THE UNIVERSITY
of EDINBURGH

Enhancing Physical Layer Security in Wireless Networks with Cooperative Approaches

Weigang Liu

A thesis submitted for the degree of Doctor of Philosophy.

The University of Edinburgh.

June 21, 2016

Abstract

Motivated by recent developments in wireless communication, this thesis aims to characterize the secrecy performance in several types of typical wireless networks. Advanced techniques are designed and evaluated to enhance physical layer security in these networks with realistic assumptions, such as signal propagation loss, random node distribution and non-instantaneous channel state information (CSI).

The first part of the thesis investigates secret communication through relay-assisted cognitive interference channel. The primary and secondary base stations (PBS and SBS) communicate with the primary and secondary receivers (PR and SR) respectively in the presence of multiple eavesdroppers. The SBS is allowed to transmit simultaneously with the PBS over the same spectrum instead of waiting for an idle channel. To improve security, cognitive relays transmit cooperative jamming (CJ) signals to create additional interferences in the direction of the eavesdroppers. Two CJ schemes are proposed to improve the secrecy rate of cognitive interference channels depending on the structure of cooperative relays. In the scheme where the multiple-antenna relay transmits weighted jamming signals, the combined approach of CJ and beamforming is investigated. In the scheme with multiple relays transmitting weighted jamming signals, the combined approach of CJ and relay selection is analyzed. Numerical results show that both these two schemes are effective in improving physical layer security of cognitive interference channel.

In the second part, the focus is shifted to physical layer security in a random wireless network where both legitimate and eavesdropping nodes are randomly distributed. Three scenarios are analyzed to investigate the impact of various factors on security. In scenario one, the basic scheme is studied without a protected zone and interference. The probability distribution function (PDF) of channel gain with both fading and path loss has been derived and further applied to derive secrecy connectivity and ergodic secrecy capacity. In the second scenario, we studied using a protected zone surrounding the source node to enhance security where interference is absent. Both the cases that eavesdroppers are aware and unaware of the protected zone boundary are investigated. Based on the above scenarios, further deployment of the protected zones at legitimate receivers is designed to convert detrimental interference into a beneficial factor. Numerical results are investigated to check the reliability of the PDF for reciprocal of channel gain and to analyze the impact of protected zones on secrecy performance.

In the third part, physical layer security in the downlink transmission of cellular network

is studied. To model the repulsive property of the cellular network planning, we assume that the base stations (BSs) follow the Matérn hard-core point process (HCPP), while the eavesdroppers are deployed as an independent Poisson point process (PPP). The distribution function of the distances from a typical point to the nodes of the HCPP is derived. The noise-limited and interference-limited cellular networks are investigated by applying the fractional frequency reuse (FFR) in the system. For the noise-limited network, we derive the secrecy outage probability with two different strategies, i.e. the best BS serve and the nearest BS serve, by analyzing the statistics of channel gains. For the interference-limited network with the nearest BS serve, two transmission schemes are analyzed, i.e., transmission with and without the FFR. Numerical results reveal that both the schemes of transmitting with the best BS and the application of the FFR are beneficial for physical layer security in the downlink cellular networks, while the improvement due to the application of the FFR is limited by the capacity of the legitimate channel.

Lay Summary

Wireless communication is nowadays experiencing exponential growth. This has attracted extensive research on advanced techniques. However, the security schemes to protect security in ongoing transmission technologies remain elusive. This thesis is carried out to enhance and evaluate physical layer security in various wireless networks.

The first part studies security in cognitive radio network. The primary and secondary base stations (PBS and SBS) communicate with the primary and secondary receivers, respectively. The SBS is allowed to transmit simultaneously with the PBS over the same channel. To improve security, cognitive relay(s) transmit cooperative jamming (CJ) to create extra noise at the eavesdroppers. Two CJ schemes are raised depending on the existence of relays. When there is a relay equipped with multiple-antennas, the combined approach of CJ and beamforming is investigated. When there are multiple relays, the combined approach of CJ and relay selection is analyzed. Numerical results show that both these two schemes are effective in improving security in cognitive radio network.

The second part investigates security in the random wireless network. Three scenarios are investigated to analyze the impact of various factors on security. In scenario one, the basic scheme without protected zone and interference is studied. The probability distribution function (PDF) of channel gain with both fading and path loss has been derived. In the second scenario, we studied using a protected zone surrounding the source node to enhance the security. Both the cases that eavesdroppers are aware and unaware of the protected zone boundary are investigated. Further, the structure with protected zones surrounding legitimate receivers is designed to turn the interference into a beneficial factor. Numerical results are investigated to check the reliability of the distribution function of channel gain and to analyze the impact of protected zones on security.

The third part studies security of the downlink in cellular networks. To model the repulsive property, we assume that the base stations (BSs) follow the Matérn hard-core point process (HCPP). The noise-limited and interference-limited cellular networks are investigated to analyze the impact of frequency reuse. For the noise-limited network, we derive the secrecy performance in two different schemes, by analyzing the statistics of channel gains. For the interference-limited network, the schemes of transmission with and without the FFR are analyzed. Numerical results reveal that both the schemes of transmitting with the best BS and FFR are beneficial for physical layer security in the downlink cellular networks.

Declaration of Originality

I hereby declare that the research recorded in this thesis and the thesis itself were composed and originated entirely by myself in the School of Engineering at The University of Edinburgh.

Weigang Liu

Acknowledgements

"The future belongs to those who believe in the beauty of their dreams."

First of all, I would like to give my gratitude to my supervisor, Professor Tharmalingam Ratnarajah, who provided me with the opportunity to carry out this inspiring and meaningful research and also spent precious time to guide me. The valuable experience during the past four years would be extremely rewarding for my future career. Meanwhile, I appreciate all the constructive discussions with my colleagues, as well as their considerate proof-reading and support beyond research. I could never have accomplished this thesis without the support from EPSRC and CSC, and sincerely hope that my efforts will repay the expectations.

I also present most sincere respect to my parents, who always support whatever I decide to chase and make me sure that there is always a solid foundation that I can expect. I understand that what I am thankful for is far beyond the past four years, indeed dating back to all the caring since my childhood and all the journeys of delivering meals to the middle school. Meanwhile, I would like to give special thanks to Miss Zhang for the considerate encouragement and caring during the past five years. Finally, thank you to all the other family members. The most valuable treasure I have is your love and support.

Last but not least, I want to encourage myself whenever faced with challenges: always strive to figure out the solution rather than excuse and always be thankful.

Contents

List of Figures

List of Tables

Acronyms and Abbreviations

AWGN	Additive White Gaussian Noise
BS	Base Station
CCDF	Complementary Cumulative Distribution Function
CDF	Cumulative Density Function
CJ	Cooperative Jamming
CSI	Channel State Information
CTS	Clear to Send
DF	Decode and Forward
FFR	Fractional Frequency Reuse
HCPP	Hard Core Point Process
ICIC	Inter-cell Interference Coordination
IoT	Internet of Thing
LSC	Least Significant Combination
MGF	Moment Generating Function
i.i.d.	Independent and Identical Distribution
MIMO	Multiple-Input-Multiple-Output
MISO	Multiple-Input-Single-Output
MMSE	Minimum Mean Square Error
MSC	Most Significant Combination
PBS	Primary Base Station
PDF	Probability Density Function
PGFL	Probability Generating Functional
PHY	Physical
PPP	Poisson Point Process

PR	Primary Receiver
PU	Primary User
QoS	Quality of Service
RTS	Request to Send
Rx	Receiver
SBS	Secondary Base Station
SNR	Signal-to-Noise Ratio
SINR	Signal-to-Interference-Noise Ratio
SIR	Signal-to-Interference Ratio
SISO	Single-Input-Single-Output
SR	Secondary Receiver
SU	Secondary User
Tx	Transmitter
ZF	Zero-Forcing

Nomenclature

$\bigcup$	Union operation
$\bigcap$	Intersection operation
$\approx$	Approximately equal to
$\mapsto$	Mapping
$\mathbb{C}$	Complex number
$\mathbb{C}^{m\times n}$	$m \times n$ complex matrix
δ	Ratio between dimension number and path-loss exponent
$\mathbb{N}$	Natural number
$\mathbb{R}$	Real number
$\mathbb{R}^d$	d-dimensional Euclidean space
$\mathbb{R}_+^d$	d-dimensional array with positive components
α	Path-loss exponent
Λ_{opz}	Intensity measure of the random network with secrecy protected zone
λ	Transmitter intensity in a Poisson network
λ_Ξ	Intensity of point process Ξ
λ_c	Intensity of the random set Φ_c
λ_M	Intensity of Φ_M
λ_l	Intensity of Φ_l
λ_e	Intensity of Φ_e
λ_{eqc}	Intensity of the Poisson hole process
λ_{hcpp}	Intensity of HCPP
λ_{opz}	Intensity of the random networks with secrecy protected zone
λ_p	Intensity of parent point process
$B(x,r)$	Circular region surrounding the node x with radius r
$\mathcal{B}^2$	2-dimensional Borel set
$\mathcal{CN}(\cdot,\cdot)$	Complex normal distribution
$\mathbb{I}(X;Y)$	Mutual information between X and Y

$\mathbf{I}_k$	The $k \times k$ identity matrix
$N(\mathcal{A})$	Counting measure of the region $\mathcal{A}$
$N_M(\mathcal{A})$	Counting measure of the region $\mathcal{A}$ in the MHCPP
$N_p(\mathcal{A})$	Counting measure of the region $\mathcal{A}$ in the parent point process
$\mathcal{N}$	Normal distribution
Ξ	Path loss process with small scale fading
Ξ_M	Path loss process with small scale fading at the legitimate receivers in HCPP
$\Xi[0, x)$	Counting measure induced by a random circular set of Ξ centered at the origin with radius x
$\mathbb{P}_{XY\|Z}(\cdot)$	Conditional probability of XY given Z
Φ	Point process
Φ_c	Set of cooperative nodes
Φ_l	Point process of the legitimate receivers
Φ_e	Point process of the eavesdroppers
Φ_p	Parent point process
Φ_M	Matérn HCPP
Φ_{php}	Poisson hole point process
$(x)^+$	$\max\{0, x\}$
$(\cdot)'$	Derivative operation
$(\cdot)^\dagger$	Conjugation transpose
$(\cdot)^T$	Transpose
$(\cdot)^\perp$	Orthogonal vector or space
$\|\cdot\|$	Lebesgue measure for a set or absolute value for a number
$\|\|\cdot\|\|$	2-norm or Euclidean norm
$\|\|\cdot\|\|_F$	Frobenius Norm
$(\cdot)!$	Factorial
$\Lambda(\cdot)$	Intensity measure
$\Gamma(\cdot)$	Gamma function
$\Gamma(\cdot, \cdot)$	Upper incomplete gamma function
$\gamma(\cdot, \cdot)$	Lower incomplete gamma function

$\mathrm{erf}(\cdot)$	Error Function
$\delta_x(\cdot)$	Dirac measure
$\mathbf{1}_A(\cdot)$	Indicator function of the set A
Ψ	Path-loss process
$\Phi(\cdot)$	Counting measure of point process Φ
${}_2F_1[\cdot]$	Hypergeometric function
$\mathbb{E}[\cdot]$	Expectation operation
E_i	Exponential integral
$f^{-1}(\cdot)$	Inverse function
$f_{\xi_k}(\cdot)$	PDF of the path loss process with fading at the k_{th} node
$f_{\gamma_{s:e}}(\cdot)$	PDF of the SINR at the eavesdropper
$eig(\cdot)$	Eigen decomposition
$F_{\xi_k}(\cdot)$	CDF of the path loss at the k_{th} node
$F_{\gamma_{s:e}}(\cdot)$	CDF of the SINR at the eavesdropper
$G(\cdot)$	Meijer-G function
$\log_2(\cdot)$	Logarithmic function with base 2
$\ln(\cdot)$	Natural logarithmic function
$\mathcal{L}_I(s)$	Laplace transform of interference I
$\mathbb{P}(\cdot)$	Probability that an event occurs
$qr(\cdot)$	QR decomposition
$V(\cdot)$	Voronoi cell of a point

Chapter 1
Introduction

Wireless communication is nowadays experiencing exponential growth in the huge volume of data transmission, the massive mobile devices and the rapid development of network models. This has attracted extensive research on advanced techniques of wireless communication. However, the security schemes to protect confidentiality in ongoing transmission technologies, such as the fifth generation (5G) network and the Internet of Things (IoT) remain elusive.

This chapter presents a brief overview of the literature and the main motivations in Section 1.1, and specifies the layout and contributions of this thesis in Section 1.2.

1.1 Literature and Motivation

Due to the mobility of users and network components, wireless channels are susceptible to both active and passive security attacks such as channel jamming, unauthorized access, eavesdropping and many other formats. Modern secrecy approaches protecting wireless communication through cryptographic techniques are founded on the assumption of the efficiency gap between the legitimate users and the adversaries; i.e., adversaries have limited computational capabilities to break the security scheme. The transmitter encrypts the message with a key and sends the cipher text to a receiver over an insecure channel. On the receiver side, the source message is extracted from the cipher text with an associated decryption key; however, for the eavesdropper, due to practical computational limitations, it cannot correctly interpret the message without knowing the decryption key. The approach of using cryptography was first proposed by Shannon [3] in 1949. Two types of encryption have been developed in cryptography in recent years: secret-key

encryption and public-key encryption. Secret-key encryption uses a common secret key for encryption and decryption; in public-key encryption, the transmitter and the receiver use a public key and a private key to encrypt and decrypt, respectively.

However, the technique of using cryptographic approaches, which uses encryption keys to transmit confidential message in the open air, faces challenges from both active and passive attacks [4]. Firstly, there is no guarantee of security with cryptography. Many codes that were regarded as secure twenty years ago are now easily breakable with off-the-shelf computers. Secondly, the secret key is more vulnerable to eavesdropping as it requires a common key must be kept secret at both ends during the secret-key agreement and the subsequent data transmission. While the public-key scheme does not need a secret key, its throughput rate is several orders of magnitude slower than that of the secret-key schemes, which places a bottleneck on meeting increasing data requirements in wireless applications. Moreover, in the large-scale, dynamic and decentralized wireless networks, the use of an unconditional trust third party (TTP) for key management may not be possible.

To explore the possibility of securing communication links without using cryptography in the presence of transparent eavesdroppers[1], great effort has been made to develop physical layer security schemes. To this end, researchers have sought novel information-theoretic techniques to secure wireless networks without the usage of secret keys. Compared to public-key algorithms and hybrid-key algorithms, information-theoretic security is robust to the man-in-the middle attack [5]. Besides, as designed for a different layer, physical layer security could be implemented on existing cryptographic systems to add an additional level of protection [5]. Moreover, physical layer security can characterize the fundamental metrics of security in a wireless network.

This principle of perfect security was first proposed by Shannon in his paper with the notion of *perfect* secrecy [3], which does not rely on any assumptions of the computational capability of the eavesdroppers. The communication channel between the transmitter and the legitimate receiver is called the legitimate channel (the main channel), while the channel between the transmitter and the eavesdropper is termed the eavesdropping

[1] By '*transparent eavesdropper*' we refer to an intruder as described by Wyner, with full knowledge of the system used by the legitimate pair.

channel. From the prospective of the physical layer, the received signal at the legitimate receiver and the eavesdropper are different due to the propagation effect (the large-scale and small-scale fading), the interference from other transmitters, and the thermal noise at the receivers. Large-scale fading is generated by signal attenuation due to signal propagation over large distances and diffraction around large objects in the propagation path, i.e. path loss and shadowing. Small-scale fading is a self-interference result caused by the multi-path propagation of radio waves.

By analyzing the information-theoretic security of discrete memoryless channels [6], Wyner introduced the concept of wire-tap channels. It is shown that perfect secrecy could be achieved when the legitimate receiver has a better channel than that of the eavesdroppers. This notion was further generalized to additive white Gaussian noise (AWGN) channels by Cheong and Hellman [7]. In [8], Csiszár and Körner considered the broadcast wireless channels and showed that the security of a transmission can still be guaranteed by applying sophisticated channel codes, even if the eavesdropping channel is not a degraded version of the legitimate channel. It is proven to be secure for the wireless systems with perfect or noisy channels [5].

Accordingly, various secrecy metrics have been put forward to evaluate physical layer security. The rate at which information can be transmitted secretly from the source to its intended destination is called achievable *secrecy rate*, while the maximum achievable secrecy rate is called the *secrecy capacity*. By taking channel propagation effects into consideration, the secrecy capacity of wireless fading channels was investigated in [9], and expressions of the average secrecy capacity and the *secrecy outage* for quasi-static fading channels were derived in [10]. Exact expression of the secrecy capacity is hard to obtain, due to the limited knowledge of CSI and path loss in legitimate and eavesdropping channels. Ergodic secrecy capacity, derived from statistics of CSI and distances which are easier to obtain, can provide a single letter characterization [2] for the secrecy capacity of an arbitrary wire-tap channel. It can also provide a helpful reference for the design of networks such as allocating the transmission power [9] and [12].

[2] Although the single-letter characterization has not been generally defined, Csiszar and Korner [11] suggested to define it through the notion of computability, i.e., a problem has a single-letter solution if it systematically accounts underlying quantities that can serve as information measures in various contexts and to clarify their relations.

Based on the analysis of secrecy metrics in wireless networks, many transmission strategies have been developed to improve physical layer security, from the perspective of multiple antennas [13–16], cooperative relay networks [17, 18], cooperative jamming [19–25], network coding and other signal processing techniques [26, 27], according to different wireless network models.

Previous works on physical layer security primarily focused on point-to-point transmissions [22, 28, 29]. Compared to the investigations of traditional transmission models, security characteristics in large-scale networks are more dynamic and complex. The tools of stochastic geometry were recently adopted to achieve a better understanding of the large-scale networks where multiple transceivers are randomly deployed [30–34]. During studies of security in random wireless networks via stochastic geometric tools [35], the notion of *secrecy graphs* emerged in [36]. An important distinction between secrecy graphs and the conventional point-to-point wire-tap channel is that the *topology* of networks, with respect to both the legitimate and eavesdropping nodes, plays a major role not only in *how much* secrecy rate is available, but also in *how to measure* it. Following this instinct, secrecy rate scaling laws were studied in [37], while the secrecy rates of unicast links in the presence of multiple eavesdroppers were studied in [38]. Secrecy connectivity over large-scale networks were widely investigated in [35, 36] and [39]. To enhance physical layer security in large-scale networks, various strategies were investigated, such as guard zones [36,40,41], sectorized transmission [42], precoding [43] and the use of artificial noise [44–46].

Physical layer security can help us to understand the secrecy limits of various wireless networks and provide insights to design secured schemes. This thesis is devoted to enhance and evaluate physical layer security in various wireless networks.

1.2 Thesis Layout and Contributions

In this section, we briefly describe the layout and contributions of the thesis as follows.

Chapter 2 provides a technical background for the work in the thesis. This chapter starts with the effects of wireless channels, i.e., the small-scale fading effect and the large-

scale fading, i.e., the path-loss effect. Afterwards, fundamentals of wireless network models and related mathematical tools are introduced for further application in later study. Finally, some metrics are presented to measure the performance of physical layer security.

Chapter 3 considers secret communication through relay-assisted cognitive interference channels in the presence of multiple eavesdroppers. The PBS and SBS communicate with PR and SR respectively in the presence of multiple eavesdroppers. The SBS is allowed to transmit simultaneously with the PBS over the same channel instead of waiting for an idle channel. To improve the secrecy, cognitive relays transmit CJ signals to create additional interference in the direction of the eavesdroppers. Two CJ schemes are proposed to improve the secrecy rate of cognitive interference channels depending on the structure of cooperative relays:

- In the scheme where the multiple-antenna relay transmits weighted jamming signals, the combined approach of CJ and zero-forcing is investigated. Both scenarios, with and without the CSI of the eavesdropper are studied.
- In the scheme with multiple relays transmitting weighted jamming signals, the combined approach of CJ and relay selection is analyzed. To reduce the complexity of cooperation, the algorithm of relay selection is designed to minimize the source power.

Numerical results show that both these schemes are effective in improving physical layer security of cognitive interference channel, compared to the direct transmission with beamforming.

Chapter 4 characterizes the secrecy performance of random wireless networks and exploits the effect of applying interferer protected zones and secrecy protected zones. The contributions of this chapter are summarized as follows:

- We derive the distribution of channel gains from the transmitter to receivers, which are ordered either according to the distance or the strength of the channel gain. The PDF for the distribution of the channel gain is an important tool for calculating the capacity at the worst-case eavesdropper[3], which can be applied to derive the secrecy

[3]The worst-case eavesdropper means the eavesdropper which can obtain the largest instantaneous capacity.

outage probability and the ergodic secrecy capacity.

- The ergodic secrecy capacity of random wireless networks is analyzed by considering both large scale path loss and small scale fading. Additionally, we derive the distribution of path loss for the nodes outside the secrecy protected zone.
- Besides the secrecy protected zone, we also employ interferer protected zones to restructure interference and enhance physical layer security without introducing artificial noise. It is worth to notice that interference is different from jamming noise, because it is the signal broadcasted by other transmitters. Moreover, the distribution of the interference from the active cooperative transmitters that follow a Poisson-hole process has also been exploited.

By employing protected zones, positive ergodic secrecy capacity can be achieved even if the intensity of the legitimate nodes is smaller than that of the eavesdropping nodes in random wireless networks. It is shown that the application of secrecy and interferer protected zones leads to a significant improvement in the security depending on different system parameters.

Chapter 5 studies enhancing physical layer security in the downlink transmission of cellular networks with FFR. To model the repulsive property of the cellular networks, we assume that the locations of the base stations (BSs) follow the HCPP. The contributions of this research are summarized as follows:

- We derive the distance distribution of HCPP, which is then applied to investigate the secrecy performance of transmission with the best BS.
- For the noise-limited cellular network, two transmission schemes are investigated; the downlink transmission with and without FFR. For the scheme without FFR, two transmission strategies are analyzed by selecting different BSs: the nearest BS versus the best BS. In particular, the distribution of the channel gain from the best BS is derived by exploiting the characteristic of point process.
- We further study the application of the FFR to enhance physical layer security in interference-limited cellular networks. The PDFs of the signal-to-interference ratio (SIR) are derived for both the scenarios with and without FFR, based on the analysis

of the inter-cell interference.

Numerical results reveal that increasing the frequency reuse factor contributes to enhancing the security, while the improvements will be less significant when the number of frequency reuse factor is high. Besides, transmitting with the best BS, increasing the intensity of BSs, and reducing the repulsive distance of the BSs can all help to improve the secrecy performance.

Finally, Chapter 6 provides conclusions based on the work presented in the main chapters and discusses possible future research directions.

Chapter 2
Background

This chapter provides a background of the thesis, starting with the properties of wireless channels. Then, the system model of cognitive radio and its properties are introduced. Furthermore, the fundamental concepts and models of stochastic geometry are presented to introduce the system model of random networks and cellular networks, which will be investigated later in the main part of the thesis.

2.1 Wireless Channel

Studying the propagation of radio signals in the wireless channels is the primary challenge in wireless communications. It is much more complex than any other communication system because of the physical properties of electromagnetic waves. Roughly, large-scale fading and small-scale fading should be considered in order to characterize the mobile wireless channel.

Most previous works on beamforming schemes focus on small-scale fading [47–49]. It is appropriate when the strength of interference is comparable to the desired signal and the objective is to design an efficient communication system. However, when dealing with relevant issues such as large-scale wireless network planning, consideration of the large-scale fading is of critical importance.

2.1.1 Fading

Fading is defined as the deviation of the attenuation affecting signals over a certain propagation medium. Some related terms used in this thesis are given as follows [50]:

- **Large-scale fading:** When the receiver moves through a distance of the order of hundreds of wavelengths, the received signal is affected by *large-scale fading* consisting of *path-loss*, which is a function of distance, and *shadowing* which is caused by large objects such as buildings and hills.
  - **Path-loss:** This is the mean signal attenuation in terms of the distance between the transmitter and the receiver. The path-loss is the deterministic part of a channel and is well studied in the urban areas in [51]. Path-loss is of critical importance in this thesis and, thus, will be discussed in detail in the next subsection.
- **Small-scale fading:** With the distance between the transmitter and the receiver changing in the order of wavelength, the received signal changes dramatically due to constructive and destructive interference caused by the multi-path effect between the transmitter and the receiver. This effect is usually called *small-scale fading*, or *fading* for simplicity.
  - **Rayleigh fading:** Rayleigh fading is a reasonable model when there are many objects that scatter the signal before it arrives at the receiver. Fundamentally, it is the envelope of a circularly symmetric complex normal distributed random variable. Statistical information of Rayleigh fading can be found in [52].
  - **Nakagami-m fading:** Although Nakagami-m fading is out of the scope of this thesis, it is a very useful model for large-scale wireless networks. When the parameter m increases from one to infinity, the Nakagami-m fading model varies from the Rayleigh fading model to the path-loss only model [53, 54].

2.1.2 Path-Loss Effect

Path-loss is the reduction in power density of an electromagnetic wave as it propagates through space. According to the laws of physics in free space, the received power will decay as r^{-2} where r is the distance between the transmitter and the receiver. However, because the reflected signals reduce the direct signal and the obstacles might also absorb some power, the received power will decay considerably faster than r^{-2}. According to

Environment	Path-Loss Exponent α
Infinite Free Space	2.0
Urban Area	2.7 to 3.5
Suburban Area	3.0 to 5.0
Office	2.6 to 3.0
Store	1.8 to 2.2

Table 2.1: Path-loss exponent values in various environments [2].

empirical evidence, the received power decays as r^{-2} near the transmitter and decays exponentially at a distance far from the transmitter.

The inverse exponential relationship between received signal power and distance is commonly known, i.e., $\frac{P_r}{P_t} \propto r^{-\alpha}$, where α is called the *path-loss exponent* and P_r, P_t are the received and transmit power with units in Watts (W), respectively. Although a singular point exists in this path-loss model, its tractability has attracted a considerable amount of work, such as [55–60]. Table 2.1 lists the empirical path-loss exponent values in various environments.

2.2 Cognitive Radio

Due to the continual increase in demand for additional bandwidth, spectrum policy makers and researchers are seeking solutions for spectrum scarcity. The study of spectrum measurement, on the other hand, shows that the licensed spectrum is inefficiently used among the time and frequency slots [61]. For the purpose of improving the spectrum utilization efficiency and providing high bandwidth to mobile users, the next generation of communication networks [62] program was developed to implement spectrum policy intelligent radios, also known as cognitive radios introduced by Mitola [63], by dynamic spectrum access techniques. Furthermore, the IEEE has organized a new working group, known as the wireless regional area network, IEEE 802.22 [64] to develop cognitive radio techniques and allow sharing of geographically unused television (TV) spectrum [65].

2.2.1 The Mechanism of Cognitive Radio

As defined in Haykin's paper [66], "cognitive radio is an intelligent wireless communication system that is aware of its surrounding environment (i.e., outside world), uses the methodology of understanding-by-building to learn from the environment and adapts its internal states to statistical variations in the incoming RF stimuli by making corresponding changes in certain operating parameters (e.g., transmit-power, carrier-frequency, and modulation strategy) in real-time, with two primary objectives in mind:

- highly reliable communications whenever and wherever needed; and
- efficient utilization of the radio spectrum."

To standardize cognitive radio networks, IEEE 802.22 [67] open the access of fallow TV bands to infrastructure single-hop cognitive radio networks, with BS performing spectrum management. This standard supports the provision of broadband fixed wireless data in rural areas where the population is sparse.

To function properly, a cognitive-radio device should follow the closed-loop cycle. This Observe-Decide-Act-Learn cognitive cycle is based on (1) observing the channel status, (2) deciding the fallow spectrum available for secondary transmission, (3) acting appropriately to achieve the required configurations of transmission, and (4) learning from previous channel activity. This cycle allows the cognitive-radio device to self-decide and optimally self-reconfigure its components to physically adjust the selected mode of communication [68].

The functionalities of the cognitive radio can be summarized as [69]:

- Spectrum sensing: The function of the spectrum sensing is to allow secondary users (SUs) to detect which portions of the spectrum are available, and monitor the activity of the primary users (PUs).
- Spectrum management: The goal of spectrum management is to provide flexible, fair, and efficient usage of the radio resource. According to the result of the spectrum analysis, spectrum management can improve the spectral utilization efficiency by providing appropriate spectrum holes to the cognitive radio users, as

well as by considering their QoS requirements.

- Spectrum sharing: When there are several coexisting cognitive radio users, it is very important to coordinate the usage of the spectrum with other SUs, by considering both fairness and spectral efficiency. These sharing strategies should depend not only on the spectrum availability, but also on the QoS requirements of the users.

- Spectrum mobility: When the current operating frequency becomes unavailable during communication due to either changes over time, or movements of the cognitive radio users, the system needs to switch to other bands in a seamless manner.

The mechanisms of cognitive radio can be classified into two modes:

- *Spectrum overlay* (interweave): This mode allows SUs to utilize idle band gaps, i.e. white space. The SUs can transmit in this mode without any power limits. Since SUs need to detect the white spaces, there could be the chance of collision due to the error of spectrum sensing. It is assumed that in the overlay mode the secondary transmitter has a priori knowledge of the primary transmissions [70];

- *Spectrum underlay*: This mode allows the SUs to use the whole frequency band while constraining their total interference level to the PUs. Unlike the spectrum overlay, both PUs and SUs can occupy the same frequency bands in this mode.

Finally, it is noted that power control is also a crucial aspect in cognitive radio networks. Specifically, since wireless users communicate via an air interface over a common shared medium, power control is a problem that affects all users (PUs and SUs). In general, each user's transmission power can be considered as source of interference for all the other users, as it can deteriorate their signal-to-interference-plus-noise ratio (SINR). In addition, power control is also required since data transmission consumes valuable battery life. Now, typically, the goal for most users is to achieve a high SINR while expending the smallest amount of energy. Hence, there is a clear trade-off between achieving high SINR levels and lowering energy consumption in cognitive radio networks.

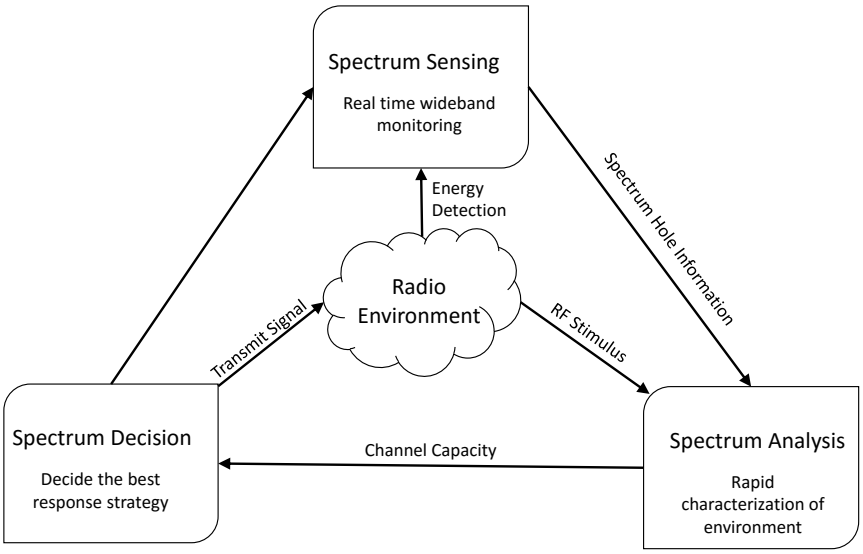

Figure 2.1: Cognitive cycle.

2.2.2 Cognitive Cycle

The operations that a cognitive radio performs for adaptive operation are referred to as the cognitive cycle. The cognitive cycle consists of the following mechanisms [71]:

1. Spectrum sensing: In this process, the SUs detect the channel activity. In the standard of IEEE 802.22, the energy detection method has been used due to its simplicity and low computational overhead.

2. Spectrum analysis: Based on the feedback from spectrum sensing, several environment characteristics, such as bit error rate, capacity and delay, can be analyzed for each spectrum hole. The analysis result will be further applied to make spectrum decision.

3. Spectrum decision: Either performed by a single or multiple cognitive radios, this process will select the most appropriate spectrum hole for transmission.

In the cognitive radio network, SUs not authorized the rights to use the spectrum can utilize the temporally unused licensed bands that are authorized to the PUs [72]. As a result, in a cognitive radio network architecture, the communication system includes both a secondary network and a primary network, as shown in Figure 2.2. A secondary

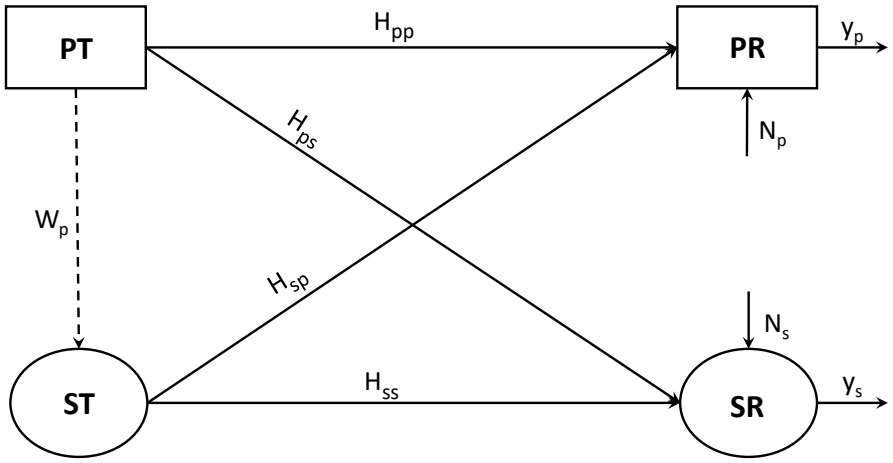

Figure 2.2: The overlay mode of cognitive radio. PT, PR, ST and SR represent the primary transmitter, the primary receiver, the secondary transmitter and the secondary receiver, respectively. Dashed curve represents a priori knowledge of primary message W_p at the secondary transmitter [1].

network refers to a network constituted by a set of SUs with or without a SBS. SUs can only access the licensed spectrum when the transmissions of PUs are absent. Therefore, besides detecting the spectrum white space and utilizing the best spectrum band, the secondary network need to immediately detect the communication of a PU and direct the secondary transmission to another available band of the spectrum to avoid interfering with the transmission of primary network [72].

2.3 Stochastic Geometry

Stochastic geometry technique deals with random spatial patterns, where point processes are the most important and typical objects. According to [33, 73, 74], stochastic geometry technique is devoted to the study of connectivity and signal power in wireless networks where the transmitters and receivers are placed according to a certain distribution. In this thesis, the stochastic geometry techniques will be applied to model the characteristics of wireless networks and to analyze their secrecy performances.

2.3.1 Borel σ-algebra

A 2-dimensional Borel set $\mathcal{B}^2$ is any set in a 2-dimensional topological space that can be formed by taking the complement, countable unions and intersections of closed, open or half-open sets. A collection of all Borel sets forms the *Borel σ-algebra*.

If a set consists of a countable number of singletons, it is a countable set. In a 2-dimensional space, a set $A \subseteq \mathbb{R}^2$ is said to be bounded if there exists a point $x \in \mathbb{R}^2$ and value $r \in \mathbb{R}$ so that a ball centered at x with radius r, denoted as $B(x, r)$, has $A \subset B(x, r)$. If a bounded set is also closed, it is *compact*.

2.3.2 Fundamentals of Point Process

The following text is a brief introduction of point process, which provides the mathematical model to investigate the properties of random point patterns.

Definition

According to [33], a point process Φ is a countable random collection of points that reside in some measurable space, usually a 2-dimensional Euclidean space. The associated σ-algebra consists of the Borel sets $\mathcal{B}^2$, and the measure used is the Lebesgue measure.

Formalism

Generally, there are two approaches to formalize a 2-dimensional point process: the *random set formalism* and the *random measure formalism*. In a random set formalism, a point process is regarded as a countable set consisting of random variables. In this thesis, the random measure formalism is considered, which characterizes a point process by the counting measures of sets.

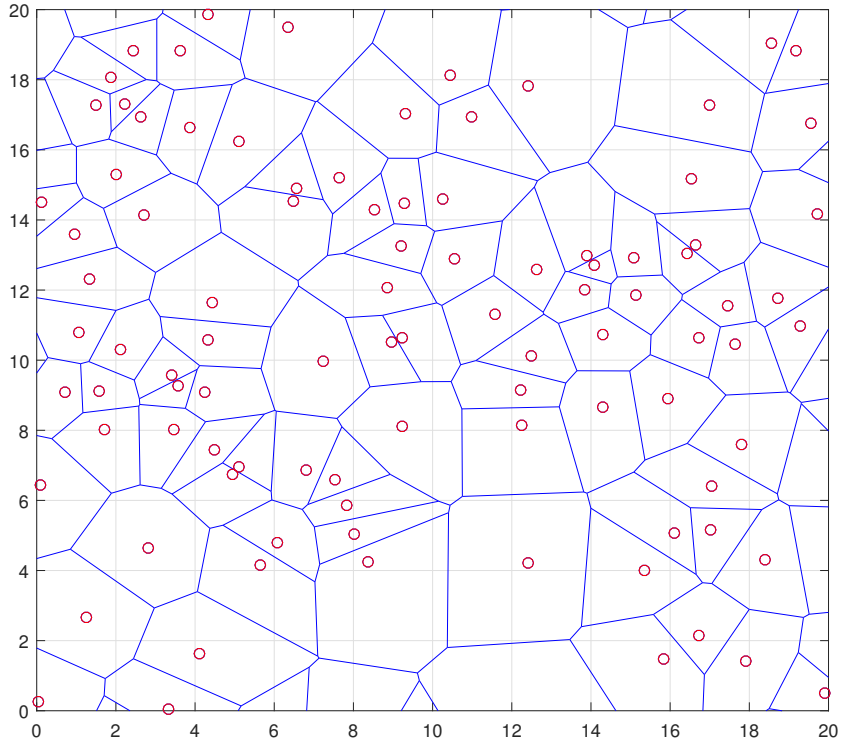

Figure 2.3: Voronoi tessellation of a PPP in 2-dimensional space.

Voronoi Cell

The *Voronoi cell* of a point x in a point process Φ, denoted as $V(x)$, consists of locations in the Euclidean space of which the distances to x are not greater than the distance to any other point in Φ, i.e.,

$$V(x) = \{y \in \mathbb{R}^2 : \|x - y\| \leq \|z - y\|, \forall z \in \Phi \backslash \{x\}\}.$$

The *Voronoi tessellation* of Φ divides the space into separated regions, each of which is the Voronoi cell of a point in Φ. Figure 2.3 illustrates the Voronoi tessellation of a 2-dimensional PPP with unit intensity in a 20×20 area.

The Voronoi cell is a very important tool in wireless network planning. Inside the cell of the i-th BS, the mean signal power from the i-th BS is larger than that of any other BSs due to the path-loss effect. Therefore, BSs typically only serve the terminals inside their

own Voronoi cells. If the BSs have different transmit power, a weighted Voronoi diagram should be considered instead, as in [75, 76].

2.3.3 Measurability in 2-Dimensional Space

Generally, an ordered pair $(A, \mathcal{A})$ is called a measurable space if $\mathcal{A}$ is a σ-algebra on the subsets of A. Note that the point patterns in this thesis, i.e., $(\mathbb{R}^2, \mathcal{B}^2)$, are measurable. A function $f : \mathbb{R}^2 \mapsto \mathbb{R}$ is $\mathcal{B}^2$-measurable if and only if the pre-image of 1-dimensional Borel set $A \in \mathcal{B}$ is an element of $\mathcal{B}^2$, i.e.,

$$f^{-1}(A) = \{x \in \mathbb{R}^2 : f(x) \in A\} \in \mathcal{B}^2.$$

Consider all pairwise disjoint sets $A_i \in \mathcal{A}, i = 1, 2, \ldots, n$ and $n \in \mathbb{N} \cup \{\infty\}$. A measure ν is a function $\nu : \mathcal{A} \to \mathbb{R} \cup \{\infty\}$ with countable additivity, i.e.,

$$\nu\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} \nu(A_i),$$

and satisfying $\nu(\emptyset) = 0$, where $\emptyset$ is the empty set.

Lebesgue Measure

The Lebesgue measure, denoted as $|\cdot|$, is a commonly used measure in this thesis and is basically a measurement of volume in Euclidean space. For example, the Lebesgue measure of an area of a disk with radius 3 centered at point x in a 2-dimensional Euclidean space is $|B(x, 3)| = 9\pi$.

Dirac Measure

The Dirac measure, denoted as $\delta_x(A)$, is a measure at point x for a set $A \subset \mathcal{B}^2$ which is equal to 1 if $x \in A$ and 0 otherwise. The Dirac measure can be expressed by indicator function $\mathbf{1}_A(\cdot)$ as:

$$\delta_x(A) = \mathbf{1}_A(x).$$

Counting Measure

For a point process Φ, the counting measure $\Phi(A)$, where $A \subset \mathcal{B}^2$, is to count the number of singletons in Φ that fall in the set A. The counting measure can be expressed as:

$$\Phi(A) = \sum_{x \in \Phi} \delta_x(A).$$

It will be shown that the counting measure is the most important measure to describe a 2-dimensional point process.

Intensity Measure

The intensity measure $\Lambda(\cdot)$ for a set A, where $A \subset \mathcal{B}^2$, can be expressed by the following equation:

$$\Lambda(A) = \mathbb{E}[\Phi(A)],$$

where $\mathbb{E}[\cdot]$ is the expectation operation. The intensity measure can be explained as the expected number of points falling in a set.

