JACOBS
UNIVERSITY

# Physical Layer Wireless Security in Random Networks

BY

**Satyanarayana Vuppala**

A Thesis submitted in partial fulfillment
of the requirements for the degree of

**Doctor of Philosophy**
**in Electrical Engineering**

Approved Dissertation Committee

Prof. Dr. Eng. Giuseppe Abreu, Jacobs University Bremen

Prof. Dr.-Ing. Werner Henkel, Jacobs University Bremen

Prof. Dr. Tharmalingam Ratnarajah, University of Edinburgh

Date of Defense: October 30, 2014

Engineering and Science

# Acknowledgments

I have been extremely fortunate to work under the supervision of Prof. Giuseppe Abreu. I would like to express my gratitude and heartfelt thanks to my supervisor, for his excellent supervision and support in this research. He is a great motivator, dedicated instructor, and above all a helpful friend. His constructive comments were invaluable for the completion of this thesis. His encouragement has been an inspiration to me. I would also like to express my sincere thanks to my co-supervisor Prof. Werner Henkel for his continuous guidance.

I am indebted to my co-supervisor Prof. Tharmalingam Ratnarajah who provided me with an opportunity to work in his group at University of Edinburgh.

In short, without my supervisors generous guidance and encouragement, it would have been difficult to achieve the goals and objectives of this research. The benefit of their guidance will not be limited to this research; I will also benefit from their knowledge, advice and wisdom in my future endeavors.

My thanks also extend to my colleagues and friends, who provided such a friendly environment both inside and outside the office. It has been an enjoyable experience interacting with these wonderful and talented people. Their advice and friendship have helped me to enjoy and learn a great deal from my PhD experience.

My short stay in Edinburgh was a tremendously rewarding experience, and Weigang, Sudip, Kishore deserves most of the praise for making it a success.

A big thank you out to my family - to Mom and Dad, to Brother (Srikanth), to all of my extended family. Especially, to my wife - Harika, thanks for your encouragement and inspirations.

The undertaking and completion of the Ph.D. program has proved to be a journey of discovery, filled with challenges and efforts, both personal and professional. Therefore, I am full of gratitude to those, who have provided me with inspiration, moral support, and technical direction.

# Abstract

A continuing trend of miniaturization and a growing demand for information are two major responsible drivers of new communication systems, which therefore increasingly rely on embedded technology, as illustrated by the Internet of Things and Cyber-Physical Systems. The embedded nature of future wireless networks implies not only power-limitation of devices, but also a likelihood that a greater share of traffic will include highly sensitive and personal information, which together call for new wireless security mechanisms that do not rely on the overhead-heavy and coordination-intense cryptographic protocols of today. Physical layer security is an upcoming research area that makes use of properties of the physical layer and seeks the possibility of achieving perfect secrecy in the wireless channel.

In this thesis, we study the impact of topology and interference onto the physical layer wireless security of random networks. In particular, we derive closed-form expressions for the secrecy rate distribution, average secrecy rate, secrecy outage probability, secrecy transmission capacity of Poisson Point Process (PPP) based random networks under various fading channels (Rayleigh, Nakagami-$m$, Shadowing), and colluding eavesdroppers with or without considering correlated channels. We also analyze the impact of interference on the secrecy metrics of corresponding random networks. Specifically, we study the aggregation of interference in random networks and its impact on secrecy, by utilizing results of PPP.

At the end, we perform an analysis of the secrecy outage of random networks under the Matérn Hard-core Point Process model, with the objective of shedding light on the security limitations/capabilities inherently encountered in cellular systems.

# Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

## 1.1 Background and Motivation

As the variety and the number of users of the wireless media grows, wireless security is becoming crucial in communication systems, leading the research community to investigate information theoretic approaches to achieve secrecy in the wireless channel.

One approach to meet current requirements is physical-layer information-theoretical security [1–5], which aims at eliminating the need of cryptography altogether. The foundations of information-theoretic wireless security were laid by Ozarow and Wyner [6], who coined the term "*wire-tap*" channel in reference to a communication channel in which an intruder (hereafter eavesdropper) shares with the receiver full information on the encoding and randomization procedures introduced by the transmitter. In that work, the *secrecy capacity* region of a discrete memoryless channel was characterized.

Also considering a discrete memoryless channel, Csiszár and Kröner arrived independently at a result to the same effect, by establishing that a broadcasting source can simultaneously send secret information to a user [7], which has became known as the broadcast channel with confidentiality (BCC). This notion of secrecy capacity was subsequently generalized to the additive white Gaussian noise (AWGN) channel by Cheong and Hellman [8], who furthermore showed that the maximum rate achievable in the wire-tap channel is in fact the difference between the capacities of the direct and the tap channels, respectively.

These seminal works established the notion that any wireless channel has an intrinsic **secrecy capacity**, which is fundamentally determined by how the power of the signal at a legitimate destination compares against that at an eavesdropper. For two decades the area of information-thoretic security remained active only in a small circle within the information and communication theory communities. Recently, however, Cheong and Hellman's result from the AWGN channel was generalized to fading channels in two independent works [9,10], and simultaneously, Csiszár and Kröner's BCC result [7] was also generalized to fading channels by Liang *et al.* [11].

Obviously, early works in the area such as those aforementioned are marked by significant abstraction from practical applicability, with various factors of relevance ignored for the sake of simplicity, to include: *a*) the fact that wireless channels are often *subjected to fading*; *b*) the fact that communicating devices compose *networks* often of *unknown topology* (randomly distributed nodes); and *c*) the possibility that intruders *cooperate* in order to eavesdrop on legitimate nodes' messages; *d*) *interference* exists in between devices in wireless networks.

A few decades later, the increasing prospect of putting information theoretical secrecy concepts to actual use has motivated the community to deepen its understanding of the inherent secrecy capabilities of wireless systems by taking into account more realistic conditions of the wireless medium. Addressing point *a*, for instance, the secrecy capacity of wireless fading channels was investigated in [10, 11], with expressions for the outage probability and average secrecy capacity of quasi-static fading channels also derived in [9].

Considering point *b*, and specifically when studying wireless secrecy in random networks using stochastic-geometric tools [12], the notion of *secrecy graphs* has emerged [13,14].

Beyond the obvious implications on the likelihood of legitimate and eavesdropping signal-to-noise ratios (SNRs), an important distinction between secrecy graphs and the "conventional" point-to-point wiretap channel is that distributions and densities of nodes (both legitimate and eavesdropping) play a major role not only on how much secrecy rate is achievable, but also on how to measure it. Indeed, a debate on how to assess the achievable communication rates in random networks had been initiated a decade earlier by Gupta and Kumar [15], producing various results ranging from the capacity of single channels [16] within the network, to their scaling laws [17], to network-wide metrics such as the *transmission capacity* [18].

Work on the secrecy rates of random networks is thus naturally following on the footsteps of that earlier discussion. For instance, the secrecy rate of unicast sessions in the presence of multiple eavesdroppers was studied in [19, 20], the scaling laws of secrecy rates were studied in [21–23] and the *secrecy transmission capacity* of random networks for given connection and secrecy outage were studied in [24].

To draw another parallel with the literature on random networks with reference to the point *c*, since it has been well demonstrated that cooperation is fundamental to increase the capacity and reduce the outage of communication systems subjected to the fading and unknown topologies [25–28], it can be said that ignoring cooperation amongst eavesdroppers (*i.e.*, collusion) when addressing the question of achievable secrecy outage and average secrecy capacity of random networks is somewhat contradictory to Wyner's original notion of "wire tapping". In other words, if cooperation is a part of the communication system used by legitimate nodes, it must be assumed that the same strategy will be exploited by intruders as well.

