mathbb{E}\{L_m^2 \mid R=r\}$ by function $m_{L_m^2}(r)$. Following the same process, we can prove that the Laplace transform of $m_{L_m^2}(r)$ is

$$M_{L_m^2}(s) = \frac{1}{\lambda+s}\ \frac{2}{s\lambda}\int_0^{+\infty}\ln(\frac{\lambda}{s}e^{-x}+1)\ \mathrm{d}x\ . \tag{K.3}$$

Following (4.31) and (K.3), we can calculate $\mathbb{D}\{L_m \mid R=r\}$ as

$$\begin{aligned}
&\mathbb{D}\{L_m \mid R=r\} = m_{L_m^2}(r) - m_{L_m}^2(r) \\
=& \frac{2}{\lambda^2}\int_0^{\lambda r}\int_y^{\lambda r}\frac{1-e^{-y}}{y}\frac{e^{-x}-e^{x-\lambda r}}{x}\mathrm{d}x\mathrm{d}y \\
=& \frac{2}{\lambda^2}\int_0^{\lambda r}\int_0^{y}\frac{1-e^{-x}}{x}\frac{e^{-y}-e^{y-\lambda r}}{y}\mathrm{d}x\mathrm{d}y\ ,
\end{aligned} \tag{K.4}$$

where

$$\int_0^y \frac{1-e^{-x}}{x}\mathrm{d}x = \sum_{n=0}^{\infty}(-1)^n \frac{y^{n+1}}{(n+1)!(n+1)} \ .$$

We have

$$\frac{2}{\lambda^2}\int_0^{\lambda r}\int_0^y \frac{1-e^{-x}}{x}\frac{e^{-y}}{y}\mathrm{d}x\mathrm{d}y = \frac{2}{\lambda^2}\int_0^{\lambda r}\sum_{n=0}^{\infty}(-1)^n \frac{y^n}{(n+1)!(n+1)}e^{-y}\mathrm{d}y \ .$$

Since

$$\int_0^{\lambda r} y^n e^{-y}\mathrm{d}y = n! - \left(\sum_{k=0}^{n}\frac{n!}{(n-k)!}(\lambda r)^{n-k}\right)e^{-\lambda r} \ ,$$

then

$$\lim_{r\to\infty}\frac{2}{\lambda^2}\int_0^{\lambda r}\sum_{n=0}^{\infty}(-1)^n \frac{y^n}{(n+1)!(n+1)}e^{-y}\mathrm{d}y = \frac{2}{\lambda^2}\sum_{n=0}^{\infty}\frac{(-1)^n}{(n+1)^2} = \frac{\pi^2}{6\lambda^2} \ .$$

Also note that

$$\lim_{r\to\infty}\frac{2}{\lambda^2}\int_0^{\lambda r}\int_0^y \frac{1-e^{-x}}{x}\frac{e^{y-\lambda r}}{y}\mathrm{d}x\mathrm{d}y = 0 \ .$$

So the conditional variance of $\mathbb{D}\{L_m \mid R = r\}$ satisfies

$$\lim_{r\to\infty}\mathbb{D}\{L_m \mid R = r\} = \frac{\pi^2}{6\lambda^2} \ .$$

APPENDIX L

Proof of Theorem 4.3

Recall that Φ is the PPP of the relays over $(0, R)$. The number of relays, N, is a random variable following Poisson distribution of mean λR. Given the value of N, the relays are uniformly distributed over $(0, R)$. Denote the longest hop distance given $N = n$ by $L_m(n)$. The average end-to-end throughput can be expressed as

$$\begin{aligned}\mathbb{E}\{T_{\text{end}} \mid R\} &= \sum_{n=0}^{+\infty} e^{-\lambda R} \frac{(\lambda R)^n}{n!} \, \mathbb{E}\{\frac{1}{N+1} P_s(L_m) \mid N = n\} \\ &= \sum_{n=0}^{+\infty} e^{-\lambda R} \frac{(\lambda R)^n}{(n+1)!} \, \mathbb{E}\{P_s\,(\ L_m(n)\ )\}\ .\end{aligned}$$

Note that $L_m(n)$ is the longest hop distance for n uniformly distributed relays over $(0, R)$. Define $p_n(r) \stackrel{\triangle}{=} \mathbb{E}\{P_s\,(\ L_m(n)\ ) \mid R = r\}$, then we have

$$\mathbb{E}\{T_{\text{end}} \mid R\} = \sum_{n=0}^{+\infty} e^{-\lambda R} \frac{(\lambda R)^n}{(n+1)!} \, p_n(R)\ .$$

Moreover, note that $p(x, r) = \sum_{n=0}^{+\infty} e^{-xr} \frac{(xr)^n}{n!} \, p_n(r)$.

For routing distance R, define

$$h(t) \stackrel{\triangle}{=} \sum_{n=0}^{+\infty} \frac{t^{(n+1)}}{(n+1)!} \, p_n(R)\ .$$

The first order derivative of $h(t)$ can be calculated as

$$h'(t) = \sum_{n=0}^{+\infty} \frac{t^n}{n!}\ p_n(R) = e^t\ p(\frac{t}{R}, R)\ .$$

It then follows that

$$h(t) = \int_0^t h'(u)\mathrm{d}u = \int_0^t e^u\ p(\frac{u}{R}, R)\ \mathrm{d}u\ ,$$

and

$$\mathbb{E}\{T_{\text{end}} \mid R\} = \frac{e^{-\lambda R}}{\lambda R}\ h(\lambda R) = \frac{e^{-\lambda R}}{\lambda R} \int_0^{\lambda R} e^u\ p(\frac{u}{R}, R)\ \mathrm{d}u\ . \tag{L.1}$$

Let $x = \frac{u}{R}$, then it follows from (L.1) that

$$\mathbb{E}\{T_{\text{end}} \mid R\} = \frac{e^{-\lambda R}}{\lambda} \int_0^{\lambda} e^{Rx}\ p(x, R)\ \mathrm{d}x\ .$$

This completes the proof.