Campbell's Theorem

Campbell's theorem refers to an equation relating to the expectation of a function summed over a point process to an integral involving the intensity measure of the point process. For a function $f : \mathbb{R}^2 \mapsto [0, \infty)$ which is a measurable function and Φ is a point process, according to [77], Campbell's theorem can be expressed as:

$$\mathbb{E}\left[\sum_{x \in \Phi} f(x)\right] = \int_{\mathbb{R}^2} f(x)\Lambda(\mathrm{d}x).$$

A specific proof of the Campbell's theorem can be found in Theorem A.2 of [77].

2.3.4 Poisson Point Process

A PPP assumes total independence of the locations of nodes. That is to say, the location of any node is completely uncorrelated with the locations of all other nodes. If a point process Φ is a homogeneous PPP, i.e., a Poisson process with the same intensity λ all over the Euclidean plane, then Φ must have the following properties:

- For any compact set A, $\Phi(A)$ has Poisson distribution with mean value $\lambda|A|$;
- If $A_1, A_2, \ldots, A_n$ are disjoint bounded sets, then $\Phi(A_1), \Phi(A_2), \ldots, \Phi(A_n)$ are independent random variables.

In a 2-dimensional space, a homogenous PPP can be characterized by counting measure as the following equation:

$$\mathbb{P}\big(\Phi(A) = k\big) = \frac{\exp\big(-\lambda|A|\big)\big(\lambda|A|\big)^k}{k!},\ k \in \mathbb{N},$$

and its pattern can be seen from Figure 2.4. Note that $\mathbb{P}(\cdot)$ means the probability that an event happens. PPP is the most fundamental point process and will be studied in Chapter 5.

2.3.5 Hard-Core Point Process

A HCPP is a random point process which is more repulsive than a PPP. All the points in the HCPP are distributed at a distance larger than a minimum value to each other. A HCPP is generally obtained by removing points which violate the restriction of a more general point process, such as PPP. Two of the most well-studied models are the Matérn HCPP of types I and II as investigated in [33]. Due to the tractability of the interference [78], we will analyze type II to model wireless networks later in this thesis. Consider a parent point process $\Phi_p = \{(x_i, m_i); i = 1, 2, 3, \cdots\}$ which is a marked PPP, where x_i denotes the i_{th} point of the process and m_i stands for its mark which is uniformly distributed in the range $[0, 1]$. A HCPP can be obtained by removing all the points in Φ_p that have a neighbor within distance ϱ and have smaller marks. The deployment of the Matérn HCPP

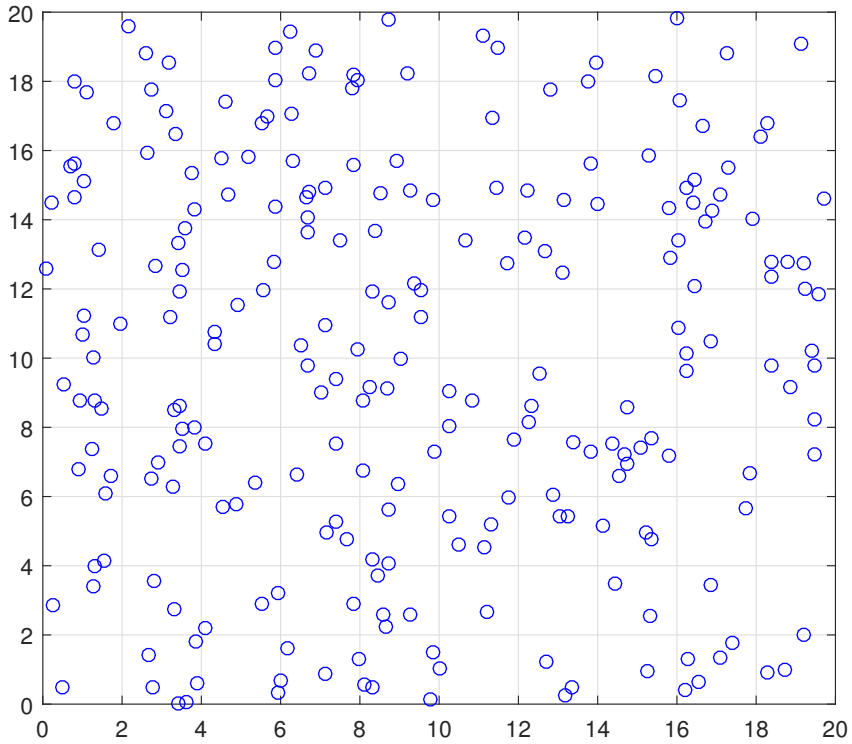

Figure 2.4: Poisson point process.

is shown in Figure 2.5.

Given a minimum distance ϱ and the intensity of the parent Poisson point process λ_p, the density of the second type of Matérn HCPP is given by [33]

$$\lambda_{hcpp} = \lambda_p \int_0^1 \exp(-t\lambda_p C_d \varrho^d) \mathrm{d}t = \frac{1 - \exp(-\lambda_p C_d \varrho^d)}{C_d \varrho^d}. \tag{2.1}$$

2.3.6 Poisson Hole Process

Let Φ_1 and Φ_2 be independent PPPs of intensities $\lambda_1 < \lambda_2$. For each $x \in \Phi_1$, remove all the points of $\{y | y \in \Phi_2 \cap \mathfrak{D}(x, r)\}$, where $\mathfrak{D}(x, r)$ is a ball centered at x with radius r. Denote the Poisson hole process as Φ_{php}, then $\Phi_{php} = \Phi_2 \setminus \bigcup\{\mathfrak{D}(x, r), x \in \Phi_1\}$. All the removed points of Φ_2 form the hole-0 process and the remaining points of Φ_2 form the hole-1 process which is defined as the Poisson hole process [33].

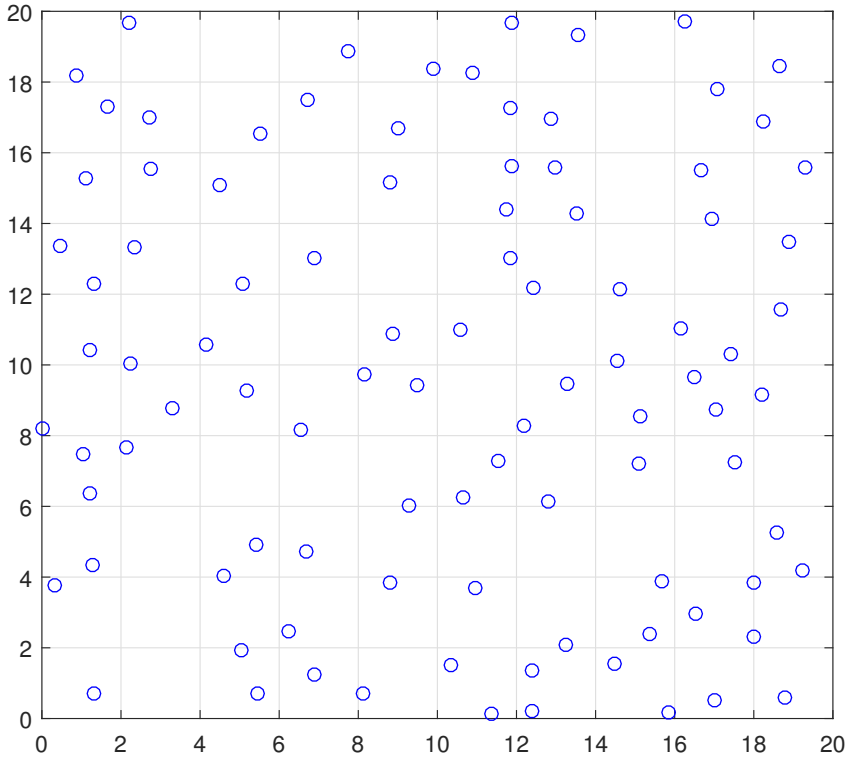

Figure 2.5: Hard-core point process.

The probability of a point being retained is the probability that it has no point of Φ_1 within distance r. It is given by

$$\lambda_{php} = \lambda_2 \exp(-\lambda_1 \pi r^2). \tag{2.2}$$

The application of the Poisson hole process can be applied to many wireless networks, such as ad-hoc networks and cognitive radio networks. An illustration of the Poisson hole process can be found in Figure 2.6.

2.3.7 Wireless Networks and Point Processes

Point processes in this thesis are collections of random points that reside in 2-dimensional spaces. Each point represents the location of one node (transmitter or receiver) in wireless networks in the real world. Figure 2.7[1] demonstrates the locations of the BSs in a central London area.

[1]Resource website: http://sitefinder.ofcom.org.uk/search

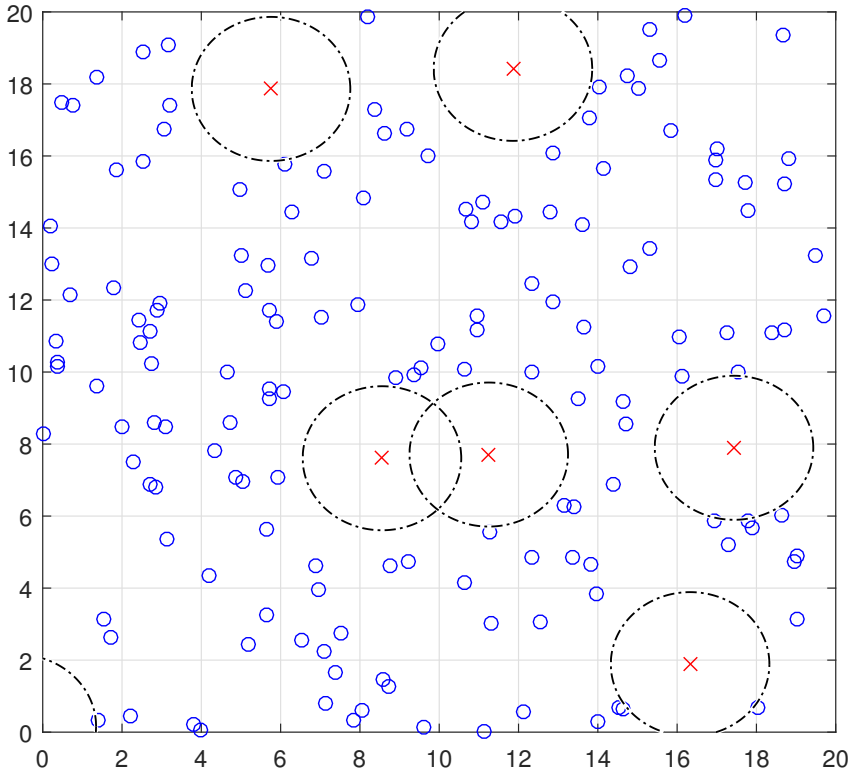

Figure 2.6: Poisson hole process.

As shown in the figure, the deployment of BSs in large cities such as London has a random allocation, rather than a deterministic pattern or lattice. Accordingly, it is rational to model the network of wireless users with stochastic geometry tools.

2.4 Physical Layer Security

2.4.1 Theory of Physical Layer Security

The basic idea of physical layer security is to use the inherent randomness of the physical medium and exploit the difference between the channel to a legitimate receiver and the channel to an eavesdropper to securely transmit confidential messages [5]. The theoretical basis for physical layer security is derived from the wire-tap channel model, and then includes a number of different information-theoretical metrics for security. Random

Figure 2.7: Locations of BSs near River Thames, central London.

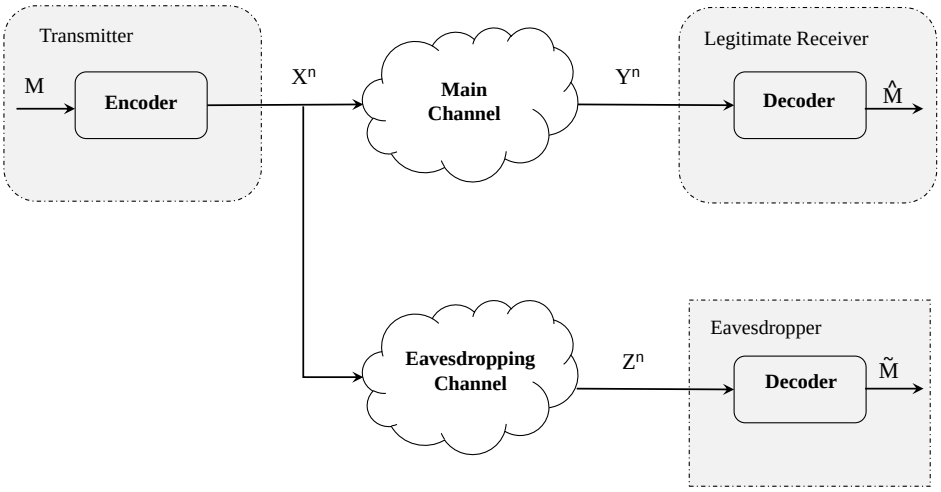

Figure 2.8: Wyner's wire-tap channel.

noise is an intrinsic element of almost all physical communication channels. In an effort to understand the role of noise in the context of secure communications, the wire-tap channel model was introduced by Wyner as illustrated in Figure 2.8 [6]. This model can be described as follows:

- the legitimate transmitter maps a message $\mathcal{M}$ into a codeword $\mathcal{X}^n$ consisting of n symbols, which is then transmitted through a wire-tap channel with a transition probability of $\mathbb{P}_{YZ|X}(\cdot|\cdot)$;
- the eavesdropper observes a noisy version, denoted by $\mathcal{Z}^n$, of the signal $\mathcal{Y}^n$ available at the legitimate receiver.

2.4.2 Performance Metric of Physical Layer Security

This subsection provides a brief overview of secrecy metrics to measure the performance of physical layer security in wireless networks, which are investigated in this thesis.

Secrecy Capacity

Like Shannon's capacity, the secrecy capacity is defined as the maximum achievable secrecy rate over all possible encoding-decoding schemes. The notion of the secrecy capacity was initiated in Wyner's seminal work [6], where a positive secrecy rate was first characterized for a degraded wire-tap channel, i.e., the eavesdropper's observation being a degraded version of the legitimate receiver's information.

Let a message $\mathcal{M}$ of length k be encoded into a codeword $\mathcal{X}^n$ of length n, and then transmitted. A legitimate receiver obtains $\mathcal{Y}^n$ over the main channel denoted Q_m, and an eavesdropper obtains $\mathcal{Z}^n$, a degraded version of $\mathcal{Y}^n$, through an additional channel called the wire-tap channel Q_w. Csiszár and Körner [8] generalized these results by removing the constraint of degraded channel, while still showed that $C_s > 0$, only if Q_m is less noisy than Q_w. These generalized the concept of wire-tap channel model and provided the expression of secrecy capacity as [8]

$$\begin{aligned} C_s &= \max_{p_X(x)} \mathbb{I}(X;Y|Z) \\ &= \max_{p_X(x)} (\mathbb{I}(X;Y) - \mathbb{I}(X;Z)) \\ &= \max_{p_X(x)} \mathbb{I}(X;Y) - \max_{p_X(x)} \mathbb{I}(X;Z) \\ &= C_l - C_e \end{aligned} \tag{2.3}$$

where C_l is the capacity of the main channel, and C_e is the capacity of the eavesdropping channel. Intuitively, the greater advantage in channel equality that a legitimate receiver can leverage over an eavesdropper, the higher the rate at which data can be encoded but remain secret.

When specifying the case of a single-input single-output (SISO) Gaussian wire-tap

channel, equation (2.3) can be further simplified as [7]

$$C_s = \Big[C_l(P) - C_e(P)\Big]^+ \tag{2.4}$$

where $[A]^+ = \max\{0, A\}$; P is the transmission power; $C_l(P)$ and $C_e(P)$ denote the (Shannon) channel capacities of the legitimate channel and the eavesdropping channel, respectively.

Ergodic Secrecy Capacity

The secrecy capacity/rate analysis requires the CSI of the eavesdropping channel, while in practice, the location of the eavesdroppers or even the presence of eavesdroppers is unknown. In the ergodic secrecy setting, it is assumed that the transmitter knows the channel information of the legitimate receiver, but is unaware of the eavesdropping channel. For analysis, the transmitter relies on the channel statistics information of the eavesdroppers. Reference [79] assumes that the legitimate and eavesdropping channels experience independent block fading, where the channel gains remain constant during each coherence interval and change independently from one coherence interval to the next. Under these assumptions, assuming unit noise power at both the legitimate receiver and the eavesdropper, when the transmitter knows the statistics of CSI for both the legitimate receiver and the eavesdropper, the ergodic secrecy capacity is given as follows [79]

$$C_s = \int_0^\infty \int_0^\infty \left[\log\left(1 + P g_l(x)\right) - \log\left(1 + P g_e(y)\right)\right] f_{g_l}(x) f_{g_e}(y) \mathrm{d}x \mathrm{d}y, \tag{2.5}$$

where $g_l(\cdot)$ and $g_e(\cdot)$ denote the channel gain of the legitimate and the eavesdropping channels, respectively.

Secrecy Outage Probability

The concept of secrecy outage probability was introduced in [10]. The fading assumption used in [10] is similar to [79], where the legitimate and eavesdropping channels experience independent block fading, and the channel gains remain quasi-static during

each coherence interval and change independently from one coherence interval to the next. If the transmitter knows the channel information of both the legitimate receiver and the eavesdropper, it can set the wire-tap code to transmit at a rate $R_s = [C_l - C_e]^+$. In such case, the legitimate receiver can receive the secret information at the rate R_s whereas Eve receives no information of it and hence the security is achieved. However, if the transmitter is unaware of the eavesdropping channel, then she can only rely on the CSI of the legitimate channel to send the secret message. If the transmitter transmits at an arbitrary rate R, then physical layer security is achieved only when $R \leq R_s$. For the case when $R > R_s$, the security of the link is compromised. Secrecy outage probability is an important system design guideline that can help the transmitter choose the wire-tap code rate R. The secrecy outage probability is defined as follows:

$$\mathbb{P}_{so}(R) = \mathbb{P}[R_s < R]. \tag{2.6}$$

Chapter 3

Security of Cognitive Radio Networks with Cooperative Jamming

3.1 Introduction

Cognitive radio networks have recently gained attention as a promising concept regarding the use of licensed frequencies more efficiently. A secondary (unlicensed) transmission system can access the resources of the primary system in an opportunistic manner when these are not used or when a threshold performance of the primary system can be guaranteed. Due to the open and dynamic nature of its architecture, the security in cognitive radio networks has attracted increased attentions in recent years [13–15, 80]. Various approaches such as secret key generation, multi-antenna transmission, CJ and cognitive relay are explored to defend against different eavesdropping attacks on the cognitive radio networks [81].

The relationship between the multi-antenna cognitive radio transmission problem and the secrecy transmission problem was developed in [13]. By using this relationship, the non-convex secrecy rate computation problem has also been transformed into a quasi-convex optimization problem for the multiple-input single-output (MISO) channel. The secrecy capacity of the MISO cognitive radio channel was studied in [14] where two numerical approaches were proposed to derive the optimal transmit covariance matrix. The first approach transferred the original quasi-convex problem into a single convex semidefinite program while the second one transferred the original quasi-convex problem into a sequence of optimization problems which helps to prove that beamforming is the optimal strategy for the secure MISO cognitive radio channel. With a confidential

message, a single-letter expression for the capacity-equivocation region was developed in [82] in the case of a discrete memoryless cognitive interference channel. The problem of optimal robust transmitter design was addressed in [15] for a MISO cognitive radio network in order to maximize the achievable secrecy rate region for the secondary user, keeping the interference at the primary receiver under a certain threshold. The secrecy capacity of a cognitive radio network with multiple primary users, secondary users and eavesdroppers was studied in [83] based on stochastic distributions.

Moreover, CJ also becomes a promising technique to enhance physical layer security in wireless networks, i.e., the artificial noise is generated by the cooperative transmitter(s) to confuse the eavesdroppers [20–24]. In [21], CJ was adopted to increase the achievable sum rate of a Gaussian multiple-access wire-tap channel and a Gaussian two-way wire-tap channel. The secrecy rate of a relay-assisted CJ scheme consisting a transmitter, a receiver and an eavesdropper was studied in [22] and showed that a CJ scheme can significantly increase the secrecy rate of the wire-tap channel. To increase the physical layer security of fading channels via distributed relays, the combination of CJ with convex optimization and one-dimensional search was investigated in [23]. Partial and full CJ strategies with linear precoding were later developed in [24] to enhance the secrecy rate of two-hop relay channels, where single or multiple data streams are transmitted with decoding-and-forwarding (DF) relays. The robust transmission schemes with multiple antennas were analyzed in [16, 26, 84, 85] with CJ to enhance the security. In [16], CJ was also designed to increase the worst-case secrecy rate and to degrade the SINR at eavesdropper for both individual and global power constraint.

Given the availability of multiple relays, cooperative communication is also a promising approach to achieve significant secrecy improvement [22–24] and [86–91]. In [22], multiple cooperating relays were investigated to address the secure communications of a source-destination pair with three cooperative schemes, i.e. decode-and-forward (DF), amplify-and-forward (AF), and CJ. Secure communication with MIMO relay networks was analyzed in [24] with linear precoding and the generalized singular value decomposition (GSVD) schemes, to increase the secrecy rate. To explore the benefits of wireless networks with multiple relays, the relay selection approaches were proposed to carry out CJ, AF or DF in [86] and [87]. The secrecy outage probabilities of different

transmission relay selection policies were analyzed to characterize the impact of the proposed policy and the interference power constraint. The joint relay and jammer selection was also investigated in [90] and [91]. In [90], the selection vector was designed to minimize the secrecy outage probability, while the study in [91] introduced several new concepts such as the reliable-and-secure connection probability and the effective secrecy throughput to characterize the security in the face of delayed CSI feedback.

In this chapter, we study the CJ scheme to enhance the physical layer security of cognitive radio networks where both primary and secondary users are allowed to transmit information simultaneously under the assumption that the CSI of eavesdropper may or may not present. According to two different settings of the cognitive radio networks, this chapter is separated into two sections. The first section mainly addresses the following aspects: i) The loss of secrecy rate of secondary user due to interference is quantified while controlling interference from secondary transmitter to primary receiver under a certain constraint. ii) A CJ scheme is developed for a cognitive radio network that will increase the secrecy rate of both primary and secondary transmissions without creating any interference to their receivers. iii) Two precoding strategies are proposed to obtain optimum secrecy rate with full CSI and partial CSI. The content of the second section includes: i) We use multiple relays to create jamming noise in the direction of eavesdropper and develop an algorithm to find the minimum number of effective relays to meet the target secrecy rate at SR. ii) We minimize the secondary transmit power with a secrecy rate constraint keeping interference at the PR under a certain threshold.

The remainder of this chapter is organized as follows. Section 3.2 presents a general system model and a brief introduction of the cognitive radio network. Section 3.3 proposes the combined approach of cooperative jamming and beamforming. Section 3.4 further investigates the scenario with multiple relays by applying relay selection. A summary is given in Section 3.5.

3.2 System Model

We first consider a cognitive radio network with a PU, a SU, a PR, a SR, an eavesdropper E and a cognitive relay with multiple antennas, as depicted in Figure 3.1. PU, PR, CR and SR are equipped with N_A, N_a, N_r and N_b antennas, respectively, while SU and E are equipped with a single antenna. The eavesdropper is assumed to be passive so that the source information is interpreted by the eavesdropper without modifying it. In the partial CSI scenario, the channel information of eavesdropper is unavailable, while other channel information can be obtained for both the primary and secondary users. The direct channel coefficient between SU and SR is $\mathbf{h}_{ss} \in \mathbb{C}^{N_b \times 1}$, while the cross-over channel coefficient between PU and SR is $\mathbf{H}_{sp} \in \mathbb{C}^{N_b \times N_A}$ and that between SU and PR is $\mathbf{h}_{ps} \in \mathbb{C}^{N_a \times 1}$. The channel coefficient between PU and E is $\mathbf{h}_{ep} \in \mathbb{C}^{1 \times N_A}$ and that between SU and E is h_{es}. The transmission channel between PU and PR is $\mathbf{H}_{pp} \in \mathbb{C}^{N_a \times N_A}$. All the channels are assumed to be Rayleigh fading. PU and SU transmit independent signals x_p and x_s to the PR and SR, respectively. Correspondingly, their transmission powers are allocated as $\mathbb{E}(|x_p|^2) = P_p$, $\mathbb{E}(|x_s|^2) = P_s$ and the power for cooperative jamming is $\mathbb{E}(|z|^2) = P_r$ where z is the jamming signal. The total power is P_o, so that $P_o = P_p + P_s + P_r$. At first, we discuss a benchmark scheme without cooperation, i.e., direct transmission to quantify the loss of secrecy rate at SR denoted by R_s due to effect of interferences. Then, we discuss the CJ schemes according to different configurations of relays and quantify the improvement in the secrecy rate of SR due to the combined approach of CJ with beamforming and relay selection, respectively.

3.3 Combined Approach of Cooperative Jamming and Beamforming

In this section, at first, we quantify the loss in R_s due to the effect of interference in the case of direct transmission. Then, we quantify the improvement in R_s due to the CJ scheme by keeping the interference at the PR under a certain threshold.

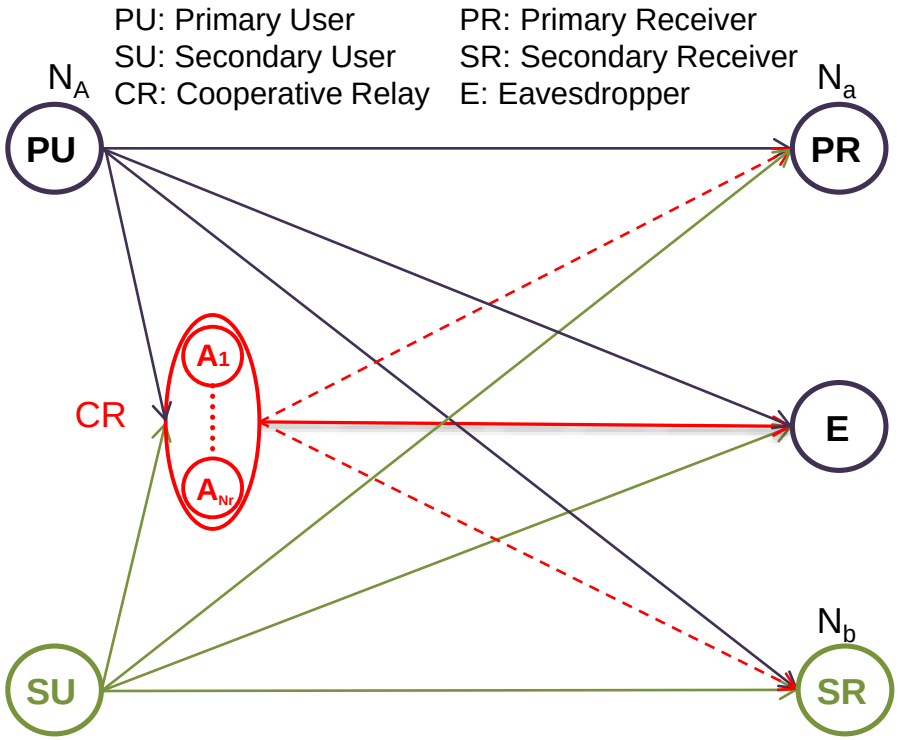

Figure 3.1: Securing cognitive radio with CJ

3.3.1 Direct Transmission

When both the PU and SU transmit simultaneously, PR and SR experience interference due to the signals of SU and PU, respectively, but E experiences interference from both the PU's and SU's signals. The powers assigned to PU and SU are denoted by P_p and P_s, respectively. Therefore, received signals at the PR, SR and E are given by

$$\begin{aligned} \mathbf{y}_p &= \mathbf{H}_{pp}\mathbf{x}_p + \mathbf{h}_{ps}x_s + \mathbf{n}_p, \\ \mathbf{y}_s &= \mathbf{h}_{ss}x_s + \mathbf{H}_{sp}\mathbf{x}_p + \mathbf{n}_s, \\ y_e &= \mathbf{h}_{ep}\mathbf{x}_p + h_{es}x_s + n_e, \end{aligned} \tag{3.1}$$

where $\mathbf{n}_p \sim \mathcal{CN}(0, \sigma_s^2\mathbf{I}_{N_a})$, $\mathbf{n}_s \sim \mathcal{CN}(0, \sigma_s^2\mathbf{I}_{N_b})$ and $n_e \sim \mathcal{CN}(0, \sigma_e^2)$ denote the Gaussian noises imposed on SR and E, respectively.

From (3.1), the rate at the SR is given by [22]

$$C_{sl} = \log_2\left(1 + \frac{P_s\|\mathbf{h}_{ss}\|^2}{P_p\|\mathbf{H}_{sp}\boldsymbol{\mu}\|^2 + \sigma_s^2}\right), \tag{3.2}$$

where $\boldsymbol{\mu} \in \mathbb{C}^{N_A \times 1}$ is a precoding vector of the primary transmission. Similarly, the rate at the eavesdropper is derived by

$$C_{se} = \log_2 \left(1 + \frac{P_s |h_{es}|^2}{P_p \|\mathbf{h}_{ep}\|^2 + \sigma_e^2} \right). \tag{3.3}$$

According to (2.4), the secrecy capacity at the SR is expressed by

$$\begin{aligned} R_{sd} &= \left[\log_2(1 + \frac{P_s \|\mathbf{h}_{ss}\|^2}{P_p \|\mathbf{H}_{sp}\boldsymbol{\mu}\|^2 + \sigma_s^2}) - \log_2(1 + \frac{P_s |h_{es}|^2}{P_p \|\mathbf{h}_{ep}\|^2 + \sigma_e^2}) \right]^+ \\ &= \left[\log_2 \left(\frac{a \left(P_p \parallel \mathbf{h}_{ep} \|^2 + \sigma_e^2 \right)}{b \left(P_p \parallel \mathbf{H}_{sp}\boldsymbol{\mu} \|^2 + \sigma_s^2 \right)} \right) \right]^+ \end{aligned} \tag{3.4}$$

where $a = P_p \parallel \mathbf{H}_{sp}\boldsymbol{\mu}\|^2 + P_s \parallel \mathbf{h}_{ss}\|^2 + \sigma_s^2$ and $b = P_p \|\mathbf{h}_{ep}\|^2 + P_s |h_{es}|^2 + \sigma_e^2$. If there is no interference, the secrecy rate at the SR is given by

$$R_{s_{\max}} = \left[\log_2 \left(\frac{\sigma_e^2 \left(P_s \parallel \mathbf{h}_{ss} \|^2 + \sigma_s^2 \right)}{\sigma_s^2 \left(P_s |h_{es}|^2 + \sigma_e^2 \right)} \right) \right]^+. \tag{3.5}$$

Therefore, the loss of secrecy rate at SR due to the effect of interference created by the PU's information signals is given by

$$\begin{aligned} R_{s_{\text{loss}}} =& R_{s_{\max}} - R_{sd} \\ =& \left[\log_2 \left(\frac{b\sigma_e^2 \left(P_s \parallel \mathbf{h}_{ss} \|^2 + \sigma_s^2 \right) \left(P_p \parallel \mathbf{H}_{sp}\boldsymbol{\mu} \|^2 + \sigma_s^2 \right)}{a\sigma_s^2 \left(P_s |\mathbf{h}_{es}|^2 + \sigma_e^2 \right) \left(P_p \parallel \mathbf{H}_{ep}\boldsymbol{\mu} \|^2 + \sigma_e^2 \right)} \right) \right]^+. \end{aligned} \tag{3.6}$$

Consequently, the loss of secrecy rate will be affected by the channel fading, transmission powers at the transmitters and the noises at the receivers. Numerical result for the loss caused by interference will be further illustrated in Figure 3.6.

3.3.2 Cooperative Jamming

The cognitive relay transmits a weighted jamming signal z which is independent of the signals transmitted by the PU and SU with the purpose of confusing the eavesdropper. Besides, the cooperative artificial noise would be orthogonal to both the primary

and secondary information signal, i.e, generating no interference to both primary and secondary transmission. We proposed a beamforming scheme to cancel the jamming interference. The precoding vector for PU, SU and cooperative relay are denoted by $\mathbf{v}_p$, v_s and $\mathbf{w}$ respectively, with $\mathbf{v}_p^\dagger \mathbf{v}_p = 1$, $v_s^\dagger v_s = 1$, and $\mathbf{w}^\dagger \mathbf{w} = 1$. where, † denotes Hermitian transposition. Therefore, received signals at the PR, SR and E are given by

$$\mathbf{y}_p = \mathbf{H}_{pp}\mathbf{v}_p x_p + \mathbf{h}_{ps} v_s x_s + \mathbf{H}_{pr}\mathbf{w} z + \mathbf{n}_p, \tag{3.7}$$

$$\mathbf{y}_s = \mathbf{h}_{ss} v_s x_s + \mathbf{H}_{sp}\mathbf{v}_p x_p + \mathbf{H}_{sr}\mathbf{w} z + \mathbf{n}_s, \tag{3.8}$$

$$y_e = \mathbf{h}_{ep}\mathbf{v}_p x_p + h_{es} v_s x_s + \mathbf{h}_{er}\mathbf{w} z + n_e, \tag{3.9}$$

where $\mathbf{H}_{pr} \in \mathbb{C}^{N_a \times N_r}$, $\mathbf{H}_{sr} \in \mathbb{C}^{N_b \times N_r}$ and $\mathbf{h}_{er} \in \mathbb{C}^{1 \times N_r}$ represent channel coefficients from cognitive relay to PR, SR and E, respectively. Receivers use beamforming vectors to cancel the jamming interferences. We assume that primary and secondary channel information are unavailable for eavesdropper. Studies about the secrecy capacity in cognitive scenarios where an eavesdropper knows about the CSI would be considered in future research. The optimal beamforming scheme of an eavesdropper in the case where the eavesdropper knows about the CSI of primary and secondary transmission will be given in following discussion. The signals after beamforming can be expressed as

$$\widehat{\mathbf{y}}_p = \mathbf{u}_p^\dagger(\mathbf{H}_{pp}\mathbf{v}_p x_p + \mathbf{h}_{ps} v_s x_s + \mathbf{H}_{pr}\mathbf{w} z + \mathbf{n}_p), \tag{3.10}$$

$$\widehat{\mathbf{y}}_s = \mathbf{u}_s^\dagger(\mathbf{h}_{ss} v_s x_s + \mathbf{H}_{sp}\mathbf{v}_p x_p + \mathbf{H}_{sr}\mathbf{w} z + \mathbf{n}_s), \tag{3.11}$$

$$\widehat{y}_e = \mathbf{h}_{ep}\mathbf{v}_p x_p + h_{es} v_s x_s + \mathbf{h}_{er}\mathbf{w} z + n_e. \tag{3.12}$$

The resulting SINRs available for primary receiver, secondary receiver and eavesdropper are given as

$$\text{SINR}_p = \frac{P_p \mid \mathbf{u}_p^\dagger \mathbf{H}_{pp}\mathbf{v}_p \mid^2}{\mathbf{u}_p^\dagger(P_s \mathbf{h}_{ps} Q_s \mathbf{h}_{ps}^\dagger + P_r \mathbf{H}_{pr}\mathbf{Q}_\mathbf{w}\mathbf{H}_{pr}^\dagger + \sigma_p^2 \mathbf{I}_{N_a})\mathbf{u}_p}, \tag{3.13}$$

$$\text{SINR}_s = \frac{P_s \mid \mathbf{u}_s^\dagger \mathbf{h}_{ss} v_s \mid^2}{\mathbf{u}_s^\dagger(P_p \mathbf{H}_{sp}\mathbf{Q}_p\mathbf{H}_{sp}^\dagger + P_r \mathbf{H}_{sr}\mathbf{Q}_\mathbf{w}\mathbf{H}_{sr}^\dagger + \sigma_s^2 \mathbf{I}_{N_b})\mathbf{u}_s}, \tag{3.14}$$

$$\text{SINR}_{ep} = \frac{P_p \mid \mathbf{h}_{ep}\mathbf{v}_p \mid^2}{P_s \mid h_{es} v_s \mid^2 + P_r \mid \mathbf{h}_{er}\mathbf{w} \mid^2 + \sigma_e^2}, \tag{3.15}$$

$$\text{SINR}_{es} = \frac{P_s \mid h_{es} v_s \mid^2}{P_p \mid \mathbf{h}_{ep}\mathbf{v}_p \mid^2 + P_r \mid \mathbf{h}_{er}\mathbf{w} \mid^2 + \sigma_e^2}, \tag{3.16}$$

where $\mathbf{Q}_p = \mathbf{v}_p\mathbf{v}_p^\dagger$, $Q_s = v_s v_s^\dagger$, $\mathbf{Q_w} = \mathbf{w}\mathbf{w}^\dagger$. Here, $\mathbf{u}_p = \mathbf{H}_{pp}\mathbf{v}_p$ and $\mathbf{u}_s = \mathbf{h}_{ss}v_s$ are beamforming vectors of primary and secondary receivers to maximize the signal power and cancel interference from cooperative jamming. For the scenario where the eavesdropper is aware of primary and secondary transmission CSI, maximizing the SINR at eavesdropper is a generalized eigenvector problem [22]. The optimum beamforming vector for the eavesdropper is

$$\mathbf{u}_e = (P_s\mathbf{h}_{es}Q_s\mathbf{h}_{es}^\dagger + P_r\mathbf{h}_{er}\mathbf{Q_w}\mathbf{h}_{er}^\dagger + \sigma_e^2\mathbf{I})^{-1}\mathbf{h}_{ep}\mathbf{v}_p,$$

when its target is primary information signal or

$$\mathbf{u}_e = (P_p\mathbf{h}_{ep}\mathbf{Q_p}\mathbf{h}_{ep}^\dagger + P_r\mathbf{h}_{er}\mathbf{Q_w}\mathbf{h}_{er}^\dagger + \sigma_e^2\mathbf{I})^{-1}\mathbf{h}_{es}\mathbf{v}_s,$$

when its target is secondary information signal.

With total power constraint, we use part of the source power to transmit information signals and use the remaining power for cooperative jamming. Power allocations are optimized to maximize the secrecy rate at SR.

In this research, we assume that primary power limit P_p is fixed and given. To maximize the secrecy rate, the right singular vector $\mathbf{v}_p$ of $\mathbf{H}_{pp}$ with the largest singular value is chosen as the precoding vector for the primary transmission. For the secondary user, we choose v_s for precoding. In our design, we aim at transmitting primary resource and secondary resource according to the waterfilling principle and arranging extra power for cooperative jamming that will not generate any interference to the primary or secondary receiver, that is, using ZF to cancel cooperative jamming at PR and SR. Even though the optimal CJ has been investigated in point to point transmission, the models are solved by the combination of a suboptimal problem and a one-dimensional search [23], or the Newton method [92]. As optimal relay weights are intractable and difficult to obtain, we consider the suboptimal constraint of ZF [22] [24], i.e., for CJ, the jamming signal is completely nulled out at the destination. Then, the precoding vectors should meet the following requirements

$$\mathbf{H}_{pp}\mathbf{v}_p \perp \mathbf{H}_{pr}\mathbf{w}, \tag{3.17}$$

$$\mathbf{h}_{ss} v_s \perp \mathbf{H}_{sr}\mathbf{w}. \tag{3.18}$$

As $\mathbf{v}_p$ is the singular vector corresponding to the largest singular value of $\mathbf{H}_{pp}$, $\mathbf{H}_{pr}\mathbf{w}$ can be expressed by a linear combination of $N_A - 1$ right singular vectors of $\mathbf{H}_{pp}$ with smaller singular values. We define

$$\mathbf{H}_{pr}\mathbf{w} = \mathbf{T}\boldsymbol{\lambda}, \tag{3.19}$$

where $\mathbf{T} = [\mathbf{v}_2\ \mathbf{v}_3\ \dots\ \mathbf{v}_{N_A}]$, in which $\mathbf{v}_i$ is the i_{th} orthogonal vector corresponding to the i_{th} eigenvector of $\mathbf{H}_{pp}$, $\|\mathbf{v}_i\|^2 = 1$ and $\mathbf{v}_i^\dagger \mathbf{v}_j = 0\ (i \neq j)$, $i, j \in \{2, 3, \cdots, N_A\}$. $\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \dots, \lambda_{N_A-1})^\dagger \in \mathbb{C}^{(N_A-1)\times 1}$ is the linear combining coefficient vector. Notice that $\mathbf{T}$ is obtained from $\mathbf{H}_{pp}$ by first using eigen decomposition to obtain the space of eigenvectors and then using QR decomposition to acquire orthogonal basis to represent the orthogonal subspace of the other $N_A - 1$ eigenvectors of $\mathbf{H}_{pp}$ using Algorithm 3.3.1.

Algorithm 3.3.1: CJ precoding vector design

1 : **Input:** $\mathbf{H}_{pp}, \mathbf{H}_{pr}, \boldsymbol{\lambda}$.
2 : **begin**
3 : Calculate eigen decomposition of $\mathbf{H}_{pp}$, $[\mathbf{V}, \mathbf{D}] = eig(\mathbf{H}_{pp})$, producing matrices of eigenvalues $\mathbf{D}$ and eigenvectors $\mathbf{V}$ of $\mathbf{H}_{pp}$.
4 : Fetch precoding vector $\mathbf{v}_p$, the first column of $\mathbf{V}$.
5 : Calculate QR decomposition of $\mathbf{V}$, $[\mathbf{Q}, \mathbf{R}] = qr(\mathbf{V})$, producing orthogonal unitary matric $\mathbf{Q}$ and upper triangular matrix $\mathbf{R}$.
6 : $\mathbf{T} = \left[\mathbf{Q}_{i,j}\right], i \neq 1$, $\mathbf{Q}_{i,j}$ denotes an element of $\mathbf{Q}$.
7 : $\mathbf{w} = \mathbf{H}_{pr}^{-1}\mathbf{T}\boldsymbol{\lambda}$.
8 : **end**
9 : **Output:** $\mathbf{v}_p, \mathbf{w}, \mathbf{T}$.