Literature on the impact of eavesdroppers' collusion in random networks is not vast, but the issue has not entirely escaped the attention of the community. For instance, the secrecy capacity of a legitimate link in the presence of colluding eavesdroppers in AWGN was studied in [29], and the MIMO secrecy non-outage in Rayleigh fading and eavesdroppers' collusion was studied in [30]. More recently, the scaling laws on secrecy capacity in large-scale wireless networks by considering eavesdroppers' collusion were characterized in [23, 31].

With reference to point *d*, besides topology, interference is another key parameter in characterising the performance of a random network. To some extent interference is related to the network topology [32], in the sense that modifications of the latter lead to variations in the former. In light of the need to modernize topological models – as already discussed – such relationship in itself again speaks in favor of paying more attention to the impact of interference onto the secrecy of random networks.

In this thesis, we investigate various parameters of interest such as the node degree of secrecy graphs, the secrecy outage probability, the unicast secrecy capacity, and the secrecy transmission capacity of random networks of various topological characteristics, employing emerging stochastic geometric models, as well as alternative techniques beyond stochastic geometry itself. Furthermore, we investigate the impact of interference, considering the case of interference aggregation.

## 1.2 Thesis Overview and Contributions

In this section, we briefly describe the contributions of the thesis.

**Chapter 3**

In Chapter 3, we consider the single antenna systems of random networks, as modeled by $\mathcal{S}$-Graphs. We conducted a detailed analysis of the probability of non-zero secrecy capacity of a unicast channel under Nakagami-$m$ block fading with a single eavesdropper in its vicinity.

**The contributions of this chapter are:**

- Obtaining the expression for probability of non-zero secrecy capacity of unicast channel under AWGN channel.
- Deriving the expression of probability of non-zero secrecy capacity of unicast channel in presence of single eavesdropper under Nakagami-$m$ fading channel.
- Deriving a new compact expression for connection outage probability under fading channel.

**Chapter 4**

In Chapter 4, we investigate the secrecy outage probability of unicast channels in random networks exposed to unknown numbers of randomly located eavesdroppers, obtaining original expressions which include uncertainty in terms of the location of legitimate nodes relative to eavesdroppers, the number of eavesdroppers, and fading.

**The contributions of this chapter are:**

- Characterizing the best path loss distribution and the best path gain distribution of eavesdroppers.
- Obtaining best path gain distribution of eavesdroppers and consequently we compute probability of secrecy outage of unicast channels in presence of multiple eavesdroppers under Nakagami-$m$ fading channel.

### Chapter 5

Chapter 5 investigates the secrecy outage of random networks under Nakagami-$m$ fading and mutually correlated legitimate and eavesdropping channels. We derive an integral formula for the secrecy outage probability incorporating various transmission factors including node density, correlation coefficient and fading parameter. This chapter also contains closed-form asymptotic expressions of the secrecy rate (both distribution and average), the secrecy outage, and the secrecy transmission capacity of random networks exposed to randomly located colluding eavesdroppers.

**The contributions of this chapter are:**

- Obtaining the expression for secrecy outage probability of unicast channel under mutually correlated fading channels.
- Approximate the aggregate path gain distribution of colluding eavesdroppers.
- Computing closed form expressions for secrecy rate and transmission capacity of a random network.

### Chapter 6

Chapter 6 examines the secrecy outage of unicast links in the presence of interference from other users and model the interference power with suitable approximation techniques. Precisely, we perform a thorough analysis of the secrecy outage under the impact of Nakagami-$m$ fading and Shadowing.

**The contributions of this chapter are:**

- Approximate aggregate interference with Gamma and Log-Normal random variables.
- Deriving the secrecy outage probability under Nakagami fading channel and Log-Normal fading channels.

### Chapter 7

Chapter considers the case of multiple antenna systems, perform an analysis of the secrecy outage of random networks under Nakagami-m fading with multiple transmit

antennas. Specifically, using a network model that accounts for uncertainties both in node locations (distances) and channel coefficients (fading), we derive the distribution of the best path gain of eavesdroppers using Probability Generating Functional property of PPP. Using this result, the secrecy outage probability and the conditional secrecy outage probability of random networks with multiple eavesdroppers are obtained.

**The contributions of this chapter are:**

- Deriving the distribution of the best path gain of eavesdroppers.
- Deriving the secrecy outage probability under Nakagami fading channel with basic factors such as the density of eavesdropping nodes, the number of transmit antennas and the fading figure.

### Chapter 8

Chapter 8 investigates the secrecy outage probability of downlink cellular network, employing emerging stochastic geometric model Matern Hard-Core Point Process Model (MHCPP).

**The contributions of this chapter are:**

- Model the downlink cellular network with MHCPP.
- Deriving the secrecy outage probability under nearest BS and optimal BS serving scenerios.

# Chapter 2

# State of the Art

**Summary:**

*This chapter provides a brief overview of wireless security techniques and need for physical layer security in current context of networks. We first introduce the notion of secrecy capacity of a simple wiretap channel, and then extend our discussion to fading channels and interference channels. This chapter does not contain new results, and it is intended to give some brief information necessary for the understanding the rest of the thesis.*

## 2.1 Need for Security in Wireless Networks

The open access nature of wireless media makes communication inherently prone to security threats. Due to huge demand of memory and energy, the cryptographic algorithms cannot be employed to wireless network which is typically conformed of many small nodes that are battery and hardware limited. Therefore, wireless networks are vulnerable to various forms of attacks specific to the requirement of exchanging confidential information such as available channel frequencies, location, identity and maximum transmit power, between the sensor nodes. The design of a security scheme to assure the safety of the network during the nodes deployment and during the lifespan of the network is essential and must take into account several network characteristics. The messaging interface between the sensor nodes is designed so as to combat all security breaches and mitigate malicious perceiving/manipulation in the communication interface. To this end, any security scheme must possess the following key characteristics:

- Authentication should be enforced between the nodes.
- Secure exchanges between nodes should be established.

In the sequel, possible security threats, corresponding security measures and security implementations inherent to wireless networks are described.

### 2.1.1 Security Threats

Mainly, security threats in the wireless networks context can be classified into two categories: threats at the communication interface, and threats against devices. The possible threats categorized in that fashion are summarized in the Table 2.1, and described in more detail below.

The communication links can be eavesdropped by malicious users, regardless of its wired or wireless nature. For instance, an attacker may steal the confidentiality of data transmitted or could disturb the integrity by modifying the data during message transfer. The location and identity information of the device could be tracked by the attacker who may use this information for future attacks.

All the possible attacks directed at the communication interface and on the device can further be sub-divided into following categories.

Table 2.1: Possible security threats

| | Type | Description |
|---|---|---|
| **On Communication Interface** | Interference | Unintentional disruption of radio signal by another transmitter. |
| | Jamming | Intentional disruption of the radio signal by a powerful transmitter of the attacker. |
| | Wormhole | An attacker could create a bridge between the devices. |
| | Disclosure | An attacker reveals sensitive information of devices. |
| | Flooding | An attacker opens a large number of half opened TCP connections. |
| | Impersonation | MAC or IP address of an existing legitimate device is falsely used by an attacker . |
| | Repudiation | An attacker may mislead the devices by transmitting invalid information. |
| **On Devices** | Tampering | Physical devices could be accessed by an attacker. |
| | Backdoors | An installed or modified software/hardware entity to bypass normal authentication. |
| | Masquerade | An attacker pretends to be valid legitimate device. |

- Man-in-Middle (MitM) Attack: An attacker node, hereafter MitM node [33], is inserted in between two nodes. This MitM node acts as a bridge between the source and legitimate device, and can transparently transmit, receive, view, and modify the traffic between them consequently could launch interference, jamming, wormhole and repudiation attacks.