APPENDIX M

Proof of Proposition 4.2

Based on Proposition 4.1, the end-to-end throughput given $R = r$ can be expressed as

$$T_{\text{end}}(r) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} e^{j\omega r} \int_{0}^{+\infty} P_s(l) \frac{(j\omega + \lambda)}{\lambda + j\omega e^{(j\omega+\lambda)l}} \mathrm{d}l\mathrm{d}\omega \ .$$

Recall that $P_s(l) = \exp(-\kappa l^2)$. According to Jensen's inequality, for any $g(x) > 0$ and $\int_{-\infty}^{+\infty} g(x)\mathrm{d}x = 1$, it follows that

$$\int_{-\infty}^{+\infty} \exp(-\kappa x^2) g(x)\mathrm{d}x \geq \exp\{-\kappa \int_{-\infty}^{+\infty} x^2 g(x)\mathrm{d}x\} \ .$$

So the end-to-end throughput $T_{\text{end}}(r)$ is lower bounded by

$$C(r) \exp(-\kappa \frac{\int_0^{+\infty} \int_{-\infty}^{+\infty} l^2 \frac{e^{j\omega r}}{2\pi} \frac{(j\omega+\lambda)}{\lambda+j\omega e^{(j\omega+\lambda)l}} \mathrm{d}\omega\mathrm{d}l}{C(r)}) \ , \tag{M.1}$$

where $C(r)$ is defined as

$$C(r) \triangleq \int_{0}^{+\infty} \int_{-\infty}^{+\infty} \frac{e^{j\omega r}}{2\pi} \frac{(j\omega + \lambda)}{\lambda + j\omega e^{(j\omega+\lambda)l}} \mathrm{d}\omega\mathrm{d}l \ .$$

Basing on Cauchy's integral theorem, $C(r)$ can be calculated as

$$\begin{aligned} C(r) &= \int_{-\infty}^{+\infty} \frac{e^{j\omega r}}{2\pi} \int_{0}^{+\infty} \frac{1}{\lambda + j\omega e^{l}} \mathrm{d}l \mathrm{d}\omega \\ &= \int_{0}^{+\infty} e^{-l} e^{-\lambda e^{-l} r} \mathrm{d}l = \frac{1 - e^{-\lambda r}}{\lambda r} \ . \end{aligned} \tag{M.2}$$

Similarly, we have

$$\begin{aligned} & \int_{0}^{+\infty} \int_{-\infty}^{+\infty} l^2 \frac{e^{j\omega r}}{2\pi} \frac{(j\omega + \lambda)}{\lambda + j\omega e^{(j\omega+\lambda)l}} \mathrm{d}\omega \mathrm{d}l \\ &= \int_{-\infty}^{+\infty} \int_{0}^{+\infty} \frac{e^{j\omega r}}{2\pi} \frac{1}{(\lambda + j\omega)^2} \frac{l^2}{\lambda + j\omega e^{l}} \mathrm{d}l \mathrm{d}\omega \\ &= \int_{0}^{+\infty} \frac{l^2 e^{-l}}{\lambda^2 (1 - e^{-l})^2} \left(e^{-\lambda e^{-l} r} - \left[1 + \lambda (1 - e^{-l}) r \right] e^{-\lambda r} \right) \mathrm{d}l \\ &= \int_{0}^{+\infty} \frac{l^2 e^{-l}}{\lambda^2 (1 - e^{-l})^2} \left(e^{-\lambda e^{-l} r} - e^{-\lambda r} \right) \mathrm{d}l - A \frac{r e^{-\lambda r}}{\lambda} \ , \end{aligned} \tag{M.3}$$

The first term in (M.3) can be calculated as

$$\begin{aligned} & \int_{0}^{+\infty} \frac{l^2 e^{-l}}{\lambda^2 (1 - e^{-l})^2} \left(e^{-\lambda e^{-l} r} - e^{-\lambda r} \right) \mathrm{d}l \\ &= e^{-\lambda r} \int_{0}^{1} \frac{\ln^2 (1 - t)}{\lambda^2 t^2} (e^{\lambda t r} - 1) \mathrm{d}t \ (\text{letting } t \triangleq 1 - e^{-l}) \\ &< e^{-\lambda r} \int_{0}^{1} \frac{1}{\lambda^2} [\ln^2 (1 - t) + c] (e^{\lambda t r} - 1) \mathrm{d}t \\ &= \int_{0}^{1} \frac{1}{\lambda^2} [\ln^2 t + c] e^{-\lambda t r} \mathrm{d}t - e^{-\lambda r} \int_{0}^{1} \frac{1}{\lambda^2} [\ln^2 t + c] \mathrm{d}t \\ &= \int_{0}^{1} \frac{1}{\lambda^2} \ln^2 t \ e^{-\lambda t r} \mathrm{d}t + \frac{c}{\lambda^3 r} (1 - e^{-\lambda r}) - \frac{e^{-\lambda r}}{\lambda^2} (2 + c) \ , \end{aligned}$$