For the case that $N_a \neq N_r$, $\mathbf{H}_{pr}$ is not a square matrix. We use a zero-forcing equalizer $\left(\mathbf{H}_{pr}^\dagger \mathbf{H}_{pr}\right)^{-1} \mathbf{H}_{pr}^\dagger$ [93] instead of $\mathbf{H}_{pr}^{-1}$ in the algorithm to search for $\mathbf{w}$ to achieve orthogonal conditions in (3.17) and (3.18). For requirement (3.18), $\mathbf{w}$ should meet the following constraint:

$$(\mathbf{H}_{sr}\mathbf{w})^\dagger \mathbf{h}_{ss} v_s = 0, \text{ then} \tag{3.20}$$

$$\boldsymbol{\lambda}^\dagger \mathbf{T}^\dagger (\mathbf{H}_{pr}{}^{-1})^\dagger \mathbf{H}_{sr}^\dagger \mathbf{h}_{ss} v_s = 0. \tag{3.21}$$

As a result, $\mathbf{w}$ obtained from equation (3.21) will automatically achieve the criterion of

(3.17) and (3.18), i.e., generating no jamming interference to the primary and secondary receiver.

3.3.3 Known CSI of Eavesdropper

When the CSI of eavesdropper is known, we try to align cooperative jamming power along the largest eigenvalue direction of channel $\mathbf{h}_{er}$ using a Minimum Mean Square Error (MMSE) criterion while keeping the jamming signal orthogonal to primary and secondary information signal, resulting in

$$\begin{aligned} &\min_{\mathbf{w},\boldsymbol{\lambda}} \|\mathbf{h}_{er}^{\dagger} - \mathbf{w}\|_F^2 \\ &s.t.\ \mathbf{w} = {\mathbf{H}_{pr}}^{-1}\mathbf{T}\boldsymbol{\lambda},\ \ \mathbf{w}^{\dagger}\mathbf{w} \leq 1, \\ &\quad \boldsymbol{\lambda}^{\dagger}\mathbf{T}^{\dagger}({\mathbf{H}_{pr}}^{-1})^{\dagger}{\mathbf{H}_{sr}}^{\dagger}\mathbf{h}_{ss}v_s = 0. \end{aligned} \tag{3.22}$$

As the objective function and constraints are convex, the optimum value of $\mathbf{w}$ and $\boldsymbol{\lambda}$ in the minimization problem (3.22) is easy to solve using convex optimization, denoted by $\mathbf{w}^*$ and $\boldsymbol{\lambda}^*$. Define $\mathbf{Q}_{\mathbf{w}}^1 = \mathbf{w}^*\mathbf{w}^{*\dagger}$. Substitute $\mathbf{w}^*$ and $\mathbf{Q}_{\mathbf{w}}^1$ into (3.14) and (3.16), the secrecy rate of secondary user is given by

$$\begin{aligned} R_s &= [\ \log_2(1+\text{SINR}_s) - \log_2(1+\text{SINR}_{es})\ ]^+ \\ &= \left[\log_2\left(1 + \frac{P_s \mid \mathbf{u}_s^{\dagger}\mathbf{h}_{ss}v_s \mid^2}{\mathbf{u}_s^{\dagger}(P_p\mathbf{H}_{sp}\mathbf{Q}_p\mathbf{H}_{sp}^{\dagger} + P_r\mathbf{H}_{sr}\mathbf{Q}_{\mathbf{w}}^1\mathbf{H}_{sr}^{\dagger} + \sigma_s^2\mathbf{I}_{N_b})\mathbf{u}_s}\right)\right. \\ &\quad \left. - \log_2\left(1 + \frac{P_s \mid h_{es}v_s \mid^2}{P_p \mid \mathbf{h}_{ep}\mathbf{v}_p \mid^2 + P_r \mid \mathbf{h}_{er}\mathbf{w}^* \mid^2 + \sigma_e^2}\right)\right]^+ \\ &= \left[\log_2\left(\frac{b_2P_s^2 + b_1P_s + a_0}{c_1P_s + a_0}\right)\right]^+, \end{aligned} \tag{3.23}$$

where $a_0 = P_p|\mathbf{h}_{ep}\mathbf{v}_p|^2 + (P_0 - P_p)|\mathbf{h}_{er}\mathbf{w}^*|^2 + \sigma_e^2$, $a_1 = \frac{|\mathbf{u}_s^{\dagger}\mathbf{u}_s|^2}{P_p\mathbf{u}_s^{\dagger}\mathbf{H}_{sp}\mathbf{Q}_p\mathbf{H}_{sp}^{\dagger}\mathbf{u}_s + \sigma_s^2|\mathbf{u}_s^{\dagger}\mathbf{u}_s|}$,
$b_1 = a_1a_0 - |\mathbf{h}_{er}\mathbf{w}^*|^2$, $b_2 = -a_1|\mathbf{h}_{er}\mathbf{w}^*|^2$ and $c_1 = \|\mathbf{h}_{es}\|^2 - |\mathbf{h}_{er}\mathbf{w}^*|^2$.

For the cognitive network, we assume an interference constraint Γ_m on the secondary transmission to keep the PR in a certain interference temperature. As transmission power

for PR is given, its maximum secrecy rate would be fixed in a certain interference temperature Γ_m. Here, we mainly consider enhancing the security of the secondary transmission by optimizing the transmission power allocation between information and jamming signals. Secrecy rate maximization of secondary transmission is given by

$$\begin{aligned} \max_{P_s} \ & \left[\log_2\left(\frac{b_2 P_s^2 + b_1 P_s + a_0}{c_1 P_s + a_0}\right)\right]^+ \\ s.t. \ & 0 \le P_s \le P_0 - P_p, \\ & P_s \mathbf{u}_p{}^\dagger \mathbf{H}_{ps} \mathbf{Q}_s \mathbf{H}_{ps}^\dagger \mathbf{u}_p \le \Gamma_m. \end{aligned} \tag{3.24}$$

3.3.4 Unknown CSI of Eavesdropper

When the CSI of eavesdropper is unknown, the optimum choice is to first meet a fixed target rate for the secondary transmission, and then allocate the remaining power for jamming signal along the whole spatial dimensions that will not generate any interference to PR and SR. These targets can be achieved by searching for the precoding vector **w** for relay fulfilling the orthogonal conditions of (3.20) and (3.22). Rewrite (3.22) as

$$\boldsymbol{\lambda}^\dagger \boldsymbol{\eta} = 0, \tag{3.25}$$

where $\boldsymbol{\eta} = \frac{\mathbf{T}^\dagger (\mathbf{H}_{pr}{}^{-1})^\dagger \mathbf{H}_{sr}^\dagger \mathbf{h}_{ss} v_s}{\|\mathbf{T}^\dagger (\mathbf{H}_{pr}{}^{-1})^\dagger \mathbf{H}_{sr}^\dagger \mathbf{h}_{ss} v_s\|}$, $\boldsymbol{\eta} \in \mathbb{C}^{(N_A-1)\times 1}$. Define

$$\boldsymbol{\Omega} = nullspace(\boldsymbol{\eta}),$$

where $\boldsymbol{\Omega} = \{ [\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_{N_A-2}] \mid \|\mathbf{e}_i\|^2 = 1, i = \{1, 2, \cdots N_A - 2\}\}$ is a $(N_A - 1) \times (N_A - 2)$ matrix, denoting the null space of $\boldsymbol{\eta}$. Uniformly distributing jamming power along the nullspace of $\boldsymbol{\eta}$, we obtain

$$\boldsymbol{\lambda}\boldsymbol{\lambda}^\dagger = \frac{1}{N_A - 2} \boldsymbol{\Omega}\boldsymbol{\Omega}^\dagger. \tag{3.26}$$

Notice that the coefficient $\frac{1}{N_A-2}$ is chosen to maintain the power constraint of cooperative jamming. Then

$$\begin{aligned}\mathbf{Q}_{\mathbf{w}}^2 &= \mathbf{w}\mathbf{w}^\dagger = {\mathbf{H}_{pr}}^{-1}\mathbf{T}\boldsymbol{\lambda}\boldsymbol{\lambda}^\dagger \left({\mathbf{H}_{pr}}^{-1}\mathbf{T}\right)^\dagger \\ &= \frac{1}{N_A-2}{\mathbf{H}_{pr}}^{-1}\mathbf{T}\boldsymbol{\Omega}\boldsymbol{\Omega}^\dagger \left({\mathbf{H}_{pr}}^{-1}\mathbf{T}\right)^\dagger . \end{aligned} \tag{3.27}$$

Substitute expressions (3.14), (3.16) and (3.27) into expression

$$\begin{aligned} R_s =& [\, \log_2(1+\text{SINR}_s) - \log_2(1+\text{SINR}_{es}) \,]^+ \\ =& \left[\log_2\left(1+\frac{P_s \mid \mathbf{u}_s^\dagger \mathbf{h}_{ss} v_s \mid^2}{\mathbf{u}_s^\dagger(P_p\mathbf{H}_{sp}\mathbf{Q}_p\mathbf{H}_{sp}^\dagger + P_r\mathbf{H}_{sr}\mathbf{Q}_{\mathbf{w}}^2\mathbf{H}_{sr}^\dagger + \sigma_s^2\mathbf{I})\mathbf{u}_s}\right)\right. \\ & \left. - \log_2\left(1+\frac{P_s \mid h_{es} v_s \mid^2}{P_p \mid \mathbf{h}_{ep}\mathbf{v}_p \mid^2 + P_r \mid \mathbf{h}_{er}\mathbf{w}^* \mid^2 + \sigma_e^2}\right)\right]^+, \end{aligned} \tag{3.28}$$

we obtain the secrecy rate of the secondary transmission. Notice that, the channel information of the eavesdropper is unknown, and here a random channel coefficient value is generated for investigating the possible secrecy rate. Theoretically, the secrecy rate of primary transmission would also be increased as the jamming will only degrade the QoS of the eavesdropper. On the one hand, due to the unknown channel information of the eavesdropper, secrecy rate maximization for secondary transmission is also unavailable, while on the other hand, this approach still enhances the secrecy rate of the cognitive system.

3.3.5 Numerical Results

We used Monte Carol method to statistically test the system performance and all results are tested based on 10000 independent trials. In the simulation, all the channel coefficients are assumed to be i.i.d complex Gaussian. Two scenarios are considered. In the first scenario where the SINR at primary receiver, secondary receiver and eavesdropper and the secrecy rate at secondary receiver are considered, the CSI of the eavesdropper is known. In the second one where this parameter is unknown, i.e., partial CSI, the metric is secrecy rate at secondary receiver with a random CSI of the eavesdropper. The transmit power

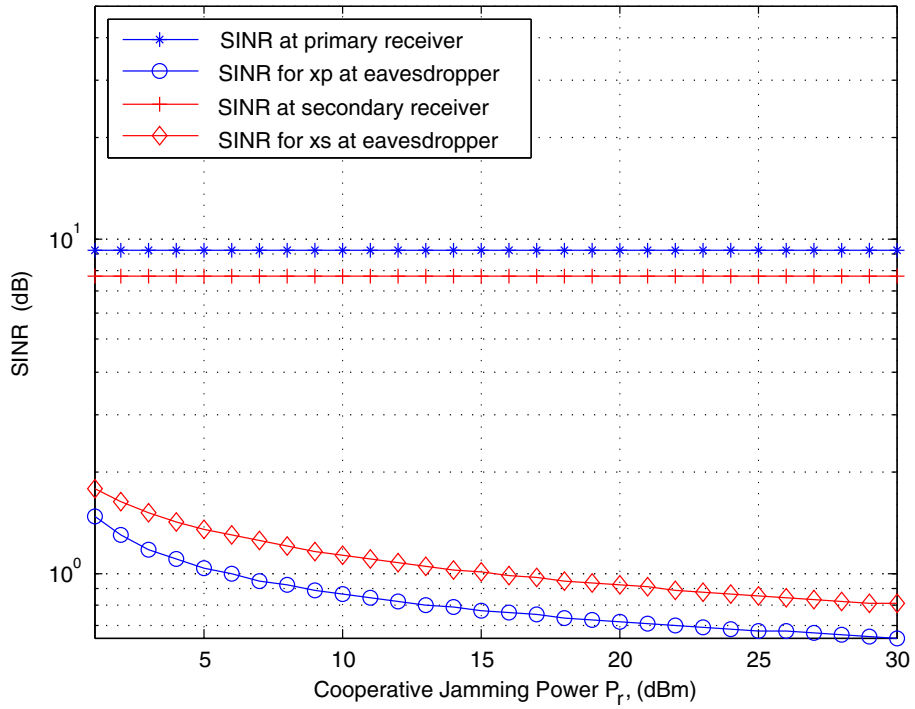

Figure 3.2: The SINR at PR, SR and E, as a function of cooperative jamming power P_r with $P_p = 10$dBm and $P_s = 10$dBm.

at the PU is $P_p = 10$dBm. The noises experienced at PR, SR and the eavesdropper are the same and given as $\sigma_p^2 = \sigma_s^2 = \sigma_e^2 = 1$dBm. The number of antennas are given as $N_A = 5, N_a = 5, N_r = 5, N_e = 1, N_B = 1$, and $N_b = 4$.

Figure 3.2 shows the impact of cooperative jamming on the SINR at the PR, the SR and the eavesdropper in the scenario with $P_s = 10$dBm. In this scenario, the primary and secondary transmission power are fixed while the SINR is investigated as a function of the power of cooperative jamming with the CSI of eavesdropper available. Results in Figure 3.2 show that when increasing the power of cooperative jamming, both the SINRs of the primary and secondary receiver are not affected. However, both the SINRs of the primary and secondary signal at the eavesdropper are degraded which lead to increasing the secrecy capacity at the primary and secondary receiver. Note that, we analyze the SINR rather than the secrecy capacity to show an underlying cause of security performance improvement. As shown in Figure 3.2, there exist gaps between the SINRs at the legitimate receiver and that at the eavesdropper. The differences are due to the application of precoding at the transmitters which is aimed at enhancing the legitimate transmission.

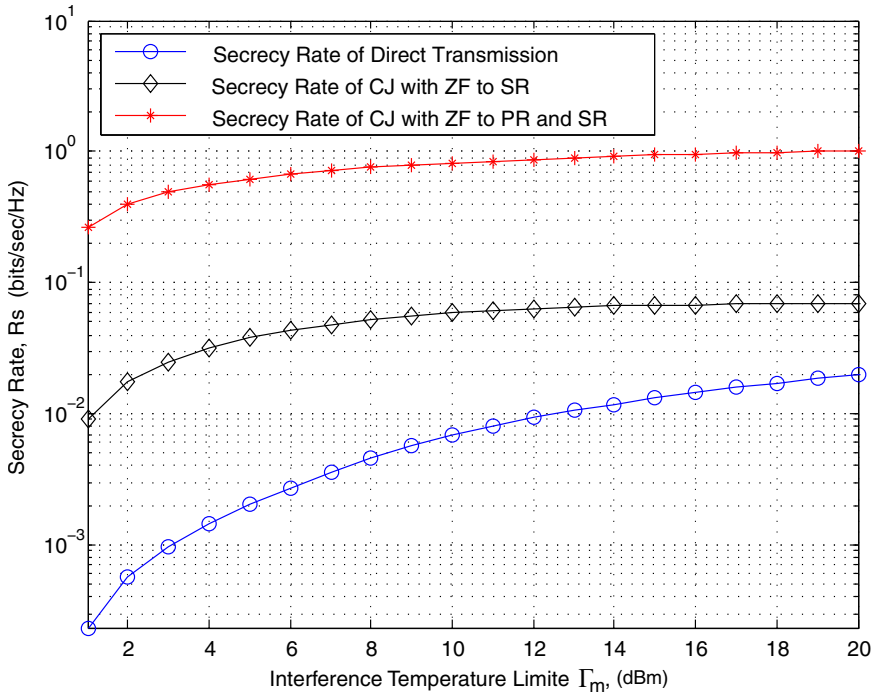

Figure 3.3: The secrecy rate, R_s, as a function of interference constraint Γ_m with $P_o = 40$dBm and $P_p = 10$dBm.

Figure 3.3 shows the secrecy rate R_s as a function of interference temperature limit Γ_m with $P_o = 40$dBm. The power allocation between P_r and P_s is optimized to achieve maximum secrecy rate at SR. The results are based on the assumption that the CSI of the eavesdropper is known. According to Figure 3.3, the secrecy rate of the scheme using CJ with ZF only to SR is larger than direct transmission, while smaller than the scheme using a well-designed CJ scheme with ZF to both primary and secondary receivers. All the secrecy rates of the three schemes are zero when the interference constraint at the primary receiver is zero. Note that these points in the figure are not shown as we use the function of semilogy for description.

Figure 3.4 investigated the impact of CJ on the secrecy rate at the SR in the scenario with partial CSI. The CSI of the eavesdropper is generated randomly without being used for optimizing the cooperative communication. The secrecy rate R_s is considered as a function of the jamming power P_r and the transmission power at the SR is assumed to be fix, i.e., $P_s = 10$dBm. As shown in Figure 3.4, even though the CSI of eavesdropper is unknown, CJ still can be adopted and optimized to increase the secrecy rate at the secondary receiver. Even though a certain secrecy rate cannot be assured, the power of CJ

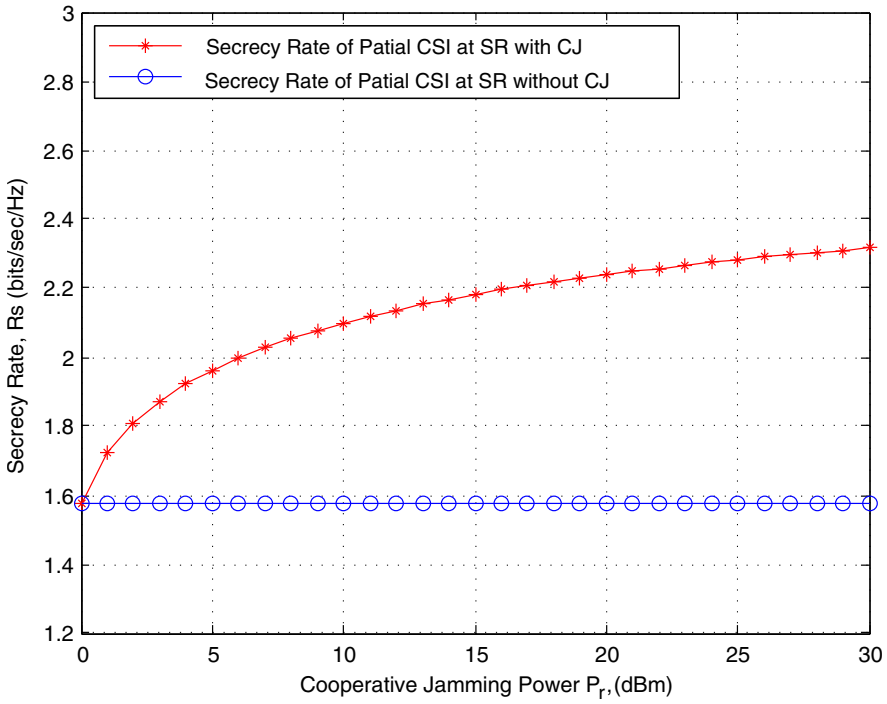

Figure 3.4: The secrecy rate, R_s, as a function of P_r with $P_p = 10$dBm and $P_s = 10$dBm.

can be optimized to enhance the security of the legitimate transmission. The upper bound for the improvement is the capacity of SR.

3.4 Combined Approach of Cooperative Jamming and Relay Selection

In the case of low-density network (i.e., networks with a small number of relays), the secrecy rate changes rapidly with an increase in the number of relays [83]. Motivated with this issue, we proposed a solution to choose the smallest set of active relays that meet the predetermined performance goal instead of using all the available relays, as shown in Figure 3.5. The total number of relays is denoted as N_r and each of them is assumed to be equipped with single antenna.

The relays are connected with the PU and SU using backhauls. As the CSIs need to be shared among the base stations and relays for decision, timing and synchronization are crucial for the performance of the network. Consequently, the ideal technologies for backhaul in our case include leased T1/E1 copper, optical fiber and wireless backhaul

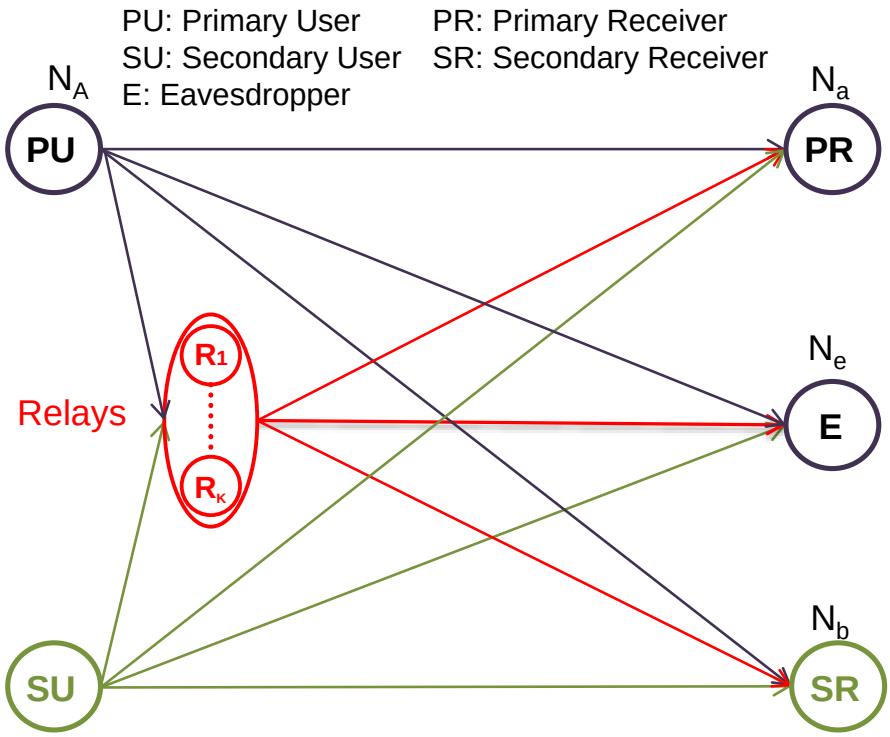

Figure 3.5: Securing cognitive radio with CJ

with microwave [94, 95]. When deployment of fiber is inconvenient or even unavailable, such as mobile backhaul with the relay on vehicles and trains, wireless backhaul with microwave can be applied to solve the challenge of infrastructure installation. However, the technology of microwave has the line of sight (LOS) requirement [94] and may leak the CSI to eavesdropper. Considering about the security of CSI, we assume that wired connections are available and optical fiber or copper is implemented for backhaul in this work. There is a system controller which enable the scheduling of the relays in a centralized manner [96]. The controller can use a scheduling vector relying on the collected system state information. According to the transmission target and networking dynamics, the system controller selects a set of relays which reflects an optimization objective.

Note that, in Figure 3.1, it is assumed that only one relay exists with multiple antenna, while in Figure 3.5, we analyzed relay selection for the scenario that there are multiple relays. To be more conservative about the capability of the eavesdropper, it is assumed to be equipped with multiple antennas in Figure 3.5 and its antenna number is N_e. In this section, the combined approach of CJ and relay selection will be applied to investigate the problem of secrecy capacity maximization and power minimization, respectively.

3.4.1 Cooperative Jamming

When both PU and SU transmit simultaneously without relays, we have $\mathbf{H}_{sr} = \mathbf{H}_{er} = \mathbf{0}$. Similar to equation (3.4), the secrecy rate at SR can be derived as

$$R_{sd} = \left[\log_2 \left(\frac{a \left(P_p \parallel \mathbf{H}_{ep}\boldsymbol{\mu} \right\|^2 + \sigma_e^2 \right)}{b \left(P_p \parallel \mathbf{H}_{sp}\boldsymbol{\mu} \right\|^2 + \sigma_s^2 \right)} \right) \right]^+, \tag{3.29}$$

where $a = P_p \parallel \mathbf{H}_{sp}\boldsymbol{\mu} \|^2 + P_s \parallel \mathbf{h}_{ss} \|^2 + \sigma_s^2$, $b = P_p \| \mathbf{H}_{ep}\boldsymbol{\mu} \|^2 + P_s \| \mathbf{h}_{es} \|^2 + \sigma_e^2$ and $\boldsymbol{\mu}$ is the precoding vector of the primary transmission. If there is no interference, the maximum secrecy rate at SR is given by

$$R_{s_{\max}} = \left[\log_2 \left(\frac{\sigma_e^2 \left(P_s \parallel \mathbf{h}_{ss} \right\|^2 + \sigma_s^2 \right)}{\sigma_s^2 \left(P_s \| \mathbf{h}_{es} \|^2 + \sigma_e^2 \right)} \right) \right]^+. \tag{3.30}$$

Therefore, due to the effect of interference, the loss of secrecy rate at SR can be derived as

$$\begin{aligned} R_{s_{\text{loss}}} =& R_{sd} - R_{s_{\max}} \\ =& \left[\log_2 \left(\frac{b\sigma_e^2 \left(P_s \parallel \mathbf{h}_{ss} \right\|^2 + \sigma_s^2 \right) \left(P_p \parallel \mathbf{H}_{sp}\boldsymbol{\mu} \right\|^2 + \sigma_s^2 \right)}{a\sigma_s^2 \left(P_s \| \mathbf{h}_{es} \|^2 + \sigma_e^2 \right) \left(P_p \parallel \mathbf{H}_{ep}\boldsymbol{\mu} \right\|^2 + \sigma_e^2 \right)} \right) \right]^+. \end{aligned} \tag{3.31}$$

With the assumption that the interference at the PR is maintained under a certain threshold Γ_m, secrecy rate at the SR is given by,

$$\begin{aligned} R_{sc}\left(\mathbf{w}, P_s\right) = \max_{\mathbf{w}, P_s} & \left[\log_2 \left(1 + \frac{P_s \parallel \mathbf{h}_{ss} \|^2}{P_p \parallel \mathbf{H}_{sp}\boldsymbol{\mu} \|^2 + \parallel \mathbf{H}_{sr}\mathbf{w} \|^2 + \sigma_s^2} \right) \right. \\ & \left. - \log_2 \left(1 + \frac{P_s \| \mathbf{h}_{es} \|^2}{P_p \parallel \mathbf{H}_{ep}\boldsymbol{\mu} \|^2 + \parallel \mathbf{H}_{er}\mathbf{w} \|^2 + \sigma_e^2} \right) \right]^+ \\ \text{s.t.} \quad & P_s \parallel \mathbf{h}_{ps} \|^2 + \| \mathbf{H}_{pr}\mathbf{w} \|^2 \leq \Gamma_m, \end{aligned} \tag{3.32}$$

where $P_s \| \mathbf{h}_{ps} \|^2$ and $\| \mathbf{H}_{pr}\mathbf{w} \|^2$ denote interferences at the PR due to the signals of SU and relays, respectively. Since the secrecy rate of (3.32) can be viewed as a product of correlated generalized eigenvectors, the problem of secrecy rate maximization at the SR

can be expressed as

$$\begin{aligned} &\arg\max_{\mathbf{w}} \|\mathbf{H}_{er}\mathbf{w}\|^2 \\ &\quad \text{s.t.} \quad \mathbf{H}_{sr}\mathbf{w} = \mathbf{0}_{n_s\times 1}, \\ &\qquad \|\ \mathbf{w}\|^2 \le P_o - (P_p + P_s) \ \text{ and} \\ &\qquad P_s\ \|\ \mathbf{h}_{ps}\|^2 + \|\mathbf{H}_{pr}\mathbf{w}\|^2 \le \Gamma_m. \end{aligned} \tag{3.33}$$

In order to satisfy the constraint of $\mathbf{H}_{sr}\mathbf{w} = \mathbf{0}_{n_s\times 1}$, $\mathbf{w}$ must lie in the null space of $\mathbf{H}_{sr}$. The projection of null space matrix of $\mathbf{H}_{sr}$ can be expressed as

$$\mathbf{\Lambda} = \mathbf{I}_K - \mathbf{H}_{sr}\left(\mathbf{H}_{sr}^{\dagger}\mathbf{H}_{sr}\right)^{-1}\mathbf{H}_{sr}^{\dagger}, \tag{3.34}$$

so that, $\mathbf{\Lambda w} = \mathbf{w}$ and $\mathbf{w}^{\dagger}\mathbf{\Lambda} = \mathbf{w}^{\dagger}$. The maximization of $\|\mathbf{H}_{er}\mathbf{w}\|^2$ is equivalent to the maximization of $\|\mathbf{w}^{\dagger}\mathbf{\Lambda}\mathbf{H}_{er}^{\dagger}\|^2$. Since $\mathbf{\Lambda}$ is a Hermitian matrix, $\mathbf{w}^{\dagger}$, $\mathbf{\Lambda}\mathbf{H}_{er}^{\dagger}$ are both in the null space of $\mathbf{H}_{sr}$ and the norm of $\mathbf{w}$ and $\mathbf{\Lambda}\mathbf{H}_{er}^{\dagger}$ are fixed. Therefore, the maximization problem can be realized by setting $\mathbf{w} = \frac{\sqrt{P_o-(P_p+P_s)}}{\|\mathbf{\Lambda}\mathbf{H}_{er}^{\dagger}\|}\mathbf{\Lambda}\mathbf{H}_{er}^{\dagger}$.

We see that $\mathbf{w}$ is proportional to $\sqrt{P_o - (P_p + P_s)}$. Let us define

$$\mathbf{w} = \sqrt{P_o - (P_p + P_s)}\mathbf{v}, \tag{3.35}$$

where $\mathbf{v} = \frac{\mathbf{\Lambda}\mathbf{H}_{er}^{\dagger}}{\|\mathbf{\Lambda}\mathbf{H}_{er}^{\dagger}\|}$. Substituting (3.35) into (3.32), we have

$$R_{sc}\left(\mathbf{w}, P_s\right) = \log_2\left(\frac{c_2 + b_3P_s + a_2P_s^2}{\eta P_s + c_2}\right), \tag{3.36}$$

where

$$\begin{aligned} a_2 &= -\frac{\|\ \mathbf{h}_{ss}\|^2\|\mathbf{H}_{er}\mathbf{v}\|^2}{P_p\ \|\ \mathbf{H}_{sp}\boldsymbol{\mu}\|^2 + \sigma_s^2}, \eta = \|\mathbf{h}_{es}\|^2 - \|\mathbf{H}_{er}\mathbf{v}\|^2, \\ b_3 &= \frac{\|\ \mathbf{h}_{ss}\|^2\left(P_p\|\mathbf{H}_{ep}\boldsymbol{\mu}\|^2 + P_o|\mathbf{H}_{er}\mathbf{v}|^2 + \sigma_e^2\right)}{P_p\ \|\ \mathbf{H}_{sp}\boldsymbol{\mu}\|^2 + \sigma_s^2} - \|\mathbf{H}_{er}\mathbf{v}\|^2 \\ &\text{and}\ \ c_2 = P_p\|\mathbf{H}_{ep}\boldsymbol{\mu}\|^2 + P_0\|\mathbf{H}_{er}\mathbf{v}\|^2 + \sigma_e^2. \end{aligned}$$

Now the maximization of $R_{sc}\left(\mathbf{w}, P_s\right)$ is equivalent to maximize $\frac{c_2+b_3P_s+a_2P_s^2}{\eta P_s+c_2}$. Let us

Table 3.1: All possible combinations for the selection of relays.

Number of Relays (K)	Possible Combinations of Relays: LSC → MSC														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Relay 1:	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
Relay 2:	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
Relay 3:	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
Relay 4:	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

assume that $\frac{c_2+b_3P_s+a_2P_s^2}{\eta P_s+c_2} \geq t$ where $t \geq 0$. Define $\mu_{(P_s)} = c_2 + b_3P_s + a_2P_s^2$, $\nu_{(P_s)} = \eta P_s + c_2$ and $\phi_{t(P_s)} = \mu_{(P_s)} - t\nu_{(P_s)}$. Since $\mu''_{(P_s)} = \alpha \leq 0$, $\mu_{(P_s)}$ is concave. Moreover, $\nu_{(P_s)}$ is affine. So, $\phi_{t(P_s)}$ is a decreasing function of t and the maximization problem of (3.33) can be expressed as

$$\begin{aligned} &\max_{t,\, P_s} \; t \\ &\text{s.t. } t \geq 0, \phi_{t(P_s)} \geq 0 \text{ and} \\ &P_s \in \left[0, \min\left\{P_o, \frac{\Gamma_m - \|\mathbf{H}_{pr}\mathbf{w}\|^2}{\|\,\mathbf{h}_{ps}\|^2}\right\}\right]. \end{aligned} \tag{3.37}$$

The optimal t which maximizes $R_{sc}(\mathbf{w}, P_s)$ can be obtained from the solution of (3.37). Let t^* denotes the optimal t. Then, the optimized secrecy rate at the SR is given by

$$R^*_{sc}(\mathbf{w}, P_s) = \log_2(t^*). \tag{3.38}$$

Therefore, from (3.38) and (3.29), the improvement of secrecy rate at SR due to CJ can be derived as

$$R_{s_{\text{improve}}} = \left[\log_2\left(\frac{t^*\left(P_p\|\mathbf{H}_{sp}\boldsymbol{\mu}\|^2 + \sigma_s^2\right)\left(P_p\|\mathbf{H}_{ep}\boldsymbol{\mu}\|^2 + P_s\|\mathbf{h}_{es}\|^2 + \sigma_e^2\right)}{\left(P_p\|\mathbf{H}_{ep}\boldsymbol{\mu}\|^2 + \sigma_e^2\right)\left(P_p\|\mathbf{H}_{sp}\boldsymbol{\mu}\|^2 + P_s\|\mathbf{h}_{ss}\|^2 + \sigma_e^2\right)}\right)\right]^+. \tag{3.39}$$

3.4.2 Selection of Effective Relays

In the case of low-density networks (i.e., networks with a small number of relays), the secrecy rate changes rapidly with an increase in the number of relays [83]. Motivated with

this issue, in this subsection, we provide a solution to choose the smallest set of active relays that meet the predetermined performance goal instead of using all the available relays. Note that, cooperative jamming provided by the selected relays still maintain interference temperature limit on the PR under Γ_m.

In order to select the number of effective relays, let us define the target secrecy rate as

$$R_{s_{\text{target}}} = \theta R_{sc_{\max}}(\mathbf{w}, P_s), \quad 0 \leq \theta \leq 1. \tag{3.40}$$

where $R_{sc_{\max}}(\mathbf{w}, P_s)$ is the maximum value of $R_{sc}(\mathbf{w}, P_s)$. Let $\mathbf{q} = (q_1, q_2, ..., q_K)^T$ denotes the relay selection vector where q_i, $i = 1, 2, ..., K$ is defined as

$$q_i = \begin{cases} 1, & \text{if } i\text{th relay is active,} \\ 0, & \text{otherwise.} \end{cases} \tag{3.41}$$

Therefore, the channel vector from relays to E can be expressed as

$$\mathbf{H}_{er} = (q_1\mathbf{h}_{er_1}, q_2\mathbf{h}_{er_2}, ..., q_K\mathbf{h}_{er_K})^T, \tag{3.42}$$

where $\mathbf{h}_{er_i}$ denotes the channel coefficient of ith relay to E. To some extent, the selection of effective relays is like searching for the effective relay channels. Substituting (3.42) into (3.36), the secrecy rate is estimated as

$$\tilde{R}_{sc}(\mathbf{w}, P_s) = \left[\log_2\left(\sum_{i=1}^{K}\sum_{j=1}^{K} q_i q_j \Big(w_i w_j^{\dagger}\mathbf{h}_{er_i}\mathbf{h}_{er_j}^{\dagger} + \frac{P_s\|\mathbf{h}_{es}\|^2 + \sigma_e^2}{Q_q}\Big)\frac{P_p\|\mathbf{H}_{sp}\boldsymbol{\mu}\|^2 + P_s\|\mathbf{h}_{ss}\|^2 + \sigma_s^2}{(P_p \parallel \mathbf{H}_{sp}\boldsymbol{\mu}\|^2 + \sigma_s^2)(P_s\|\mathbf{h}_{es}\|^2 + Q_s)}\right)\right]^+,$$

where $Q_q = \sum_{i=1}^{K}\sum_{j=1}^{K} q_i q_j$ and $Q_s = \sum_{i=1}^{K}\sum_{j=1}^{K} q_i q_j (w_i w_j^{\dagger}\mathbf{h}_{er_i}\mathbf{h}_{er_j}^{\dagger} + \frac{P_p\|\mathbf{H}_{ep}\boldsymbol{\mu}\|^2+\sigma_e^2}{Q_q})$. w_i and w_j denote the weight of ith and jth relay, and $\mathbf{h}_{er_i}$ and $\mathbf{h}_{er_j}$ denote the channel coefficients from ith and jth relay to E, respectively. Therefore, the optimization problem for the selection of effective relays can be expressed as

$$\min_{q_i \in \{0,1\}} \sum_{i=1}^{K} q_i,$$

$$s.t. \quad \tilde{R}_{sc}\left(\mathbf{w}, P_s\right) \geq R_{s_{target}}, \tag{3.43}$$

where $q_i \in \{0, 1\}$ indicates that q_i is either 0 or 1. The i_{th} relay is selected when q_i is 1. $\tilde{R}_{sc}(\mathbf{w}, Ps)$ can be maximized using the similar procedure as discussed above. The number of effective relays is estimated based on $\tilde{R}_{sc_{\max}}\left(\mathbf{w}, P_s\right)$, where $\tilde{R}_{sc_{\max}}\left(\mathbf{w}, P_s\right)$ denotes the maximum of $\tilde{R}_{sc}\left(\mathbf{w}, P_s\right)$. At first, we generate a $K \times 2^K$ matrix in which each column indicates a possible combination of relay selections. For example, in the case of four relays, i.e., for $K = 4$, all possible combinations of relay selections are shown in Table I. In the 5th combination, 2nd and 4th relays are activated and 1st and 3rd relays are kept inactive. Let N_r denotes the number of effective relays. Initially, we assign $N_r = 1$ and calculate $\tilde{R}_{sc_{\max}}\left(\mathbf{w}, P_s\right)$ for all possible combinations of relays satisfying $N_r = \sum_{i=1}^{K} q_i$. In order to find the final value of N_r, at first, $\tilde{R}_{sc_{\max}}\left(\mathbf{w}, P_s\right)$ of each combination is compared with $R_{s_{\text{target}}}$. If $\tilde{R}_{sc_{\max}}\left(\mathbf{w}, P_s\right) \geq R_{s_{\text{target}}}$, then $N_r = 1$, and it is 4th relay as shown in Table I. If $\tilde{R}_{sc_{\max}}\left(\mathbf{w}, P_s\right) < R_{s_{\text{target}}}$, then we increase N_r by 1 and calculate $\tilde{R}_{sc_{\max}}\left(\mathbf{w}, P_s\right)$ for all possible combinations of relays satisfying $N_r = \sum_{i=1}^{K} q_i$. Again, the $\tilde{R}_{sc_{\max}}\left(\mathbf{w}, P_s\right)$ of each combination is compared with $R_{s_{\text{target}}}$. In this way, $\tilde{R}_{sc_{\max}}\left(\mathbf{w}, P_s\right)$ of each combination starting from least significant combination (LSC) to most significant combination (MSC) is compared with $R_{s_{\text{target}}}$ until $\tilde{R}_{sc_{\max}}\left(\mathbf{w}, P_s\right) \geq R_{s_{\text{target}}}$. If $\tilde{R}_{sc_{\max}}\left(\mathbf{w}, P_s\right) \geq R_{s_{\text{target}}}$ for a certain combination, N_r is determined from that combination. For example, if $\tilde{R}_{sc_{\max}}\left(\mathbf{w}, P_s\right) \geq R_{s_{\text{target}}}$ is found at the 5th combination, then $N_r = 2$, and they are the 2nd and 4th relays in Table I. The following algorithm summarizes the selection process of effective relays.

Note that, the complexity of this algorithm increases exponentially with the selected number of relays and the optimization of the secrecy capacity is iterated. This approach has a complexity of $\sim O(2^K)$ [97]. To reduce the complexity for the scenarios with large numbers of relays, the individual relay selection algorithm and the beamforming weights norm algorithm [97] can be applied.

Algorithm 3.4.1: Selection of effective relays

1 : **Input:** $P_o, P_p, \sigma_s, \sigma_e, K, R_{s_{\text{target}}}, \mathbf{q}, \mathbf{H}_{sp}, \mathbf{h}_{ss}, \mathbf{H}_{ep}, \mathbf{h}_{es}, \mathbf{H}_{er}$.
2 : Generate a $K \times 2^K$ matrix to express all possible combinations of relay selections.
3 : $N_r = 1$.
4 : **begin**
5 : Calculate $\tilde{R}_{sc_{\max}}(\mathbf{w}, P_s)$ for all possible combinations of relays satisfying $N_r = \sum_{i=1}^{K} q_i$.
6 : Compare $\tilde{R}_{sc_{\max}}(\mathbf{w}, P_s)$ of each combination with $R_{s_{\text{target}}}$.
7 : **if** $\tilde{R}_{sc_{\max}}(\mathbf{w}, P_s) \geq R_{s_{\text{target}}}$, exit.
8 : **else** $N_r = N_r + 1$.
9 : Repeat steps 5, 6, 7 and 8 until $\tilde{R}_{sc_{\max}}(\mathbf{w}, P_s) \geq R_{s_{\text{target}}}$.
10 : **end**
11 : Find the number of effective relays, N_r, from the combination.
12 : **Output:** N_r.