- Denial of Service (DoS) Attack: The attacker, which is located between communicating peers, may indicate no channel availability at a location resulting in denial of service to a legitimate device [33]. Flooding and Impersonation attacks are come under this attack category.

- Tampering Attack: The device may be found in vulnerable locations, so that the attacker may have physical access to the node in invasive manner, *e.g.*, access to the node hardware, or non-invasive manner, *e.g.*, electromagnetic listening. This is known as physical tampering attack [34].

- Masquerade Attack: An attacker may successfully masquerade any node and provide malicious responses to a legitimate device resulting in legitimate-device-generated interference to users of the spectrum. This attack is known as masquerade attack otherwise known as spoofing attack [34].

### 2.1.2 Essentials of Security Measure

To mitigate the above threats, any communication system will incorporate a number of high level security countermeasures which are summarized in Table 2.2 and described further in the sequel.

**Mutual Authentication:** To protect from attacks such as MiTM and DoS, a proper mutual authentication between the legitimate devices should be performed using certificates or pre-shared keys.

**Data Protection:** All the communication should ensure maintained integrity, confidentially, and replay protection from unauthorized devices.

**Trusted Environment (TrE):** The TrE shall be a logical entity which provides a trustworthy environment for the execution of sensitive functions and the storage of sensitive data.

In summary, the following security features have been adopted in any current network framework to achieve TrE secure communications between the legitimate devices. The identity of the legitimate devices are authenticated by means of either IPSec's IKE mechanism or TLS Handshake protocol. The connection between the source and the legitimate is kept private with the help of IPSec or TLS. The messages transmitted during connection between the source and the legitimate are confidentiality protected by the above security implementations.

Table 2.2: Security essentials and its implementations

| Essentials | Implementations |
|---|---|
| Confidentiality | Cryptographic techniques such as Advanced Encryption Standards are provided to achieve this. |
| Integrity | Secure hash functions, message authentication codes establish data integrity. |
| Accessibility | By incorporating either TLS [35] or IPSec [36], legitimate is made available all the time to the devices. |
| Authentication | TLS Handshake or Internet Key Exchange ensures mutual authentication of white space devices. |
| Non-repudiation | Public key cryptography techniques such as digital signatures fulfills this requirement. |
| Key Exchange | Secure key exchange between devices is provided by the Diffie-Hellman algorithm [37]. |

However, the above mentioned counter measures and security techniques use cryptography which require high end device capabilities and therefore mayn't suit for wireless networks. One approach to alleviate the need of cryptography is physical-layer information-theoretical security.

## 2.2 Need for Physical Layer Security

In one hand, the application layer security protocols involve often *nonce* and limited response timing in order to avoid known attacks (as replay attack for example). The key deployment is another open issue as symmetric cryptography needs the key sharing and asymmetric cryptography remains costly for small devices or raises privacy problems. Actually, several works focus on the generation of non-deterministic random number inside a small device with limited resources. This could enable nodes to generate by itself true *nonce* for cryptographic protocols or its own secret key which must not be revealed to other entities.

On the other hand, physical layer prepares the sequence of bits containing information before its transmission on a wireless link. It can realize data encoding, constellation mapping, scrambling, modulation, CRC computation, $\cdots$ etc according to a given wireless standard specifications. An important characteristic of the wireless link is that all the messages are broadcasted. This is not convenient to assure the security and the confidentiality of the communications! Adding security features to the physical layer is then essential in order to guarantee security principles: Availability, Confidentiality, Integrity, Authentication and Non-repudiation.

## 2.3 Security at Physical Layer

Physical layer security provides a set of mechanisms that makes use of the properties of the physical layer to make eavesdropping harder. It aims at exploiting the randomness which is inherent in noisy channels to provide an additional level of protection at the physical layer. It is also an upcoming research area that seeks the possibility of achieving perfect secrecy in the wireless communications while the presence of eavesdroppers and leaking minimum possible information to them. The interesting concept is to make use of physical layer characteristics to improve the security and reliability. Information theoretic security is a notion of measuring secrecy in communications system which was based on Shannon's perfect secrecy. The foundations of information-theoretic security was laid by the work of Ozarow and Wyner [6], in which the term wire-tap channel was first coined in reference to the communication problem where an eavesdropper shares with the receiver full information on the encoding and randomization procedures introduced by the transmitter. After these breakthrough results, security started playing a role at physical layer along with traditional error correction coding mechanisms.

## 2.4 Stochastic Geometry and Secrecy

Mostly, the propagation effects of the received signals challenge the wireless networks. Several mathematical techniques have been proposed in literature in order to model these effects and to provide communication-theoretic results based on the networks geometrical configuration. The nodes of the wireless network often treated as random, and modelled with stochastic geometry and the theory of random geometric graphs. Stochastic geometry [38] is a one of applied probability technique, related to the theory of point processes, which allows the study of random phenomena on the plane or

in higher dimensions. In addition to point process theory, percolation theory, and probabilistic combinatorics have been considered for analyzing the connectivity, the capacity, the outage probability, interference and other fundamental limits of wireless networks.

In general, the network is modelled using point process (PP) which captures the network properties. The spatial point processes we considered lie in the Euclidean plane $\mathbb{R}^d$. Informally, a point process is a countable random collection of points in $\mathbb{R}^d$. If it is simple (there is only one point at each location a.s.), it can be represented as a countable random set $\phi = \{x_1, x_2, \cdots\}$, where $x_i \in \mathbb{R}^d$ are the points. Usually, it is characterized by a random counting measure $N \in \mathcal{N}$, where $\mathcal{N}$ is the set of counting measures on $\mathbb{R}^2$. $N(B)$ is a random variable that denotes the number of points in set $B \in \mathbb{R}^d$ for a point process $\Phi$. A concrete realization of $\Phi$ is denoted as $\psi$. Hence $\psi(B)$ is a deterministic counting measure that denotes the number of points in B.

We start with the definitions of most popular PPs used in wireless communication systems, then we analyse the suitability of the PP with respect to network models.

**Poisson point process (PPP)**:
A PP $\Phi = \{x_i; i = 1, 2, 3, ...\} \in \mathbb{R}^d$ is a PPP if and only if the number of points inside any compact set $B \in \mathbb{R}^d$ is a Poisson random variable, and the numbers of points in disjoint sets are independent.

**Hard core point process (HCPP)**:
An HCPP is a repulsive point process where no two points of the process coexist with a separating distance less than a predefined hard core parameter $d$. A PP $\Phi = \{x_i; i = 1, 2, 3, ...\} \in \mathbb{R}^d$ is an HCPP if and only if $||x_i - x_j|| \geq d, \forall x_i, x_j \in \Phi, i \neq j$, where $d \geq 0$ is a predefined hard core parameter.

**Poisson cluster process (PCP)**:
The PCP models the random patterns produced by random clusters. The Poisson cluster process is constructed from a parent PPP $\Phi = \{x_i; i = 1, 2, 3, ...\}$ by replacing each point $x_i \in \Phi$ with a cluster of points $M_i, \forall x_i \in \Phi$, where the points in $M_i$ are independently and identically distributed in the spatial domain.

### 2.4.1 Secrecy and Network Topology

#### Problem Description

Shannon has defined the capacity of a channel as the maximum rate with which information can be conveyed without errors over the channel. If a device transmits with power $P$ to another at a distance $r$, subjected to a path loss exponent $\alpha$, noise and interference with powers respectively given by $N_0$ and $P_{\mathcal{I}}$, and through a channel with gain $h$, the Shannon capacity becomes

$$\mathcal{C} = \log_2\left(1+\frac{|h|^2 P}{r^{\alpha}(N_0+P_{\mathcal{I}})}\right) = \log_2(1+\text{SINR})\,, \tag{2.1}$$

where, we implicitly defined the quantity $\text{SINR} \triangleq \dfrac{|h|^2 P}{r^{\alpha}(N_0+P_{\mathcal{I}})}$.