Here, the first term

$$\begin{aligned}
&\int_0^1 \frac{1}{\lambda^2} \ln^2 t \; e^{-\lambda t r} \mathrm{d}t = \int_0^1 -\frac{1}{\lambda^3 r} \ln^2 t \; \mathrm{d}(e^{-\lambda t r} - 1) \\
&= \frac{2}{\lambda^3 r} \int_0^1 \ln t \frac{e^{-\lambda t r} - 1}{t} \mathrm{d}t = \frac{2}{\lambda^3 r} \int_0^{\lambda r} \ln \frac{\lambda r}{u} \frac{1 - e^{-u}}{u} \mathrm{d}u \\
&= \frac{2}{\lambda^3 r} \left[\int_0^1 \ln \frac{\lambda r}{u} \frac{1 - e^{-u}}{u} \mathrm{d}u + \int_1^{\lambda r} \ln \frac{\lambda r}{u} \frac{1 - e^{-u}}{u} \mathrm{d}u \right] \\
&= \frac{1}{\lambda^3 r} \left[\ln^2(\lambda r) + 2B(\lambda r) \ln(\lambda r) + 2C(\lambda r) \right]. \qquad \text{(M.4)}
\end{aligned}$$

Now, (4.42) can be obtained by noting the fact that $x^n e^{-x} \to 0$ as $x \to +\infty$ for any n.

APPENDIX N

Proof of Corollary 4.2

Finding out the optimal relay λ given routing distance r is equivalent to finding out the optimal mean of hop number given r. By letting $\lambda r = e^x$, we can rewrite (4.42) as a function of x and r, which is

$$\exp(-\frac{\kappa r^2}{e^{2x}}\left[x^2+2Bx+2C+c\right]-x)\ . \tag{N.1}$$

Define function $s(x)$ as

$$s(x)\stackrel{\triangle}{=}-\frac{\kappa r^2}{e^{2x}}\left(x^2+2Bx+2C+c\right)-x\ , \tag{N.2}$$

which has the same monotonicity as (N.1). The derivative of $s(x)$ is

$$s'(x)=\frac{2\kappa r^2}{e^{2x}}\left[x^2+(2B-1)x+2C+c-B\right]-1\ . \tag{N.3}$$

It follows that the optimal x^* should satisfy $s'(x^*)=0$. As $(2B-1)\approx 0.15$ is very small, $s'(x)$ can be approximated by

$$s'(x)\approx\frac{2\kappa r^2}{e^{2x}}\left[x^2+2C+c-B\right]-1\ . \tag{N.4}$$

The root of equality $e^{2x} = ax^2$ in $(0, +\infty)$ is $x = \frac{1}{\sqrt{a}} \exp\left(-W_{-1}(-\frac{1}{\sqrt{a}})\right)$. So we have

$$s'(\frac{1}{r\sqrt{2\kappa}} \exp\left(-W_{-1}(-\frac{1}{r\sqrt{2\kappa}})\right)) > 0 \ .$$

Thus $x^* > \frac{1}{r\sqrt{2\kappa}} \exp\left(-W_{-1}(-\frac{1}{r\sqrt{2\kappa}})\right)$. Similarly, since $s'(x)$ can also be expressed as

$$\frac{2\kappa r^2}{e^{2x}} \left[(x + \sqrt{2C + c - B})^2 - 2\sqrt{2C + c - B}\ x\right] - 1 \ ,$$

we have $x^* < \frac{e^{-\sqrt{2C+c-B}}}{r\sqrt{2\kappa}} \exp\left(-W_{-1}(-\frac{e^{-\sqrt{2C+c-B}}}{r\sqrt{2\kappa}})\right)$.

APPENDIX O

Proof of Theorem 4.5

Given the location of first hop $|\boldsymbol{X}_1'|$, the following equation holds for $l_0 \leq l < r$

$$\Pr\{L_m \leq l \mid R = r\} = \int_{d_0}^{r} \Pr\{L_m \leq l \mid R = r, |X_1| = x\} f_{|X_1|}(x) \mathrm{d}x \ . \tag{O.1}$$

Following the same rule as in the proof of Theorem 4.1, we can formulate (O.1) as an AR system and solve it using Laplace transform, where (4.55) is obtained accordingly.

Denote the conditional mean of L_m', $\mathbb{E}\{L_m' \mid R = r\}$, by $m_{L_m'}(r)$. According to (4.55), it can be derived that the Laplace transform of $m_{L_m'}(r)$ for $r > l_0$, $M_{L_m'}(s) = \int_{l_0}^{+\infty} m_{L_m'}(r) e^{-sr} \mathrm{d}r$, is

$$M_{L_m'}(s) = \frac{l_0}{s} \cdot e^{-sl_0} + \frac{1}{s\lambda} \ln\left(\frac{\lambda + s}{\lambda - \lambda e^{-sl_0} + s}\right). \tag{O.2}$$

Since function $\ln\left(\frac{\lambda+\frac{1}{x}}{\lambda-\lambda e^{-\frac{1}{x}l_0}+\frac{1}{x}}\right)$ is slowing varying as $x \to \infty$, according to the Tauberian theorem [127, Chapter VIII, Theorem 2], it can be proved that

$$m_{L_m'}(r) \sim \frac{1}{\lambda} \ln r \quad \text{as} \quad r \to +\infty. \tag{O.3}$$

Define function $w(r)$ as

$$w(r) \triangleq \frac{1}{\lambda}\left(u(r-1)\ln r + \ln\frac{\lambda}{\lambda l_0+1} + B\right) + l_0,\ r>0,$$

where $u(\cdot)$ is the unit step function. The Laplace transform of $w(r)$ is

$$W(s) = \frac{1}{s\lambda}E_1(s) + \frac{\frac{\lambda}{\lambda l_0+1}+B}{s\lambda} + \frac{l_0}{s}\ ,$$

where $E_1(\cdot)$ is the exponential integral function. It can be proved that $M_{L'_m}(s) - W(s)$ converges as $s \to 0^+$, which implies $\lim_{r\to+\infty} m_{L'_m}(r) - w(r) = 0$. Thus, (4.56) is obtained.