3.4.3 Source Power Optimization

In order to achieve the target secrecy rate at SR with the minimum source power, in this subsection, we optimize the transmit power of SU under the secrecy rate constraint. Since P_p (i.e., the power of PU) acts as an interferer for the SR, P_p is assumed to be constant to optimize the SU's power, P_s. On the other hand, the secrecy rate at the SR is determined by the P_s and the jamming power $P_r \geq \|\mathbf{w}\|^2$. Therefore, for a fixed value of P_o, the problem of transmit power minimization at the SU can be defined as

$$\begin{aligned} \arg\min_{\mathbf{w}} \quad & P_s + \|\mathbf{w}\|^2 \\ s.t. \quad & \mathbf{H}_{sr}\mathbf{w} = \mathbf{0}_{n_s \times 1}, \\ & \|\mathbf{H}_{er}\mathbf{w}\|^2 \geq \kappa, \end{aligned} \tag{3.44}$$

where

$$\kappa = \frac{P_s \parallel \mathbf{h}_{es}\|^2}{2^{-R_{s_{\text{target}}}}(1 + \frac{P_s\|\mathbf{h}_{ss}\|^2}{P_s\|\mathbf{H}_{sp}\|^2 + \sigma_s^2}) - 1} - (P_p\|\mathbf{H}_{ep}\|^2 + \sigma_e^2),$$

$\mathbf{w} = \sqrt{\kappa}\mathbf{v}$ and $\|\mathbf{w}\|^2$ denotes the jamming power.

Substituting the values of κ and $\mathbf{w}$ in (3.44), we have

$$P_s + \|\mathbf{w}\|^2 = \frac{a_3 P_s^2 + b_4 P_s}{a_3 P_s + c_3} - (P_p\|\mathbf{H}_{ep}\|^2 + \sigma_p^2)\|\mathbf{v}\|^2, \tag{3.45}$$

where $a_3 = \frac{2^{R_{s_{\text{target}}}}\|\mathbf{h}_{ss}\|^2}{P_p\|\mathbf{H}_{sp}\|^2+\sigma^2}$, $b_4 = 2^{R_{s_{\text{target}}}} + \|\mathbf{h}_{es}\|^2\|\mathbf{v}\|^2 - 1$ and $c_3 = 1 - 2^{-R_{s_{\text{target}}}}$. Let us define, $\frac{a_3P_s^2+b_4P_s}{a_3P_s+c_3} \geq \tau$ and $\psi_{(\tau,P_s)} = (a_3P_s^2 + b_4P_s) - \tau\,(a_3P_s + c_3)$. Therefore, the minimization problem of (3.44) can be expressed as

$$\begin{aligned} \max_{\mathbf{w}} \quad & \tau \\ s.t. \quad & \psi_{(\tau,P_s)} \geq 0, \\ & P_s \in \left[0, \min\left\{P_o, \frac{\Gamma_m - \|\mathbf{H}_{pr}\mathbf{w}\|^2}{\|\mathbf{h}_{ps}\|^2}\right\}\right]. \end{aligned} \tag{3.46}$$

From the solution of (3.46), we get the optimal τ^* and P_s^* for minimizing $P_s + \|\mathbf{w}\|^2$.

It should be noted that, in the above analysis, the jamming signal causes an additional interference at the PR (i.e., $\|\mathbf{H}_{pr}\mathbf{w}\|^2$). However, it is possible to eliminate this interference by designing a suitable precoding vector for the relays as discussed in [25].

3.4.4 Numerical Results

Similar to Section 3.3.4, we used Monte Carol method to statistically test the system performance. The channel coefficients are assumed to be i.i.d complex Gaussian. The noises experienced at SR and the eavesdropper are given as $\sigma_s^2 = \sigma_e^2 = 1$dBm.

Figure 3.6 shows the secrecy rate at SR as a function of the interference temperature limit Γ_m with $P_o = 40$dBm, $P_p = 2$dBm and the number of relays, $K = 10$. In the absence of relays, when both the PU and SU transmit simultaneously, interference causes a reduction in the secrecy rate at SR as shown in the figure. We see that the secrecy rate R_s can also be improved by allowing more interference at the PR which limits the transmission power at the SU and the relays. On the other hand, for a fixed value of Γ_m, the secrecy rate R_s is improved by a CJ scheme that creates additional interference at the eavesdropper by transmitting jamming signals from the relay nodes.

Figure 3.7 shows the impact of total transmission power and the interference temperature limit on secrecy rate R_s with $P_p = 5$dBm and $K = 5$. This figure illustrates that R_s increases with the rise of the total transmit power P_o. R_s is found to increase with the interference temperature limit Γ_m up to the value of P_o, while it will reach an upper bound

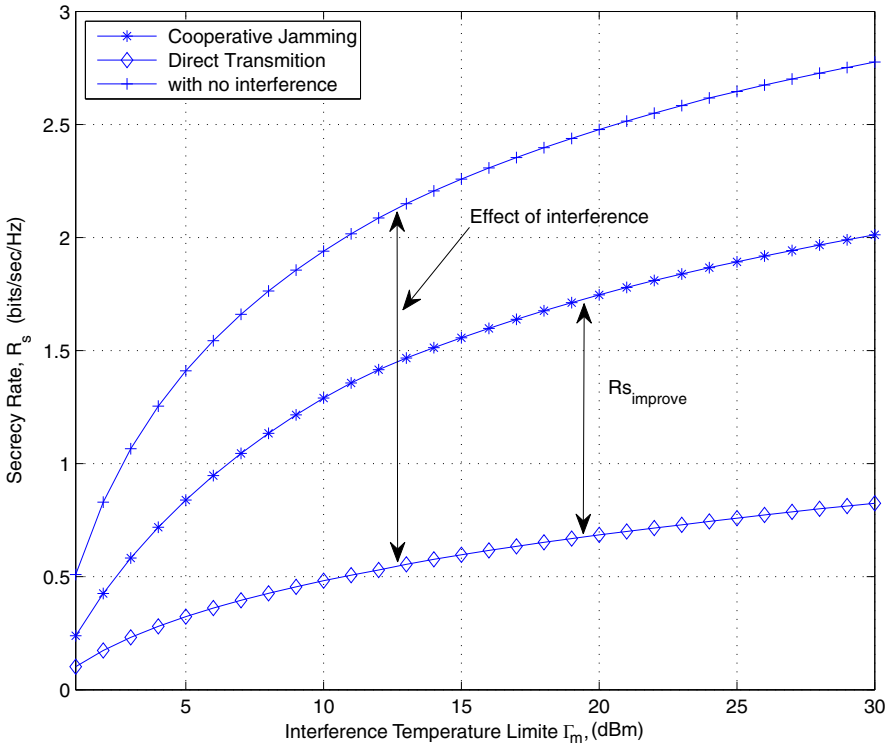

Figure 3.6: The secrecy rate at SR, R_s, as a function of interference constraint Γ_m with $P_o = 40$dBm, $P_p = 2$dBm and $K = 10$.

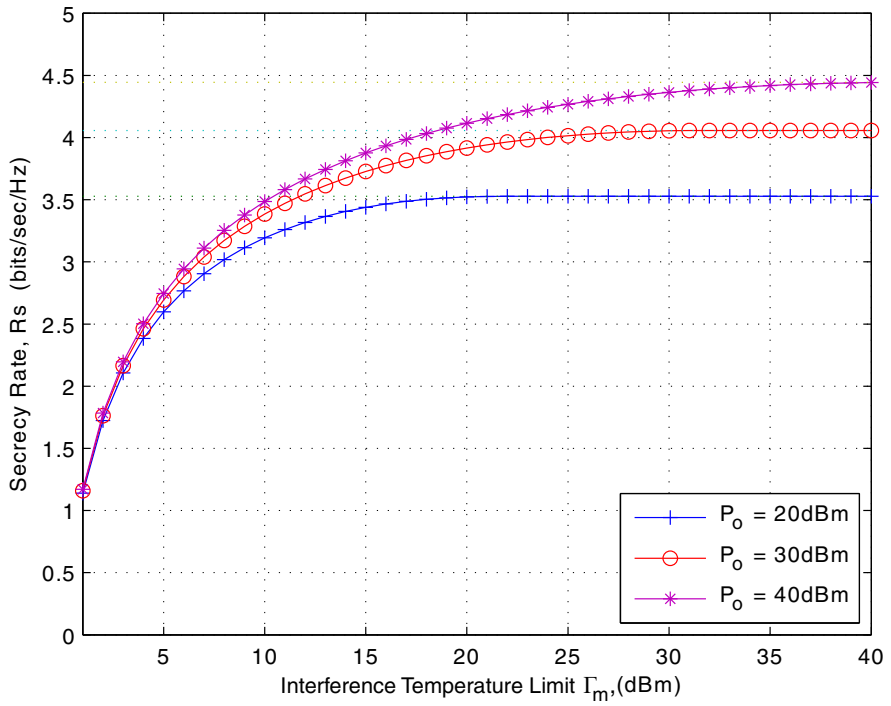

Figure 3.7: The secrecy rate, R_s as a function of interference constraint Γ_m for selected values of P_o with $P_p = 5$dBm and $K = 5$.

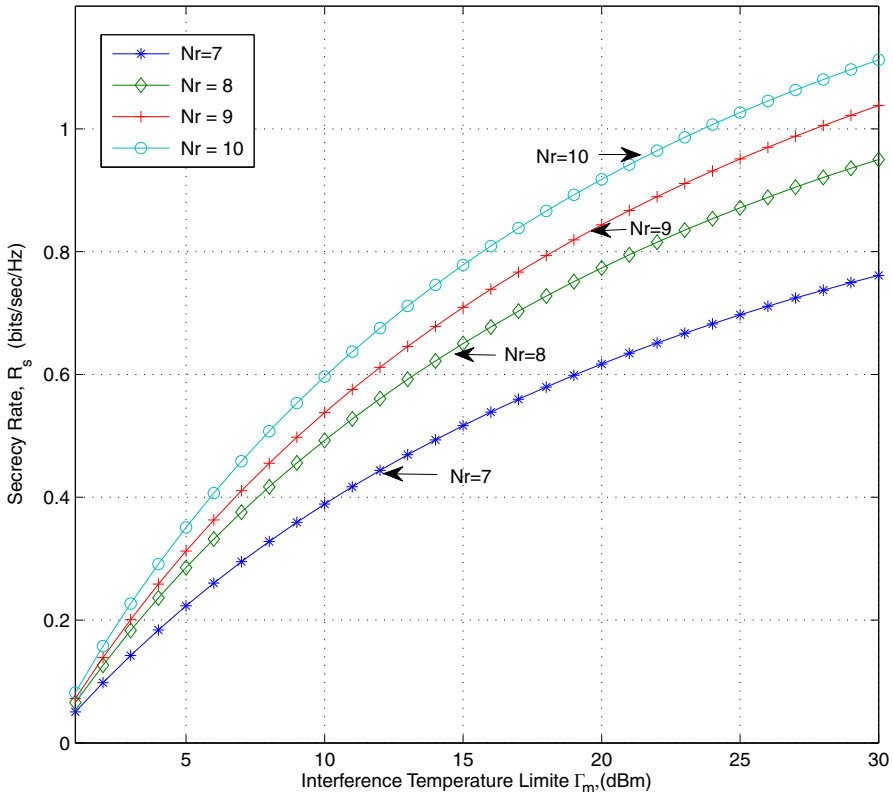

Figure 3.8: The secrecy rate, R_s, as a function of interference constraint Γ_m for selected values of N_r with $P_o = 22$dBm and $P_p = 2$dBm.

for larger value of Γ_m. As the maximum values of P_r and P_s are limited by P_o, allowing more interference at the PR will not increase the secrecy rate at the SR. Moreover, the impact of antenna numbers on secrecy rate has been illustrated in Figure 3.8. It shows that R_s increases with the number of effective relays, while the improvement is more significant for the scenarios with small number of relays. This is obvious as implementing more antennas will increase the channel diversity.

3.5 Summary

In this chapter, we considered the problem of secrecy transmission in the relay-assisted scheme of a cognitive radio network where the SU can transmit information simultaneously with the PU. Considering the setup of the cooperative relays, the approaches of combining CJ with ZF and CJ with relay selection are investigated separately.

In the case that there is a cooperative relay with multiple antennas, strategies using CJ are developed to enhance the security for both full CSI and partial CSI scenarios. In the full CSI scenario, we proposed a CJ strategy using ZF which will not generate any interference to PR or SR to increase the secrecy capacity of the cognitive system. The CJ scheme is also designed using precoding for the legitimate transmission to optimize the power allocation. In the scenario where channel information regarding the eavesdropper is unknown, a different CJ scheme which still meets the jamming interference cancelling target at both PR and SR, is also designed with ZF to enhance the security. Simulation results show that a combined approach of ZF precoding with CJ scheme is significant in improving the secrecy rate of cognitive interference channels in both full CSI and partial CSI scenarios.

For the case that there are multiple relays, we evaluated the performance of a CJ scheme in enhancing physical layer security of cognitive interference networks with the approach of relay selection. Multiple relays are used to transmit jamming signals and an algorithm is developed to select the effective relays which meet the target secrecy rate. Based on our formulation and from the observation of numerical results, we can conclude that, although interference due to the PU's signals deteriorates the secrecy rate of SR, the target secrecy rate at SR can be achieved by the CJ scheme designed with the developed relay selection algorithm without increasing the SU's transmission power.

Chapter 4

Security of Random Wireless Networks with Protected Zones

4.1 Introduction

By taking channel propagation effects into consideration, the secrecy capacity of wireless fading channels was investigated in [9], and expressions of the average secrecy capacity and the *secrecy outage* for quasi-static fading channels were derived in [10]. Exact expression of the secrecy capacity is hard to obtain, due to the limited knowledge of CSI and path loss in legitimate and eavesdropping channels. Ergodic secrecy capacity, derived from statistics of CSI and distances which are easier to obtain, can provide a single letter characterization for the secrecy capacity of an arbitrary wire-tap channel. It can also provide a helpful reference for the design of networks such as allocating the transmission power and application of protected zones. The ergodic secrecy capacity of fading channels without considering path loss was derived independently in [9] and [12].

Previous works of physical layer security primarily focused on point-to-point transmissions [22, 28, 29]. Recent efforts are to achieve a better understanding of the inherent secrecy capabilities of wireless systems under more realistic conditions, such as the distribution of randomly deployed users in large-scale networks. When studying security in random wireless networks via stochastic-geometric tools [35], the notion of *secrecy graphs* emerged in [36]. An important distinction between secrecy graphs and the conventional point-to-point wire-tap channel is that the *topology* of networks, with respect to both the legitimate and eavesdropping nodes, play a major role not only on *how much* secrecy rate is available, but also on *how to measure* it. Following this instinct,

secrecy rate scaling laws were studied in [37], while the secrecy rates of unicast links in the presence of multiple eavesdroppers were studied in [38]. Secrecy connectivity over large-scale network were widely investigated in [35, 36] and [39].

To enhance physical layer security in large-scale networks, various strategies were investigated, such as guard zones [40, 41], sectorized transmission [42], precoding [43] and the use of artificial noise [44–46]. Specifically, guard zones were studied in [36] to improve secrecy connectivity without considering fading, while the study of [40] investigated how to enhance the secrecy transmission capacity using a guard zone, based on the assumption of fixed distances between transmitters and the intended receivers. The concept of secrecy protected zones [45] that extinct the eavesdroppers in the zone is different from the guard zone that allows the existence of eavesdroppers inside the protected area. The authors of [45] considered the use of artificial noise and a secrecy protected zone to enhance the security of random networks, in the presence of eavesdroppers and interferers randomly deployed according to two homogeneous PPPs. The study investigated the use of a secrecy protected zone surrounding the transmitter in order to stop eavesdroppers approaching, while still being affected by interference from other legitimate transmitters. Analysis in [40] and [45] derived the upper bound of the secrecy outage probability based on the uniform distribution of eavesdroppers and the lower bound by the distribution of the nearest eavesdropper, respectively.

In this chapter, we investigate how to enhance physical layer security in random wireless networks with a secrecy protected zone surrounding the transmitter as well as interferer protect zones surrounding the legitimate receivers. The impacts of fading, interference and protected zones are studied in order to analyze the secrecy performance. For large-scale networks, interference has usually been viewed as a harmful factor. However, the interference can be well structured by using interferer protected zones to benefit the secrecy transmission in a similar manner to artificial noise. Notice that, the interference studied in this work refers to the signals between other transmitters and receivers, rather than artificial noise introduced additionally as in the work of [40], [98] and [99]. Besides, the locations of interferers follow a Poisson hole process, due to the existence of the interferer protected zones. The contributions of this research are summarized as follows:

- We derive the distribution of channel gains from the transmitter to receivers which are ordered either according to the distance or their strength. The expression for the distribution of channel gains is an important tool for calculating the capacity at the worst-case eavesdropper, which can be applied to derive the secrecy outage, the probability of secure connection, and the ergodic secrecy capacity.

- The ergodic secrecy capacity of random wireless networks is analyzed by considering both large scale path loss and small scale fading. Additionally, we derive the distribution of path loss for the nodes outside the secrecy protected zone.

- Besides the secrecy protected zone, we also employ interferer protected zones to restructure interference and enhance physical layer security. The distance distribution of legitimate receivers outside the secrecy protected zone is studied.

- By adopting interferer protected zones at legitimate receivers, interference can be restructured to benefit the security at the legitimate receiver without introducing artificial noise. It is worth to notice that interference is different from jamming noise, because it is the signal broadcasted by other transmitters outside of the legitimate network. Moreover, the distribution of the active cooperative transmitters that follow a Poisson-hole process has also been exploited.

The rest of this chapter is organized as follows. The system model and mathematical concepts for stochastic geometry modelling are presented in Section 4.2. In Section 4.3, we study the security in random wireless networks by deriving the distribution for the composite channel gain. The performance of adopting the protected zones with and without considering interference are presented in Section 4.4 and 4.5, respectively. The numerical results of secrecy characteristics are discussed in Section 4.6. Finally, concluding marks are drawn in Section 4.7.

4.2 System Model

4.2.1 Random Network Model

In this chapter, we consider a wireless network deployed in an unbound two dimensional space consisting of nodes modeled by a homogeneous PPP with intensity λ and denoted as Φ. According to the stationarity of PPP, we fix the source node at the origin as the distribution of Φ is translation-invariant. Let $\Xi = \left\{\xi_k = \frac{r_k^\alpha}{|h_k|^2}\right\}, k \in \mathbb{N}$ be the path loss process with small scale fading [35], where α is the path loss exponent, r_k and h_k denote the distance and the fading coefficient between the source node and k_{th} receiving node, respectively. Ξ is also a PPP which will be discussed in Section 4.3. Note that $\{\xi_k\}$ is not ordered according to distance $\{r_k\}$ [35], but ordered by the combination of path loss and fading.

Let the aforementioned model be applied to two overlaid networks of legitimate nodes and eavesdroppers, respectively, with corresponding densities denoted as λ_l and λ_e. The source node aims to transmit a signal to the k_{th} legitimate receiver in presence of eavesdroppers located at unknown distances. Both the legitimate and eavesdropping channels are subject to block ergodic fading and path loss.

Three scenarios are studied in this work. In the first scenario, the basic random network is studied without a protected zone. While in the second scenario, secrecy protected zone surrounding the source node is used to enhance security in noise limited networks. In addition, two cases in which eavesdroppers are aware and unaware of the secrecy protected zone are investigated. Besides of utilizing a secrecy protected zone, in the third scenario we analyze the impact of interference restructuring on security by adopting interferer protected zones.

4.2.2 Problem Formulation

Secrecy Capacity

The secrecy capacity is the maximum data rate at which the legitimate receiver can decode the signal information with arbitrarily small error, while the eavesdroppers' error probabilities of decoding approach to one. The secrecy capacity of the transmission from the source node to the k_{th} legitimate node is given by [8]

$$C_{l:k} = \left[\log_2\left(1+\frac{P}{\xi_k\sigma_l^2}\right) - \log_2\left(1+\frac{P}{\xi_e\sigma_e^2}\right)\right]^+, \tag{4.1}$$

where $\xi_e = \frac{r_e^\alpha}{|h_e|^2}$; P, σ_l^2 and σ_e^2 denote the transmission power at the source node, the noise at the legitimate node and the noise at the worst-case eavesdropper, respectively.

Secrecy Outage Probability and Probability of Secure Connection

Secrecy outage probability, known as the outage probability of secrecy capacity under quasi-static small scale fading, can be given by [10]

$$\mathbb{P}_{out}(\varrho) \triangleq \mathbb{P}\left\{C_{l:k} \leq \varrho\right\} = \mathbb{P}\left\{\log_2\left(\frac{1+\eta_l/\xi_k}{1+\eta_e/\xi_e}\right) < \varrho\right\}, \tag{4.2}$$

where $\eta_l = \frac{P}{\sigma_l^2}$ and $\eta_e = \frac{P}{\sigma_e^2}$. The probability of secure connection is the probability to have a positive secrecy capacity from the source node to the legitimate receiver [100], which can be obtained by substitute $\varrho = 0$ into equation (4.2).

Ergodic Secrecy Capacity

The ergodic capacity from the source node to the k_{th} legitimate receiver and the worst-case eavesdropper can be obtained, respectively, as [101]

$$\begin{aligned} R_{s:k} &= \mathbb{E}_{h_k,r_k}\left\{\log_2\left(1+\frac{|h_k|^2P}{r_k^\alpha\sigma_l^2}\right)\right\}, \\ R_{s:e} &= \mathbb{E}_{h_e,r_e}\left\{\log_2\left(1+\frac{|h_e|^2P}{r_e^\alpha\sigma_e^2}\right)\right\}. \end{aligned} \tag{4.3}$$

The ergodic secrecy capacity can be derived by assuming that the worst-case eavesdropper can keep achieving the largest channel gain. Consequently, the ergodic capacity of the worst-case eavesdropper obtained in equation (4.3) is an upper bound. Because of this, a lower bound of the ergodic secrecy capacity can be obtained as [46, 102, 103]

$$C_{s:k} = [R_{s:k} - R_{s:e}]^+ . \tag{4.4}$$

4.3 Security in Random Wireless Networks without Protected Zone

In this section, we will first derive the PDF of the composite channel gain in the interference-free scenario without considering protected zone. Afterwards, this PDF will be used to analyze the distribution of the secrecy capacity, the probability of secure connection and the ergodic secrecy capacity.

4.3.1 PDF for the Composite Channel Gain

To obtain the distribution of $C_{l:k}$ for random networks under Nakagami-m fading, we need to derive the PDF of ξ_k and ξ_e. We define the path loss $x_k = r_k^\alpha$ and denote the intensity of the set $\Xi = \{x_k/h_k, k \in \mathbb{N}\}$ as λ_Ξ. Then the intensity function of Ξ is given in Lemma 1.

Lemma 1. *Given that intensity of Φ is λ and the shape parameter of Nakagami fading is denoted as m, Ξ is a PPP and the intensity function of Ξ can be expressed by*

$$\lambda_\Xi(x) = A_0 x^{\delta-1}, \tag{4.5}$$

where $\delta = \frac{2}{\alpha}$ and $A_0 = \pi\lambda\delta\frac{\Gamma(\delta+m)}{m^\delta\Gamma(m)}$.

Proof: The point process of Ξ can be obtained from the PPP of $\Phi = \{r_k\}$ by a deterministic mapping and independent displacement. According to the displacement

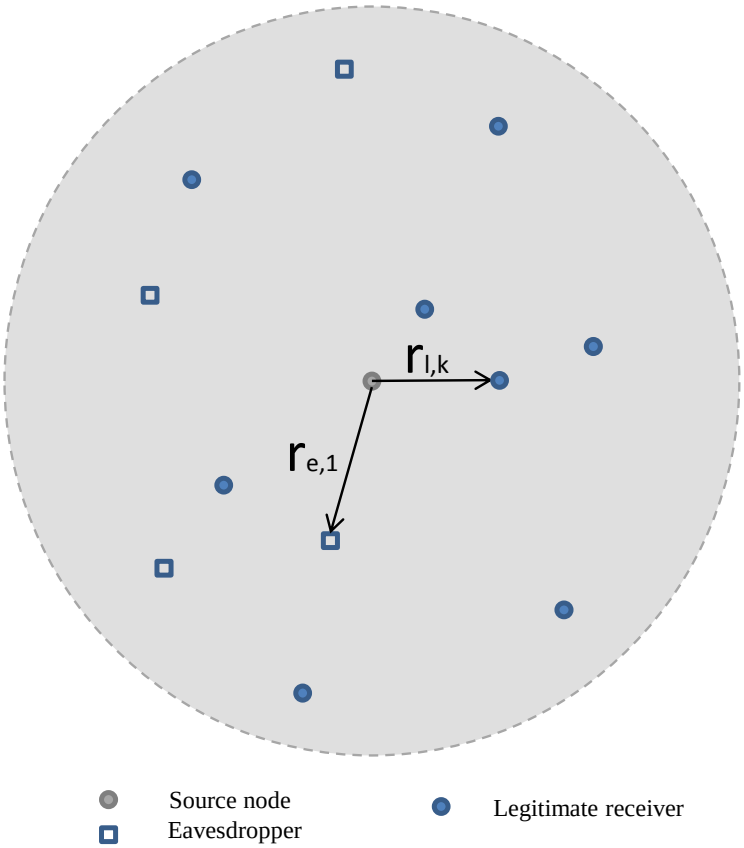

Figure 4.1: Random network without protected zone.

theorem and mapping theorem for point process transformations, Ξ is also a PPP [35]. First, the intensity function of $\Psi = \{x_k\}$ can be derived from $\mathbb{E}\{\Phi([0,x))\} = \lambda\pi x^2$ by mapping theorem

$$\lambda_\Psi(x) = \lambda\pi\delta x^{\delta-1}. \tag{4.6}$$

Then, the intensity function $\lambda_\Xi(x)$ can be obtained by displacement theorem for the general Nakagami-m fading model by following Theorem 2.33 in [33].

Theorem 1. *The PDF of ξ_k under Nakagami-m fading is*

$$f_{\xi_k}(s) = \exp(-A_1 s^\delta)\frac{\delta(A_1 s^\delta)^k}{s\Gamma(k)}, \tag{4.7}$$

where $A_1 = \frac{A_0}{\delta}$.

Proof: As Ξ is a PPP, the cumulative distribution function (CDF) of ξ_k can be expressed by

$$\begin{aligned} F_{\xi_k}(s) &= P(\xi_k < s), \\ &= 1 - \mathbb{P}\left(\Xi[0,s) < k\right), \\ &= 1 - \sum_{n=0}^{k-1} \exp\left(-\int_0^s \lambda_\Xi(x)\,\mathrm{d}x\right) \frac{(\int_0^s \lambda_\Xi(x)\,\mathrm{d}x)^n}{n!}, \\ &\overset{(a)}{=} 1 - \sum_{n=0}^{k-1} \exp\left(-A_1 s^\delta\right) \frac{(A_1 s^\delta)^n}{n!}, \end{aligned} \tag{4.8}$$

where $\Xi[0,s)$ denotes the counting measure induced by a random circular set of Ξ centered at the origin with radius s, and (a) follows from

$$\int_0^s \lambda_\Xi(x)\,\mathrm{d}x = \int_0^s A_0 x^{\delta-1}\,\mathrm{d}x = \frac{A_0}{\delta} s^\delta. \tag{4.9}$$

By denoting $A_1 = \frac{A_0}{\delta}$ and taking the derivative of $F_{\xi_k}(s)$, we can obtain the PDF for the composite channel gain as expressed in (4.7).

Note that, the ordering in Theorem 1 is based on the combined effect of path loss and small-scale fading, which will be used to derive the distribution of the secrecy capacity and the probability of secure connections in Section 4.3-A, B and C. The investigation of the legitimate receivers based on the ordering of the combined effect of path loss and fading can reflect the order of their secrecy capacity and the probability of secure connection, which is a better indication of how the fading and the point distribution affect the secrecy of a network. Besides, ordering the legitimate receivers based on the combined effects can also provide more insights, as the analysis of secrecy capacity at the worst-case eavesdropper is also based on the combined effect.

Figure 4.2 is the Monte Carlo simulation plotted to compare the PDF for the composite channel gain derived in (4.7) for various nodes. It shows that the proposed PDF is accurate, as verified by the simulation.

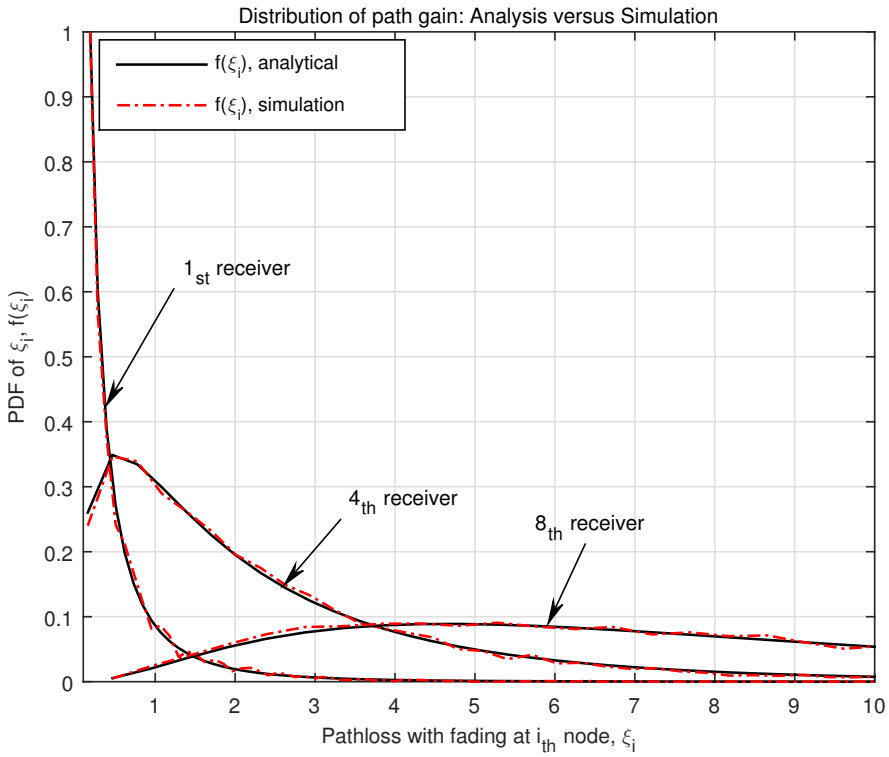

Figure 4.2: PDF of ξ from the source node to the 1st, 4th and 8th receivers with $\lambda = 1$, $m = 1.5$ and $\alpha = 4$.

4.3.2 Distribution of the Secrecy Capacity

To derive the distribution of the secrecy capacity, we first investigate the distribution of the capacity at the legitimate receiver. The outage probability of the capacity at the k_{th} legitimate receiver can be derived by:

$$\begin{aligned}
\mathbb{P}_{out}(R_{s:k} < \tau) &= \mathbb{P}\left(\log_2(1+\frac{\eta_l}{\xi_k}) < \tau\right), \\
&= 1 - \int_0^{\frac{\eta_l}{2^\tau - 1}} f_{\xi_k}(s)\,\mathrm{d}s, \\
&\overset{(a)}{=} 1 - \frac{\delta A_1^k}{\Gamma(k)} \int_0^{\frac{\eta_l}{2^\tau - 1}} \exp(-A_1 s^\delta) s^{\delta k - 1}\,\mathrm{d}s, \\
&\overset{(b)}{=} \frac{\Gamma\left(k, A_1\left[\frac{\eta_l}{(2^\tau - 1)}\right]^\delta\right)}{\Gamma(k)},
\end{aligned} \tag{4.10}$$

where (a) follows from Theorem 1 and (b) follows [104, Eq. 3.381]. The PDF of the maximum achievable rate at the k_{th} legitimate receiver can be acquired by taking the

derivation of $\mathbb{P}_{out}\left(R_k < \tau\right)$ as follows:

$$f_{R_k}(\tau) = \ln 2\ \eta_l^{\delta k} \frac{\delta A_1^k}{\Gamma(k)} \frac{2^\tau}{(2^\tau - 1)^{\delta k+1}} \exp\left(-A_1 \left(\frac{\eta_l}{2^\tau - 1}\right)^\delta\right). \tag{4.11}$$

Similarly, the PDF of the maximum achievable rate at the worst-case eavesdropper can be obtained by setting $k = 1$ and $A_e = \pi\lambda_e \frac{\Gamma(\delta+m)}{m^\delta \Gamma(m)}$ as

$$f_{R_e}(\tau) = \ln 2\ \eta_e^{\delta} \frac{2^\tau \delta A_e}{(2^\tau - 1)^{\delta+1}} \exp\left(-A_e \left(\frac{\eta_e}{2^\tau - 1}\right)^\delta\right). \tag{4.12}$$

Then the distribution of the secrecy capacity at the k_{th} legitimate node can be easily obtained through the convolution of $f_{R_k}(\tau)$ for the k_{th} legitimate receiver and the worst-case eavesdropper similar to the steps used in [39] which ignored the effect of small scale fading. Note that in this scenario, we derive the PDF of the maximum achievable rate for the network under Nakagami-m fading. Since the PDF of ξ_k has already included the effect of fading, the density function for the composite channel gain of the worst-case eavesdropper can be calculated briefly by setting $k = 1$. Otherwise, deriving the distribution of the channel gain at the worst-case eavesdropper will be formidable task [38] if considering distribution of fading coefficient and path loss separately. An approximation of such a distribution has been derived in [38].

4.3.3 Probability of Secure Connection

Probability of secure connection is the probability to have a positive secrecy rate from the source node to the k_{th} legitimate receiver [100]. It can be derived from the secrecy outage probability in (4.2) and expressed by

$$\mathbb{P}_{sc,k} = \mathbb{P}\left\{\log_2\left(1 + \frac{\eta_l}{\xi_k}\right) - \log_2\left(1 + \frac{\eta_e}{\xi_e}\right) > 0\right\}. \tag{4.13}$$

By using an algebraic operation similar to the one derived in (4.13) and Theorem 1, the probability of secure connection can be obtained as

$$\mathbb{P}_{con,k} = 1 - \left(\frac{\lambda_l}{\lambda_l + \lambda_e}\right)^k. \tag{4.14}$$

Comparing with the derivation in [39], this result shows that fading does not affect the probability of secure connection which is determined only by the ratio of intensities.

4.3.4 Ergodic Secrecy Capacity without Protected Zone

In the scenario without the protected zone, the legitimate nodes and eavesdroppers are distributed as two independent PPPs with different intensities, λ_l and λ_e. It is worth to notice that the legitimate receivers are ordered by the distance between the source node and the legitimate receiver, meanwhile the ergodic capacity at the k_{th} legitimate receiver can be obtained based on Theorem 2. The ergodic capacity at the worst-case eavesdropper will be derived by applying the distribution of ξ_e as shown in the following theorem.

Theorem 2. *The ergodic capacity of the channel between the source node and the k_{th} legitimate node ordered by distance can be expressed as*

$$R_{s:k} = \frac{(\pi\lambda_l)^k \delta m^m}{\ln 2 \Gamma(m)\Gamma(k)} \int_0^\infty \int_0^\infty s^{m-1} \ln(1+\eta_l s)\, y^{k\delta+m-1} \exp\left(-msy - \lambda_l \pi y^\delta\right) \mathrm{d}y\, \mathrm{d}s. \tag{4.15}$$

Proof: We denote the distance from the source node to the k_{th} legitimate receiver as r_k, and $x_{k,l} = r_k^\alpha$. According to the mapping theorem, the random variable $x_{k,l}$ is also distributed as a PPP [105] with its distribution given by

$$f_{x_{k,l}}(x) = \frac{(\pi\lambda_l)^k \delta}{\Gamma(k)} x^{k\delta-1} \exp(-\pi\lambda x^\delta). \tag{4.16}$$

The distribution of Nakagami-m (power) fading model is given by [35]

$$f_{|h_{k,l}|^2}(x) = \frac{m^m x^{m-1} exp(-mx)}{\Gamma(m)}. \tag{4.17}$$

Accordingly, the PDF of the channel gain $\zeta_k = \frac{|h_{k,l}|^2}{x_{k,l}}$ can be derived from the joint distribution as

$$\begin{aligned} f_{\zeta_k}(s) &= \int_{-\infty}^{\infty} |y| f_{|h_{k,l}|^2,\, x_{k,l}}(sy, y)\, \mathrm{d}y, \\ &= \int_{0}^{\infty} y f_{|h_{k,l}|^2}(sy) f_{x_{k,l}}(y)\, \mathrm{d}y, \\ &= \int_{0}^{\infty} y \frac{m^m (sy)^{m-1} \exp(-msy)}{\Gamma(m)} \frac{(\pi\lambda_l)^k \delta}{\Gamma(k)} y^{k\delta-1} \exp(-\pi\lambda y^\delta)\, \mathrm{d}y, \\ &= \frac{(\pi\lambda_l)^k \delta m^m}{\Gamma(m)\Gamma(k)} \int_{0}^{\infty} s^{m-1} y^{k\delta+m-1} \exp(-msy - \lambda_l \pi y^\delta)\, \mathrm{d}y. \end{aligned} \tag{4.18}$$

By using (4.3) and (4.18), the ergodic capacity at the k_{th} legitimate receiver can be derived as

$$\begin{aligned} R_{s:k} &= \mathbb{E}_{\zeta_k}\left\{ \log_2 (1 + \eta_l \zeta_k) \right\}, \\ &= \frac{1}{\ln 2} \int_{0}^{\infty} \ln (1 + \eta_l s)\, f_{\zeta_k}(s)\, \mathrm{d}s, \\ &= \frac{1}{\ln 2} \int_{0}^{\infty} \ln (1 + \eta_l s) \frac{(\pi\lambda_l)^k \delta m^m}{\Gamma(m)\Gamma(k)} \int_{0}^{\infty} s^{m-1} y^{k\delta+m-1} \exp\left(-msy - \lambda_l \pi y^\delta\right) \mathrm{d}y\, \mathrm{d}s, \\ &= \frac{(\pi\lambda_l)^k \delta m^m}{\ln 2 \Gamma(m)\Gamma(k)} \int_{0}^{\infty} \int_{0}^{\infty} s^{m-1} \ln (1 + \eta_l s)\, y^{k\delta+m-1} \exp\left(-msy - \lambda_l \pi y^\delta\right) \mathrm{d}y\, \mathrm{d}s. \end{aligned} \tag{4.19}$$

Note that, when analyzing the ergodic secrecy capacity, the legitimate receivers are ordered by their distances to the source node. This is different from the ordering based on the combined effect of path loss and small-scale fading. Since the derivation of the ergodic secrecy capacity should be based on the communication between the same transmitter-receiver pair over a period of time, it will be reasonable to order the legitimate receivers according to their distances to the source node.

For the case of $\alpha = 4$ and $m = 1$ which is corresponding to Rayleigh fading, the ergodic

capacity at the nearest legitimate receiver can be obtained as follows:

$$\begin{aligned} R_{s:1} &= \frac{\pi\lambda_l}{2\ln 2}\int_0^\infty\int_0^\infty \ln\left(1+\eta_l s\right) y^{\frac{1}{2}} \exp\left(-sy-\lambda_l\pi y^{\frac{1}{2}}\right) \mathrm{d}s\,\mathrm{d}y, \\ &\overset{(a)}{=} \frac{\pi\lambda_l}{2\ln 2}\int_0^\infty y^{-\frac{1}{2}} \exp\left(-\lambda_l\pi y^{\frac{1}{2}}\right) G_{3,2}^{3,1}\left(\frac{\eta_l}{y}\middle|\begin{matrix}0,1,1\\ \\ 1,0\end{matrix}\right)\mathrm{d}y, \\ &\overset{(b)}{=} \frac{1}{\ln 2\sqrt{\pi}} G_{4,3}^{3,3}\left(\frac{4}{\eta_l(\pi\lambda_l)^2}\middle|\begin{matrix}0,\frac{1}{2},0,1\\ \\ 1,0,0\end{matrix}\right), \end{aligned} \tag{4.20}$$

where $G(\cdot)$ is the Meijer-G function; (a) follows by expressing $\ln(1+x)$ as Meijier G-function $\ln(1+x) = G_{2,2}^{1,2}\left(x\middle|\begin{matrix}1,1\\ \\ 1,0\end{matrix}\right)$ and applying the integration relationship [104, Eq. 7.813.1]; (b) follows from [104, Eq. 7.813.2]. Similarly, by using (4.3) and (4.7), the ergodic capacity of the channel between the source node and the worst-case eavesdropper can be expressed by

$$\begin{aligned} R_{s:e} &= \mathbb{E}_{\xi_e}\left\{\log_2\left(1+\frac{\eta_e}{\xi_e}\right)\right\}, \\ &= \frac{\delta A_e}{\ln 2}\int_0^\infty \ln\left(1+\frac{\eta_e}{s}\right) s^{\delta-1}\exp\left(-A_e s^\delta\right)\mathrm{d}s, \\ &= \frac{\delta A_{1e}}{\ln 2}\int_0^\infty s^{\delta-1}\exp\left(-A_e s^\delta\right) G_{2,2}^{1,2}\left(\frac{\eta_l}{s}\middle|\begin{matrix}1,1\\ \\ 1,0\end{matrix}\right)\mathrm{d}s, \\ &\overset{(a)}{=} \frac{1}{\ln 2\sqrt{\pi}} G_{4,2}^{2,3}\left(\frac{4}{\eta_e A_e^2}\middle|\begin{matrix}0,\frac{1}{2},0,1\\ \\ 1,0\end{matrix}\right), \end{aligned} \tag{4.21}$$

where (a) follows from $\alpha = 4$ and [104, Eq. 7.813.2]. Then, substitute (4.15) and (4.21) into (4.4), the lower bound of the ergodic secrecy capacity at the k_{th} legitimate node in the random network without a protected zone can be derived.