Similarly, if the communication occurs in the presence of a single eavesdropper, it has been shown [8, 9] that the rate with which information can be conveyed without errors and **secretly** between the "legitimate" pair – *i.e.* the **secrecy capacity** associated with the pair – is given by

$$\mathcal{C}_s = \max\{\log_2(1+\text{SINR}_{\ell}) - \log_2(1+\text{SINR}_{\text{e}}), 0\}\,, \tag{2.2}$$

where $\text{SINR}_{\ell}$ and $\text{SINR}_{\text{e}}$ are quantities similar to those implicitly defined in equation (2.1), but with $h$, $r$ and $P_{\mathcal{I}}$ replaced by corresponding values experienced by the legitimate node and the eavesdropper, respectively.

Another important secrecy metric is the **secrecy outage probability**, which is defined as

$$\mathcal{P}_{\text{out}}(R_s) \triangleq \Pr\{\mathcal{C}_s \leq R_s\} = 1 - \Pr\{\mathcal{C}_s > R_s\}, \tag{2.3}$$

where $R_s$ is a given secrecy rate threshold.

Yet another metric, more specific to the context of random networks with uniformly distributed nodes, is the **secrecy transmission capacity**, defined as

$$\tau \triangleq \bar{R}_s(1-\mathcal{P}_{co})\lambda_{\ell}, \tag{2.4}$$

where $\bar{R}_s$ is an **average** secrecy rate, $\lambda_{\ell}$ is the density of the legitimate nodes, and $\mathcal{P}_{co}$ is the connection outage probability, given by $\mathcal{P}_{co}(R) \triangleq \Pr\{\mathcal{C} \leq R\}$.

Embedded in all the aforementioned expressions is the distance between legitimate

nodes, and between those and eavesdroppers. The key role played by the relative location of devices, together with the lack of exact knowledge on the latter, lead to the widespread utilisation of stochastic-geometric approaches when analysing secrecy in random networks.

**Discussion and Current Literature**

- **On the Generalization of Topological Models within PPP:**

  As described earlier, fading is one of the various sources of uncertainty faced in wireless channel. Another relevant source of uncertainty that emerges when breaking beyond point-to-point communications towards multipoint networks, is the stochastic nature of distances between communicating pairs. Therefore, a further step in better understanding information-theoretical wireless security is to study its properties in the context or random networks [39, Ch. 2], [12,13,40], which gives rise to the notion of *secrecy graphs* [41].

  Moving in that direction, Zhou *et al.* [24] analyzed the secrecy outage probability similarly to [9], but in the context of random networks modeled as PPP and subjected to Rayleigh fading. More recently, the effect of interference on the secrecy capacity of random networks with fading and cognitivity was studied by Shu *et al.* [42], and the secrecy capacity scaling law in random networks subjected to fading was also studied by Koyluoglu *et al.* [43].

  In this direction, take for instance the work in [24], where the Probability Generating Functional (PGFL) of PPPs is utilised to obtain simple and closed-form upper and lower bounds for the secrecy outage probability in random networks with uniform random topologies. Clearly such results do not generalise to networks where a minimum distance between any pair of nodes must be maintained – as is the case of WiFi and Cellular Networks [44, 45] – which are known to require HCPPs models instead [44,45]. In fact, already within the discussion in [24], the difficulty to handle the case when a secrecy guard zone exists was encountered, and somewhat avoided by considering a highly artificial assumption that all legitimate pairs in the network have the same distance. In spite of the limitation of the model, the same procedure was again followed in [46] when studying the secrecy rates of cellular networks.

  Most of current works focus on systems with single antenna and mainly study prorogation without fading or with Rayleigh fading [24]. Nakagami-$m$ fading

matches some empirical fading conditions which are more or less severe than that of Rayleigh fading and has the advantage of including Rayleigh fading as a special case [47]. In this thesis, we contribute to this area with an analysis of the secrecy outage experienced between a pair of legitimate nodes in random networks subjected to Nakagami fading and exposed to an unknown number of randomly located eavesdroppers. We derive the outage probability distribution under such fairly general conditions, characterizing the impact of individual environmental factors (*e.g.* fading, noise, and relative node-densities) onto the secrecy outage probability of unicast links in the network [41]. To put the work into context our results can be seen, for instance, as a generalization of [40], where secrecy outage was studied in a random network but subjected only to AWGN; as well as a more accurate alternative to [24], where the secrecy outage in a Poisson network subjected to fading was studied, but under the rather strong assumption that all pairs of communicating legitimate nodes are apart by the *same* distance, while in our analysis the network is truly random, such that the distances between a source and a legitimate node, as well as between a source and eavesdropping nodes, are random and unknown.

- **On the Generalization of Topological Models beyond PPP:**

  The fact that PPPs are not sufficiently accurate to capture the structure of various random networks of interest is a modern topic in wireless communications both within and without the particular question of secrecy. To cite a few recent works that shed some light on this problem, Nguyen *et al.* were one of the first to employ HCPP to model WiFi network, studying a number of parameters of relevance such as throughput and coverage [44]. In [48] the approach in [44] was revisited and improved by replacing average quantities for corresponding distributions, including an approximate distribution of the distance between a source and the nearest node, under an HCPP, which is of relevance to the secrecy problem considered in this proposal.

  In [49] the HCPP model was combined with fading by replacing the purely geometric channel model (*i.e.*, dependent only on distances) for one in which the statistics of the received power is considered instead, similarly to what had been done for uniformly distributed random networks [12].

  Following this trend, in this thesis we will look beyond the PPP model and study the secrecy of random networks under MHCPP. We should also point out that to

the best of our knowledge, the analysis of secrecy of random networks outside the PPP model have not yet been attempted in currently literature. In that regard, therefore, this thesis bridge a gap between the progress made on the study of random networks outside and inside the secrecy question.

- **On the Flexibilization of Analytical Tools beyond Stochastic Geometry:**

  Since the seminal work by Gilbert on the application of point processes to model random networks, Stochastic Geometry has become the tool of choice when analysing wireless communication systems from a network perspective [38]. Despite the elegance and the wide range of results achievable with this tool, many of which were discussed above, a wave of self-criticism has started to permeate the communication theory community, due to lack of the accuracy of the underlying assumptions typically adopted.

  Hand in hand with the relationship between point processes and networks, however, is an equally strong relationship between graphs and networks. Obviously strong connections between point processes and graphs also exist, but the two models are not always applicable with equivalency.

  To exemplify, consider the recently emerging notion of security via deniability [50], in which messages are continuously interleaved with noisy signals, such that the level of secrecy in a communication link becomes dependent on the ratio between actual messages and intentionally generated noise. In such systems, information theoretical security is achieved not on the basis of SINR, but on the basis of the likelihood, in absence of a prior, that a codeword can be extracted amidst noise by an eavesdropper, such that **distances between eavesdropper and legitimate nodes play no significantly role**; instead, in this case the **number of eavesdroppers** is the key parameter. If ported to a network scale, the problem is therefore more strongly connected to unweighted graphs than to point processes.

In other occasions, purely statistical tools can also be invoked which do not have a strong relationship with point processes either. One example is order statistics, which for instance was effectively employed in [51] to smooth over the implication of specific policies and network conditions to characterise the distribution of the number of hops required by routing algorithms to reach destinations in random networks. As a result of this approach, hop count distributions have been obtained, which can be used to model networks of various types, eliminating the need for point process to be directly invoked. Finally, in [52] it was show that

random walk models can also be used to describe a number of spatially distributed processes including random networks.