APPENDIX P

Proof of Corollary 4.4

Define $m_{L'_m}(r) \stackrel{\triangle}{=} \mathbb{E}\{L'_m \mid R = r\}$. From Theorem 4.7, we can express the average end-to-end throughput as a function of slot number M and routing distance r, which is

$$T_{\text{end}}(M, r) = \frac{1}{M} \exp\left(-\frac{1}{M}\bar{\kappa} m^2_{L'_m}(r)\right) P_i(M, r) \ , \tag{P.1}$$

where function $P_i(M, r)$ is obtained by letting $l = m_{L'_m}(r)$ in function $P_i(l)$ of Lemma 4.2. Let $M = \bar{\kappa} m^2_{L'_m}(r)$ and from the lower bound given in (4.23), it follows that

$$\lim_{r\to\infty} P_i(\bar{\kappa} m^2_{L'_m}(r), r) = 1.$$

Note that $M = \bar{\kappa} m^2_{L'_m}(r)$ is the optimal M that maximizes $\frac{1}{M} \exp\left(-\frac{1}{M}\bar{\kappa} m^2_{L'_m}(r)\right)$. We denote $\bar{\kappa} m^2_{L'_m}(r)$ by $\tilde{M}^*(r)$. As $M^*(r)$ is the optimal M that maximizes $T_{\text{end}}(M, r)$ for a given r, and note that $P_i(M, r) \leq 1$, we have

$$\begin{aligned} T_{\text{end}}(\tilde{M}^*(r), r) &\leq T_{\text{end}}(M^*(r), r) \\ &\leq \frac{1}{M^*(r)} \exp\left(-\frac{1}{M^*(r)}\bar{\kappa} m^2_{L'_m}(r)\right) \\ &\leq \frac{1}{\tilde{M}^*(r)} \exp\left(-\frac{1}{\tilde{M}^*(r)}\bar{\kappa} m^2_{L'_m}(r)\right), \end{aligned}$$

from which we can prove that

$$\lim_{r\to\infty} \frac{T_{\text{end}}(M^*(r), r)}{T_{\text{end}}(\tilde{M}^*(r), r)} = 1. \tag{P.2}$$

As $\ln P_i(M, r)$ is a concave function w.r.t. M for any given r, it can be verified that $M^*(r) > \tilde{M}^*(r)$, which implies that

$$\lim_{r\to\infty} P_i(M^*(r), r) = 1. \tag{P.3}$$

From $\tilde{M}^*(r) = \bar{\kappa} m^2_{L'_m}(r)$ and (P.3), (P.2) can be expressed as

$$\lim_{r\to\infty} \frac{\bar{\kappa} m^2_{L'_m}(r)}{M^*(r)} \exp\left(-\frac{\bar{\kappa} m^2_{L'_m}(r)}{M^*(r)}\right) = e^{-1} \tag{P.4}$$

Then the result of Corollary 4.4 follows.

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (Release 10)," *3GPP TS 36.300 V10.4.0 (2011-06)*, 2011.

[2] M. Shafi, A. F. Molisch, P. J. Smith, T. Haustein, P. Zhu, P. D. Silva, F. Tufvesson, A. Benjebbour, and G. Wunder, "5g: A tutorial overview of standards, trials, challenges, deployment, and practice," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 6, pp. 1201–1221, June 2017.

[3] M. Thurfjell, A. Simonsson, O. Lundberg, and O. Rosin, "Narrow beam channel characteristics measured on an 5g nr grid-of-beam test-bed," in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, June 2018, pp. 1–4.

[4] B. Halvarsson, A. Simonsson, A. Elgcrona, R. Chana, P. Machado, and H. Asplund, "5g nr testbed 3.5 ghz coverage results," in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, June 2018, pp. 1–5.

[5] Y. Inoue, Y. Kishiyama, Y. Okumura, J. Kepler, and M. Cudak, "Experimental evaluation of downlink transmission and beam tracking performance for 5g mmw radio access in indoor shielded environment," in *2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Aug 2015, pp. 862–866.

[6] K. Yamazaki, T. Sato, Y. Maruta, T. Okuyama, J. Mashino, S. Suyama, and Y. Okumura, "Dl mu-mimo field trial with 5g low shf band massive mimo antenna," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, June 2017, pp. 1–5.

[7] "IEEE Standard for Local and metropolitan area networks-Part 16: Air Interface for Fixed Broadband Wireless Access Systems," *IEEE Std 802.16-2004*, 2004.

[8] S. Weinstein and P. Ebert, "Data transmission by frequency-division multiplexing using the discrete fourier transform," *IEEE Transactions on Communication Technology*, vol. 19, no. 5, pp. 628–634, Oct. 1971.

[9] T. Hwang, C. Yang, G. Wu, S. Li, and G. Y. Li, "Ofdm and its wireless applications: A survey," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 4, pp. 1673–1694, May 2009.

[10] R1-166056, "Final report of 3gpp tsg ran1 metting 85," 3rd Generation Partnership Project (3GPP), Tech. Rep.