4.4 Enhancing Security with Secrecy Protected Zone

To enhance the security of the legitimate transmission, we adopt the scheme of the secrecy protected zone [98] where the source node can keep a circular area free of eavesdroppers, denoted as $\Theta(0,\ \rho_t)$ and ρ_t is the radius of the secrecy protected zone. Notice that legitimate nodes are still deployed as a PPP in $\mathbb{R}^2$ while eavesdroppers are distributed as a PPP in $\bar{\Theta}$, where $\bar{\Theta}$ represents the complement set of $\Theta(0,\ \rho_t)$ in $\mathbb{R}^2$. In this chapter, we will study the case that eavesdroppers are not colluding.

Since the ergodic capacity of the general case in this scenario is complicated to derive, we will first consider the worst case, i.e., the eavesdroppers try to approach the source node and stay at the boundary of the secrecy protected zone. In this case, the distance between the source node and the nearest eavesdropper is the radius of the secrecy protected zone, ρ_t. Later in this section, it will be proved that the nearest eavesdropper is the worst-case eavesdropper since it can acquire the largest ergodic capacity. Furthermore, the scenario that the eavesdroppers are distributed as a PPP outside the secrecy protected zone will also be investigated.

4.4.1 Eavesdropper on the Boundary of Secrecy Protected Zone

For the case that eavesdroppers are aware of the secrecy protected zone, we study the worst case that the eavesdroppers try to maximize their data rate by approaching the boundary of the zone. We will first prove that the nearest eavesdropper to the source node has the largest ergodic capacity in Proposition A and then derive the ergodic capacity at the worst-case eavesdropper.

Proposition 1. *The ergodic capacity $R_{s:r}$ of the channel between the source node and the receiving node is monotonically decreasing with their distance r for arbitrary fading channels.*

Proof: See Appendix A.

From Proposition A, we can see that the nearest eavesdropper can obtain the largest ergodic capacity. Therefore, the worst case is that there will be eavesdroppers on the

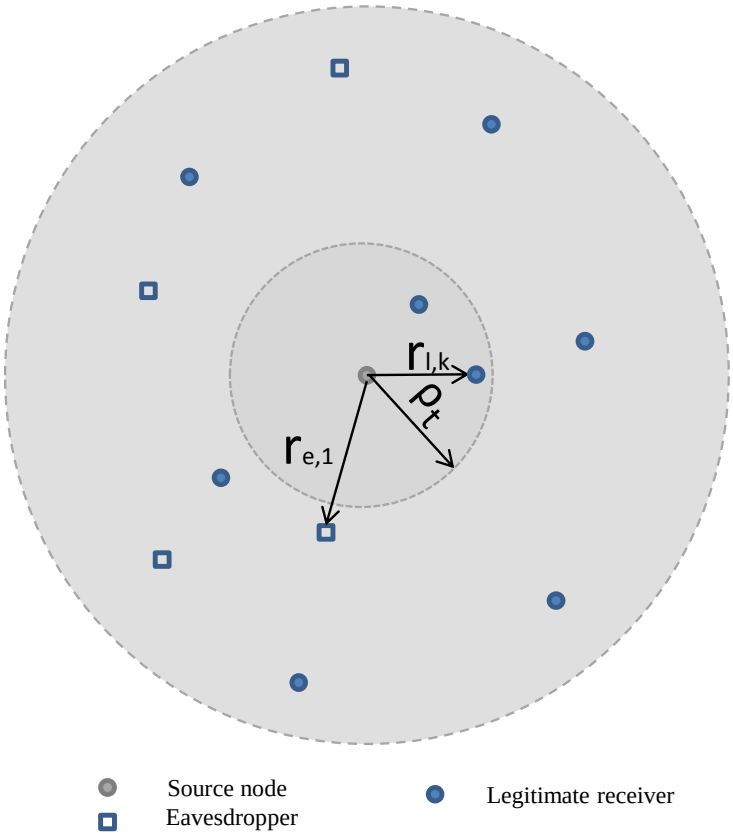

Figure 4.3: Random network with the secrecy protected zone.

boundary of the secrecy protected zone, i.e. $r_e = \rho_t$. By expressing $\ln(1+x)$ as Meijier G-function and applying the integration relationships [104, Eq. 7.813.1] and [104, Eq. 7.813.2], the ergodic capacity of the channel between the source node and the nearest eavesdropper can be calculated by

$$\begin{aligned} R_{s:e} &= \mathbb{E}_{|h_e|^2}\left\{\log_2\left(1+\frac{\eta_e|h_e|^2}{\rho_t^\alpha}\right)\right\}, \\ &= \frac{1}{\ln 2}\int_0^\infty \ln\left(1+\frac{\eta_e}{\rho_t^\alpha}x\right) f_{|h_e|^2}(x)\,\mathrm{d}x, \\ &= \frac{m^m}{\ln 2\Gamma(m)}\int_0^\infty \ln\left(1+\frac{\eta_e}{\rho_t^\alpha}x\right) x^{m-1}\exp(-mx)\,\mathrm{d}x. \\ &= \frac{m^m}{\ln 2\Gamma(m)}\int_0^\infty x^{m-1}\exp(-mx) G_{2,2}^{1,2}\left(\frac{\eta_e}{\rho_t^\alpha}x\,\middle|\,\begin{matrix}1,1\\1,0\end{matrix}\right)\mathrm{d}s, \\ &= \frac{1}{\ln 2\Gamma(m)} G_{3,2}^{1,3}\left(\frac{\eta_e}{m\rho_t^\alpha}\,\middle|\,\begin{matrix}1-m,1,1\\1,0\end{matrix}\right). \end{aligned} \tag{4.22}$$

For the case with Nakagami-m fading, the ergodic secrecy capacity lower bound at the k_{th} legitimate receiver with a secrecy protected zone can be obtained by substituting (4.15) and (4.22) into (4.4). For the case with Rayleigh fading, (4.22) can be simplified as

$$\begin{aligned} R_{s:e} &\overset{(a)}{=} \frac{1}{\ln 2}\int_0^{\infty} \ln\left(1+\frac{\eta_e}{\rho_t^{\alpha}}x\right)\exp(-x)\,\mathrm{d}x, \\ &\overset{(b)}{=} \frac{1}{\ln 2} G_{3,2}^{1,3}\left(\begin{array}{c|c} \dfrac{\eta_e}{\rho_t^4} & \begin{array}{c} 0,1,1 \\ \\ 1,0 \end{array} \end{array}\right), \end{aligned} \tag{4.23}$$

where (a) follows from that h_e is Rayleigh fading and its power is exponentially distributed; (b) follows from [104, Eq. 7.813.1] and E_i is the exponential integral.

4.4.2 Random Eavesdroppers Outside of Secrecy Protected Zone

For the general case, the eavesdroppers may be unaware of the boundary that their locations are still distributed as a PPP in the field outside the secrecy protected zone. According to Proposition 1, the worst-case eavesdropper is the nearest eavesdropper which will obtain the largest ergodic capacity. To calculate the ergodic capacity at the worst-case eavesdropper, we derive the distribution of its distance from the source node as shown in Theorem 3.

Theorem 3. *Consider a random network in which the nodes are modeled by a PPP outside a circular area. The PDF of the distance from the origin to the n_{th} nearest node is given by*

$$d_n(r) = 2\pi\lambda r \exp\left[-\pi\lambda\left(r^2-\rho^2\right)\right]\frac{\left[\pi\lambda\left(r^2-\rho^2\right)\right]^{n-1}}{(n-1)!},\ r>\rho, \tag{4.24}$$

where λ is the intensity and ρ is the radius of the circular area.

Proof: See Appendix B.

The PDF of the distance from the source node to the n_{th} receiving node outside a circular area in (4.24) has been verified by Monte Carlo simulations in Figure 4.4. When there is no protected zone, i.e. $\rho = 0$, the distribution of the distance from the origin to n_{th} node

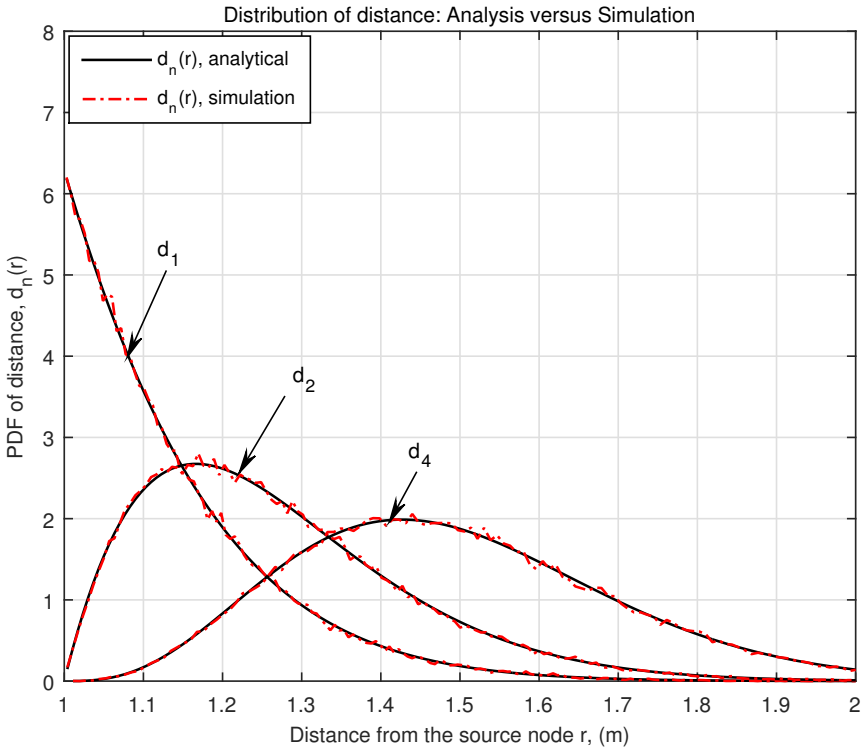

Figure 4.4: PDF of the distance from the source node to the n_{th} neighbor with $\lambda = 1, \rho_t = 1$; d_1, d_2 and d_4 show the distribution of the distances from the source node to the 1st, 2nd, and 4th nodes, respectively.

can be obtain from (4.24) as

$$d_n(r) = 2\pi\lambda r \exp(-\pi\lambda r^2)\frac{(\pi\lambda r^2)^{n-1}}{(n-1)!}. \tag{4.25}$$

This is exactly the PDF of the Euclidean distance from the source node to the n_{th} neighbor provided in [105]. The distribution of the distance from the nearest node to the origin can be obtained by setting $n = 1$ in (4.24) as

$$d_1(r) = 2\pi\lambda r \exp[-\pi\lambda(r^2 - \rho^2)],\ r > \rho. \tag{4.26}$$

Consequently, the ergodic capacity at the worst-case eavesdropper can be obtained by

$$\begin{aligned} R_{s:e} &= \mathbb{E}_{h_e, r_{e,1}} \left\{ \log_2 \left(1 + \frac{\eta_e |h_e|^2}{r_{e,1}^{\alpha}} \right) \right\}, \\ &= \mathbb{E}_{r_{e,1}} \left\{ \int_0^{\infty} \log_2 \left(1 + \frac{\eta_e}{r_{e,1}^{\alpha}} x \right) f_{|h_e|^2}(x)\, \mathrm{d}x \right\}, \\ &= \int_{\rho_t}^{\infty} \int_0^{\infty} \log_2 \left(1 + \frac{\eta_e}{y^{\alpha}} x \right) f_{|h_e|^2}(x)\, \mathrm{d}x f_{r_{e,1}}(y)\, \mathrm{d}y, \\ &= -\frac{2\pi\lambda_e}{\ln 2} \exp(\pi\lambda_e \rho^2) \int_0^{\infty} y \exp\left(\frac{y^{\alpha}}{\eta_e} - \pi\lambda_e y^2 \right) Ei\left(-\frac{y^{\alpha}}{\eta_e} \right) \mathrm{d}y. \end{aligned} \tag{4.27}$$

Notice that, to avoid confusion, we use $f_{r_{e,1}}(y)$ to denote the function of $d_1(r)$. Similarly, the lower bound on the ergodic secrecy capacity can be obtained by substituting (4.15) and (4.27) into (4.4).

4.5 Enhancing Security with both Secrecy and Interferer Protected Zones

4.5.1 Problem Formulation

In addition to adopting a secrecy protected zone around the source node, we introduce the interferer protected zones which will contribute to restructuring the interference and enhance the physical layer security. For the interference limited random network, properly restructuring the interference can reduce its detriment to the legitimate receivers more than that of the eavesdroppers. To reduce the interference in the legitimate channels, the legitimate receivers will broadcast beacon signals with the same power P_b [106]. The cooperative nodes that have received the beacon signals will stop transmission. Note that these cooperative nodes are different from those externally introduced jammers in [40], but similar to secondary transmitters in cognitive radio networks. The legitimate receivers will formulate another kind of protected zones $\Phi_d = \{\mathfrak{D}(x, \rho_d) | x \in \Phi_l\}$, where $\mathfrak{D}(x, \rho_d)$ is the circular area centered at x with radius ρ_d and x is the coordinate of the legitimate

receiver. Then, the set of the cooperative nodes can be expressed by

$$\Phi_c = \left\{ u_i \middle| u_i \in \left\{ \mathbb{R}^2 - \bigcup_{x \in \Phi_l} \mathfrak{D}(x, \rho_d) \right\} \right\}, \ i \in \mathbb{N}.$$

The description of the system model is given as follows and illustrated in Figure 4.5,

- The distribution of the source node and the legitimate receivers are the same as the previous scenarios in Section 4.2, 4.3 and 4.4;
- The cooperative nodes are modeled by a homogeneous PPP with intensity λ_c;
- To reduce the detriment from the interference, interferer protected zones are adopted surrounding the legitimate receivers. The legitimate receivers will prevent cooperative nodes that are located in a nearby region from transmitting signals inside the interferer protected zones, by adopting the request-to-send/clear-to-send (RTS/CTS) protocol in IEEE 802.11 [99].

To calculate the ergodic secrecy capacity, we will first derive the distribution of the aggregate interference and the ergodic capacity at the legitimate receivers and the eavesdroppers.

4.5.2 Distribution of the Aggregated Interference and Ergodic Capacity at the Legitimate Receiver

The locations of the active cooperative nodes are depending on the exclusion regions which are set up by the legitimate receivers. The random set of active cooperative nodes can be considered as a Poisson hole process [33] with its intensity denoted as λ_{eqc}. The probability of a point retained in the Poisson hole process is the probability that no active cooperative node exists within the distance r from the legitimate receiver. Consequently, the intensity of the Poisson hole process is given by

$$\lambda_{eqc} = \lambda_c \exp\left(-\lambda_l \pi r^2\right). \tag{4.28}$$

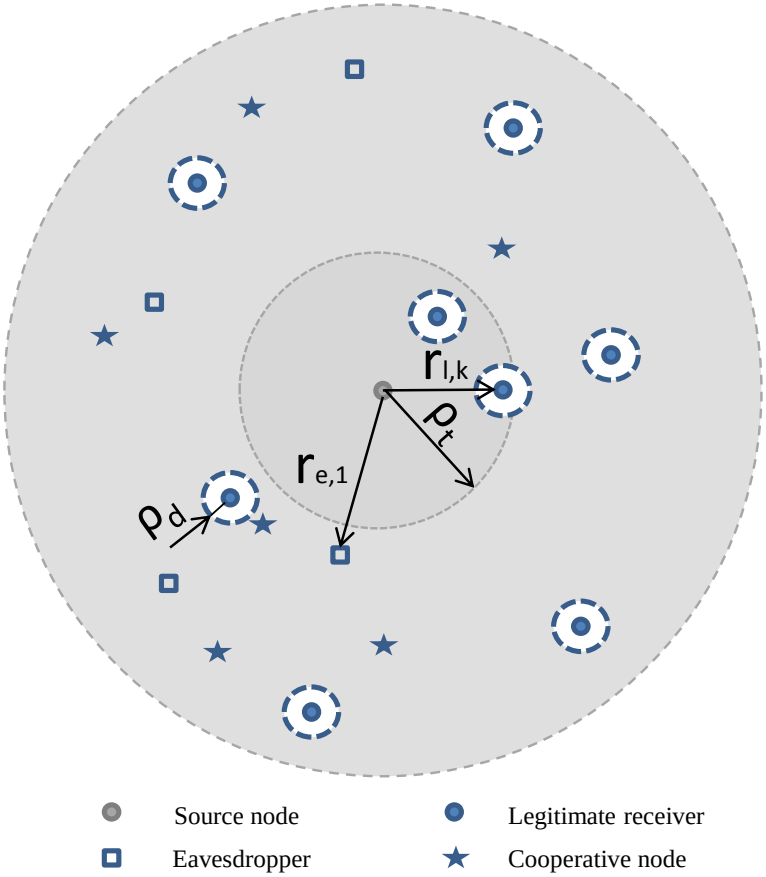

Figure 4.5: Random network with a secrecy protected zone at the source node denoted by $\mathfrak{D}(0, \rho_t)$ and interferer protected zones surrounding the legitimate receivers denoted by $\mathfrak{D}(x, \rho_d)$.

The distribution of the active cooperative nodes is restructured by independent thinning of the cognitive users outside the exclusion regions. In the following subsection, we will calculate the distribution of the aggregate interference from the cooperative nodes to the legitimate receivers based on this approximation.

Interference at the Legitimate Receivers

The point process of the active cooperative nodes is not a PPP but a Poisson hole process. According to the properties of point process transformation, independent thinning of the cooperative nodes outside the interference protected zones with probability of $\exp(-\lambda_l \pi \rho_d^2)$ yields a good approximation on I_{cd} [107]. To make the characteristic of interference more tractable, the interference from the Poisson hole process can be modeled by a virtual PPP. The parent PPP has to be independently thinned to match the

density of the PPP with that of Poisson hole process, which affects the local neighborhood of interferers that surround the legitimate receiver [108]. As a result, the accuracy of the approximation will reduce when the repulsive distance increases. The approximation in this research is based on the assumption of small repulsive distance. The aggregate interference from the cooperative nodes to the legitimate receivers can be obtained by using equation (3.46) in [109], while the interference in our case is analyzed based on a virtual PPP with intensity $\lambda_c \exp(-\lambda_l \pi r^2)$. Denote the moment generating function (MGF) of aggregated interference at the legitimate receivers as $\mathcal{L}_{I_{cd}}(s)$, it is given by

$$\mathcal{L}_{I_{cd}}(s) = \exp\left\{ -\lambda_{eqc}\pi\left(s^{\delta}\mathbb{E}_h\left(h^{\delta}\gamma(1-\delta, sh\rho^{-\alpha})\right) - \rho^2\mathbb{E}_h\left(1-\exp(-sh\rho^{-\alpha})\right)\right)\right\}. \tag{4.29}$$

For Rayleigh fading, equation (4.29) can be written as

$$\mathcal{L}_{I_{cd}}(s) = \exp\left\{-\lambda_{eqc}\pi\left(\frac{s\Gamma(2)}{(1-\delta)\rho^{\alpha(1-\delta)}}\,{}_2F_1(1-\delta, 2; 2-\delta; -s\rho^{-\alpha}) + \frac{s\rho^2}{s+\rho^{\alpha}}\right)\right\}, \tag{4.30}$$

where ${}_2F_1(\cdot)$ stands for Hypergeometric function.

Ergodic Capacity at the Legitimate Receivers

We denote the SINR at the k_{th} legitimate receiver as $\gamma_{s:k}$, then

$$\begin{aligned}\gamma_{s:k} &= \frac{P|h_k|^2 r_k^{-\alpha}}{P_c\sum_{i\in\Phi_c}|h_{i,k}|^2 r_{i,k}^{-\alpha} + \sigma_k^2}, \\ &= \frac{S_{td}}{I_{cd}+N_{cd}},\end{aligned} \tag{4.31}$$

where $h_{i,k}$ denotes the fading coefficient between the i_{th} cooperative node and the k_{th} legitimate receiver; N_{cd} denotes the noise at the legitimate receiver. Assuming that the noise at the legitimate receivers are dominated by the interference, the success probability

at the k_{th} legitimate receiver can be derived by

$$\begin{aligned}\mathbb{P}_{td}(\tau) &\approx \mathbb{P}\left(\gamma_{s:k} > \tau\right), \\ &= \mathbb{P}\left(S_{td} > \tau I_{cd}\right), \\ &\overset{(a)}{=} \mathbb{E}_{I_{cd}}\left(\exp(-\tau P^{-1} r_k^{\alpha} I_{cd})\right), \\ &\overset{(b)}{=} \mathcal{L}_{I_{cd}}\left(\frac{\tau}{P\, r_k^{-\alpha}}\right),\end{aligned} \tag{4.32}$$

where (a) follows from that of $|h_k|^2$ is exponentially distributed and (b) follows from Laplace transformation. Substitute (4.30) into (4.32), we can obtain the expression of success probability at the k_{th} legitimate receiver. The CDF of the SIR at the k_{th} legitimate receiver can be denoted by $F_{\gamma_{s:k}}(\tau) = 1 - \mathcal{L}_{I_{cd}}\left(\frac{\tau}{Pr_k^{-\alpha}}\right)$. Then we derive the PDF of the SIR from $F_{\gamma_{s:k}}(z)$ and analyze the ergodic capacity at the k_{th} legitimate receiver as [101]. Assuming that the distance r_k is known at the transmitter, the ergodic capacity at the k_{th} legitimate receiver can be obtained as

$$\begin{aligned}R_{s:k} &= \int_0^{\infty} \log_2(1+\tau) f_{\gamma_{s:k}}(\tau)\, \mathrm{d}\tau, \\ &= \frac{1}{\ln 2}\int_0^{\infty} \ln(1+\tau)\, \mathrm{d}\left[1 - \mathcal{L}_{I_{cd}}\left(\frac{\tau}{Pr_k^{-\alpha}}\right)\right], \\ &= (-1)\frac{1}{\ln 2}\ln(1+\tau)\mathcal{L}_{I_{cd}}\left(\frac{\tau}{Pr_k^{-\alpha}}\right)\Big|_0^{\infty} + \frac{1}{\ln 2}\int_0^{\infty} \mathcal{L}_{I_{cd}}\left(\frac{\tau}{Pr_k^{-\alpha}}\right)\frac{1}{1+\tau}\,\mathrm{d}\tau, \\ &= \frac{1}{\ln 2}\int_0^{\infty} \mathcal{L}_{I_{cd}}\left(\frac{\tau}{Pr_k^{-\alpha}}\right)\frac{1}{1+\tau}\,\mathrm{d}\tau.\end{aligned} \tag{4.33}$$

The ergodic capacity in (4.33) can be calculated by using numerical methods. Since deriving the closed-form expression of the ergodic capacity at the k_{th} legitimate receiver is complicated, we analyze the lower bound of the interference at the legitimate receiver and obtain

$$\begin{aligned}\mathcal{L}_{I_{cd}}(s) &= \exp\Big\{ -\lambda_{eqc}\pi\Big[s^{\delta}\mathbb{E}_h(h^{\delta}\gamma(1-\delta, sh\rho^{-\alpha})) - \rho^2\mathbb{E}_h(1-\exp(-sh\rho^{-\alpha}))\Big]\Big\}, \\ &\overset{(a)}{\geq} \exp\Big\{ -\lambda_{eqc}\pi\Big[s^{\delta}\mathbb{E}_h(h^{\delta}\Gamma(1-\delta)) - \rho^2\mathbb{E}_h(1-\exp(-sh\rho^{-\alpha}))\Big]\Big\}, \\ &= \exp\Big\{ -\lambda_{eqc}\pi\Big[s^{\delta}\Gamma(1+\delta)\Gamma(1-\delta) - \frac{s\rho^2}{s+\rho^{\alpha}}\Big]\Big\},\end{aligned} \tag{4.34}$$

where (a) follows from $\gamma(a,x) \leq \Gamma(a)$ according to the definition of the lower incomplete gamma function and gamma function, as $\int_0^x t^{a-1}e^{-t}\,\mathrm{d}t \leq \int_0^\infty t^{a-1}e^{-t}\,\mathrm{d}t$. According to (4.33), the lower bound of the ergodic capacity at the k_{th} legitimate receiver can be expressed by

$$\begin{aligned}
R_{s,k} &\overset{(a)}{=} \frac{Pr_k^{-\alpha}}{\ln 2}\int_0^\infty \mathcal{L}_{I_{cd}}(s)\frac{1}{1+Pr_k^{-\alpha}s}\,\mathrm{d}s,\\
&\overset{(b)}{\geq} \frac{Pr_k^{-\alpha}}{\ln 2}\int_0^\infty \frac{1}{1+Pr_k^{-\alpha}s}\exp\Big\{\lambda_{eqc}\pi\frac{s\rho^2}{s+\rho^\alpha}\Big\}\\
&\quad\times\exp\Big\{-\lambda_{eqc}\pi\Gamma(1+\delta)\Gamma(1-\delta)s^\delta\Big\}\,\mathrm{d}s,\\
&\overset{(c)}{=} \frac{Pr_k^{-\alpha}\Gamma(1+\frac{1}{\delta})}{a^{\frac{1}{\delta}}\ln 2}\mathbb{E}_s\Big[\frac{1}{1+Pr_k^{-\alpha}s}\exp\Big(\lambda_{eqc}\pi\frac{s\rho^2}{s+\rho^\alpha}\Big)\Big],\\
&\overset{(d)}{\geq} \frac{Pr_k^{-\alpha}\Gamma(1+\frac{1}{\delta})}{a^{\frac{1}{\delta}}\ln 2}\frac{1}{1+Pr_k^{-\alpha}\mathbb{E}_s(s)}\exp\Big(\lambda_{eqc}\pi\frac{\mathbb{E}_s(s)\rho^2}{\mathbb{E}_s(s)+\rho^\alpha}\Big),
\end{aligned} \tag{4.35}$$

where (a) follows by substituting τ with $Pr_k^{-\alpha}s$; (b) follows from (4.34); (c) follows by defining the PDF of s as $f_s(x) = \frac{a^{1/\delta}}{\Gamma(1+1/\delta)}\exp(-ax^\delta)$ and $a = \pi\lambda_{eqc}\Gamma(1+\delta)\Gamma(1-\delta)$; (d) follows from Jenson's inequality with the expectation of s been given by $\mathbb{E}_s(s) = \int_0^\infty s f_s(x)\,\mathrm{d}s = \frac{\Gamma(2/\delta)}{\delta a^{1/\delta}\Gamma(1+1/\delta)}$.

4.5.3 Distribution of the Aggregated Interference and Ergodic Capacity at the Worst-Case Eavesdropper

The Interference at the Eavesdroppers

Similarly, the aggregate interference from the cooperative nodes to the eavesdroppers can be obtained by using equation (3.21) in [109] and

$$\mathcal{L}_{I_{ce}}(s) = \exp\left(-\lambda_{eqc}\pi s^\delta\frac{\pi\delta}{\sin(\pi\delta)}\right). \tag{4.36}$$

Ergodic Capacity at the Eavesdroppers

Ergodic capacity at the eavesdroppers can be derived following the work of [101]. Denoting the SINR at the eavesdropper as $\gamma_{s:e}$, we have

$$\begin{aligned}\gamma_{s:e} &= \frac{P|h_e|^2 r_e^{-\alpha}}{P_c \sum_{i\in\Phi_c} |h_{i,e}|^2 r_{i,e}^{-\alpha} + \sigma_e^2}, \\ &= \frac{S_{te}}{I_{ce} + N_{ce}},\end{aligned} \tag{4.37}$$

where $h_{i,e}$ denotes the fading coefficient from i_{th} cooperative node to the nearest eavesdropper; N_{ce} denotes the noise at the legitimate receiver. Assuming that the noise at the eavesdroppers are dominated by the interference, the success probability at the eavesdroppers is given by

$$\begin{aligned}\mathbb{P}(\tau) &\approx \mathbb{P}(S_{te} > \tau I_{ce}), \\ &= \mathbb{E}_h \left(\exp(-\tau P^{-1} r_e^{\alpha} I_{ce})\right), \\ &= \mathcal{L}_{I_{ce}} \left(\frac{\tau}{P\, r_e^{-\alpha}}\right).\end{aligned} \tag{4.38}$$

Substitute (4.28) and (4.36) into (4.38), we can obtain the success probability at the eavesdroppers. The CDF of the SIR at the eavesdroppers can be denoted by

$$\begin{aligned}F_{\gamma_{s:e}}(\tau) &= 1 - \mathcal{L}_{I_{ce}} \left(\frac{\tau}{P r_e^{-\alpha}}\right), \\ &= 1 - \exp\left(-b_e r_e^2 \tau^{\delta}\right),\end{aligned} \tag{4.39}$$

where $b_e = \frac{\pi^2 \lambda_{eqc} \delta}{P^{\delta} \sin(\pi\delta)}$. Then the PDF of the SIR $f_{\gamma_{s:e}}(\tau)$ can be derived from $F_{\gamma_{s:e}}(\tau)$ as

$$f_{\gamma_{s:e}}(\tau) = \delta b_e r_e^2 \tau^{\delta-1} \exp\left(-b_e r_e^2 \tau^{\delta}\right). \tag{4.40}$$

Considering the security constraint, we study the ergodic capacity at the nearest eavesdropper which can obtain the maximum ergodic capacity as shown in Proposition 1.

The ergodic capacity at the nearest eavesdropper is given by

$$\begin{aligned} R_{s,e} &= \int_{\rho_t}^{\infty} \int_{0}^{\infty} \log_2(1+\tau) f_{\gamma_{t:e}}(\tau) f_{r_e}(x)\, \mathrm{d}\tau\, \mathrm{d}x, \\ &= \frac{1}{\ln 2} \int_{\rho_t}^{\infty} f_{r_e}(x) \int_{0}^{\infty} \ln(1+\tau)\, \mathrm{d}\left[-F_{\gamma_{s:e}}(\tau)\right] \mathrm{d}x, \\ &= \frac{1}{\ln 2} \int_{\rho_t}^{\infty} f_{r_e}(x) \int_{0}^{\infty} \exp(-b_e x^2 \tau^{\delta}) \frac{1}{1+\tau} d\tau\, \mathrm{d}x, \\ &= \frac{2\pi\lambda \exp(\pi\lambda\rho_t^2)}{\ln 2} \int_{\rho_t}^{\infty} \int_{0}^{\infty} \frac{x}{1+\tau} \exp\left[-(\pi\lambda + b_e\tau^{\delta}) r_{e,1}^2\right] \mathrm{d}x\, \mathrm{d}\tau, \\ &= \frac{\pi\lambda}{\ln 2} \int_{0}^{\infty} \frac{\exp(-b_e\rho_t^2\tau^{\delta})}{(1+\tau)(\pi\lambda + b_e\tau^{\delta})}\, \mathrm{d}\tau. \end{aligned} \tag{4.41}$$

Accordingly, the lower bound on the ergodic secrecy capacity at the k_{th} legitimate receiver can be obtained by substituting (4.35) and (4.41) into (4.4).

4.6 Numerical Results

In Section 4.3 and 4.4, we have simulated the distribution of the composite channel gain and the PDF of the distance in Figure 4.2 and Figure 4.4, respectively. In this section, we will investigate the effect of various factors on the lower bound of the ergodic secrecy capacity, including the intensity ratio, the radius of the protected zone, path loss, interference and transmission power.

4.6.1 Probability of Secure Connection in Noise Limited Network

The analytical result for the probability of secure connection in noise limited network is given in (4.14). It is shown that the probability of secure connection is determined by the ratio of intensities, i.e., λ_l/λ_e, while it is not affected by the channel fading. Intuitively, this is because that channel fading affect both the legitimate nodes and the eavesdroppers in the same way, i.e., the fading of the legitimate channels and the eavesdropping channel have the same distribution.

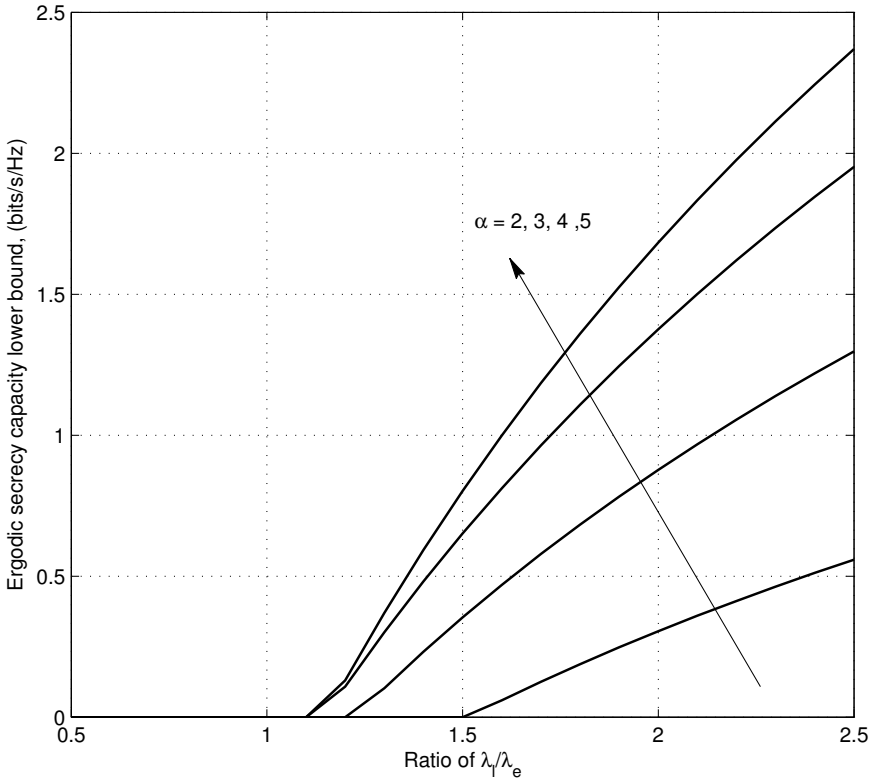

Figure 4.6: The ergodic secrecy capacity as a function of the ratio, λ_l/λ_e with different path-loss exponents with $\lambda_e = 1$ and $m = 1$.

4.6.2 Ergodic Secrecy Capacity in Noise Limited Network

Figure 4.6 illustrates the lower bound of the ergodic secrecy capacity between the source node and the legitimate receivers without a protected zone. In this scenario, the impact of path loss and the intensity ratio between the legitimate receivers and eavesdroppers is investigated. As shown in Figure 4.6, the lower bound of ergodic secrecy capacity is monotonically increasing with the increase of the intensity ratio between the legitimate and eavesdropping nodes. When the legitimate receivers and eavesdroppers experience the same fading and path loss, the ergodic secrecy capacity at all the legitimate receivers are zero if their intensity is equal to or smaller than the intensity of eavesdroppers, i.e. $\lambda_l/\lambda_e \leq 1$. An interesting point shown in Figure 4.6 is that increasing the path loss exponent is beneficial for enhancing the ergodic secrecy capacity which is due to the difference of their distance to the source under the condition of $\lambda_l/\lambda_e > 1$.

Figure 4.7 reveals the impact of adopting a secrecy protected zone surrounding the source

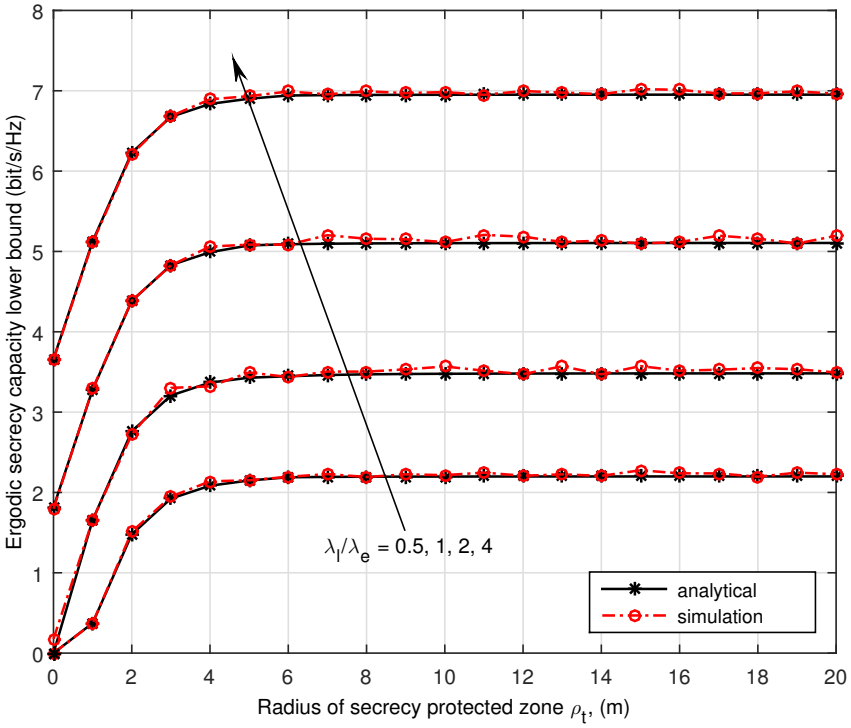

Figure 4.7: The impact of the secrecy protected zone on the ergodic secrecy capacity with $P_t/\sigma_l^2 = P_t/\sigma_e^2 = 20, \lambda_e = 0.1, \alpha = 4$ and $\rho_d = 2$.

node to enhance the ergodic secrecy capacity. ρ_t denotes the radius of the secrecy protected zone, i.e., there is no eavesdropper in the circular area which is surrounding the source node with a radius of ρ_t. As shown in Figure 4.7, for the same intensity ratio between the legitimate receivers and the eavesdroppers, increasing the radius of the protected zone can be helpful to enhance the ergodic secrecy capacity. This is obvious as increasing the radius of the secrecy protected zone will increase the minimum distance from source node to the nearest eavesdropper. Compared to the results shown in Figure 4.6 where the ergodic secrecy capacity will be zero if $\lambda_l/\lambda_e \leq 1$, the application of a protected zone ensures that positive ergodic secrecy capacity can still be achieved even if $\lambda_l/\lambda_e \leq 1$, for example, $\lambda_l/\lambda_e = 0.5$. Another insight gained from Figure 4.7 is that the increase of ρ_t has limited impact on the ergodic secrecy capacity. This limitation is the value of the ergodic capacity at the legitimate receiver, since the ergodic secrecy capacity cannot be larger than ergodic capacity at the legitimate receiver.

Figure 4.8 and Figure 4.9 show the impact of the secrecy protected zone surrounding the source node, as well as the impact of the intensity ratio on ergodic secrecy capacity. The

legitimate receiving nodes are ordered by their distances to the source node. As shown in Figure 4.8, it is clear that, if the radius of the protected zone is zero, i.e., there is no protected zone, the three scenarios have the same secrecy performance. For different scenarios with the same value of intensity ratio and protected zone radius, adopting a protected zone will significantly improve the lower bound of the ergodic secrecy capacity. When eavesdroppers are aware of the secrecy protected zone boundary, security will be undermined, but it can still achieve higher ergodic secrecy capacity comparing to the case without a protected zone. Figure 4.8 also suggests that increasing the radius of the secrecy protected zone is helpful to increase ergodic secrecy capacity. Figure 4.9 further indicates that increasing the intensity ratio between legitimate receivers and eavesdroppers will lead to a higher ergodic secrecy capacity for all scenarios.

4.6.3 Ergodic Secrecy Capacity in Interference Dominated Network

Figure 4.10 shows the comprehensive impact of the protected zone radius at the legitimate receivers and the intensity of cooperative nodes. It is apparent that increasing transmission power at the source node increases the ergodic capacity lower bound at legitimate receivers. Although increasing the intensity of cooperative nodes undermine the security performance at legitimate receivers, the adoption of a secrecy protected zone can increase the ergodic secrecy capacity lower bound. In other words, combined with a secrecy protected zone, using an interferer protected zone in order to restructure interference can improve the ergodic secrecy capacity lower bound. This is because a larger interferer protected zone radius, ρ_d, will reduce interference noise at the legitimate nodes compared to that at eavesdroppers.