In this thesis, we use stochastic geometry but also incorporate some of the aforementioned ideas, including order statistics and graph theory to flexibilize the analysis of secrecy in random networks.

### 2.4.2 Secrecy and Interference

#### Problem Description

Interference is another key parameter in characterizing the network-wide secrecy throughput of large scale networks. If undesigned, interference is an aggregated sum of undesired signals due to concurrent transmissions, that may cause severe throughput degradation. Such an interference can be modelled as a stochastic process, with the random location of interferers described by point process $\mathcal{I}$. Then a generalized model of aggregate interference can be defined as

$$\mathcal{I} = \sum_{i \in \mathcal{I}} X_i \cdot r_i^{-\alpha}, \tag{2.5}$$

where $r_i$ is the distance between the receiver and the $i$-th interferer, $\alpha$ is a propagation loss coefficient and $X_i \triangleq |h_i|^2$ models the channel power.

Stochastic geometry is one of the tools that can be used to characterize the statistical behaviour of aggregate interference. A convenient way to do so is via the Laplace Transform (LT) of $\mathcal{I}$, or its characteristic function (CF), namely

$$\mathcal{L}_{\mathcal{I}}(w;\alpha) = \mathbb{E}[e^{-w\mathcal{I}}], \tag{2.6}$$

where the expectation is take over the distributions of $X_i$ and $r_i$, and the parameters of those distributions are omitted from the notation for the sake of simplicity and generality.

In the case of the PPP model, $\mathcal{L}_{\mathcal{I}}(w;\alpha)$ can then be relatively easily evaluated via Campbell's theorem, which relying on the uniformity of the PPP yields

$$\mathcal{L}_{\mathcal{I}}(w;\alpha) = \exp\left(-2\pi\lambda \int_X \int_0^\infty [1-\exp(wxr^{-\alpha})] f_X(x) f(r) r \, \mathrm{d}r \mathrm{d}x\right). \tag{2.7}$$

As argued earlier, in the case of real networks such as WiFi and cellular networks, however, the PPP model is not suitable and must instead be replaced by HCPP, SP or other models [44, 45, 53–55]. Unfortunately, in such cases Campbel's Theorem does not apply, such that the characterization of aggregate interference in general topologies via the Laplace Functional and PGFL is a challenging problem.

**Discussion and Current Literature**

- **On the Aggregation of Interference in Random Networks:**

  To cite a few examples, in [56] the characteristic function of the aggregate interference in a AWGN channel (no fading) was derived, leading to infinite series expressions for the probability density function of interference. Some time later, the approach was revisited and the results generalized to the Rayleigh fading case [57]. At the core of the approach followed in [56] and [57] is the utilisation of Campbell's Theorem [58], which can be easily evaluated in the case of PPP-modeled networks subjected to AWGN or Rayleigh fading. In both these examples, therefore, closed-form expressions for the aggregate interference were obtained.

  Even when limiting themselves to PPP-modeled networks, the generalization of the latter results to other types of wireless channels, including alternative fading models and superposition with shadowing, however, proves a formidable problem. This is illustrated for instance by the work done in [59], [60] and [61], all of which considered the interference aggregation problem under various fading models, ultimately resorting to Log-normal, Truncated-stable and Gamma approximations for its aggregate interference distribution.

  The limitation of the Campbell-Theorem-based approach becomes more evident when considering non PPP-netoworks. One example of the latter can be found in [53], where the mean aggregate interference in CSMA networks was considered by attempting to transform the corresponding HCPP into non-homogeneous PPPs, which ultimately led to the conclusion that the approach is inaccurate. Another is given in [62], where the problem encountered in [53] is avoided by attempting to obtain the desired distribution directly, in the form of a series expansion of point process functionals.

  In this thesis, we continue the modern effort in this area and study the aggregation of interference in random networks and its impact on secrecy, both by utilizing results on point processes, and by applying more recently approaches.

# Chapter 3

# Single Antenna Systems in Unicast Channels: Single Eavesdropper

**Summary:**

*In this chapter, we offer a characterization of the impact of noise, path loss, density and fading onto the secrecy capacity achieved between a pair of legitimate nodes of a network in the possible presence of randomly located single eavesdropper. We obtained the expression of probability of non-zero secrecy capacity for the case of a single eavesdropper per neighborhood.*

## 3.1 Introduction

By incorporating more realistic conditions faced in wireless media, the earlier contributions on secrecy capacity substantially expand the potential reach of the information-theoretic secrecy concept for wireless communication systems. Indeed, the combination of these fundamental results on the secrecy capacity of wireless channels [8–11] with emerging stochastic-geometric models of wireless networks [39, Ch. 2], [12, 13] gave rise to the notion of *secrecy graphs* [41]. To mention a few works in this direction, distributions for the in- and out-degrees of a Poisson $\mathcal{S}$-graph and the corresponding implication of those distributions on the connectivity of random networks was studied in [14].

A similar work was also done in [22], where the authors have considered that the location of eavesdroppers was not entirely random, but known within an amount of uncertainty. Both of these contributions [14, 22] share with [40, 41, 63] a percolation-theoretical perspective in approaching the secure connectivity of nodes in a random network subject to eavesdroppers, what we shall hereafter refer to simply as $\mathcal{S}$*-connectivity*.

Such a "generic" model of $\mathcal{S}$-connectivity suffices to understand "macro" characteristics of $\mathcal{S}$-graphs, such as their girth and critical densities, but is insufficient to quantify the secrecy capacity of specific (possibly multi-hop) links over the $\mathcal{S}$-graph.

In this regard, the work in [29] offers a better approach in which the results of [14] are extended and applied to the study of the $\mathcal{S}$-connectivity of a source to a specific neighbor – that is, a *unicast* link – subject to path-loss and AWGN disturbance.

In addition to addressing unicast links, the analysis in [29] also considers the collusion of eavesdroppers, yielding again in that regard a more general characterization of $\mathcal{S}$-connectivity than that found in [14, 22, 41].

Unlike [41], however, the approach in [14, 29] is far less permitting of generalization to fading channels. To clarify, firstly, the result achieved in [14, App. B] is that the distribution of the out-degree – as opposed to the distribution of the probability of non-zero secrecy capacity – is invariant to fading. Secondly, the latter result is supported by arguments on the homogenization and mapping of heterogeneous Poisson processes.

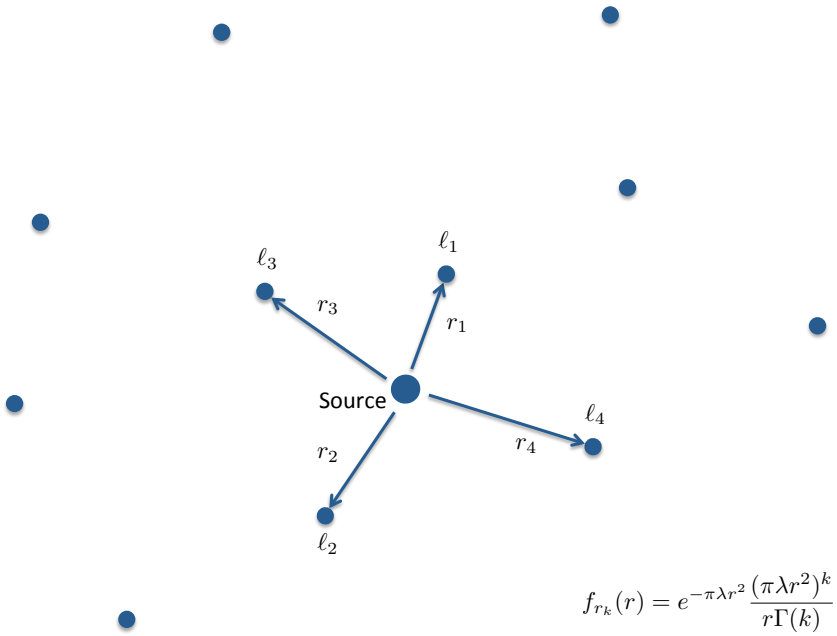



Figure 3.1: Random network

In other words, both the result and the supporting argument given in [29] are adequate if one is concerned with the *number* of nodes around the source that are safe from eavesdropping, number which can be modeled by Poisson statistics. Instead, when one is concerned with the probability that a unicast link subject to different channel conditions retains a non-zero secrecy capacity, a more detailed analysis is required.