[11] A. Osseiran, F. Boccardi, V. Braun, K. Kusume, P. Marsch, M. Maternia, O. Queseth, M. Schellmann, H. Schotten, H. Taoka, H. Tullberg, M. A. Uusitalo, B. Timus, and M. Fallgren, "Scenarios for 5g mobile and wireless communications: the vision of the metis project," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 26–35, May 2014.

[12] B. Farhang-Boroujeny, "Filter bank multicarrier modulation: A waveform candidate for 5g and beyond," vol. 2014, 12 2014.

[13] C. Kim, K. Kim, Y. H. Yun, Z. Ho, B. Lee, and J. Y. Seol, "Qam-fbmc: A new multi-carrier system for post-ofdm wireless communications," in *2015 IEEE Global Communications Conference*, Dec 2015, pp. 1–6.

[14] Z. Zhao, M. Schellmann, Q. Wang, X. Gong, R. Boehnke, and W. Xu, "Pulse shaped ofdm for asynchronous uplink access," in *2015 49th Asilomar Conference on Signals, Systems and Computers*, Nov 2015, pp. 3–7.

[15] H. Lin, "Flexible configured ofdm for 5g air interface," *IEEE Access*, vol. 3, pp. 1861–1870, 2015.

[16] F. Schaich and T. Wild, "Relaxed synchronization support of universal filtered multi-carrier including autonomous timing advance," in *2014 11th International Symposium on Wireless Communications Systems (ISWCS)*, Aug 2014, pp. 203–208.

[17] X. Zhang, M. Jia, L. Chen, J. Ma, and J. Qiu, "Filtered-ofdm - enabler for flexible waveform in the 5th generation cellular networks," in *2015 IEEE Global Communications Conference*, Dec 2015, pp. 1–6.

[18] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive mimo for next generation wireless systems," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 186–195, February 2014.

[19] X. Gao, F. Tufvesson, O. Edfors, and F. Rusek, "Measured propagation characteristics for very-large mimo at 2.6 ghz," in *2012 Conference Record of the Forty Sixth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, Nov 2012, pp. 295–299.

[20] A. J. Viterbi, *CDMA: Principles of Spread Spectrum Communication*. Redwood City, CA, USA: Addison Wesley Longman Publishing Co., Inc., 1995.

[21] L. Jun, J. H. Andrian, and C. Zhou, "Bit error rate analysis of jamming for ofdm systems," in *2007 Wireless Telecommunications Symposium*, April 2007, pp. 1–8.

[22] S. Amuru and R. M. Buehrer, "Optimal jamming against digital modulation," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2212–2224, Oct 2015.

[23] L. Mailaender, "Anti-jam communications using frequency-hopped ofdm and ldpc with erasure decoding (minotaur)," in *IEEE Military Communications Conference*, Nov 2013, pp. 84–88.

[24] T. C. Clancy, "Efficient ofdm denial: Pilot jamming and pilot nulling," in *IEEE International Conference on Communications*, June 2011, pp. 1–5.

[25] P. Cuccaro and G. Romano, "Non uniform power allocation pilot tone jamming in ofdm systems," in *International Conference on Telecommunications and Signal Processing*, July 2017, pp. 152–155.

[26] M. J. L. Pan, T. C. Clancy, and R. W. McGwier, "Jamming attacks against ofdm timing synchronization and signal acquisition," in *IEEE Military Communications Conference*, Oct 2012, pp. 1–7.

[27] L. Lightfoot, L. Zhang, J. Ren, and T. Li, "Secure collision-free frequency hopping for ofdma-based wireless networks," *EURASIP J. Adv. Signal Process*, vol. 2009, pp. 1:1–1:11, Mar. 2009.

[28] T. Basar, "The gaussian test channel with an intelligent jammer," *IEEE Transactions on Information Theory*, vol. 29, no. 1, pp. 152–157, Jan 1983.

[29] M. Medard, "Capacity of correlated jamming channels," in *Allerton Conference on Communications, Computing and Control*, 1997.

[30] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on mimo gaussian fading channels," *IEEE Transactions on Information Theory*, vol. 50, no. 9, pp. 2119–2123, Sept 2004.

[31] T. Song, W. E. Stark, T. Li, and J. K. Tugnait, "Optimal multiband transmission under hostile jamming," *IEEE Transactions on Communications*, vol. 64, no. 9, pp. 4013–4027, Sept 2016.

[32] A. Lapidoth and P. Narayan, "Reliable communication under channel uncertainty," *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2148–2177, Oct 1998.

[33] T. Song, K. Zhou, and T. Li, "Cdma system design and capacity analysis under disguised jamming," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2487–2498, Nov 2016.

[34] L. Zhang and T. Li, "Anti-jamming message-driven frequency hopping-part ii: Capacity analysis under disguised jamming," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 80–88, January 2013.

[35] T. Song, Z. Fang, J. Ren, and T. Li, "Precoding for ofdm under disguised jamming," in *2014 IEEE Global Communications Conference*, Dec 2014, pp. 3958–3963.

[36] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. New York, NY, USA: Cambridge University Press, 2012.

[37] J. Andrews, F. Baccelli, and R. Ganti, "A tractable approach to coverage and rate in cellular networks," *Communications, IEEE Transactions on*, vol. 59, no. 11, pp. 3122–3134, November 2011.

[38] T. Shu and M. Krunz, "Privacy-preserving and truthful detection of packet dropping attacks in wireless ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 14, no. 4, pp. 813–828, April 2015.

[39] Q. Li and G. Cao, "Mitigating routing misbehavior in disruption tolerant networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 664–675, April 2012.