4.7 Summary

In this work, we studied physical layer security in random wireless networks. The PDF of the channel gains by considering both fading and path loss was considered and a closed form expression of its reciprocal is derived. This result was then applied to analyze the probability of secure connection and ergodic secrecy capacity. The ordering of receivers

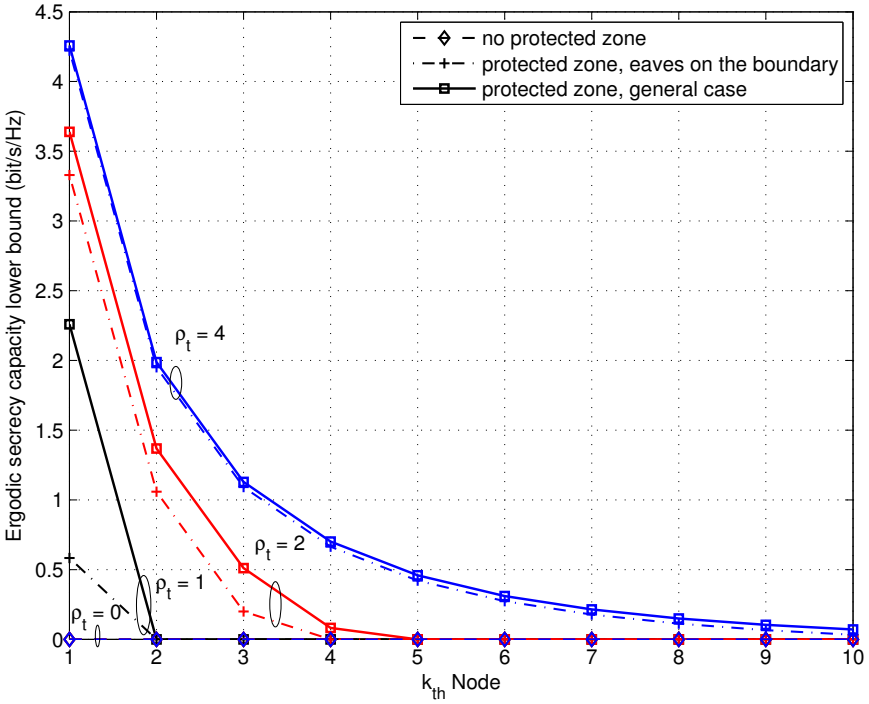

Figure 4.8: The impact of the secrecy protected zone size on ergodic secrecy capacity with $P_t/\sigma_l^2 = P_t/\sigma_e^2 = 20, \lambda_l = \lambda_e = 0.2, \alpha = 4$ and $\rho_d = 2$.

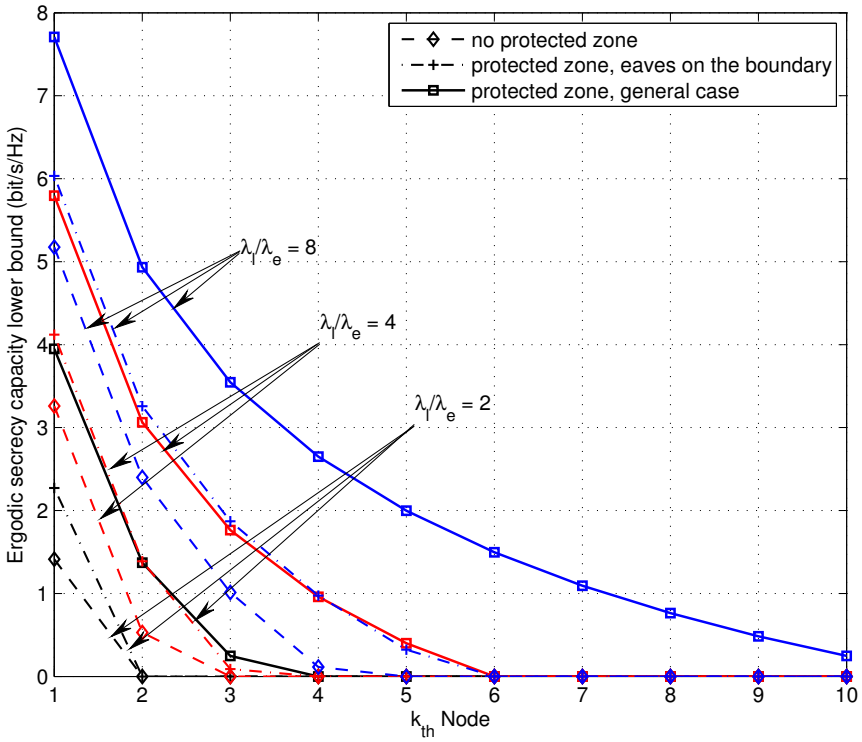

Figure 4.9: The impact of intensity ratio on ergodic secrecy capacity with $P_t/\sigma_l^2 = P_t/\sigma_e^2 = 20, \lambda_e = 0.2, \alpha = 4, \rho_t = 1$ and $\rho_d = 2$.

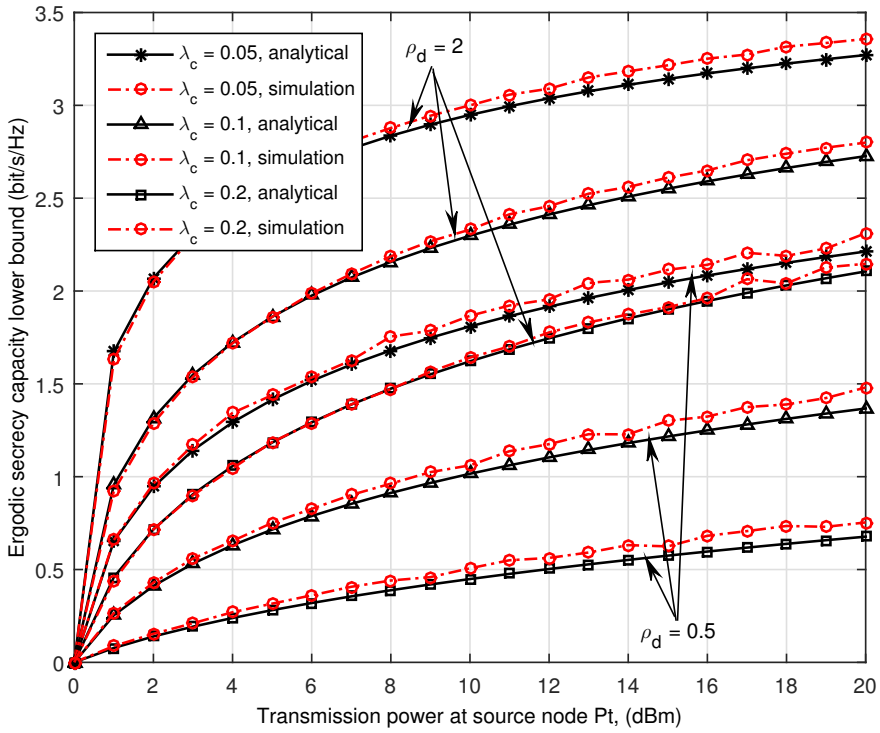

Figure 4.10: The impact of the interferer protected zones on ergodic secrecy capacity, with $\alpha = 4, \lambda_l = \lambda_e = 0.1, \rho_t = 5$ and $P_c/\sigma_l^2 = P_c/\sigma_e^2 = 1$.

was based on the composite effect of fading and path loss in deriving the probability of secure connection, while the ordering of receivers for deriving ergodic secrecy capacity was based on their path loss. Furthermore, we investigated the scenario with a secrecy protected zone to enhance physical layer security and the analytical expression of ergodic secrecy capacity is obtained. Moreover, interferer protected zones surrounding legitimate receivers are also considered to reduce the detriment from interference.

By employing protected zones, positive ergodic secrecy capacity can be achieved even if the intensity of the legitimate nodes is smaller than that of the eavesdropping nodes in random wireless networks. The application of interferer protected zones can make the interference beneficial to the security of the wireless network. Both the PDFs of the channel gains and the concept of ergodic secrecy capacity provided in this chapter can be easily extended to the analysis of other secrecy characteristics in random wireless networks, such as secrecy outage probability. They can also be extended to investigate the cases with eavesdroppers colluding and multiple antennas at the source node.

Chapter 5

Security of Downlink Cellular Networks with Fractional Frequency Reuse

5.1 Introduction

To incorporate physical layer security into practical usages, recent works extended the implementation of stochastic geometric tools to cellular networks in [30] and [31]. In these papers, the locations of the BSs are modeled by homogeneous PPPs to analyze the average secrecy rate, coverage of secure connection and secrecy outage probability. Although PPP is a favorable model for the deployment of the BSs due to its tractability, the locations of the BSs appear to form a more regular pattern since they are repulsive to each other. Consequently, a better solution is to model the deployment of the BSs as a more regular point process, such as the HCPP [32]. HCPP is a point process where the distance between each pair of the points are larger than a certain minimum value [33]. In [34], HCPP was exploited to characterize the secrecy performance, i.e., the secrecy outage probability of the downlink AWGN channel of the cellular network, by assuming that the target mobile station (MS) is interference-free.

Related Work

To improve the performance of the cellular network, FFR was proposed as an inter-cell interference coordination (ICIC) strategy with the absence of an eavesdropper in [110] and [111]. The basic idea of FFR is to partition the bandwidth of the cell to reduce interference at the cell users. Another benefit is that FFR can make cell-edge users free from the interference of the adjacent cells. Similar concept to enhance security is

the sectorized transmission which was studied in [36], [42] and [112]. The sectorized transmission was accomplished by transmitting independent signals in several sectors of the cell by using directional antennas [36]. Based on the strategy of sectorized transmission, [42] analyzed the effect of adopting multiple antennas to enhance security in the interference-free scenario. The combination of sectoring and artificial noise was further analyzed in [112]. The transmitter sends the source information in the sector where the target user is located, and transmits artificial noise to other sectors. Although the approach of FFR is similar to that of sectorized transmission as they both partition the whole cell into separate sectors, FFR requires BSs to transmit with different sub-bands of the total bandwidth to different sectors. Consequently, from the view of security, FFR will also contribute towards increasing the secrecy rate by reducing interference at the cell users, due to the division of frequency bands.

The study in [31] investigated physical layer security in cellular networks by comparing the approaches of communicating with the nearest BS and the optimum BS, by ignoring the channel fading and interference. To enhance physical layer security in an ad-hoc network, the combined effect of artificial noise and sectoring was analyzed in [112], by using the same frequency for all the sectors. Analysis of secrecy outage probability in the downlink of cellular networks was studied in [30] by approximating the PDF of interference.

In comparison, this work considered the repulsive property of the BSs by modeling the cellular network as a HCPP. The strategy of FFR investigated in this paper is also distinct from the sectorized transmission due to different characteristics of the interference. Moreover, the secrecy outage probability studied in this paper is analyzed by comparing the secrecy capacity with a threshold value, rather than comparing the SIR at the eavesdropper with a target value [112].

Contributions

The contributions of this research are summarized as follows:

- We derived the approximated distance distribution of HCPP. Further analysis and

simulation showed that the distance distribution can be approximated with a virtual PPP, which is applied to investigate the secrecy performance of transmission with the best BS.

- For the noise-limited cellular network, two transmission schemes are investigated, i.e., the downlink transmission with and without FFR. For the scheme without FFR, two transmission strategies are analyzed by selecting different BSs, i.e., the nearest BS versus the best BS. The distribution of the channel gain from the nearest BS to the user was obtained by combining the distribution of the small scale fading and path loss, while the derivation for the distribution of the channel gain from the best BS was based on exploiting the characteristic of a PPP.

- For the scenario of interference-limited networks, we further study the application of the FFR to enhance physical layer security in the downlink transmission of cellular networks. To analyze the secrecy outage probability in the downlink cellular networks, the PDFs of the SIRs are derived for both the scenarios with and without using FFR, based on the analysis of the inter-cell interference.

- The statistical characteristics of interference in downlink cellular networks are also investigated to study the effect of FFR.

This chapter is organized as follows. Section 5.2 presents the system model and problem formulation. In Section 5.3, we analyze the security outage probability of the downlink transmission in noise-limited cellular networks for the following transmission schemes: i) best BS without FFR; ii) nearest BS without FFR; iii) nearest BS with FFR. The secrecy outage probability in interference-limited cellular networks are investigated in Section 5.4 for the schemes with and without FFR. Numerical results are presented in Section 5.5. Conclusions and topics of interest for future work are discussed in Section 5.6.

5.2 System Model and Problem Formulation

5.2.1 Downlink System Model

We consider the downlink of a cellular network where the BSs are deployed according to the repulsive property, which is thinned from a parent homogeneous PPP Φ_p with intensity λ_p. The parent point process $\Phi_p = \{(x_i, m_i); i = 1, 2, 3, ...\}$ is a marked PPP, where x_i denotes the i_{th} point of the process and m_i stands for its mark, which is uniformly distributed in the range $[0, 1]$. The repulsive point process guarantees the minimum distance ϱ between any two BSs in the network. In this chapter, we model this repulsive point process as a Matérn hard-core point process (MHCPP) of type II Φ_M with intensity λ_M [78]. Φ_M is obtained by removing all the points in Φ_p that have a neighbor within distance ϱ that has a smaller mark. The cellular network deployment is shown in Figure 5.1, where r_l and r_e denotes the distance from the transmitting BS to the legitimate receiver and the eavesdropper, respectively. The eavesdroppers are distributed as an independent PPP, i.e. Φ_e, with their intensity being denoted as λ_e. The BSs are assumed to transmit with the same power P. We consider the security at a typical legitimate user. We assume that all the BSs transmit with the same power P.

Path Loss Process with Fading

Let $\Xi_M = \{\xi_{i,l} = \frac{r_{i,l}^{\alpha}}{|h_{i,l}|^2}, i = 1, 2, 3, ..., n\}$ be the path-loss process with fading at the legitimate user [35], where α is the path loss exponent, $r_{i,l}$ and $h_{i,l}$ denote the distance and the fading coefficient from the i_{th} BS to the typical legitimate user, respectively. Consequently, Ξ_M is also a PPP [35] and its intensity will be discussed in section 5.3. For the eavesdroppers, the path loss process with fading can be denoted as $\Xi_e = \{\xi_{k,e} = \frac{r_{k,e}^{\alpha}}{|h_{k,e}|^2}, k = 1, 2, 3, ..., n\}$, where $r_{k,e}$ and $h_{k,e}$ denote the distance and fading coefficient from the serving BS to the k_{th} eavesdropper, respectively.

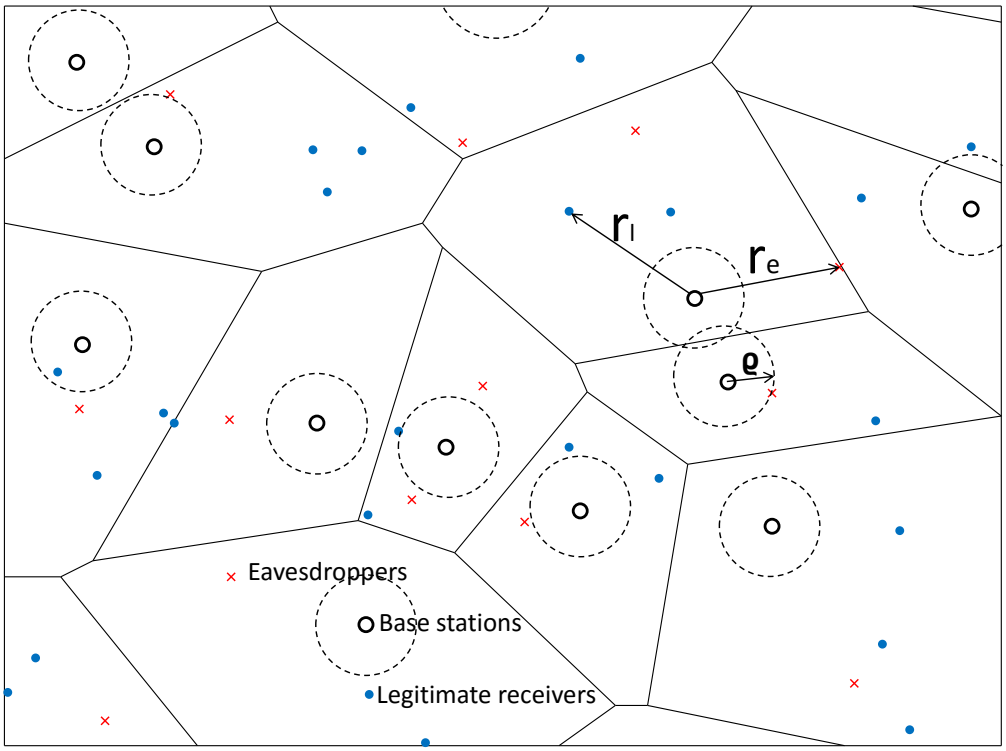

Figure 5.1: Illustration of a cellular network.

Interference Modeling

The inter-cell interference at the receiver is the sum of the received powers from all other BSs except that of the target BS. The inter-cell interference at the legitimate user can be written as

$$I_l = P \sum_{i \in \Phi_M \setminus \{o\}} |h_{i,l}|^2 r_{i,l}^{-\alpha}, \tag{5.1}$$

where P stands for the transmission power at other BSs.

We denote the SINR at the legitimate user as γ_l, which is given by

$$\gamma_l = \frac{P/\xi_l}{I_l + \sigma_l^2}, \tag{5.2}$$

where $\xi_l = \frac{r_l^\alpha}{|h_l|^2}$ denotes the path loss with fading from the serving BS to the typical legitimate user and σ_l represents the noise power at the typical legitimate user. Similarly, the inter-cell interference at the worst-case eavesdropper can be expressed as

$$I_e = P \sum_{i \in \Phi_b \setminus \{o\}} |h_{i,e}|^2 r_{i,e}^{-\alpha}, \tag{5.3}$$

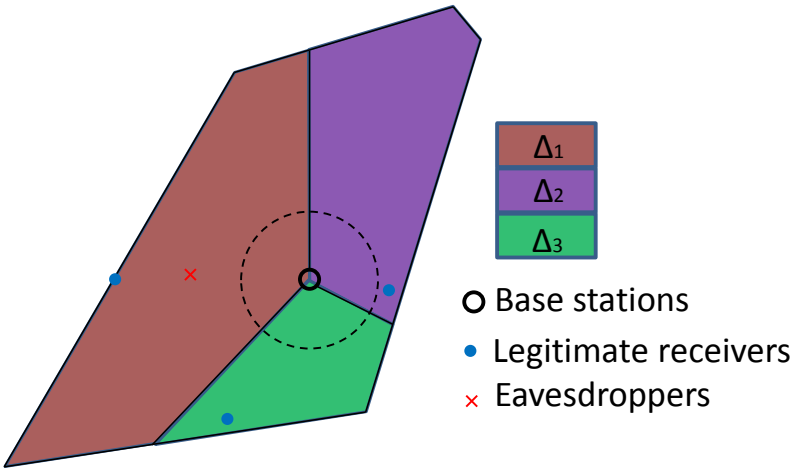

Figure 5.2: Transmission scheme of a Voronoi cell with FFR.

where $r_{i,e}$ and $h_{i,e}$ denote the distance and the fading coefficient from the i_{th} BS to the worst-case eavesdropper, respectively. We denote the SINR at the worst-case eavesdropper as γ_e, which can be written as

$$\gamma_e = \frac{P/\xi_e}{I_e + \sigma_e^2}, \tag{5.4}$$

where $\xi_e = \frac{r_e^\alpha}{|h_e|^2}$ denotes the path loss with fading from the serving BS to the worst-case eavesdropper and σ_e represents the noise power at the worst-case eavesdropper.

FFR

In the scenarios with FFR, we assume that each of the Voronoi cell in the cellular network is partitioned into L sectors and each of the sectors is served by its BS with a sub-band of the total bandwidth. Accordingly, the frequency reuse factor is L. The set of interfering base stations are base stations in other Voronoi cells that use the same sub-band as the receivers, i.e. the legitimate receivers and the eavesdroppers. To differentiate from the scheme without FFR, the interference in the cellular network with FFR at the legitimate user and the worst-case eavesdropper are denoted as $\hat{I}_l$ and $\hat{I}_e$. Figure 5.2 displays the transmission scheme of using FFR in a Voronoi cell from Figure 5.1. The same transmission scheme is also deployed in other Voronoi cells of the cellular network. For a typical legitimate receiver, the detriment of its secrecy rate is from eavesdroppers that communicate using the same sub-band.

5.2.2 Problem Formulation

We consider a scenario where the serving BS transmits confidential messages to a typical legitimate user in the presence of randomly distributed eavesdroppers. By assuming that there is no collusion among the eavesdroppers, the secrecy capacity of the transmission from the serving BS to the legitimate user is given by [8]

$$R_s = \Big[\log_2(1+\gamma_l) - \log_2(1+\gamma_e)\Big]^+. \tag{5.5}$$

Accordingly, the secrecy outage probability which is also known as the outage probability of secrecy capacity under slow fading, can be expressed as [10]

$$\mathbb{P}_{out}(\tau) = 1 - \mathbb{P}\left[R_s > \tau\right] = 1 - \mathbb{P}\left[\frac{1+\gamma_l}{1+\gamma_e} > 2^{\tau}\right], \tag{5.6}$$

where τ is the target secrecy rate. We denote the PDF of γ_l and γ_e as f_{γ_l} and f_{γ_e}, respectively. Then, the secrecy outage probability at the legitimate user can be further derived as

$$\begin{aligned}
\mathbb{P}_{out}(\tau) &= \mathbb{P}\left[\frac{1+\gamma_l}{1+\gamma_e} < 2^{\tau}\right], \\
&= \mathbb{P}\left[\gamma_e > 2^{-\tau}(1+\gamma_l) - 1\right], \\
&= 1 - \int_0^{\infty} f_{\gamma_l}(y) \int_0^{2^{-\tau}(1+y)-1} f_{\gamma_e}(x)\,\mathrm{d}x\,\mathrm{d}y, \\
&= 1 - \int_0^{\infty} f_{\gamma_l}(y) F_{\gamma_e}\left(2^{-\tau}(1+y) - 1\right)\mathrm{d}y,
\end{aligned} \tag{5.7}$$

where F_{γ_e} is the CDF of γ_e. Accordingly, the secrecy outage probability of downlink transmission can be obtained if f_{γ_l} and F_{γ_e} can be derived.

5.3 Secrecy Outage Probability of Noise-Limited Cellular Networks

In the noise-limited cellular networks, the interference from other BSs can be ignored or has the same level of power compared to the noise [31]. The analysis in this section are

organized in two parts. In the first part, the PDFs of the distances from a typical point $u \in \mathbb{R}^d$ to the nodes of a HCPP are derived to study the distribution of the BSs. In the second part, the secrecy outage probabilities of the downlink cellular networks are derived by investigating two different transmission schemes, i.e., with and without FFR.

To avoid confusion, we denote the SNR at the typical legitimate user and the eavesdropper as $\tilde{\gamma}_l$ and $\tilde{\gamma}_e$ which can be expressed as

$$\tilde{\gamma}_l = \frac{P|h_l|^2 r_l^{-\alpha}}{\sigma_l^2}, \tag{5.8}$$

and

$$\tilde{\gamma}_e = \frac{P|h_e|^2 r_e^{-\alpha}}{\sigma_e^2}. \tag{5.9}$$

5.3.1 Distance Distribution of HCPP

The PDF of the Euclidean distance from a typical point to the n_{th} nearest node of a Matérn HCPP can be derived using the following theorem.

Theorem 4. *In a Matérn HCPP of type II, which is generated from a homogenous PPP with intensity λ_p and repulsive distance ϱ, the PDF of the Euclidean distance from a typical point to the n_{th} nearest node can be approximated by*

$$f_{r_n}(r) = \exp(-\lambda_M C_d r^d) \frac{d(\lambda_M C_d r^d)^n}{r\Gamma(n)}, \tag{5.10}$$

where $\lambda_M = \frac{1-\exp\left(-\lambda_p C_d \varrho^d\right)}{C_d \varrho^d}$.

Proof. See Appendix C. □

The PDF of the distance from a typical point to the n_{th} neighbor in a MHCPP in (5.10) has been verified by Monte Carlo simulations in Figure 5.3. It shows that the approximated analytical results for small ratios, i.e., $\rho \leq 0.3$, match the simulation quite well.

Notice that, the intensity of base stations $\lambda_p = 3.7 \times 10^{-5}$ can be assumed for urban regions [32], while the actual intensity in the rural regions according to the actual locations

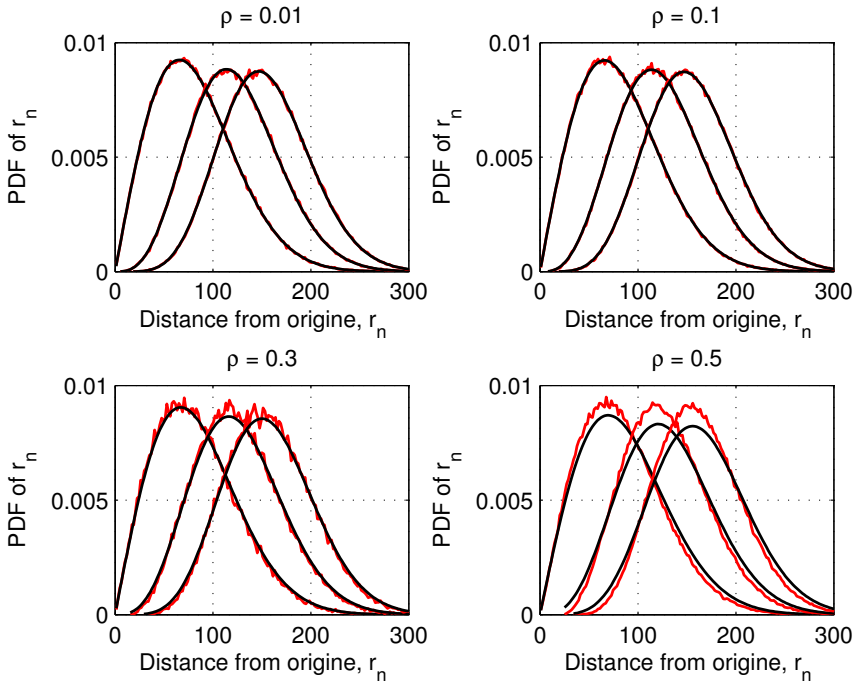

Figure 5.3: The PDF of distance from the typical node to the n_{th} neighbor in HCPP with the ratio between the repulsive distance and the radius of the average coverage area, $\rho = \frac{\varrho}{1/\sqrt{\pi\lambda_p}} = \varrho\sqrt{\pi\lambda_p}$. The curves from left to right in each of the figures show the PDF of r_n from the typical node to the 1_{st}, 2_{nd} and 3_{rd} nodes, respectively.

of the BSs is about $\lambda_p = 2 \times 10^{-8}$. Accordingly, the radius of the average coverage area is about 100m in the urban regions and around 4000m in the rural regions, which can be derived by $1/\sqrt{\pi\lambda_p}$. As $\varrho = \rho/\sqrt{\pi\lambda_p}$, the approximated results can be applied in the case when the repulsive distance of BSs is less than 30m in urban regions and less than 1200m in rural regions[1].

Remarks:

- The distance distribution in (5.10) is derived based on the definition of HCPP, which is similar to the distance distribution of a PPP. This is because when the repulsive distance ϱ approaches zero, the HCPP will converge into a PPP. The expression of distance distribution in (5.10) along with the work of [78] indicate that interference based performance in Matérn HCPP of type II can be safely approximated with a

[1]We acknowledge that there are chances that ρ might be larger and lead to more deviation from the approximation. In that case, the analyze of BS serve in this work might not be effective, while other strategies still work by simply replacing the distribution of the distance to the nearest point in (5.12) with some existent results as given in [113]. For interference-based performance analysis, MHCPP of type II can be safely approximated by the corresponding virtual PPP [78].

virtual PPP process when the repulsive distance is small.

- The distribution of the contact distance[2] can be obtained by substituting $n = 1$ into (5.10) as

$$f_{r_1}(r) = d\lambda_M C_d r^{d-1} \exp(-\lambda_M C_d r^d). \tag{5.11}$$

For 2-dimension spaces, it can be written as

$$f_{r_1}(r) = 2\lambda_M \pi r \exp(-\lambda_M \pi r^2). \tag{5.12}$$

5.3.2 Secrecy Outage Probability without FFR

In this subsection, we analyze the secrecy outage probability of the downlink transmission in two scenarios, i.e., served by the nearest and the best BSs. Selection of the serving BS according to different criterions are implemented through the cooperation of the BSs by exchanging the location and identity information of the legitimate users.

Nearest BS

The nearest BS to a legitimate user is in fact the BS of the Voronoi cell where the user is located, as shown in Figure 5.1. To study the secrecy outage probability of the downlink transmission, the distributions of channel gains from the nearest BS to the typical legitimate user and the worst-case eavesdropper will be investigated, respectively. The secrecy outage probability can be obtained by substituting the PDF of γ_l and the CDF of γ_e into (5.7).

We assume that both the channels from the BS to the legitimate user and the worst-case eavesdropper are subjected to Rayleigh fading. Denoting the path loss from the nearest BS to the legitimate user as $r_l^\alpha = x_l$, the PDF of x_l is given by [35]

$$f_{x_l}(x) = \pi\lambda_M \delta s^{\delta-1} \exp(-\lambda_M \pi s^\delta), \tag{5.13}$$

[2]The contact distance at an arbitrary location $u \in \mathbb{R}^d$ of a point process Φ is $\|u - \Phi\|$, i.e., the distance from u to the nearest point in Φ [33, Def. 2.37].

where $\delta = d/\alpha$. The PDF of the channel gain $\zeta_l = \frac{|h_l|^2}{x_l}$ can be derived by

$$\begin{aligned} f_{\zeta_l}(x) &= \int_0^\infty |y| f_{|h_l|^2,\, x_l}(xy, y)\, \mathrm{d}y, \\ &\overset{(a)}{=} \int_0^\infty y f_{|h_l|^2}(xy) f_{x_l}(y) dy, \\ &= \pi\lambda_M \delta \int_0^\infty y^\delta \exp\left(-xy - \lambda_M \pi y^\delta\right) \mathrm{d}y, \end{aligned} \tag{5.14}$$

where $f_{|h_l|^2,\, x_l}(x, y)$ denotes the joint PDF of $|h_l|^2$ and x_l, and (a) follows the assumption that the fading coefficient is independent of the path loss. Correspondingly, the PDF of $\tilde{\gamma}_l$ from the nearest BS to the legitimate user can be derived by

$$\begin{aligned} f_{\tilde{\gamma}_l}(x) &= \frac{\sigma_l^2}{P} f_{\zeta_l}\left(\frac{\sigma_l^2}{P} x\right), \\ &= \frac{\sigma_l^2}{P} \pi\lambda_l \delta \int_0^\infty y^\delta \exp\left(-\frac{\sigma_l^2}{P} xy - \lambda_l \pi y^\delta\right) \mathrm{d}y. \end{aligned} \tag{5.15}$$

According to the definition of secrecy capacity, the SNR at the worst-case eavesdropper is taken into account to analyze the secrecy outage probability. Note that, in this scenario the eavesdroppers are trying to interpret the source information from the serving BS.

Proposition 2. *The PDF for the path-loss process with fading $\xi_{k,e} = \frac{r_{k,e}^\alpha}{|h_{k,e}|^2}$ can be derived from [35, Corollary 2] as*

$$f_{\xi_{k,e}}(s) = \exp\left(-A_e s^\delta\right) \frac{\delta (A_e s^\delta)^k}{s\Gamma(k)}, \tag{5.16}$$

where $A_e = \pi\lambda_e \frac{\Gamma(\delta+m)}{m^\delta \Gamma(m)}$ includes both the effect of path loss and small scale fading.

The worst-case eavesdropper has the largest channel gain which corresponds to $\xi_{1,e}$. For simplicity, we will use ξ_e to represent the channel gain at the worst-case eavesdropper. Consequently, the PDF of ξ_e can be expressed by

$$f_{\xi_e}(s) = \delta A_e s^{\delta-1} \exp\left(-A_e s^\delta\right). \tag{5.17}$$

By substituting (5.15) and (5.17) into (5.7), the secrecy outage probability of the

legitimate user communicating with the nearest BS can be derived as

$$\begin{aligned}\mathbb{P}_{n\_out}(\tau) &= 1-\mathbb{P}\left[\log_2\frac{1+\gamma_l}{1+\frac{P}{\sigma_e^2}\frac{1}{\xi_e}}>\tau\right],\\ &= 1-\int_0^\infty f_{\gamma_l}(y)\int_{\frac{\frac{P}{\sigma_e^2}}{2^{-\tau}(1+\gamma_l)-1}}^\infty f_{\xi_{n,e}}(x)\,\mathrm{d}x\,\mathrm{d}y,\\ &= \frac{\sigma_l^2}{P}\pi\lambda_l\delta\int_0^\infty\left(1-\exp\left(-A_e\frac{\frac{P^\delta}{\sigma_e^{2\delta}}}{\left(2^{-\tau}(1+y)-1\right)^\delta}\right)\right)\\ &\quad\times\int_0^\infty z^\delta\exp\left(-\frac{\sigma_l^2}{P}yz-\lambda_l\pi z^\delta\right)\mathrm{d}z\,\mathrm{d}y.\end{aligned}\tag{5.18}$$

For the case of high SNR, the secrecy outage probability of the legitimate user communicating with the nearest BS can be simplified as

$$\begin{aligned}\tilde{\mathbb{P}}_{n\_out}(\tau) &= 1-\mathbb{P}\left[\xi_e>\frac{2^\tau}{\zeta_l}\right],\\ &= \int_0^\infty f_{\zeta_l}(y)\int_0^{\frac{2^\tau}{y}} f_{\xi_e}(x)\,\mathrm{d}x\,\mathrm{d}y,\\ &= \pi\lambda_M\delta\int_0^\infty\left(1-\exp\left(-A_e\left(\frac{2^\tau}{y}\right)^\delta\right)\right)\\ &\quad\times\int_0^\infty z^\delta\exp\left(-yz-\lambda_M\pi z^\delta\right)\mathrm{d}z\,\mathrm{d}y.\end{aligned}\tag{5.19}$$

Best BS

In this scheme, the legitimate user will be served by the BS from which the user can get the largest channel gain. Similar to the analysis of the channel gain at the worst-case eavesdropper, PDF for the path-loss process with fading from the best BS to the legitimate user can be directly obtained from (5.16) as

$$f_{\xi_l}(s)=\delta A_l s^{\delta-1}\exp\left(-A_l s^\delta\right),\tag{5.20}$$

where $A_l = \pi\lambda_l\delta\frac{\Gamma(\delta+m)}{m^\delta\Gamma(m)}$. The secrecy outage probability of the legitimate user served by the best BS can be derived by

$$\begin{aligned}\mathbb{P}_{bst\_out}(\tau) &= 1 - \mathbb{P}\left[\log_2\frac{1+\frac{P}{\sigma_l^2\xi_l}}{1+\frac{P}{\sigma_e^2\xi_e}} > \tau\right], \\ &= \int_0^\infty f_{\xi_e}(y)\int_{\frac{P}{\sigma_l^2\left(2^\tau(1+\frac{P}{\sigma_e^2\xi_e})-1\right)}}^\infty f_{\xi_l}(x)\,\mathrm{d}x\,\mathrm{d}y, \\ &= \int_0^\infty \delta A_e y^{\delta-1}\exp\left(-A_e y^\delta - \frac{A_l P^\delta}{\sigma_l^{2\delta}\left(2^\tau(1+\frac{P}{\sigma_e^2 y})-1\right)^\delta}\right)\mathrm{d}y.\end{aligned} \tag{5.21}$$

Similarly, for the case of high SNR, the approximation of secrecy outage probability of the legitimate user communicating with the best BS is given by

$$\begin{aligned}\mathbb{P}_{bst\_out}(\tau) &= 1 - \mathbb{P}\left[\log_2\frac{\frac{1}{\xi_l}}{\frac{1}{\xi_e}} > 2^\tau\right], \\ &= 1 - \int_0^\infty f_{\xi_l}(y)\int_{2^\tau y}^\infty f_{\xi_e}(x)\,\mathrm{d}x\,\mathrm{d}y, \\ &= 1 - \int_0^\infty \exp\left(-A_l y^\delta\right)\delta A_l y^{\delta-1}\exp\left(-A_e 2^{\delta\tau}y^\delta\right)\mathrm{d}y, \\ &= 1 - \int_0^\infty \exp\left[-\left(1+\frac{A_e}{A_l}2^{\delta\tau}\right)t\right]\mathrm{d}t, \\ &= 1 - \frac{A_l}{A_l + A_e 2^{\delta\tau}}.\end{aligned} \tag{5.22}$$

5.3.3 Secrecy Outage Probability with FFR

In the scheme of FFR, the intensity of the path-loss process with fading is reduced by frequency reuse, which works as independent thinning of the eavesdroppers. The number of eavesdroppers in each sector is $1/L$ of the total number in the cell, i.e., the intensity measure of each sector is reduced by L. Accordingly, the parameter A_e as given in (5.16) will also be affected by the frequency reuse. To avoid confusion, we denote the value of A_e in the scheme of FFR as $\hat{A}_e$, then $\hat{A}_e = \frac{A_e}{L}$. The legitimate users in each sector of the Voronoi cells are allocated a common subband, Δ_x, of the total bandwidth transmitted from the BS. To analyze the effect of implementing FFR, the legitimate user is assumed

to be located at a distance of r_0 from its nearest BS. The secrecy outage probability at the legitimate user served with the strategy of FFR can be derived by

$$\begin{aligned}\mathbb{P}_{sct\_out}(\tau) &= 1-\mathbb{P}\left[\log_2\frac{1+\frac{P}{\sigma_l^2}|h_l|^2 r_0^{-\alpha}}{1+\frac{P}{\sigma_e^2\xi_e}}>\tau\right], \\ &= \int_0^\infty \exp(-y)\left(1-\exp\left(-\hat{A}_e\frac{\frac{P}{\sigma^2}}{2^{-\tau}\left(1+\frac{P}{\sigma^2}r_0^{-\alpha}y\right)-1}\right)\right)\mathrm{d}y.\end{aligned} \tag{5.23}$$

For the case of high SNR, the secrecy outage probability at the legitimate user served by the strategy of FFR can be simplified as

$$\begin{aligned}\mathbb{P}_{sct\_out}(\tau) &= 1-\mathbb{P}\left[\log_2\frac{|h_l|^2 r_0^{-\alpha}}{\frac{1}{\xi_e}}>\tau\right], \\ &= \int_0^\infty \exp(-y)\left(1-\exp\left(-\hat{A}_e\left(\frac{2^\tau}{y r_0^{-\alpha}}\right)^\delta\right)\right)\mathrm{d}y.\end{aligned} \tag{5.24}$$

The expression in (5.24) is similar to that in (5.19), and only the parameter $\hat{A}_e$ is affected by FFR due to the change of intensity.

5.4 Secrecy Outage Probability of Interference-Limited Cellular Networks

In this section, we analyze the scenarios in the interference-limited cellular networks where interference has a much larger impact than the noise power on the values of γ_l and γ_e. Similar to the structure of the previous section, the analysis of the secrecy outage probability in interference-limited cellular networks is also categorized in two subsections, i.e., secure transmission without and with FFR.