Such an analysis, specifically, the study of the impact of individual environmental factors (*e.g.* fading, noise, and relative node-densities) onto unicast links of an $\mathcal{S}$-graph, is the contribution of this chapter. Specifically, focusing on a link metric (unicast over a single hop), we offer a characterization of the impact of noise, path loss, density, and fading onto the secrecy capacity achieved between a pair of legitimate nodes of a network in the presence of single eavesdropper.

**System Model**

First we consider a random network (Fig. 3.1) in a Euclidean space of dimension $d$, modeled by a stationary PPP [64, 65] of intensity $\lambda$ in $\mathbb{R}^d$. Let us select an arbitrary reference point (Source) defining the origin of the space, and order the remaining points $k \in \mathbb{N}$ according to their Euclidean distances $r_k$ to this reference. This property is implicitly used henceforth to support the assumption that each node in the network can be *unequivocally identified* by its distance to the origin (source).

Let the aforementioned model be applied to two overlaid networks of *legitimate* nodes and *eavesdroppers*, respectively, with corresponding densities $\lambda_\ell$ and $\lambda_e$ as shown in Fig. 3.2. Consider that a source located at the origin (without lack of generality) wishes to unicast to the legitimate node, located at the unknown distance $r_k$, in the presence of an eavesdropper located at the unknown distance $r_e$, subject to AWGN[1] and path loss governed by the exponent $\alpha$.

Then, the *secrecy capacity* of the unicast channel under AWGN is [8]

$$\mathcal{C}_{s:k} = \log_2\left(1+\frac{P}{r_k^\alpha N_0}\right) - \log_2\left(1+\frac{P}{r_e^\alpha N_0}\right), \tag{3.1}$$

where, $P$ and $N_0$ are the power densities of the transmit signal and noise, respectively.

[1]For simplicity, we commit a slight abuse of notation by using the subscript "e" to denote the eavesdropper, since under AWGN conditions, it is sufficient to consider the *nearest* eavesdropper.

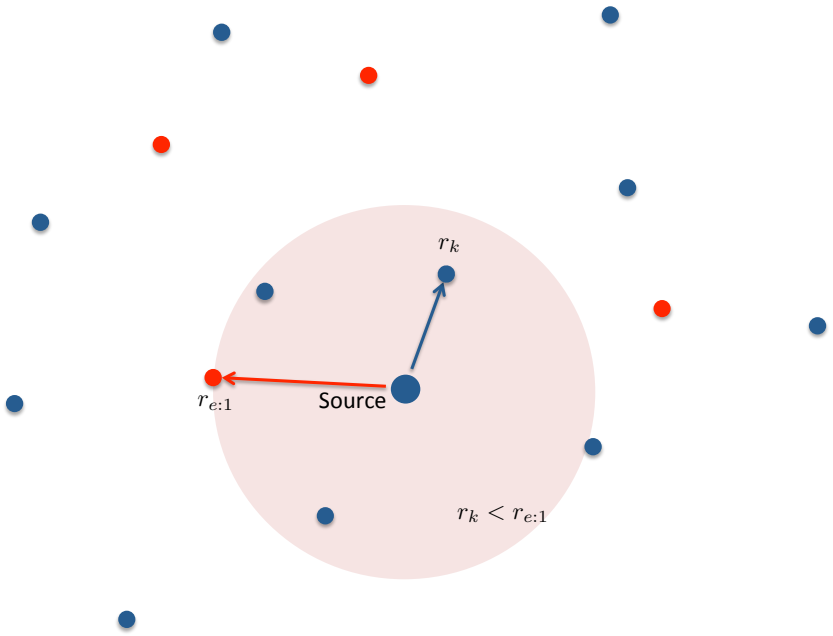



Figure 3.2: $\mathcal{S}$-Graph in AWGN.

## 3.2 AWGN Case

By treating $\mathcal{C}_{s:k}$ as a random variable and evaluating its cumulative density function (CDF), in the most significant case of planar networks with $\alpha = 2$, Pinto *et al.* have shown that the probability that the secrecy capacity in the unicast channel of an $\mathcal{S}$-graph in AWGN is given by [29]

$$\Pr\{\mathcal{C}_{s:k} > 0\} = p_{\text{AWGN}}(\varrho; k) = \left(\frac{\lambda_\ell}{\lambda_\ell + \lambda_e}\right)^k = \left(\frac{\varrho}{\varrho + 1}\right)^k, \tag{3.2}$$

where the parameter $\varrho$ is defined as

$$\varrho \triangleq \frac{\lambda_\ell}{\lambda_e}, \tag{3.3}$$

The proof of Eq. (3.2) offered in [29] is elegant and succinct, but unfortunately does not yield insight on how the result can be extended to account for fading. In the sequel, we offer a brief alternative direct (laborious) proof that is subsequently extended to study the unicast problem subject to fading. To this end, let us consider the path loss, which in the case of a network modeled as a PPP has distribution [12, 66]

$$p_{\xi_k}(x; k, \lambda) = e^{-\pi\lambda x}\frac{(\pi\lambda x)^k}{x\Gamma(k)}. \tag{3.4}$$

Notice that in the AWGN case the nearest eavesdropper is certain to experience the smallest path loss amongst non-legitimate nodes. From that fact, and from Eq. (3.1) it follows that the secrecy capacity of the channel between the source and the $k$-th node is non-zero if and only if (iff)

$$\Delta \triangleq \xi_k - \xi_e \leq 0, \tag{3.5}$$

where $\xi_k$ and $\xi_e$ are governed by $p_{\xi_k}(x; k, \lambda_\ell)$ and $p_{\xi_e}(x; 1, \lambda_e)$, respectively.