[40] J. Staddon, D. Balfanz, and G. Durfee, "Efficient tracing of failed nodes in sensor networks," in *Proceedings of ACM International Workshop on Wireless Sensor Networks and Applications*, 2002, pp. 122–130.

[41] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in manets," *IEEE Transactions on Mobile Computing*, vol. 6, no. 5, pp. 536–550, May 2007.

[42] Q. Wang, L. Vu, K. Nahrstedt, and H. Khurana, "Mis: Malicious nodes identification scheme in network-coding-based peer-to-peer streaming," in *Proceedings of IEEE INFOCOM*, March 2010, pp. 1–5.

[43] S. Buchegger and J. . L. Boudec, "Self-policing mobile ad hoc networks by reputation systems," *IEEE Communications Magazine*, vol. 43, no. 7, pp. 101–107, July 2005.

[44] L. Zhang, H. Wang, and T. Li, "Anti-jamming message-driven frequency hopping-part i: System design," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 70–79, January 2013.

[45] M. Haenggi, *Stochastic Geometry for Wireless Networks*, 1st ed. New York, NY, USA: Cambridge University Press, 2012.

[46] M. Haenggi, J. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 7, pp. 1029–1046, September 2009.

[47] F. Baccelli and B. Blaszczyszyn, "Stochastic geometry and wireless networks, volume 1: Theory," *Foundations and Trends in Networking*, vol. 3, no. 3-4, pp. 249–449, 2009.

[48] ——, "Stochastic geometry and wireless networks, volume 2: Applications," *Foundations and Trends in Networking*, vol. 4, no. 1-2, pp. 1–312, 2009. [Online]. Available: http://dx.doi.org/10.1561/1300000026

[49] P. Cardieri, "Modeling interference in wireless ad hoc networks," *Communications Surveys Tutorials, IEEE*, vol. 12, no. 4, pp. 551–572, Fourth 2010.

[50] H. ElSawy, E. Hossain, and M. Haenggi, "Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 15, no. 3, pp. 996–1019, Thirdquarter 2013.

[51] P. H. J. Nardelli, P. Cardieri, and M. Latva-aho, "Efficiency of wireless networks under different hopping strategies," *IEEE Transactions on Wireless Communications*, vol. 11, no. 1, pp. 15–20, January 2012.

[52] M. J. Farooq, H. ElSawy, Q. Zhu, and M. S. Alouini, "Optimizing mission critical data dissemination in massive iot networks," in *2017 15th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*, May 2017, pp. 1–6.

[53] J. G. Andrews, S. Weber, M. Kountouris, and M. Haenggi, "Random access transport capacity," *IEEE Transactions on Wireless Communications*, vol. 9, no. 6, pp. 2101–2111, June 2010.

[54] K. Stamatiou and M. Haenggi, "Delay characterization of multihop transmission in a poisson field of interference," *IEEE/ACM Transactions on Networking*, vol. 22, no. 6, pp. 1794–1807, Dec 2014.

[55] F. Baccelli, B. Blaszczyszyn, and P. Muhlethaler, "An aloha protocol for multihop mobile wireless networks," *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 421–436, Feb 2006.

[56] E. S. Sousa and J. A. Silvester, "Optimum transmission ranges in a direct-sequence spread-spectrum multihop packet radio network," *IEEE Journal on Selected Areas in Communications*, vol. 8, no. 5, pp. 762–771, Jun 1990.

[57] S. P. Weber, X. Yang, J. G. Andrews, and G. de Veciana, "Transmission capacity of wireless ad hoc networks with outage constraints," *IEEE Transactions on Information Theory*, vol. 51, no. 12, pp. 4091–4102, Dec 2005.

[58] P. H. Nardelli, M. de Castro Tom, H. Alves, C. H. de Lima, and M. Latva-aho, "Maximizing the link throughput between smart meters and aggregators as secondary users under power and outage constraints," *Ad Hoc Networks*, vol. 41, no. Supplement C, pp. 57 – 68, 2016.

[59] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," *Wireless Personal Communications*, vol. 29, no. 3, pp. 367–388, Jun 2004.

[60] T. Ericson, "The noncooperative binary adder channel," *IEEE Transactions on Information Theory*, vol. 32, no. 3, pp. 365–374, May 1986.

[61] R. Ahlswede, "Elimination of correlation in random codes for arbitrarily varying channels," *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, vol. 44, no. 2, pp. 159–175, 1978.

[62] D. Blackwell, L. Breiman, and A. J. Thomasian, "The capacities of certain channel classes under random coding," *Ann. Math. Statist.*, vol. 31, no. 3, pp. 558–567, 09 1960.

[63] F. P. Miller, A. F. Vandome, and J. McBrewster, *Advanced Encryption Standard*. Alpha Press, 2009.

[64] J. J. van de Beek, M. Sandell, and P. O. Borjesson, "ML estimation of time and frequency offset in OFDM systems," *IEEE Transactions on Signal Processing*, vol. 45, no. 7, pp. 1800–1805, July 1997.

[65] J. R. Barry, D. G. Messerschmitt, and E. A. Lee, *Digital Communication: Third Edition*. Norwell, MA, USA: Kluwer Academic Publishers, 2003.

[66] "IEEE standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," *IEEE Std 802.11-2012*, pp. 1–2793, March 2012.

[67] T. Lv and J. Chen, "ML estimation of timing and frequency offset using multiple OFDM symbols in OFDM systems," in *IEEE Global Telecommunications Conference*, vol. 4, Dec 2003, pp. 2280–2284.

[68] A. Klenke, *Probability Theory: A Comprehensive Course*. London, UK: Springer, 2008.