5.4.1 Secrecy Outage Probability without FFR

To analyze the improvements of incorporating FFR, we will first derive the CDF of SIR at the legitimate user and the worst-case eavesdropper. The CDF of SINR at the legitimate

user can be derived by

$$\begin{aligned} F_{\gamma_l}(\beta) &= 1 - \mathbb{P}\left[\gamma_l > \beta\right], \\ &= 1 - \mathbb{E}_{r_l}\left[\mathbb{P}\left[\gamma_l > \beta | r_l\right]\right], \\ &= 1 - \int_0^\infty \mathbb{P}\left[h_l > \beta r_l^\alpha (\sigma^2 + \mathrm{I}_l) | r_l\right] f_{r_l}(r)\,\mathrm{d}r. \end{aligned} \tag{5.25}$$

The value of $\mathbb{P}\left[\gamma_l > \beta\right]$ is also equivalent to the coverage probability as analyzed in [114]. The expression for the coverage probability of the legitimate user for a fixed value of r_l, $\mathbb{P}(|h_l|^2 > \beta r_l^\alpha(\sigma^2 + \mathrm{I}_l)|r_l)$, can be derived based on the expectation of I_l and given by

$$\begin{aligned} \mathbb{P}(h_l > \beta r_l^\alpha(\sigma^2 + \mathrm{I}_l)|r_l) &= \exp(-\beta r_l^\alpha \sigma^2)\mathbb{E}_{I_l}\left[\exp(-\beta r_l^\alpha \mathrm{I}_l)|r_l\right], \\ &= \exp(-\beta r_l^\alpha \sigma^2)\mathbb{E}_{\Phi_r}\left[\prod_{i\in\Phi_B\setminus\{0\}} \mathbb{E}_{h_{i,l}}\left[\exp(-\beta r_l^\alpha |h_{i,l}|^2 r_{i,l}^{-\alpha})\Big| r_l\right]\right], \\ &\overset{(a)}{=} \exp(-\beta r_l^\alpha \sigma^2)\mathbb{E}_{\Phi_r}\left[\prod_{i\in\Phi_B\setminus\{0\}} \frac{1}{1+\beta r_l^\alpha r_{i,l}^{-\alpha}}\right], \\ &\overset{(b)}{=} \exp(-\beta r_l^\alpha \sigma^2)\exp\left(-\int_{r_l}^\infty \left(1 - \frac{1}{1+\beta r_l^\alpha x^{-\alpha}}\right) 2\pi\lambda_M x\,\mathrm{d}x\right), \\ &\overset{(c)}{=} \exp(-\beta r_l^\alpha \sigma^2)\exp\left(-2\lambda_M \pi r_l^2 \int_1^\infty \frac{\beta v}{\beta + v^\alpha}\,\mathrm{d}v\right), \\ &\overset{(d)}{=} \exp(-\beta r_l^4 \sigma^2)\exp\left(-\lambda_M \pi r_l^2 \sqrt{\beta}\arctan(\sqrt{\beta})\right), \end{aligned} \tag{5.26}$$

where (a) follows from the fact that the channels are subjected to Rayleigh fading, (b) follows from applying the probability generating functional (PGFL) [115], (c) follows from replacing x with vr and (d) follows from considering $\alpha = 4$ which is the path-loss exponent value for the suburban area [116]. Substituting (5.26) into (5.25), the CDF of γ_l can be written as

$$F_{\gamma_l}(\beta) = 1 - \int_0^\infty \exp(-\beta r^4 \sigma^2)\exp\left(-2\pi\lambda_M r^2 \beta \int_1^\infty \frac{v}{v^4 + \beta}\,\mathrm{d}v\right) f_{r_l}(r)\,\mathrm{d}r. \tag{5.27}$$

Accordingly, the outage probability at the typical legitimate user can be directly obtained as

$$\begin{aligned}\mathbb{P}(\gamma_l > \beta) &= 1 - F_{\gamma_l}(\beta), \\ &= \int_0^\infty \exp(-\beta r^4 \sigma_l^2) \exp\left(-2\pi\lambda_M r^2 \beta \int_1^\infty \frac{v}{v^4+\beta}\,\mathrm{d}v\right) f_{r_l}(r)\,\mathrm{d}r.\end{aligned} \tag{5.28}$$

Assuming that the legitimate user is at a distance r_0 from the nearest BS, for the case of $\alpha = 4$ and the noise is dominated by the interference, the probability of $P(\gamma_l > \beta)$ can be derived by

$$\mathbb{P}(\gamma_l > \beta) = \exp\left(-\lambda_M \pi r_0^2 \sqrt{\beta}\arctan(\sqrt{\beta})\right). \tag{5.29}$$

Referring to (5.25), the PDF of γ_l can be obtained from the derivation of $F_{\gamma_l}(\beta)$ and given by

$$f_{\gamma_l}(\beta) = \frac{1}{2}\lambda_M \pi r_0^2 \left(\frac{1}{1+\beta} + \frac{\arctan(\sqrt{\beta})}{\sqrt{\beta}}\right) \exp\left(-\lambda_M \pi r_0^2 \sqrt{\beta}\arctan(\sqrt{\beta})\right). \tag{5.30}$$

Similarly, the CDF of γ_e in cellular networks without FFR can be written as

$$\begin{aligned}F_{\gamma_e}(\beta) &= 1 - \mathbb{P}(\gamma_e > \beta), \\ &= 1 - \int_0^\infty \exp(-\beta r^4 \sigma_l^2) \exp\left(-2\pi\lambda_M r^2 \beta \int_1^\infty \frac{v}{v^4+\beta}\,\mathrm{d}v\right) f_{r_{1,e}}(r)\,\mathrm{d}r,\end{aligned} \tag{5.31}$$

where $f_{r_{1,e}}(r)$ is the PDF of the contact distance in the PPP of the eavesdroppers, given by [105] as

$$f_{r_e}(r) = 2\lambda_e \pi r \exp(-\lambda_e \pi r^2). \tag{5.32}$$

Secrecy outage probability of the downlink cellular network without FFR can be derived by substituting $f_{\gamma_l}(\beta)$ and $F_{\gamma_e}(\beta)$ into (5.7).

5.4.2 Secrecy Outage Probability with FFR

By implementing FFR, the interference at each of the receivers in the cellular network will be reduced, since only the interference that are transmitted at the same subband will

affect the SIRs at the receivers. The SIRs, γ_l and γ_e, are analyzed and applied to derive the secrecy outage probability of downlink cellular networks.

To analyze the secrecy outage probability $\mathbb{P}_{out}$, we need to derive the expression of $f_{\gamma_l}(\beta)$ and $F_{\gamma_e}(\beta)$. The CDF of γ_l is given by Theorem 5 as follows.

Theorem 5. *In the downlink transmission of cellular networks using FFR under Rayleigh fading, the CDF of γ_l can be derived by*

$$F_{\gamma_l}(\beta) = 1 - \int_0^\infty \exp(-\beta r^\alpha \sigma^2) \exp\left(-\frac{2\pi\lambda_M r^2}{L}\beta \int_1^\infty \frac{x}{x^\alpha + \beta}\,\mathrm{d}x\right) f_{r_l}(r)\,\mathrm{d}r. \quad (5.33)$$

Proof. See Appendix C. □

Remarks:

- For the case of $\alpha = 4$, we have

$$\int_1^\infty \frac{v}{v^4+\beta}\,\mathrm{d}v = \frac{\arctan(\sqrt{\beta})}{2\sqrt{\beta}}. \quad (5.34)$$

  Substituting (5.34) into (5.33), the closed form of $F_{\gamma_l}(\beta)$ can be obtained as

$$\begin{aligned} F_{\gamma_l}(\beta) = 1 - \frac{\lambda_M \pi^{\frac{3}{2}}}{2\sigma\sqrt{\beta}} \mathrm{erf}\left(\frac{\lambda_M \pi(\sqrt{\beta}\arctan(\sqrt{\beta})+1)}{2\sigma\sqrt{\beta}}\right) \\ \times \exp\left(\frac{\pi^2\lambda_M^2\left(\sqrt{\beta}\arctan(\sqrt{\beta})+1\right)^2}{4\beta\sigma^2}\right), \end{aligned} \quad (5.35)$$

  where $\mathrm{erf}(x)$ is the error function of x.

- For the case of $\alpha = 4$ and at high SIR regime, the closed form expression of $F_{\gamma_l}(\beta)$ can be simplified as

$$\begin{aligned} F_{\gamma_l}(\beta) =& 1 - \int_0^\infty \exp\left(-\frac{\pi\lambda_M}{L}\sqrt{\beta}\arctan(\sqrt{\beta})r^2\right) 2\lambda_M \pi r \exp(-\lambda_M \pi r^2)\,\mathrm{d}r, \\ \overset{y=\pi\lambda_M r^2}{=}& 1 - \int_0^\infty \exp\left(-\left(\frac{1}{L}\sqrt{\beta}\arctan(\sqrt{\beta})+1\right)y\right)\mathrm{d}y, \\ =& 1 - \frac{1}{1+\frac{1}{L}\sqrt{\beta}\arctan(\sqrt{\beta})}. \end{aligned} \quad (5.36)$$

- When the distance from the serving BS to the legitimate user is given, the PDF of

γ_l can be derived by

$$\begin{aligned} f_{\gamma_l}(\beta) =& \left[1-\exp(-\frac{\pi\lambda_M}{L}\sqrt{\beta}\arctan(\sqrt{\beta})r^2)\right]' \\ =& \frac{\pi\lambda_M r^2}{2L}\left(\frac{\arctan(\sqrt{\beta})}{\sqrt{\beta}}+\frac{1}{1+\beta}\right)\exp\left(-\frac{\pi\lambda_M r^2}{L}\sqrt{\beta}\arctan(\sqrt{\beta})\right). \end{aligned} \tag{5.37}$$

Similarly, the CDF of γ_e can be obtained by

$$F_{\gamma_e}(\beta) = 1-\int_0^\infty \exp(-\beta r^\alpha\sigma^2)\exp\left(-\frac{2\pi\lambda_M r^2}{L}\beta\int_1^\infty \frac{v}{v^\alpha+\beta}\,\mathrm{d}v\right) f_{r_e}(r)\,\mathrm{d}r. \tag{5.38}$$

For the case of $\alpha = 4$ and at high SIR regime, the closed form expression of $F_{\gamma_e}(\beta)$ can be simplified as

$$F_{\gamma_e}(\beta) = 1-\frac{1}{1+\frac{\lambda_M}{L\lambda_e}\sqrt{\beta}\arctan(\sqrt{\beta})}. \tag{5.39}$$

Then, the PDF of γ_e can be obtained by

$$\begin{aligned} f_{\gamma_e}(\beta) =& \left(1-\frac{1}{1+\frac{\lambda_M}{L\lambda_e}\sqrt{\beta}\arctan(\sqrt{\beta})}\right)', \\ =& \frac{\lambda_M\left(\frac{1}{1+\beta}+\frac{\arctan(\sqrt{\beta})}{\sqrt{\beta}}\right)}{2L\lambda_e\left(1+\frac{\lambda_M}{L\lambda_e}\sqrt{\beta}\arctan(\sqrt{\beta})\right)^2}. \end{aligned} \tag{5.40}$$

Consequently, the secrecy outage probability in downlink cellular networks with FFR can be obtained by substituting the distribution functions of γ_l and γ_e into (5.7).

5.5 Numerical Results

In this section, the numerical results are presented to show the interplay of different system parameters and their effects on the security of downlink cellular networks. The numerical results are grouped into two parts in correspondence to the derivations in Section 5.3 and 5.4, respectively. Numerical results shown in this chapter are based on Monte Carlo simulations using 100000 independent iterations. All the channel coefficients are assumed to be i.i.d Rayleigh faded. The transmit power set at the BSs

is 20 dBm and the path-loss exponent is 4.

5.5.1 Secrecy Outage Probability of Noise-Limited Cellular Networks

For the scenario of the noise-limited cellular network, the secrecy outage probabilities of the downlink transmissions from the best and nearest BSs are plotted in Figure 5.4. The analytical results are verified by Monte Carlo simulations. It is obvious that the secrecy outage probability is worse when the intensity of the eavesdroppers λ_e is higher. The increase of λ_e will reduce the expected distance from the transmitting BS to the worst-case eavesdropper, which will accordingly decrease the SNR of the eavesdropper, i.e., γ_e. Figure 5.4 indicates that the strategy of transmitting with the best BS is always helpful to improve the secrecy outage probability. However, the improvement is less beneficial when λ_e is higher. It is because that the increase of λ_e reduces the expectation of the distance from the BS to the worst-case eavesdropper.

Figure 5.5 studies the secrecy outage probability of the downlink cellular networks using FFR based on different frequency reuse factors. It shows that in the noise-limited cellular networks, the use of FFR can improve the secrecy outage probability significantly, especially when the number of frequency reuse factor is large. This is due to the application of frequency reuse which helps to reduce λ_e with an equivalent effect of independent thinning.

5.5.2 Secrecy Outage Probability of Interference-Limited Cellular Networks

From Figure 5.6 to Figure 5.9, we investigate the scenarios in interference-limited cellular networks. The impacts of various factors are studied, such as the number of frequency reuse factor (Figure 5.6 and Figure 5.9), the repulsive distance of the BSs (Figure 5.7), the ratio of intensities between the BSs and the eavesdroppers (Figure 5.7 and Figure 5.8). The coverage probability plotted in Figure 5.6 is the probability that a typical mobile user

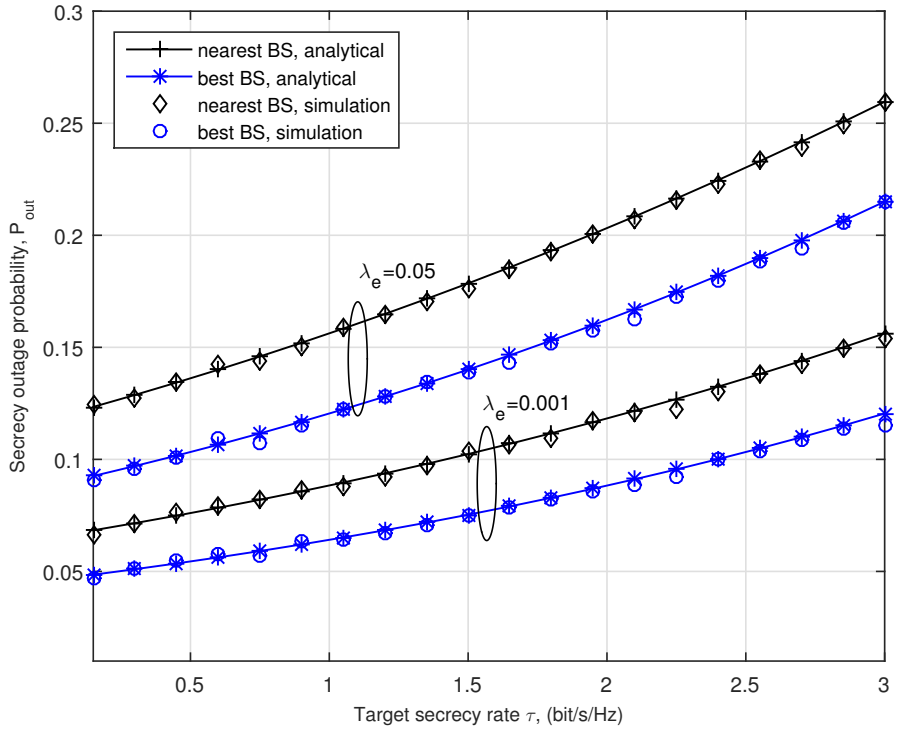

Figure 5.4: Secrecy outage probability with the best BS vs the nearest BS with $\lambda_p = 0.1$ and $\varrho = 1$.

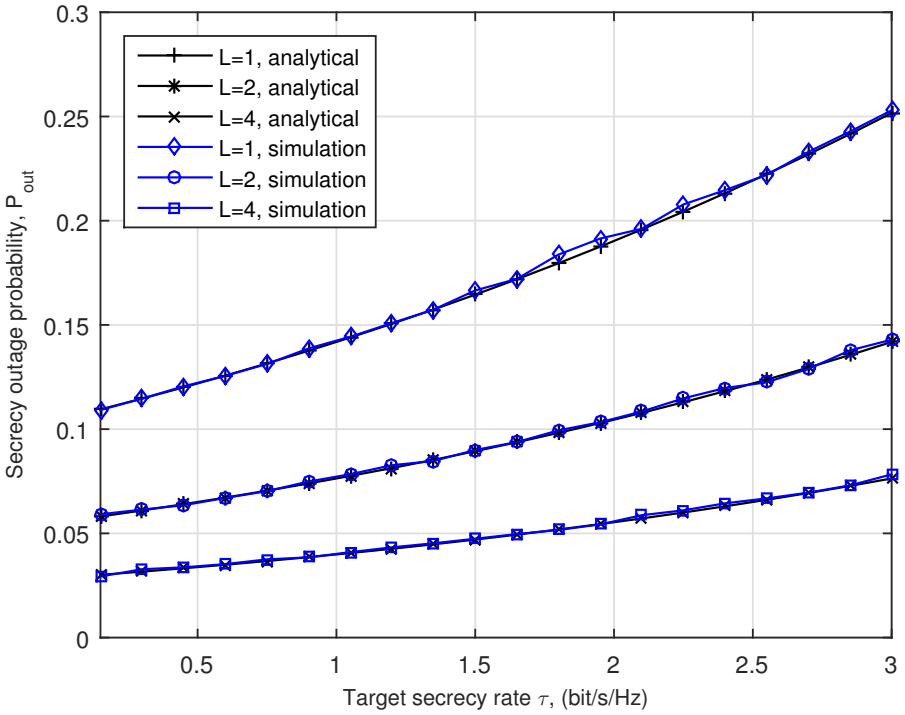

Figure 5.5: Secrecy outage probability with and without FFR, with $\lambda_p = 0.1$ and $\varrho = 1$.

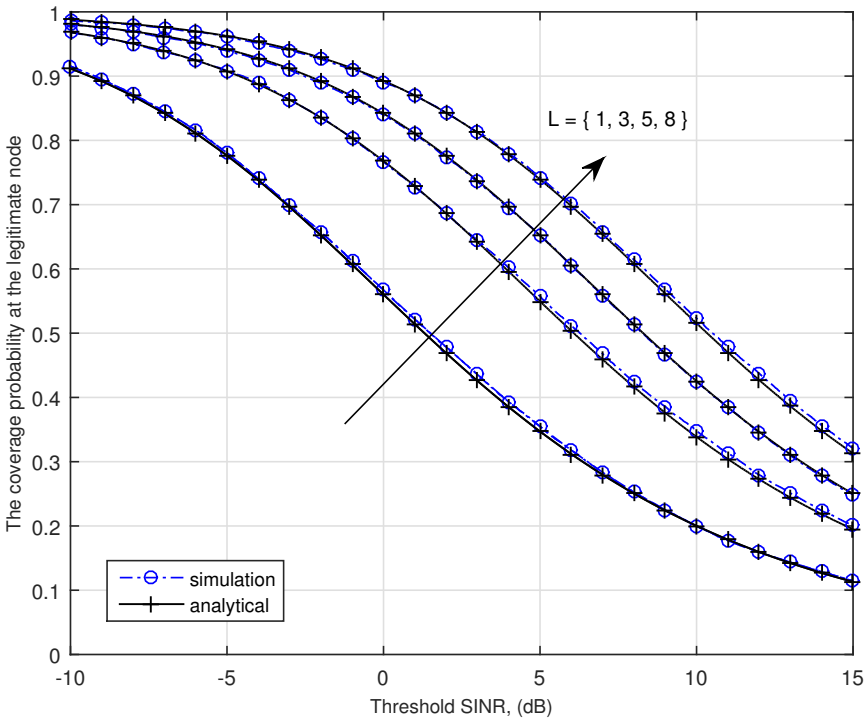

Figure 5.6: Coverage probability at the legitimate user with $\lambda_p = 0.1$ and $\varrho = 1$.

can achieve the SINR threshold. Figure 5.6 shows that increasing the frequency reuse factor can help to improve the coverage probability at the legitimate node. This is because the interference from other BSs is reduced by frequency reuse.

To analyze the impact of the repulsive distance in a MHCPP process, the secrecy outage probability is plotted as a function of intensity of the parent point process λ_p and the repulsive distance between two BSs ϱ in Figure 5.7. Specially, when the repulsive distance is zero, i.e., $\varrho = 0$, the curves represent the results of the cellular network where the deployment of the BSs follows PPP, while other curves illustrate the results of the networks with the deployment of the BSs that distributed as HCPP. It shows that increasing the repulsive distance lead to the rise of the secrecy outage probability, since the expansion of the repulsive region reduces the actual intensity of the BSs λ_M, which increases the expectation of the contact distance between the legitimate user and the target BS accordingly. Figure 5.7 shows that, although the increase of λ_p reduces the secrecy outage probability, the improvement will decrease when λ_p is large. It is because that the maximum λ_M is limited by the repulsive distance of the MHCPP.

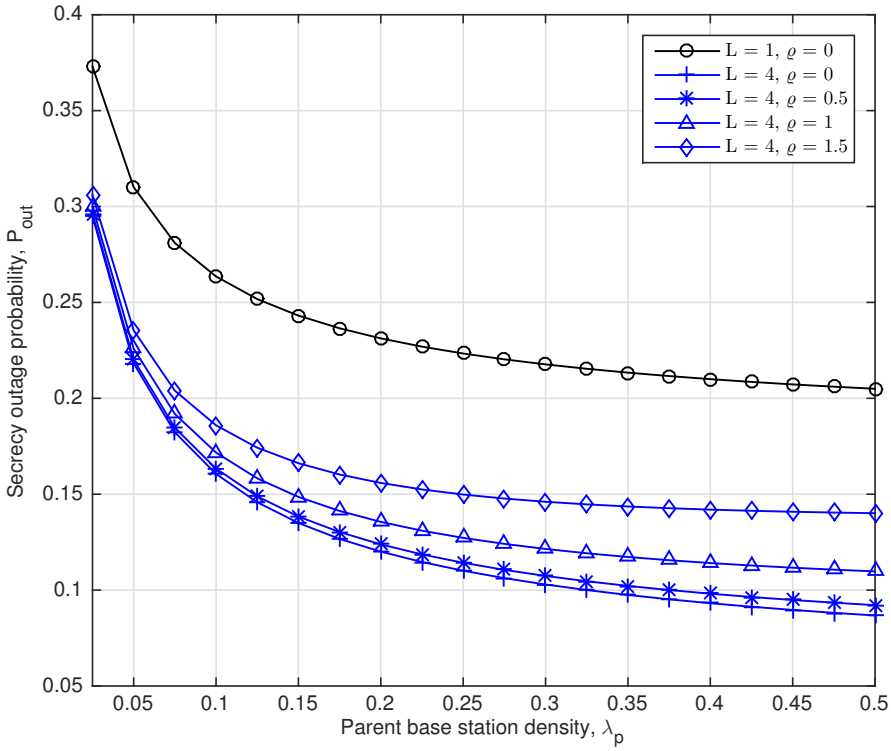

Figure 5.7: Secrecy outage probability as a function of λ_p with $\lambda_e = 0.05$.

In Figure 5.8, we investigate the effect of the intensity of the eavesdroppers λ_e on the secrecy outage probability of the downlink transmission when the intensity of the BSs is fixed. Comparing the cases of $L = 1$ and $L = 4$ with the same intensity ratio, Figure 5.8 shows that the application of FFR can significantly improve the security performance. With the same frequency reuse factor, i.e., $L = 4$, the scenarios with higher ratios of λ_M/λ_e have smaller secrecy outage probability. This can be explained by the following reasons. Considering the fixed intensity of BSs, the expectation of the distance from an arbitrary BS to its nearest eavesdropper will reduce when the intensity of eavesdroppers decreases, while the expectation of the distance between the transmission BS and the legitimate user is not changed. Accordingly, increasing the ratio of λ_M/λ_e leads to the decrease in γ_e and the reduction of the secrecy outage probability.

The impact of the frequency reuse number on secrecy outage probability in interference-limited cellular networks is studied in Figure 5.9. It shows that the increase of the frequency reuse factor will reduce the secrecy outage probability. Meanwhile, the improvement of secrecy outage probability at small fractional reuse numbers, e.g. from

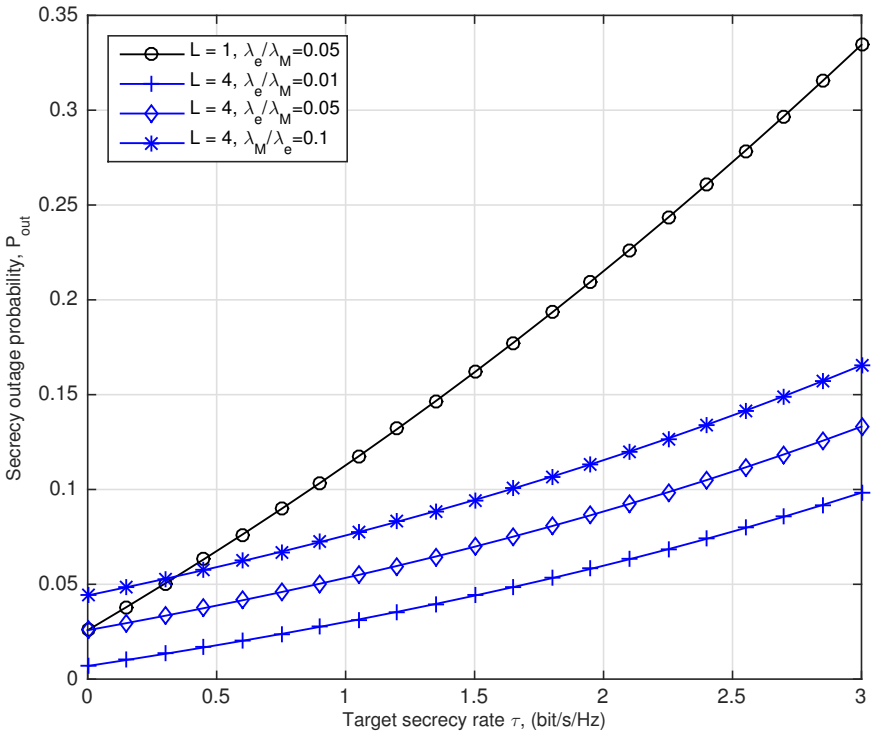

Figure 5.8: Comparison of secrecy outage probability with different ratios between the BS and eavesdroppers, with $\lambda_p = 0.1$ and $\varrho = 1$.

$L = 1$ to $L = 4$, is more significant than the improvement achieved at large reuse factors, e.g. from $L = 4$ to $L = 8$. The implementation of FFR can help to separate the eavesdroppers into different sectors and accordingly reduce the expectation of the SNR at the nearest eavesdropper. As a result, the utility of FFR will decrease the secrecy outage probability at the legitimate receiver. However, when the reuse factor is raised to high level, the secrecy rate will mainly be limited by the capacity of the legitimate channel.

5.6 Summary

In this work, we studied physical layer security in the downlink transmission of cellular networks. To analyze the repulsive property among BSs, the cellar network was modeled by a MHCPP, and the PDF of the distance distribution in MHCPP was also derived. By comparing the schemes with and without FFR, the impact of frequency reuse on secrecy outage probability in two scenarios, i.e. the noise-limited networks and the interference-

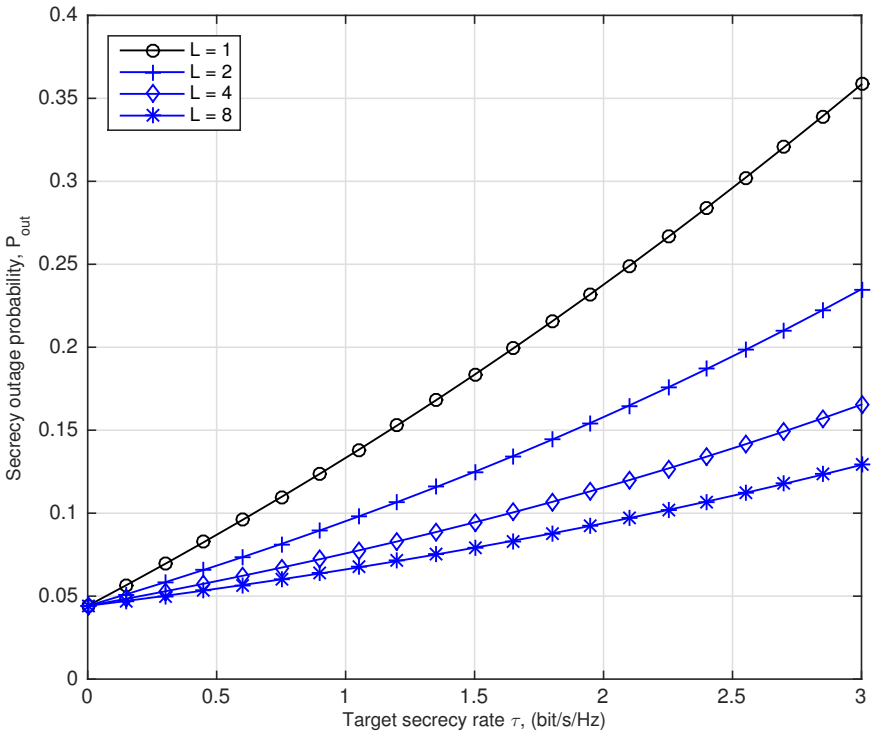

Figure 5.9: Secrecy outage probability of legitimate users with $\lambda_p = 0.1$, $\varrho = 1$ and $\lambda_e = 0.01$.

limited networks, were investigated, respectively. For the noise-limited network, we derived the secrecy outage probabilities of two transmission strategies, i.e. the best BS serve and the nearest BS serve.

Numerical results revealed that the application of FFR is beneficial for physical layer security in downlink cellular networks. Although increasing the frequency reuse factor contributes to enhance the security, the improvements will be less significant when the number of frequency reuse factor is large. Besides, the strategies of transmitting with the best BS, increasing the intensity of BSs, and reducing the repulsive distance of the BSs are helpful to improve the secrecy performance in downlink cellular network.

Chapter 6

Conclusions and Future Work

This final chapter summarizes the contributions of the thesis and suggests several directions for future work. Motivated by recent developments in wireless communication, this thesis aims at a characterization of the secrecy performances in several types of typical wireless networks. Advanced techniques are designed and evaluated to enhance physical layer security in these networks with realistic assumptions, such as signal propagation loss, random node distribution and non-instantaneous CSI.

In the remainder of this chapter, more specific conclusions from this thesis are provided in the first section. Then, by acknowledging shortcomings and limitations, some possible directions to extend the thesis are discussed.

6.1 Conclusions

This thesis has adopted some important perspectives of physical layer security to investigate confidential communication in various wireless networks. These perspectives include secrecy capacity, secrecy connectivity, ergodic secrecy capacity and secrecy outage probability. The analysis focused on the impact of fading, path loss, cooperative jamming and interference on the secrecy capacity. The overall contributions and observations of this thesis can be summarized as follows.

In Chapter 3, secret communication through relay-assisted cognitive interference channel was investigated. Two CJ schemes were proposed to improve the secrecy rate of cognitive interference channels depending on the structure of cooperative relays.

- For the network with a relay equipped with multiple antennas, the first CJ

scheme was developed to increase the secrecy rate of both primary and secondary transmissions by combining CJ with beamforming. In this scheme, two precoding strategies were proposed to obtain optimum secrecy rate for the scenarios with full CSI and partial CSI, respectively. An algorithm was designed to choose the CJ precoding vector. The introduced jamming noise only degraded the SINRs of the primary and secondary signal at the eavesdropper, while keeping both the SINRs of the primary and secondary receiver unaffected. The secrecy rate of the scheme using CJ with ZF only to the secondary receiver is larger than direct transmission, while smaller than the scheme using a well-designed CJ scheme with ZF to both primary and secondary receivers. Even when the CSI of the eavesdropper is unknown, CJ still can be adopted to increase the secrecy rate at secondary receiver.

- In a scheme with multiple relays transmitting weighted jamming signals, the combined approach of CJ and relay selection was analyzed. A selection algorithm was developed to find effective relays to meet the target secrecy rate at SR. The secrecy capacity can be improved by the CJ scheme creating additional interference at the eavesdropper with the jamming signals from the relays. Moreover, the secrecy rate increased with the number of effective relays. The problem of minimizing the secondary transmit power with a target secrecy rate was also analyzed.

To investigate the impact of the path loss, in Chapter 4, the focus shifted to physical layer security in a random wireless network where both legitimate and eavesdropping nodes were randomly distributed. Three scenarios were analyzed to investigate the impact of various factors on security.

- In scenario one, the random network without protected zone and interference was studied. The PDF of channel gain with both fading and path loss was derived and further applied to calculate secrecy connectivity and ergodic secrecy capacity. This expression for the distribution of channel gains simplified the derivation of the capacity at the worst-case eavesdropper.

- Secondly, the protected zone surrounding the source node, i.e., the secrecy protected zone, was investigated to enhance security, where interference is absent. The distance distribution of receivers outside the secrecy protected zone was

studied. The ergodic secrecy capacity of random wireless networks was derived by taking both large-scale path loss and small-scale fading into consideration. Both the cases of eavesdroppers being aware and unaware of the protected zone boundary were investigated. The closed form of the ergodic secrecy capacity was given for the case of $\alpha = 4$. The simulation showed that, increasing the intensity ratio (λ_l/λ_e), the path-loss exponent and the radius of the secrecy protected zone can be helpful to enhance the ergodic secrecy capacity. Adopting a protected zone will significantly improve the lower bound of the ergodic secrecy capacity, even when $\lambda_l < \lambda_e$. When eavesdroppers are aware of the secrecy protected zone boundary, security will be undermined, but it can still achieve a higher ergodic secrecy capacity compared to the case without a protected zone.

- Further deployment of protected zones at legitimate receivers, i.e., interference protected zones, was explored to convert detriment from interference into beneficial factors. By adopting interferer protected zones, interference was restructured to benefit the security of the legitimate receivers, similar to the effect of CJ. Moreover, the distribution of the active cooperative transmitters that follow a Poisson-hole process was also exploited. The numerical results indicated that, although increasing the intensity of cooperative nodes would undermine the secrecy capacity at legitimate receivers, the application of interferer protected zones can make interference beneficial to the security of the wireless network. The interferer protected zone contributed to restructuring interference which caused less detriment to the legitimate receivers than to the eavesdroppers.

Chapter 5 further considered the repulsive properties of wireless networks by analyzing physical layer security in the downlink transmission of cellular networks. The BSs in the cellular network was assumed to follow the Matérn HCPP, while the eavesdroppers were deployed as an independent PPP. The PDF of the distances from a typical point to the nodes of the HCPP was derived. The noise-limited and interference-limited cellular networks were investigated, separately, by applying the strategy of FFR.

- For the noise-limited cellular network, two transmission schemes were investigated: the downlink transmission with and without FFR. For the scheme without FFR, two

transmission strategies were analyzed by selecting different BSs, i.e., the nearest BS versus the best BS. The distribution of the channel gain from the nearest BS to the user was obtained by combining the distribution of the small-scale fading and path loss, while the derivation for the distribution of the channel gain from the best BS is based on exploiting the characteristic of PPP. Although communication with the best BS can always help to reduce the secrecy outage probability, the discrepancy between the two strategies is reduced when the intensity ratio between the BSs and the eavesdroppers is increased.

- For the scenario of interference-limited networks, the application of the FFR was also explored to enhance the security in the downlink transmission of cellular networks. To analyze the secrecy outage probability in the downlink cellular networks, the PDFs of the SIR were derived for both the scenarios with and without using FFR, based on the analysis of the inter-cell interference. The first moment measure of interference in downlink cellular networks was also investigated to study the effect of FFR.

The simulations revealed that for both these two scenarios above, the application of FFR is beneficial for physical layer security in downlink cellular networks, especially by using large frequency reuse number. However, the improvement of secrecy outage probability at small fractional reuse numbers was more significant than the improvement achieved at large reuse factors. Besides, increasing the intensity of BSs and reducing the repulsive distance of the BSs can help to improve the secrecy performance in downlink cellular network.

6.2 Future Work

For more practical usage of security in wireless networks, the application will lead to the consideration of more conservative adversaries; i.e., eavesdroppers might be active rather than passive and colluding to maximize their received signal powers. Besides, many promising research topics of physical layer security have emerged in recent years. The remainder of this section contains some interesting future research directions of physical

layer security that can make our work more general and practically appealing.

6.2.1 Further Exploitation of the Eavesdropper Strategies

As assumed in most of the literature and this thesis, eavesdroppers are usually supposed to be passive and act independently [117]. Accordingly, these models still need more extension on the assumption to solidify the adversary model, such as considering active eavesdroppers and their mutual collaboration.

Active Eavesdroppers

Most of the existing works on physical layer security have assumed the theoretical setup with passive eavesdroppers only. However, the eavesdroppers can launch various active attacks to enhance their eavesdropping performance [118]. These adversaries may eavesdrop, manipulate, inject, alter, duplicate, and reroute to benefit their purpose. In particular, by manipulating the environment, it is possible to bias the resulting bits in the key establishment process [119]. Another active attack, called pilot contamination attack, has been studied in [120]. In a pilot contamination attack, the eavesdropper attacks the channel training phase by injecting a virtue pilot to make the precoding beneficial to the eavesdropping channel. Several approaches have been proposed to resolve this sort of active attack [121]. Considering the various possibilities of different active attacks, such as a deceiving attack from the relay, more conservative secrecy schemes need to be proposed to overcome the weak assumption. Investigation of the physical layer security to ensure the legitimate transmission robust to adversarial attacks from more intelligent eavesdroppers will be a new avenue for further research.

Eavesdropper Colluding

For simplicity, eavesdroppers are usually assumed to be separated from each other and cannot exchange information. In fact, since cooperation is usually used by legitimate nodes, it must also be assumed that the same strategy can be exploited by intruders as well. The number of articles considering the impact of eavesdropper collusion in random

networks is comparatively small, while the issue has been occasionally considered. For instance, the secrecy capacity in random wireless networks with the presence of colluding eavesdroppers under an AWGN channel model was studied in [36], and the probability of non-zero secrecy capacity with multiple antenna transmission schemes in Rayleigh fading channels was analyzed in [100]. If eavesdroppers could employ collaborative processing, the probability that the combined effect of the eavesdropping channel better than the legitimate channel will go up quite rapidly [122]. Understanding the implications of collusion or collaboration on physical layer security will be important to solidify the adversary model.

6.2.2 Further Exploitation of Promising Networks and Techniques

Although there are many constraints that limit the practical application of physical layer security, recent advances in wireless communication have offered more technics for its practical implementation.

Wireless Sensor Networks (WSN)

Wireless sensor nodes are resource-constrained miniature devices limited by processing speed, storage capacity, and energy reservation [123]. Due to the huge demand for memory and energy, the widely utilized encryption algorithms cannot be employed to secure wireless sensor nodes. One promising direction is to develop physical layer security, which exploits wireless channel characteristics such as noise without the reliance on secret key exchange or generation. Accordingly, many characteristics and properties of the security in sensor networks can be derived based on the traditional secrecy models. The approach of CJ can be employed to enhance the security and optimize the energy efficiency. Other extensions can address a variety of issues such as designing more efficient secrecy achieving codes that are of low complexity, and investigating various propagation environments.

Internet of Thing (IoT)

The Internet of Things (IoT) is inherently a massive network of machine-type communication (MTC) devices. A significant portion of the IoT will be low-end, low-energy, and lightweight computing devices [122]. For these low end devices, most of their available resources must be devoted to executing core application functionality, and there may be little left over for supporting security. As a result, robust physical-layer security methods that can supplement or even replace lightweight cryptographic protocols are appealing solutions. Low-complexity secrecy schemes tailored for visible light communications (VLC) [124], acoustic and molecular communication channels remain largely open problems. Due to the practical constraints of IoT, many existing signal processing approaches for security will be challenged due to the availability of channel state information at the transmitter (CSIT). Investigating approaches such as ciphers or encoding for physical layer confidentiality that are efficient and have little to no message expansion is a promising direction that would greatly benefit IoT devices [125]. However, analysis of the energy-secrecy tradeoff among such MTC devices is still open to be solved.

Cross Layer Design

The security of communication networks has traditionally relied on cryptographic schemes in upper layers, albeit with the absence of the physical layer. Therefore, cross-layer analysis of secrecy to combine physical layer security and cryptographic schemes in wireless networks is another interesting research area. A cross-layer design may deploy the encryption approach for security in different layers [126]: at the application layer (e.g., secure shell (SSH) and secure sockets layer (SSL) for the end-to-end encryption), at the network layer (e.g., the IPSec protocol for the end-to-end encryption), at the data link layer and the physical layer (e.g., IEEE 802.11 wireless networks). To find such a combination approach, it is important to investigate how the physical layer security and traditional cryptographic approaches interact with each other to enhance the security of the system. Another research challenge is to define a totally new security metric that can measure the comprehensive property of information-theoretic and cryptographic

approaches [127], which might lead to a more efficient encryption scheme.

Full Duplex (FD)

Recently, a number of encouraging FD designs have been proposed to overcome the self-interference problem using novel combinations of antenna, analogue, and digital cancellations [128]. These FD designs allow the simultaneous transmission and reception over the same frequency band impractical. To overcome the defects of cooperator mobility, synchronization and trustworthiness in traditional jamming approaches which rely on the external helper, the authors in [129] considered using FD jamming. In the FD jamming scheme, the legitimate receiver can receive the signal from the source and simultaneously transmit jamming signals. It was shown that the wire-tap channel with the FD jamming achieves a better secrecy performance than the classic one with HD in terms of the outage secrecy region. Later, the networks with multi-antenna techniques and cooperative relays were also adopted to further boost the potential benefits of using the FD jamming in [130–132]. Although some more research about the scheme of using FD to enhance physical layer security turned up recently, the analysis of FD in the large-scale wireless networks, such as WSN and IoT, are still promising directions to extend.

6.2.3 Other Future Directions

Recently, many compelling topics have attracted the community, as can be found in the increase of the literature. Some more topics such as interference mitigation, machine learning, massive MIMO and LiFi can also provide the research potentials for the practical usage of physical layer security.

Appendix A

Proof of Proposition A

Proof: The ergodic capacity $R_{s:r}$ of a general fading channel with the PDF of the fading coefficient denoted as $f_{|h|^2}(x)$, can be expressed as follows:

$$\begin{aligned} R_{s:r} &= \mathbb{E}_{|h|^2}\left\{\log_2\left(1+\frac{\eta|h|^2}{r^\alpha}\right)\right\}, \\ &= \int_0^\infty \log_2\left(1+\frac{\eta}{r^\alpha}x\right) f_{|h|^2}(x)\,\mathrm{d}x. \end{aligned} \tag{A.1}$$

Then, the derivation of $R_{s:e}$ as a function of r is given by

$$\begin{aligned} \frac{\partial R_{s:r}}{\partial r} &= \int_0^\infty \left[\log_2\left(1+\frac{\eta}{r^\alpha}x\right)\right]' f_{|h|^2}(x)\,\mathrm{d}x, \\ &= -\frac{\alpha\eta}{r\ln 2}\int_0^\infty \frac{x}{r^\alpha+\eta x} f_{|h|^2}(x)\,\mathrm{d}x. \end{aligned} \tag{A.2}$$

For any fading channel, PDF $f_{|h|^2}(x) \geq 0$ always hold. It is apparent that, as $x \geq 0, \eta \geq 0$ and $r^\alpha \geq 0$, the integration

$$\int_0^\infty \frac{x}{r^\alpha+\eta x} f_{|h|^2}(x)\,\mathrm{d}x \geq 0. \tag{A.3}$$

Then we have $\frac{\partial R_{s:r}}{\partial r} \leq 0$. Thus, the ergodic capacity $R_{s:r}$ is a monotonically decreasing function of r.