The distribution of the path loss difference $\Delta$ is given by

$$\begin{aligned} p_\Delta(x; k, \lambda_e, \lambda_\ell) &= \int_{-x}^{\infty} p_{\xi_e}(\tau; 1, \lambda_e) \cdot p_{\xi_k}(x+\tau; k, \lambda_\ell)\,\mathrm{d}\tau, \\ &\xrightarrow[\text{subst. eq. (3.4)}]{} \frac{(\pi\lambda_\ell)^k \pi\lambda_e}{\Gamma(k)e^{\pi\lambda_\ell x}} \int_{-x}^{\infty} e^{-\pi(\lambda_\ell+\lambda_e)\tau}\,(x+\tau)^{k-1}\,\mathrm{d}\tau, \\ &\xrightarrow[z \triangleq x+\tau]{} \frac{(\pi\lambda_\ell)^k(\pi\lambda_e)e^{\pi\lambda_e x}}{\Gamma(k)} \int_0^{\infty} e^{-\pi(\lambda_\ell+\lambda_e)z} z^{k-1}\,\mathrm{d}z. \end{aligned} \tag{3.6}$$

A closed-form solution to the last integral can be found in [67, pp. 336, Eq. (3.351.3)], from which we obtain

$$p_{\Delta}(x;k,\varrho,\lambda_e)=\left(\frac{\varrho}{\varrho+1}\right)^k\pi\lambda_e e^{\pi\lambda_e x}. \tag{3.7}$$

Finally, since the probability that $\Pr\{\mathcal{C}_{s:k}>0\}=\Pr\{\Delta\leq 0\}$, we conclude that

$$p_{\text{AWGN}}(\varrho;k)=\left(\frac{\varrho}{\varrho+1}\right)^k\pi\lambda_e\cdot\underbrace{\int_{-\infty}^{0}e^{\pi\lambda_e x}\,\mathrm{d}x}_{=1/\pi\lambda_e}=\left(\frac{\varrho}{\varrho+1}\right)^k. \tag{3.8}$$

However, the result in Eq. (3.8) is obtained for the case of $\alpha=2$. A generalised result for any $\alpha$ is need to be considered. To this point, let us consider the path loss $\xi_k=r_k^{\alpha}$, which has a probability density function (PDF) [12,66]

$$f_{\xi_k}(x)=\exp(-\sigma x^{\delta})\frac{\delta(\sigma x^{\delta})^k}{x\Gamma(k)}, \tag{3.9}$$

where $\sigma=\pi\lambda$ and $\delta=\frac{d}{\alpha}$.

The secrecy outage in the case of AWGN can be directly evaluated from Eq. (3.1). By denoting $\rho\triangleq P/N_0$, the outage probability associated with a secrecy rate $R_s$ at the $k$-th legitimate node, subject to AWGN[2], is given by

$$\begin{aligned}\mathcal{P}_{\text{out}}(R_s)&=\Pr\{\log_2(1+\tfrac{\rho}{\xi_k})-\log_2(1+\tfrac{\rho}{\xi_e})<R_s\},\\&\overset{(b)}{=}\int_0^{\infty}\int_{\beta(y)}^{\infty}f_{\xi_k}(x)f_{\xi_e}(y)\mathrm{d}x\,\mathrm{d}y,\\&\overset{(d)}{=}\frac{\delta\cdot\sigma_{\mathrm{e}}}{\Gamma(k)}\int_0^{\infty}\exp(-\sigma_{\mathrm{e}}y^{\delta})y^{\delta-1}\Gamma(k,\sigma_{\ell}\beta^{\delta}(y))\mathrm{d}y,\\&\overset{(c)}{=}1+\frac{1}{\Gamma(k)}\int_0^{\infty}\exp(-\sigma_{\mathrm{e}}y^{\delta})\Big[-(\sigma_{\ell}\beta^{\delta}(y))^{k-1}\exp(-\sigma_{\ell}\beta^{\delta}(y))\mathrm{d}(\sigma_{\ell}\beta^{\delta}(y))\Big],\\&\overset{(d)}{=}1-\frac{\sigma_{\ell}^k\delta}{\Gamma(k)}\int_0^{\frac{\rho}{2^{R_s}-1}}\exp\left[-\sigma_{\mathrm{e}}\left(\frac{2^{R_s}\rho z}{\rho-(2^{R_s}-1)z}\right)^{\delta}\right]\exp(-\sigma_{\ell}z^{\delta})z^{\delta k-1}\mathrm{d}z,\end{aligned} \tag{3.10}$$

where (b) follows from $\beta(t)=\frac{\rho}{2^R(1+\frac{\rho}{t})-1}$, (c) follows from [67, Eq. (3.3819)], and (d)

[2]Under AWGN, the strongest eavesdropper is obviously the *nearest*.

$$\mathcal{P}_{\text{out}}(R_s) = \tag{3.12}$$
$$1 - \frac{\delta 2^R \sigma_\ell \rho^{\delta+1}}{(2^R-1)^{\delta+1}\Gamma(k)} \sum_{n=0}^{\infty} \frac{(-\sigma_{\text{e}})^n}{n!} \Big[\Gamma(\delta n + k - \delta - 2)_1F_1(\delta+1, -\delta n - k + \delta + 3, \frac{2^R\rho}{2^R-1})$$
$$+ \frac{(\frac{2^R\rho}{2^R-1})^{\delta n+k-\delta-2}\Gamma(\delta n + k - 1)\Gamma(-\delta n - k + \delta + 2)_1F_1(\delta n + k - 1, \delta n + k - \delta - 1, \frac{2^R\rho}{2^R-1})}{\Gamma(\delta+1)}\Big]$$

follows from a change of variables. The closed form solution for the Eq. (3.10) is given in Eq. (3.12).

For $R_s = 0$, the calculation of secrecy outage is equivalent to calculating secrecy connectivity [14]. In this case, the secrecy outage over AWGN channel is given by

$$\mathcal{P}_{\text{out}}(0) = \int_0^{\infty}\int_{\frac{\rho y}{\rho}}^{\infty} f_{\xi_k}(x) f_{\xi_e}(y)\, \mathrm{d}x\, \mathrm{d}y = 1 - \left(\frac{\lambda_\ell}{\lambda_\ell + \lambda_{\text{e}}}\right)^k. \tag{3.11}$$

## 3.3 Nakagami Fading Case

The presence of fading affects the applicability of the result of Section 3.2 in two fundamental ways. First, the path losses to legitimate nodes and eavesdroppers are no longer dependent only on their distances to the source, but also on their fading gains. Specifically, if $|h|$ denotes the fading envelope to a point at distance $r$, then the corresponding path loss is $\xi = r^2/|h|^2$. Consequently, different distributions for the path losses $\xi_k$ and $\xi_e$ are required to compute $\Pr\{\mathcal{C}_{s:k} > 0\}$.

Second, the path loss difference $\Delta$ is no longer governed by the *nearest*, but by the *best* eavesdropper, that is, the eavesdropper with the lowest path loss. This requires separate consideration for the scenarios when a *single* or *multiple* eavesdroppers are present in the vicinity of the source as depicted in figures 3.3 and 3.4, respectively. Both figures explain the amount of uncertainty involved while determining the secrecy capacity regions. In this chapter, we consider the single eavesdropper case.