[69] I. Csiszar and P. Narayan, "The capacity of the arbitrarily varying channel revisited: positivity, constraints," *IEEE Transactions on Information Theory*, vol. 34, no. 2, pp. 181–193, Mar 1988.

[70] I. Csiszar, "Arbitrarily varying channels with general alphabets and states," *IEEE Transactions on Information Theory*, vol. 38, no. 6, pp. 1725–1742, Nov 1992.

[71] T. Ericson, "Exponential error bounds for random codes in the arbitrarily varying channel," *IEEE Transactions on Information Theory*, vol. 31, no. 1, pp. 42–48, Jan 1985.

[72] J. M. Borden, D. M. Mason, and R. J. McEliece, "Some information theoretic saddlepoints," *SIAM Journal on Control and Optimization*, vol. 23, no. 1, pp. 129–143, 1985.

[73] D. Du and P. Pardalos, *Minimax and Applications*. Springer US, 1995.

[74] A. Morello and V. Mignone, "Dvb-s2: The second generation standard for satellite broad-band services," *Proceedings of the IEEE*, vol. 94, no. 1, pp. 210–227, Jan 2006.

[75] S.-Y. Chung, T. J. Richardson, and R. L. Urbanke, "Analysis of sum-product decoding of low-density parity-check codes using a gaussian approximation," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 657–670, Feb 2001.

[76] T. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2001.

[77] D. G. Luenberger, *Optimization by Vector Space Methods*, 1st ed. New York, NY, USA: John Wiley & Sons, Inc., 1997.

[78] J. G. Smith, "The information capacity of amplitude- and variance-constrained sclar gaussian channels," *Information and Control*, vol. 18, no. 3, pp. 203 – 219, 1971.

[79] S. Shamai and I. Bar-David, "The capacity of average and peak-power-limited quadrature gaussian channels," *IEEE Transactions on Information Theory*, vol. 41, no. 4, pp. 1060–1071, Jul 1995.

[80] I. C. Abou-Faycal, M. D. Trott, and S. Shamai, "The capacity of discrete-time memoryless rayleigh-fading channels," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1290–1301, May 2001.

[81] M. C. Gursoy, H. V. Poor, and S. Verdu, "The capacity of the noncoherent rician fading channel," Princeton University, Tech. Rep., December 2002.

[82] M. Katz and S. Shamai, "On the capacity-achieving distribution of the discrete-time noncoherent and partially coherent awgn channels," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2257–2270, Oct 2004.

[83] T. H. Chan, S. Hranilovic, and F. R. Kschischang, "Capacity-achieving probability measure for conditionally gaussian channels with bounded inputs," *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp. 2073–2088, June 2005.

[84] B. Mamandipoor, K. Moshksar, and A. K. Khandani, "Capacity-achieving distributions in gaussian multiple access channel with peak power constraints," *IEEE Transactions on Information Theory*, vol. 60, no. 10, pp. 6080–6092, Oct 2014.

[85] H. V. Vu, N. H. Tran, M. C. Gursoy, T. Le-Ngoc, and S. I. Hariharan, "Capacity-achieving input distributions of additive quadrature gaussian mixture noise channels," *IEEE Transactions on Communications*, vol. 63, no. 10, pp. 3607–3620, Oct 2015.

[86] A. ElMoslimany and T. M. Duman, "On the capacity of multiple-antenna systems and parallel gaussian channels with amplitude-limited inputs," *IEEE Transactions on Communications*, vol. 64, no. 7, pp. 2888–2899, July 2016.

[87] A. Elmoslimany and T. M. Duman, "On the discreteness of capacity-achieving distributions for fading and signal-dependent noise channels with amplitude-limited inputs," *IEEE Transactions on Information Theory*, vol. 64, no. 2, pp. 1163–1177, Feb 2018.

[88] A. Dytso, M. Goldenbaum, H. V. Poor, and S. S. Shitz, "When are discrete channel inputs optimal? – optimization techniques and some new results," in *2018 52nd Annual Conference on Information Sciences and Systems (CISS)*, March 2018, pp. 1–6.

[89] H. C. Simpson, "Some monotonicity results for ratios of modified Bessel functions," *Quarterly of Applied Mathematics*, vol. 42, pp. 95–98, April 1984.

[90] E. Neuman, "Inequalities involving modified Bessel functions of the first kind," *Journal of Mathematical Analysis and Applications*, vol. 171, no. 2, pp. 532 – 536, 1992.

[91] A. Baricz and E. Neuman, "Inequalities involving modified Bessel functions of the first kind ii," *Journal of Mathematical Analysis and Applications*, vol. 332, no. 1, pp. 265 – 271, 2007.

[92] D. Sarason, *Complex Function Theory*. American Mathematical Society.

[93] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*, 7th ed. Elsevier/Academic Press, Amsterdam, 2007.

[94] Y. Liang, J. Ren, and T. Li, "The worst jamming distribution for securely precoded OFDM," in *2018 IEEE Global Communications Conference*, Dec 2018.

[95] M. Haenggi and R. K. Ganti, "Interference in large wireless networks," *Foundations and Trends in Networking*, vol. 3, no. 2, pp. 127–248, February 2009.

[96] J. Andrews, F. Baccelli, and R. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Transactions on Communications*, vol. 59, no. 11, pp. 3122–3134, November 2011.

[97] J. G. Andrews, S. Weber, M. Kountouris, and M. Haenggi, "A simple upper bound on random access transport capacity," in *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*, Sept 2009, pp. 849–856.

[98] R. Vaze, "Throughput-delay-reliability tradeoff with arq in wireless ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 7, pp. 2142–2149, July 2011.