Appendix B

Proof of Theorem 3

Proof: To derive the distribution of the distance from the origin to the n_{th} node outside the secrecy protected zone, we first investigate the intensity function of the node at a distance $r(r > 0)$ from the origin. Then the CDF and PDF of the distance from the n_{th} node to the origin will be computed based on this intensity function. As the nodes outside the secrecy protected zone are distributed as a PPP, according to the mapping theory, the intensity measure and intensity function can be separately expressed by

$$\Lambda_{opz} = \begin{cases} \pi\lambda(r^2 - \rho^2) & \text{if } r > \rho, \\ 0 & \text{if } r \leq \rho, \end{cases} \tag{B.1}$$

and

$$\lambda_{opz}(r) = \begin{cases} 2\lambda\pi r & \text{if } r > \rho, \\ 0 & \text{if } r \leq \rho. \end{cases} \tag{B.2}$$

Since the locations of the nodes outside the secrecy protected zone can still be modeled by a PPP, the probability of k nodes located in the annual region $A_{\rho:r}$ with internal radius ρ and external radius r can be calculated by

$$\begin{aligned} P[N(A_{\rho:r}) = k] &= \exp\left(-\int_{A_{\rho:r}} \lambda_{opz}(x)\mathrm{d}x\right) \frac{\left(\int_{A_{\rho:r}} \lambda_{opz}(x)\mathrm{d}x\right)^k}{k!}, \\ &= \exp\left[-\pi\lambda(r^2 - \rho^2)\right] \frac{[\pi\lambda(r^2 - \rho^2)]^k}{k!}. \end{aligned} \tag{B.3}$$

The CDF of the distance $D_n(r)$ from the origin to the n_{th} nearest node can be computed by

$$D_n(r) = 1 - \mathbb{P}\left[N(A_{\rho:r}) < n\right] = 1 - \exp\left[-\pi\lambda(r^2 - \rho^2)\right] \sum_{k=0}^{n-1} \frac{[\pi\lambda(r^2 - \rho^2)]^k}{k!}. \quad \text{(B.4)}$$

By taking the derivation of (B.4), the PDF of the distance from the origin to the n_{th} node outside the secrecy protected zone with radius ρ can be obtained as (4.24).

Appendix C

Proof of Theorem 4

Proof. For a Matérn HCPP of type II, which is generated from a homogenous PPP, Φ_p, with intensity λ_p and repulsive distance ϱ, the intensity of the HCPP is given by [33]

$$\lambda_M = \frac{1 - \exp\left(-\lambda_p C_d \varrho^d\right)}{C_d \varrho^d}. \tag{C.1}$$

Consequently, the probability of a point being retained from Φ_p is

$$p = \frac{\lambda_M}{\lambda_p} = \frac{1 - \exp\left(-\lambda_p C_d \varrho^d\right)}{\lambda_p C_d \varrho^d}. \tag{C.2}$$

Denoting the CDF of the distance from a typical node x to its nth nearest node of the Matérn HCPP as $F_{r_n}(x)$, we have

$$\begin{aligned} F_{r_n}(x) &= 1 - \mathbb{P}\left[N_M(B(x,r)) < n\right], \\ &= 1 - \sum_{k=0}^{n-1} \mathbb{P}\left[N_M(B(x,r)) = k\right], \end{aligned} \tag{C.3}$$

where $B(x,r)$ denotes a circular region surrounding the node at x with radius r and $N_M(B(x,r))$ represents the number of the nodes from Φ_M which are located in $B(x,r)$. According to the definition of Matérn HCPP of type II which is generated from a PPP, given that the number of nodes in $B(x,r)$ is denoted by m, the probability of retaining $k (m \leq k)$ points is equivalent to eliminating $m - k$ points. The probability of k nodes

located in $B(x,r)$ can be derived by

$$\begin{aligned}
&\mathbb{P}\left[N_M(B(x,r))=k\right]\\
&=\sum_{m=k}^{\infty}\mathbb{P}\left[N_p(B(x,r))=m\right]\times\mathbb{P}\left[m-k \text{ points eliminated } |N_p(B(x,r))=m\right],\\
&\overset{(a)}{\approx}\sum_{m=k}^{\infty}\exp(-\lambda_p C_d r^d)\frac{(\lambda_p C_d r^d)^m}{m!}C_m^k p^k(1-p)^{m-k},\\
&=\exp(-\lambda_p C_d r^d)\frac{(\lambda_p C_d r^d)^k}{k!}\sum_{m=k}^{\infty}\frac{\left[(1-p)\lambda_p C_d r^d\right]^{m-k}}{(m-k)!},\\
&=\exp(-\lambda_p C_d r^d)\frac{(\lambda_p C_d r^d)^k}{k!}\exp((1-p)\lambda_p C_d r^d),\\
&=\exp(-\lambda_M C_d r^d)\frac{(\lambda_M C_d r^d)^k}{k!},
\end{aligned} \tag{C.4}$$

where (a) follows from that for ϱ small enough, $\mathbb{P}[k \text{ points are eliminated}] \approx (1-p)^k$ [133]. By substituting (C.4) into (C.3), the CDF of the distance from a typical node x to its nth nearest node of the MHCPP can be obtained as

$$\begin{aligned}
F_{r_n}(x) &= 1-\sum_{k=0}^{n-1}\mathbb{P}\left[N_M(B(x,r))=k\right],\\
&= 1-\sum_{k=0}^{n-1}\exp(-\lambda_M C_d r^d)\frac{(\lambda_M C_d r^d)^k}{k!}.
\end{aligned} \tag{C.5}$$

By taking the derivative of (C.5), the PDF of distance r_n is given by (5.10). □

Appendix D

CDF of γ_l with FFR

Proof. Similar to the scenario without FFR, the CDF of γ_l can be derived by

$$\begin{aligned} F_{\gamma_l}(\beta) &= 1 - \int_0^\infty \mathbb{P}(h > \beta r_l^\alpha(\sigma^2 + \mathrm{I}_l)|r_l) f_{r_l}(r)\,\mathrm{d}r, \\ &= 1 - \int_0^\infty \mathbb{E}_{I_l}\left[\exp(-\beta r_l^\alpha(\sigma^2 + \mathrm{I}_l))|r_l\right] f_{r_l}(r)\,\mathrm{d}r, \\ &= 1 - \int_0^\infty \exp(-\beta r_l^\alpha \sigma^2) \underbrace{\mathbb{E}_{I_l}\left[\exp(-\beta r_l^\alpha \mathrm{I}_l)|r_l\right]}_{(I)} f_{r_l}(r)\,\mathrm{d}r. \end{aligned} \tag{D.1}$$

Due to the implementation of FFR in the cellular networks, the approach of deriving the Laplace transform of I_l in [109] cannot be applied to (D.1). Instead, the expression (I) can be derived by

$$\begin{aligned} \mathbb{E}_{I_l}\left[\exp(-\beta r_l^\alpha \mathrm{I}_l)|r_l\right] =& \mathbb{E}_{I_l}\left[\exp(-\sum_{i\in\Phi_B\setminus b} \beta r_l^\alpha h_{i,l} r_{i,l}^{-\alpha} \mathbf{1}(\Delta_l = \Delta_i))\middle| r_l\right], \\ =& \mathbb{E}_{I_l}\left[\prod_{i\in\Phi_B\setminus b} \exp(-\beta r_l^\alpha h_{i,l} r_{i,l}^{-\alpha} \mathbf{1}(\Delta_l = \Delta_i))\middle| r_l\right], \\ =& \mathbb{E}_{\Phi_r}\left[\prod_{i\in\Phi_B\setminus b} \mathbb{E}_{h_{i,l},\Delta_{i,l}}\left[\exp(-\beta r_l^\alpha h_{i,l} r_{i,l}^{-\alpha} \mathbf{1}(\Delta_l = \Delta_i))\right]\middle| r_l\right]. \end{aligned} \tag{D.2}$$

For a discrete function $g(x)$, its expectation can be derived by $\mathbb{E}[g(x)] = \sum_k g(x_k)P_X(x_k)$ [134]. Accordingly, we have

$$\begin{aligned}
&\mathbb{E}_{\Delta_{i,l}}\left[\exp(-\beta r^{\alpha}h_{i,l}r_{i,l}^{-\alpha}\mathbf{1}(\Delta_l=\Delta_i))\right]\\
=&\sum_{i=1}^{L}\exp(-\beta r^{\alpha}h_{i,l}r_{i,l}^{-\alpha}\mathbf{1}(\Delta_l=\Delta_i))\mathbb{P}_{\Delta}\left(\mathbf{1}(\Delta_l=\Delta_i)\right),\\
=&\sum_{i\neq l}\exp(-\beta r^{\alpha}h_{i,l}r_{i,l}^{-\alpha}\mathbf{1}(\Delta_l=\Delta_i))\mathbb{P}_{\Delta}\left(\mathbf{1}(\Delta_l=\Delta_i)|i\neq l\right)\\
&+\sum_{i=l}\exp(-\beta r^{\alpha}h_{i,l}r_{i,l}^{-\alpha}\mathbf{1}(\Delta_l=\Delta_i))\mathbb{P}_{\Delta}\left(\mathbf{1}(\Delta_l=\Delta_i)|i=l\right),\\
\overset{(a)}{=}&\sum_{i\neq l}\frac{1-\mathbb{E}_{\Delta}\left[\mathbf{1}(\Delta_l=\Delta_i)\right]}{L-1}+\sum_{i=l}\exp(-\beta r^{\alpha}h_{i,l}r_{i,l}^{-\alpha})\mathbb{E}_{\Delta}\left[\mathbf{1}(\Delta_l=\Delta_i)\right],\\
=&(L-1)\frac{1-\mathbb{E}_{\Delta}\left[\mathbf{1}(\Delta_l=\Delta_i)\right]}{L-1}+\exp(-\beta r^{\alpha}h_{i,l}r_{i,l}^{-\alpha})\mathbb{E}_{\Delta}\left[\mathbf{1}(\Delta_l=\Delta_i)\right],\\
=&1-\mathbb{E}_{\Delta}\left[\mathbf{1}(\Delta_l=\Delta_i)\right]\left(1-\exp(-\beta r^{\alpha}h_{i,l}r_{i,l}^{-\alpha})\right),\\
=&1-\frac{1}{L}\left(1-\exp(-\beta r^{\alpha}h_{i,l}r_{i,l}^{-\alpha})\right),
\end{aligned}\tag{D.3}$$

where (a) follows from that

$$\begin{aligned}
\mathbb{E}_{\Delta}\left[\mathbf{1}(\Delta_l=\Delta_i)\right]=&\sum_{i=1}^{L}\mathbf{1}(\Delta_l=\Delta_i)\mathbb{P}_{\Delta}\left[\mathbf{1}(\Delta_l=\Delta_i)\right],\\
=&\sum_{i\neq l}\mathbf{1}(\Delta_l=\Delta_i)\mathbb{P}_{\Delta}\left[\mathbf{1}(\Delta_l=\Delta_i)|i\neq l\right]\\
&+\sum_{i=l}\mathbf{1}(\Delta_l=\Delta_i)\mathbb{P}_{\Delta}\left[\mathbf{1}(\Delta_l=\Delta_i)|i=l\right],\\
=&\mathbb{P}_{\Delta}\left[\mathbf{1}(\Delta_l=\Delta_i)|i=l\right].
\end{aligned}$$

Then, we have

$$\begin{aligned}
&\mathbb{E}_{h_{i,l},\Delta_{i,l}}\left[\exp(-\beta r^{\alpha}h_{i,l}r_{i,l}^{-\alpha}\mathbf{1}(\Delta_l=\Delta_z))\right]\\
=&\mathbb{E}_{h_{i,l}}\left[\mathbb{E}_{\Delta_{i,l}}\left[\exp(-\beta r^{\alpha}h_{i,l}r_{i,l}^{-\alpha}\mathbf{1}(\Delta_l=\Delta_z))\right]\right],\\
=&\mathbb{E}_{h_{i,l}}\left[1-\frac{1}{L}\left(1-\exp(-\beta r^{\alpha}h_{i,l}r_{i,l}^{-\alpha})\right)\right],\\
\overset{(a)}{=}&1-\frac{1}{L}\left(1-\frac{1}{1+\beta r^{\alpha}R_z^{-\alpha}}\right).
\end{aligned}\tag{D.4}$$

where (a) follows from assuming that the channel is under Rayleigh fading and

$$\begin{aligned}\mathbb{E}_{h_{i,l}}\left[\exp(-\beta r_l^{\alpha} h_{i,l} r_{i,l}^{-\alpha})\right] =& \int_0^{\infty} e^{(-\beta r_l^{\alpha} r_{i,l}^{-\alpha} x)} e^{-x}\,\mathrm{d}x, \\ =& \frac{1}{1+\beta r_l^{\alpha} R_z^{-\alpha}}.\end{aligned} \tag{D.5}$$

By substituting (D.4) into (D.2), we have

$$\begin{aligned}\mathbb{E}_{I_r}\left[\exp(-\beta r^{\alpha}\mathrm{I}_r)|r\right] =& \mathbb{E}_{\Phi_r} \prod_{i\in\Phi_B\setminus b}\left[1-\frac{1}{L}\left(1-\frac{1}{1+\beta r^{\alpha} R_z^{-\alpha}}\right)\right], \\ =& \exp\left[-\int_r^{\infty}\frac{1}{L}\left(1-\frac{1}{1+\beta r^{\alpha} x^{-\alpha}}\right) 2\pi\lambda x\,\mathrm{d}x\right], \\ \overset{x=vr}{=}& \exp\left[-\frac{2\pi\lambda r^2}{L}\int_1^{\infty}\left(1-\frac{1}{1+\beta v^{-\alpha}}\right) v\,\mathrm{d}v\right], \\ =& \exp\left[-\frac{2\pi\lambda r^2}{L}\int_1^{\infty}\frac{\beta v}{v^{\alpha}+\beta}\,\mathrm{d}v\right].\end{aligned} \tag{D.6}$$

Then, the CDF of γ_l can be obtained by substituting (D.6) into (D.1)

$$F_{\gamma_l}(\beta) = 1 - \int_0^{\infty} \exp(-\beta r^{\alpha}\sigma^2) \exp\left(-\frac{2\pi\lambda r^2}{L}\beta\int_1^{\infty}\frac{v}{v^{\alpha}+\beta}\,\mathrm{d}v\right) f_{r_l}(r)\,\mathrm{d}r. \tag{D.7}$$

□

Appendix E
List of Publications

This Appendix contains a list of published and submitted papers.

E.1 Accepted Publications

- **W. Liu**, Z. Ding, T. Ratnarajah and J. Xue, "On Ergodic Secrecy Capacity of Random Wireless Networks with Protected Zone," *IEEE Transactions on Vehicular Technology (TVT)*, vol.PP, no.99, pp.1-1, September, 2015.

- **W. Liu**, M.Z.I. Sarkar and T. Ratnarajah, "Combined Approach of Zero Forcing Precoding and Cooperative Jamming: A Secrecy Tradeoff," *In Proc. the IEEE Wireless Communications and Networking Conference (WCNC)* , April 7-10, 2013.

- **W. Liu**, M.Z.I. Sarkar and T. Ratnarajah, "On the security of cognitive radio networks: Cooperative jamming with relay selection," *European Conference on Networks and Communications (EuCNC)*, June 23-26, 2014.

- **W. Liu**, S. Vuppala, G. Abreu and T. Ratnarajah, "Secrecy Outage in Correlated Nakagami-m Fading Channels," *In Proc. the IEEE 25 Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Washington D.C., USA, September 2-5, 2014.

- S. Vuppala, **W. Liu**, T. Ratnarajah and G. Abreu, "Secrecy Outage Analysis of Cognitive Wireless Sensor Networks," *In Proc. the IEEE Forty-eight Annual Asilomar conference on Signals, Systems, and Computers (ASILOMAR)*, Pacific Grove, California, Nov. 2-5, 2014 [Nominated for student paper competition].

- S. Vuppala, **W. Liu**, G. Abreu and T. Ratnarajah, "Secrecy Outage of Nakagami-

m MISO Channels with Randomly Located Receivers," *In Proc. on the IEEE International Conference on Communications (ICC)*, At London, UK, June.8-12, 2015.

E.2 Papers under Revision

- **W. Liu** M. Z. I. Sarkar, T. Ratnarajah and H. Du, "Wireless Security with a Combined Approach of Beamforming and Cooperative Jamming", Submitted to *IET Communications*, January, 2016.
- **W. Liu**, J. Xue, T. Ratnarajah, and S. Vuppala, "On Physical Layer Security Analysis of Downlink Cellular Networks using Matérn Hard-core Point Processes", Submitted to *IEEE Transactions on Communications (TCOM)*, January, 2016.

Bibliography

[1] A. De Domenico, E. Calvanese Strinati, and M. G. Di Benedetto. A survey on MAC strategies for cognitive radio networks. *IEEE Communications Surveys Tutorials*, 14(1):21–44, January 2012.

[2] T. S. Rappaport. *Wireless communications principles and practices*. Prentice-Hall, 2002.

[3] C.E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, October 1949.

[4] A. Menezes, P. Van Oorschot, and S. Vanstone. *Handbook of applied cryptography*. CRC Press, Inc., 1997.

[5] Y. Liang, H.V. Poor, and S. Shamai. Information theoretic security. *Foundations and Trends in Communications and Information Theory*, 5(4):355–580, 2008.

[6] A.D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, October 1975.

[7] S. Leung-Yan-Cheong and M.E. Hellman. The Gaussian wire-tap channel. *IEEE Transactions on Information Theory*, 24(4):451–456, July 1978.

[8] I. Csiszar and J Korner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, May 1978.

[9] P.K. Gopala, L. Lai, and H. EI Gamal. On the secrecy capacity of fading channels. *IEEE Transactions on Information Theory*, 54(10):4687 – 4698, October 2008.

[10] M. Bloch, J. Barros, M.R.D. Rodrigues, and S.W. McLaughlin. Wireless information-theoretic security. *IEEE Transactions on Information Theory*, 54(6):2515–2534, June 2008.

[11] Thomas M. Cover and B.Gopinath. *Open Problems in Communication and*

Computation. Springer New York, 1st edition, 1987.

[12] Y. Liang, H.V. Poor, and S. Shamai. Secrecy capacity region of fading broadcast channels. *IEEE International Symposium on Information Theory (ISIT)*, pages 1291–1295, June 2007.

[13] L. Zhang, R. Zhang, Y. Liang, Y. Xin, and S. Cui. On the relationship between the multi-antenna secrecy communications and cognitive radio communications. *IEEE Transactions on Communications*, 58(6):1877–1886, June 2010.

[14] Y. Pei, Y. Liang, L. Zhang, K.C. Teh, and K.H. Li. Secure communication over MISO cognitive radio channels. *IEEE Transactions on Wireless Communications*, 9(4):1494–1502, April 2010.

[15] Y. Pei, Y. Liang, L. Zhang, K.C. Teh, and K.H. Li. Secure communication in multiantenna cognitive radio networks with imperfect channel state information. *IEEE Transactions on Signal Processing*, 59(4):1683–1693, April 2011.

[16] J. Huang and A. Lee Swindlehurst. Robust secure transmission in MISO channels based on worst-case optimization. *IEEE Transactions on Signal Processing*, 60(4):1696–1707, April 2012.

[17] J. Zhang and M.C. Gursory. Secure relay beamforming over cognitive radio channels. In *2011 45th Annual Conference on Information Sciences and Systems (CISS)*, pages 1–5, March 2011.

[18] C. Masouros and T. Ratnarajah. Interference as a source of green signal power in cognitive relay assisted co-existing MIMO wireless transmissions. *IEEE Transactions on Information Theory*, 60(2):525–536, February 2012.

[19] L. Lai and H. El Gamal. The relay-eavesdropper channel: Cooperation for secrecy. *IEEE Transactions on Information Theory*, 54(9):4005–4019, September 2008.

[20] S. Goel and R. Negi. Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications*, 7(6):2180–2189, June 2008.

[21] E. Tekin and A. Yener. The general Gaussian multiple-access and two-way

wiretap channels: achievable rates and cooperative jamming. *IEEE Transactions on Information Theory*, 54(6):2735–2751, June 2008.

[22] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor. Improving wireless physical layer security via cooperating relays. *IEEE Transactions on Signal Processing*, 58(3):1875–1888, March 2010.

[23] G. Zheng, L. Choo, and K.K. Wong. Optimal cooperative jamming to enhance physical layer security using relays. *IEEE Transactions on Signal Processing*, 59(3):1317–1322, March 2011.

[24] J. Huang and A. L. Swindlehurst. Cooperative jamming for secure communications in MIMO relay networks. *IEEE Transactions on Signal Processing*, 59(10):4871–4884, October 2011.

[25] W. Liu, M. Z. I. Sarkar, and T. Ratnarajah. Combined approach of zero forcing precoding and cooperative jamming: A secrecy tradeoff. In *Proc. IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, China*, pages 1843–1847, April 2013.

[26] A. Mukherjee and A. Lee Swindlehurst. Robust beamforming for security in MIMO wiretap channels with imperfect CSI. *IEEE Transactions on Signal Processing*, 59(1):351–361, January 2011.

[27] L. Zhang, Y. Liang, and Y. Xin. Joint beamforming and power allocation for multiple access channels in cognitive radio networks. *IEEE Journal of Selected Areas in Communication*, 26(1):38–51, January 2008.

[28] A. Khisti and G.W. Wornell. Secure transmission with multiple antennas I: The MISOME wiretap channel. *IEEE Transactions on Information Theory*, 56(7):3088–3104, July 2010.

[29] A. Khisti and G.W. Wornell. Secure transmission with multiple antennas - part II: The MIMOME wiretap channel. *IEEE Transactions on Information Theory*, 56(11):5515–5532, November 2010.

[30] G. Geraci, H.S. Dhillon, J.G. Andrews, Jinhong Yuan, and I.B. Collings. Physical

layer security in downlink multi-antenna cellular networks. *IEEE Transactions on Communications*, 62(6):2006–2021, June 2014.

[31] H. Wang, X. Zhou, and M.C. Reed. Physical layer security in cellular networks: A stochastic geometry approach. *IEEE Transactions on Wireless Communications*, 12(6):2776–2787, June 2013.

[32] A. Guo and M. Haenggi. Spatial stochastic models and metrics for the structure of base stations in cellular networks. *IEEE Transactions on Wireless Communications*, 12(11):5800–5812, November 2013.

[33] M. Haenggi. *Stochastic geometry for wireless networks*. Cambridge University Press, 2012.

[34] S. Vuppala and G. Abreu. Secrecy outage analysis in cellular networks. *IEEE Wireless Communications Letters*, 4(99):157–160, April 2015.

[35] M. Haenggi. A geometric interpretation of fading in wireless networks: Theory and applications. *IEEE Transactions on Information Theory*, 54(12):5500–5510, December 2008.

[36] P.C. Pinto, J. Barros, and M.Z. Win. Secure communication in stochastic wireless networks-part I: Connectivity. *IEEE Transactions on Information Forensics and Security*, 7(1):125–138, February 2012.

[37] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal. On secrecy capacity scaling in wireless networks. *IEEE Transactions on Information Theory*, 58(5):3000 – 3015, May 2012.

[38] S. Vuppala and G. Abreu. Unicasting on the secrecy graph. *IEEE Transactions on Information Forensics and Security*, 8(9):1469 – 1481, September 2013.

[39] P.C. Pinto, J. Barros, and M.Z. Win. Secure communication in stochastic wireless networks-part II: Maximum rate and collusion. *IEEE Transactions on Information Forensics and Security*, 7(1):139–147, February 2012.

[40] X. Zhou, R.K. Ganti, J.G. Andrews, and A Hjorungnes. On the throughput cost of

physical layer security in decentralized wireless networks. *IEEE Transactions on Wireless Communications*, 10(8):2764–2775, August 2011.

[41] N. Romero-Zurita, D. McLernon, M. Ghogho, and A Swami. Physical layer security based on protected zone and artificial noise. *IEEE Signal Processing Letters*, 20(5):487–490, May 2013.

[42] Y. Jeong, T.Q.S. Quek, and H. Shin. Stochastic wireless secure multicasting. *IEEE International Conference on Communications (ICC)*, pages 4718–4723, June 2013.

[43] G. Geraci, S. Singh, J.G. Andrews, J. Yuan, and IB. Collings. Secrecy rates in broadcast channels with confidential messages and external eavesdroppers. *IEEE Transactions on Wireless Communications*, 13(5):2931–2943, May 2014.

[44] M. Ghogho and A. Swami. Physical-layer secrecy of MIMO communications in the presence of a Poisson random field of eavesdroppers. *IEEE International Conference on Communications Workshops (ICC)*, pages 1–5, June 2011.

[45] S.H. Chae, W. Choi, J.H. Lee, and T.Q.S. Quek. Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone. *IEEE Transactions on Information Forensics and Security*, 9(10):1617–1628, October 2014.

[46] Xiangyun Zhou and M.R. McKay. Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation. *IEEE Transactions on Vehicular Technology*, 59(8):3831–3842, October 2010.

[47] S. Zhang, S.C. Liew, and H. Wang. Blind known interference cancellation. *IEEE Journal on Selected Areas in Communications*, 31(8):1572–1582, August 2013.

[48] X. Shang and H.V. Poor. Capacity region of vector Gaussian interference channels with generally strong interference. *IEEE Transactions on Information Theory*, 58(6):3472–3496, June 2012.

[49] V.S. Annapureddy and V.V. Veeravalli. Sum capacity of MIMO interference channels in the low interference regime. *IEEE Transaction on Information Theory*, 57(5):2565–2581, May 2011.

[50] D. Tse and P. Viswanath. *Fundamentals of wireless communication*. Cambridge University Press, 2005.

[51] K.T. Herring, J.W. Holloway, D.H. Staelin, and D.W. Bliss. Path-loss characteristics of urban wireless channels. *IEEE Transactions on Antennas and Propagation*, 58(1):171–177, January 2010.

[52] C. Xiao, Y.R. Zheng, and N.C. Beaulieu. Statistical simulation models for Rayleigh and Rician fading. In *Proc. IEEE International Conference on Communications (ICC)*, volume 5, pages 3524–3529, May 2003.

[53] R.K. Mallik. A new statistical model of the complex Nakagami-m fading gain. *IEEE Transactions on Communications*, 58(9):2611–2620, September 2010.

[54] H.Y. Shang, Y. Han, and J.H. Lu. Statistical analysis of Rician and Nakagami-m fading channel using multipath shape factors. In *Proc. Second International Conference on Computational Intelligence and Natural Computing Proceedings (CINC)*, volume 1, pages 398–401, September 2010.

[55] H. Wang, X. Zhou, and M.C. Reed. Physical layer security in cellular networks: A stochastic geometry approach. *IEEE Transactions on Wireless Communication*, 12(6):2776–2787, June 2013.

[56] R. Vaze, K.T. Truong, S. Weber, and R.W. Heath. Two-way transmission capacity of wireless ad-hoc networks. *IEEE Transactions on Wireless Communications*, 10(6):1966–1975, June 2011.

[57] R. Vaze. Transmission capacity of spectrum sharing ad hoc networks with multiple antennas. *IEEE Transactions on Wireless Communications*, 10(7):2334–2340, July 2011.

[58] R. Vaze and R.W. Heath. Transmission capacity of ad-hoc networks with multiple antennas using transmit stream adaptation and interference cancellation. *IEEE Transactions on Information Theory*, 58(2):780–792, February 2012.

[59] 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, 51(12):4091 –4102, December 2005.

[60] S.P. Weber, J.G. Andrews, X. Yang, and G. Veciana. Transmission capacity of wireless ad hoc networks with successive interference cancellation. *IEEE Transactions on Information Theory*, 53(8):2799–2814, August 2007.

[61] M. McHenry, E. Livsics, T. Nguyen, and N. Majumdar. XG dynamic spectrum access field test results. *IEEE Communications Magazine*, 45(6):51–57, June 2007.

[62] I.F. Akyildiz, W. Lee, M.C. Vuran, and S. Mohanty. Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Computer Networks*, 50(13):2127 – 2159, 2006.

[63] M.I. Joseph. *An integrated agent architecture for software defined radio*. Ph.D. dissertation, Royal Institute of Technology (KTH), Stockholm, Sweden, 2000.

[64] C. Stevenson, G. Chouinard, Z. Lei, W. Hu, S.J. Shellhammer, and W. Caldwell. IEEE 802.22: The first cognitive radio wireless regional area network standard. *IEEE Communications Magazine*, 47(1):130–138, January 2009.

[65] Y. Zeng, Y. Liang, A. Hoang, and R. Zhang. A review on spectrum sensing for cognitive radio: Challenges and solutions. *EURASIP Journal on Advances in Signal Processing*, 2010(2):1–15, January 2010.

[66] S. Haykin. Cognitive radio: brain-empowered wireless communications. *IEEE Journal on Selected Areas in Communications*, 23(2):201–220, February 2005.

[67] C. Cordeiro, K. Challapali, D. Birru, and N.S. Shankar. IEEE 802.22: the first worldwide wireless standard based on cognitive radios. In *IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN).*, pages 328–337, November 2005.

[68] B. Wang, K.J.R. Liu, and T.C. Clancy. Evolutionary cooperative spectrum sensing game: how to collaborate? *IEEE Transactions on Communications*, 58(3):890–900, March 2010.

[69] I.F. Akyildiz, W. Lee, M.C. Vuran, and S. Mohanty. A survey on spectrum

management in cognitive radio networks. *IEEE Communications Magazine*, 46(4):40–48, April 2008.

[70] S. Srinivasa and S.A. Jafar. Cognitive radios for dynamic spectrum access - the throughput potential of cognitive radio: A theoretical perspective. *IEEE Communications Magazine*, 45(5):73–79, May 2007.

[71] A.G. Fragkiadakis, E.Z. Tragos, and I.G. Askoxylakis. A survey on security threats and detection techniques in cognitive radio networks. *IEEE Communications Surveys Tutorials*, 15(1):428–445, January 2013.

[72] K. J. Ray Liu and Beibei Wang. *Cognitive radio networking and security: A game-theoretic view*. Cambridge University Press, 1st edition, 2010.

[73] M. Haenggi, J.G. 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 Communication*, 27(7):1029–1046, September 2009.

[74] F. Baccelli and S. Zuyev. *Frontiers in queueing: Models and applications in science and engineering*. CRC Press, Inc., 1997.

[75] F. Aurenhammer and H. Edelsbrunne. An optimal algorithm for constructing the weighted Voronoi diagram in the panel. *Pattern Recognition*, 17(2):251 – 257, 1984.

[76] R.W. Heath and M. Kountouris. Modeling heterogeneous network interference with using Poisson point processes. *IEEE Transactions on Signal Processing*, 61(16):4114–4126, August 2013.

[77] M. Haenggi and R.K. Ganti. Interference in large wireless networks. *Foundations and Trends in Networking*, 3(2), February 2009.

[78] M. Haenggi. Mean interference in hard-core wireless networks. *IEEE Communications Letters*, 15(8):792–794, August 2011.

[79] P.K. Gopala, L. Lai, and H. El Gamal. On the secrecy capacity of fading channels.

IEEE Transactions on Information Theory, 54(10):4687–4698, October 2008.

[80] Y. Zou, X. Wang, and W. Shen. Physical-layer security with multiuser scheduling in cognitive radio networks. *IEEE Transactions on Communications*, 61(12):5103–5113, December 2013.

[81] R.K. Sharma and D.B. Rawat. Advances on security threats and countermeasures for cognitive radio networks: A survey. *IEEE Communications Surveys Tutorials*, 17(2):1023–1043, May 2015.

[82] Y. Liang, A. Somekh-Baruch, H.V. Poor, S. Shamai, and S. Verdu. Capacity of cognitive interference channels with and without secrecy. *IEEE Transactions on Information Theory*, 55(2):604–619, February 2009.

[83] Z. Shu, Y. Yang, Y. Qian, and Q. Hu. Impact of interference on secrecy capacity in a cognitive radio network. In *Proc. IEEE Global Telecommunications Conference*, pages 1–6, December 2011.

[84] K. Park, T. Wang, and M.S. Alouini. On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming. *IEEE Journal on Selected Areas in Communications*, 31(9):1741–1750, September 2013.

[85] Q. Zhang, X. Huang, Q. Li, and J. Qin. Cooperative jamming aided robust secure transmission for wireless information and power transfer in MISO channels. *IEEE Transactions on Communications*, 63(3):906–915, March 2015.

[86] I. Krikidis, J.S. Thompson, and S. Mclaughlin. Relay selection for secure cooperative networks with jamming. *IEEE Transactions on Wireless Communications*, 8(10):5003–5011, October 2009.

[87] Y. Zou, X. Wang, and W. Shen. Optimal relay selection for physical-layer security in cooperative wireless networks. *IEEE Journal on Selected Areas in Communications*, 31(10):2099–2111, October 2013.

[88] Y. Zou, X. Wang, W. Shen, and L. Hanzo. Security versus reliability analysis of opportunistic relaying. *IEEE Transactions on Vehicular Technology*, 63(6):2653–2661, July 2014.

[89] Y. Liu, L. Wang, T.T. Duy, M. Elkashlan, and T.Q. Duong. Relay selection for security enhancement in cognitive relay networks. *IEEE Wireless Communications Letters*, 4(1):46–49, February 2015.

[90] H. Hui, A.L. Swindlehurst, G. Li, and J. Liang. Secure relay and jammer selection for physical layer security. *IEEE Signal Processing Letters*, 22(8):1147–1151, August 2015.

[91] L. Wang, Y. Cai, Y. Zou, W. Yang, and L. Hanzo. Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays. *IEEE Transactions on Vehicular Technology*, PP(99):1–1, 2015.

[92] J. Li, A.P. Petropulu, and S. Weber. Optimal cooperative relaying schemes for improving wireless physical layer security. *Computing Research Repository*, abs/1001.1389, December 2010.

[93] F. Miatton. Interference alignment at intermediate SNR with perfect or noisy CSI. Master's thesis, Royal Institute of Technology, May 2010.

[94] O. Tipmongkolsilp, S. Zaghloul, and A. Jukan. The evolution of cellular backhaul technologies: Current issues and future trends. *IEEE Communications Surveys Tutorials*, 13(1):97–113, First 2011.

[95] H. Raza. A brief survey of radio access network backhaul evolution: Part II. *IEEE Communications Magazine*, 51(5):170–177, May 2013.

[96] A. Apostolaras, K. Choumas, I. Syrigos, I. Koutsopoulos, T. Korakis, A. Argyriou, and L. Tassiulas. On the implementation of relay selection strategies for a cooperative diamond network. In *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pages 1753–1758, Sept 2013.

[97] S. Luo, H. Godrich, A. Petropulu, and H. V. Poor. A knapsack problem formulation for relay selection in secure cooperative wireless communication. In *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 2512–2515, May 2011.

[98] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami. PHY layer security based on protected zone and artificial noise. *IEEE Signal Processing Letters*, 20(5):487–490, May 2013.

[99] J.P. Vilela, P.C. Pinto, and J. Barros. Position-based jamming for enhanced wireless secrecy. *IEEE Transactions on Information Forensics and Security*, 6(3):616–627, September 2011.

[100] X. Zhou, R.K. Ganti, and J.G. Andrews. Secure wireless network connectivity with multi-antenna transmission. *IEEE Transactions on Wireless Communications*, 10(2):425–430, February 2011.

[101] Y. Li, M. Peng, A. Manzoor, and C. Wang. Co-channel interference in two-tier heterogeneous networks: Analytical model and ergodic capacity. *Transactions on Emerging Telecommunications Technologies*, 1(27):101–110, January 2016.

[102] L. Sun and S. Jin. On the ergodic secrecy rate of multiple-antenna wiretap channels using artificial noise and finite-rate feedback. *IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)*, pages 1264–1268, September 2011.

[103] X. Zhou and M.R. McKay. Physical layer security with artificial noise: Secrecy capacity and optimal power allocation. *3rd International Conference on Signal Processing and Communication Systems (ICSPCS)*, pages 1–5, September 2009.

[104] I. S. Gradshteyn and I. M. Ryzhik. *Table of integrals, series, and products*. Academic, San Diego, CA, 6th edition, 2000.

[105] M. Haenggi. On distances in uniformly random networks. *IEEE Transactions on Information Theory*, 51(10):3584–3586, October 2005.

[106] L. Zhang, H. Yang, and M.O. Hasna. On ergodic capacity of wireless transmission subject to Poisson distributed interferers over Rayleigh fading channels. *IEEE 77th Vehicular Technology Conference (VTC)*, pages 1–6, June 2013.

[107] C. Lee and M. Haenggi. Interference and outage in Poisson cognitive networks. *IEEE Transactions on Wireless Communications*, 11(4):1392–1401, April 2012.

[108] Zeinab Yazdanshenasan, Harpreet S. Dhillon, Mehrnaz Afshang, and Peter Han Joo Chong. Poisson hole process: Theory and applications to wireless networks. *CoRR*, abs/1601.01090, Feb 2016.

[109] M. Haenggi and R.K. Ganti. Interference in large wireless networks. *Foundations and Trends in Networking*, 3(2):127–248, November 2009.

[110] T.D. Novlan, R.K. Ganti, A. Ghosh, and J.G. Andrews. Analytical evaluation of fractional frequency reuse for OFDMA cellular networks. *IEEE Transactions on Wireless Communications*, 10(12):4294–4305, December 2011.

[111] R. Ullah, N. Fisal, H. Safdar, W. Maqbool, Z. Khalid, and A.S. Khan. Voronoi cell geometry based dynamic fractional frequency reuse for OFDMA cellular networks. *IEEE International Conference on Signal and Image Processing Applications (ICSIPA)*, pages 435–440, October 2013.

[112] X. Zhang, X. Zhou, and M.R. McKay. Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks. *IEEE Transactions on Information Forensics and Security*, 8(11):1802–1814, November 2013.

[113] G. Alfano, M. Garetto, and E. Leonardi. New insights into the stochastic geometry analysis of dense CSMA networks. *in Proceedings IEEE International Conference on Computer Communications (INFOCOM)*, pages 2642–2650, April 2011.

[114] J.G. Andrews, F. Baccelli, and R.K. Ganti. A tractable approach to coverage and rate in cellular networks. *IEEE Transactions on Communications*, 59(11):3122–3134, November 2011.

[115] F. Baccelli and B. Błaszczyszyn. Stochastic geometry and wireless networks: Volume I theory. *Foundations and Trends in Networking*, 3(3-4):249–449, 2008.

[116] S.R. Theodore. *Wireless communications: Principles and practice*. Prentice Hall communications engineering and emerging technologies series. Dorling Kindersley, 2009.

[117] A. Mukherjee and A.L. Swindlehurst. Jamming games in the MIMO wiretap channel with an active eavesdropper. *IEEE Transactions on Signal Processing*,

61(1):82–91, January 2013.

[118] D. Kapetanovic, G. Zheng, and F. Rusek. Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks. *IEEE Communications Magazine*, 53(6):21–27, June 2015.

[119] S.N. Premnath, S. Jana, J. Croft, P.L. Gowda, M. Clark, S.K. Kasera, N. Patwari, and S.V. Krishnamurthy. Secret key extraction from wireless signal strength in real environments. *IEEE Transactions on Mobile Computing*, 12(5):917–930, May 2013.

[120] X. Zhou, B. Maham, and A. Hjorungnes. Pilot contamination for active eavesdropping. *IEEE Transactions on Wireless Communications*, 11(3):903–907, March 2012.

[121] Q. Xiong, Y. Liang, K.H. Li, and Y. Gong. An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems. *IEEE Transactions on Information Forensics and Security*, 10(5):932–940, May 2015.

[122] W. Trappe. The challenges facing physical layer security. *IEEE Communications Magazine*, 53(6):16–20, June 2015.

[123] D. Dardari, A. Conti, C. Buratti, and R. Verdone. Mathematical evaluation of environmental monitoring estimation error through energy-efficient wireless sensor networks. *IEEE Transactions on Mobile Computing*, 6(7):790–802, July 2007.

[124] A. Mostafa and L. Lampe. Physical-layer security for MISO visible light communication channels. *IEEE Journal on Selected Areas in Communications*, 33(9):1806–1818, September 2015.

[125] A. Mukherjee. Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints. *Proceedings of the IEEE*, 103(10):1747–1761, October 2015.

[126] F. Foukalas, V. Gazis, and N. Alonistioti. Cross-layer design proposals for wireless mobile networks: A survey and taxonomy. *IEEE Communications Surveys Tutorials*, 10(1):70–85, January 2008.

[127] L.J. Rodriguez, N.H. Tran, T.Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty. Physical layer security in wireless cooperative relay networks: State of the art and beyond. *IEEE Communications Magazine*, 53(12):32–39, December 2015.

[128] L. Li, Z. Chen, D. Zhang, and J. Fang. A full-duplex Bob in the MIMO Gaussian wiretap channel: Scheme and performance. *IEEE Signal Processing Letters*, 23(1):107–111, January 2016.

[129] W. Li, M. Ghogho, B. Chen, and C. Xiong. Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis. *IEEE Communications Letters*, 16(10):1628–1631, October 2012.

[130] G. Zheng, I. Krikidis, J. Li, A.P. Petropulu, and B. Ottersten. Improving physical layer secrecy using full-duplex jamming receivers. *IEEE Transactions on Signal Processing*, 61(20):4962–4974, October 2013.

[131] Y. Zhou, Z. Xiang, Y. Zhu, and Z. Xue. Application of full-duplex wireless technique into secure MIMO communication: Achievable secrecy rate based optimization. *IEEE Signal Processing Letters*, 21(7):804–808, July 2014.

[132] S. Parsaeefard and T. Le-Ngoc. Improving wireless secrecy rate via full-duplex relay-assisted protocols. *IEEE Transactions on Information Forensics and Security*, 10(10):2095–2107, October 2015.

[133] A.M. Ibrahim, T. ElBatt, and A. El-Keyi. Coverage probability analysis for wireless networks using repulsive point processes. *IEEE 24th International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)*, pages 1002–1007, September 2013.

[134] A. Leon-Garcia. *Probability, statistics, and random processes for electrical engineering*. Pearson/Prentice Hall, 2008.