[99] K. Stamatiou, F. Rossetto, M. Haenggi, T. Javidi, J. R. Zeidler, and M. Zorzi, "A delay-minimizing routing strategy for wireless multi-hop networks," in *Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, 2009. WiOPT 2009. 7th International Symposium on*, June 2009, pp. 1–6.

[100] K. Stamatiou and M. Haenggi, "The delay-optimal number of hops in poisson multi-hop networks," in *2010 IEEE International Symposium on Information Theory*, June 2010, pp. 1733–1737.

[101] ——, "Optimal spatial reuse in poisson multi-hop networks," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, Dec 2010, pp. 1–6.

[102] A. Crismani, U. Schilcher, S. Toumpis, G. Brandner, and C. Bettstetter, "Packet travel times in wireless relay chains under spatially and temporally dependent interference," in *2014 IEEE International Conference on Communications (ICC)*, June 2014, pp. 2002–2008.

[103] C. H. M. de Lima, P. H. J. Nardelli, H. Alves, and M. Latva-aho, "Contention-based geographic forwarding strategies for wireless sensors networks," *IEEE Sensors Journal*, vol. 16, no. 7, pp. 2186–2195, April 2016.

[104] F. Baccelli, B. Blaszczyszyn, and P. Muhlethaler, "On the performance of time-space opportunistic routing in multihop mobile ad hoc networks," in *2008 6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops*, April 2008, pp. 307–316.

[105] H. Feng and L. J. Cimini, "On the optimum number of hops in a multi-hop linear network with randomly located nodes," in *2012 IEEE International Conference on Communications (ICC)*, June 2012, pp. 2329–2333.

[106] Y. Chen and J. G. Andrews, "An upper bound on multihop transmission capacity with dynamic routing selection," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3751–3765, June 2012.

[107] B. Blaszczyszyn and P. Mhlethaler, "Random linear multihop relaying in a general field of interferers using spatial aloha," *IEEE Transactions on Wireless Communications*, vol. 14, no. 7, pp. 3700–3714, July 2015.

[108] M. Abdelhakim, Y. Liang, and T. Li, "Mobile access coordinated wireless sensor networks - design and analysis," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 3, no. 1, pp. 172–186, March 2017.

[109] ——, "Mobile coordinated wireless sensor network: An energy efficient scheme for real-time transmissions," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 5, pp. 1663–1675, May 2016.

[110] T. Li, M. Abdelhakim, and J. Ren, "N-hop networks: a general framework for wireless systems," *IEEE Wireless Communications*, vol. 21, no. 2, pp. 98–105, April 2014.

[111] J. Lee, H. Shin, I. Lee, and J. Heo, "Optimal linear multihop system for df relaying in a poisson field of interferers," *IEEE Communications Letters*, vol. 17, no. 11, pp. 2029–2032, November 2013.

[112] M. Sikora, J. N. Laneman, M. Haenggi, D. J. Costello, and T. E. Fuja, "Bandwidth- and power-efficient routing in linear wireless networks," *IEEE Transactions on Information Theory*, vol. 52, no. 6, pp. 2624–2633, June 2006.

[113] M. Haenggi and R. Smarandache, "Diversity polynomials for the analysis of temporal correlations in wireless networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 11, pp. 5940–5951, November 2013.

[114] M. Haenggi, "Outage, local throughput, and capacity of random wireless networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 8, pp. 4350–4359, August 2009.

[115] R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey, and D. E. Knuth, "On the lambertw function," *Advances in Computational Mathematics*, vol. 5, no. 1, pp. 329–359, 1996.

[116] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: a survey," *IEEE Communications Surveys Tutorials*, vol. 11, no. 2, pp. 52–73, Second 2009.

[117] Y. Zhang, L. Lazos, and W. Kozma, "Amd: Audit-based misbehavior detection in wireless ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 15, no. 8, pp. 1893–1907, Aug 2016.

[118] J. Chang, P. Tsou, I. Woungang, H. Chao, and C. Lai, "Defending against collaborative attacks by malicious nodes in manets: A cooperative bait detection approach," *IEEE Systems Journal*, vol. 9, no. 1, pp. 65–75, March 2015.

[119] V. P. Illiano and E. C. Lupu, "Detecting malicious data injections in wireless sensor networks: A survey," *ACM Computing Surveys*, vol. 48, no. 2, pp. 24:1–24:33, Nov 2015.

[120] T. Li, M. Abdelhakim, and J. Ren, "N-hop networks: A general framework for wireless systems," *IEEE Wireless Communications*, vol. 21, no. 2, pp. 98–105, 2014.

[121] D. Thaler and C. Hopps, "Multipath issues in unicast and multicast next-hop selection," United States, 2000.

[122] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications*, Feb 1999, pp. 90–100.

[123] J. Katz and Y. Lindell, *Introduction to Modern Cryptography.* Chapman & Hall/CRC, 2007.

[124] P. Rogaway and T. Shrimpton, "Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance," in *International Workshop on Fast Software Encryption*, 2004, pp. 371–388.

[125] C. M. Joshi and S. K. Bissu, "Some inequalities of bessel and modified bessel functions," *Journal of the Australian Mathematical Society. Series A. Pure Mathematics and Statistics*, vol. 50, no. 2, pp. 333–342, 1991.

[126] T. M. Cover and J. A. Thomas, *Elements of Information Theory.* New York, NY, USA: Wiley-Interscience, 1991.

[127] W. Feller, *An introduction to probability theory and its applications. Vol. II.*, ser. Second edition. New York: John Wiley & Sons Inc., 1971.