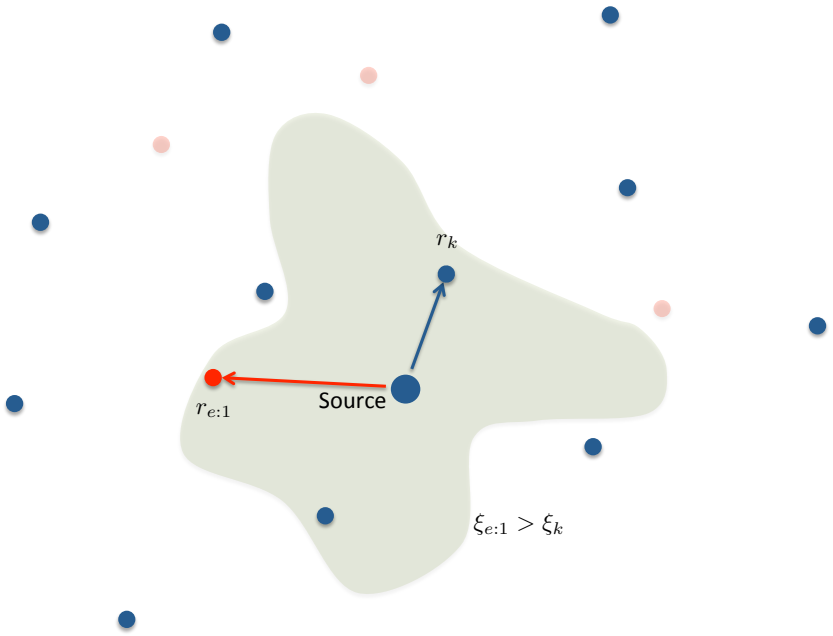



Figure 3.3: Irregular secrecy neighborhoods

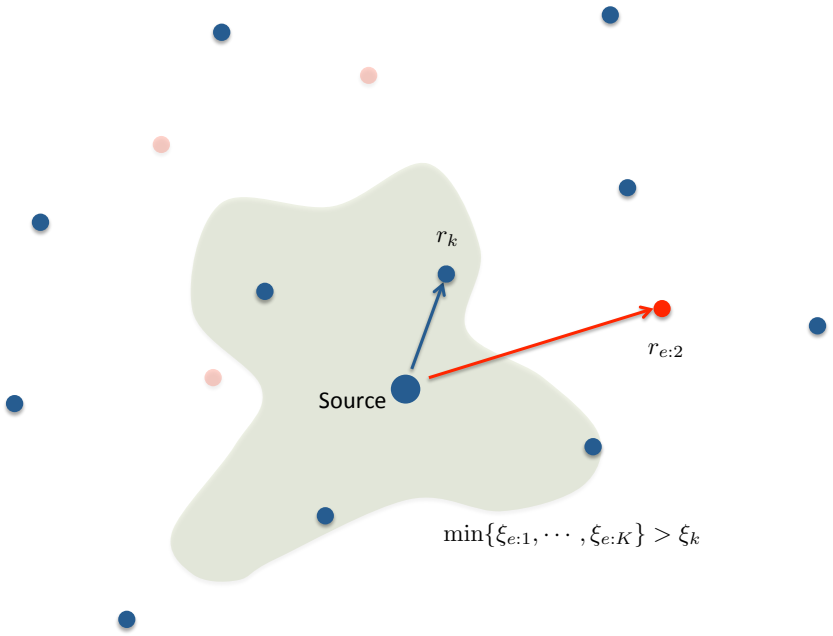



Figure 3.4: Uncertainty of dominant eavesdropper

These fundamental distinctions between the AWGN and the fading cases prevent the straightforward extension of the analysis offered in [29] to arbitrary fading via homogenization arguments as done in [14]. Therefore, in order to study the conditions under which unicasting on the $\mathcal{S}$-Graph is successful, we derive in the sequel the probabilities $\Pr\{\mathcal{C}_{s:k} > 0\}$ under Nakagami-$m$ fading, motivated by its flexibility.

Then, the secrecy capacity of unicast legitimate link $k$ in the presence of an eavesdropper located at the unknown distance $r_{\mathrm{e}}$, subjected to nakagami-$m$ fading and path loss governed by the exponent $\alpha$ can be re-written as [8, 9]

$$\mathcal{C}_{s:k} = \log_2\!\left(1+ \frac{|h_k|^2 P}{r_k^{\alpha} N_0}\right) - \log_2\!\left(1+ \frac{|h_{\mathrm{e}}|^2 P}{r_{\mathrm{e}}^{\alpha} N_0}\right). \tag{3.13}$$

Consequently, the probability that the secrecy capacity of the channel $(s \to k)$ is below a given threshold $R_s \geq 0$ – here after is referred to as *secrecy outage probability* – is defined as [24]

$$\mathcal{P}_{\mathrm{out}}(R_s) \triangleq \Pr\{\mathcal{C}_{s:k} \leq R_s\} = 1 - \Pr\{\mathcal{C}_{s:k} > R_s\}. \tag{3.14}$$

From (3.13), the *secrecy non-outage probability* $\Pr\{\mathcal{C}_{s:k} > R\}$ can be written as

$$\tilde{\mathcal{P}}_{\mathrm{out}}(R_s) \triangleq \Pr\{\mathcal{C}_{s:k} > R_s\} = \Pr\left\{\log_2\!\left(\frac{\rho^{-1}+\xi_k^{-1}}{\rho^{-1}+\xi_{\mathrm{e}}^{-1}}\right) > R_s\right\}. \tag{3.15}$$

Under Nakagami-$m$ fading, the distribution of the path loss to the $k$-th closest node is given by [12, Eq. (7)]

$$p_{\xi_k}(x; k, m, \sigma) = A(k; m, \sigma) \cdot \frac{x^{k-1}}{(\sigma + x)^{m+k}}, \tag{3.16}$$

where

$$A(k; m, \sigma) \triangleq m\, \sigma^m \tbinom{m+k-1}{m}, \tag{3.17}$$

$$\sigma \triangleq \frac{m}{\lambda \pi}. \tag{3.18}$$

Recall that $m$ captures the *intensity of fading*, while $\lambda\pi$ is the *intensity of the point process*, such that $\sigma$, which absorbs those two key environmental parameters into a single quantity, can be adequately referred to as the *intensity ratio*. The intensity

ratio of legitimate and eavesdropping nodes will be henceforth denoted by $\sigma_\ell$ and $\sigma_e$, respectively. Under the mentioned fading model, the secrecy capacity of unicast channel is determined as depicted in Fig. 3.5.

Assuming that both eavesdroppers and legitimate nodes are under equal fading statistics, it follows from Eq. (3.16) and Eq. (3.5) that

$$p_\Delta(x;k,m,\sigma_e,\sigma_\ell) = \tag{3.19}$$

$$\int_{-x}^{\infty} p_{\xi_{e:1}}(\tau;1,m,\sigma_e)\cdot p_{\xi_k}(x+\tau;k,m,\sigma_\ell)\,\mathrm{d}\tau \xrightarrow[\text{subst. Eq. (3.16)}]{} A_e A_\ell \int_{-x}^{\infty} \frac{(x+\tau)^{k-1}}{(\sigma_e+\tau)^{m+1}(\sigma_\ell+x+\tau)^{m+k}}\,\mathrm{d}\tau,$$

$$\xrightarrow[z\triangleq x+\tau]{} A_e A_\ell \int_0^{\infty} \frac{z^{k-1}}{(\sigma_e-x+z)^{m+1}(\sigma_\ell+z)^{m+k}}\,\mathrm{d}z \xrightarrow[y\triangleq 1+\frac{z}{\sigma_\ell}]{} \frac{A_e A_\ell}{\sigma_\ell^{2m+1}} \int_1^{\infty} \frac{(y-1)^{k-1}}{(a+y)^{m+1}y^{m+k}}\,\mathrm{d}y,$$

where, in the last expression,

$$a \triangleq \tfrac{\sigma_e-\sigma_\ell-x}{\sigma_\ell} = \varrho - 1 - x/\sigma_\ell. \tag{3.20}$$

In the last equality we used the fact that under the assumption that legitimate nodes and eavesdroppers are subjected to equal fading, $\frac{\sigma_e}{\sigma_\ell} = \frac{\lambda_\ell}{\lambda_e} \triangleq \varrho$. Alluding to the latter, we will henceforth refer to $\varrho$ as the *relative intensity ratio*. Furthermore, since under equal fading $\sigma_e > \sigma_\ell \implies \varrho > 1$ implies that the density of legitimate nodes is larger than that of eavesdroppers, we shall focus on the case where $\varrho > 1$.

Returning to the derivation, using the Binomial Theorem

$$(y-1)^{k-1} = \sum_{j=0}^{k-1} (-1)^j \binom{k-1}{j} y^{k-j-1}, \tag{3.21}$$

and substituting Eq. (3.17) for $A_e$ and $A_\ell$ into Eq. (3.19) we obtain

$$p_\Delta(x;k,m,\varrho,\sigma_\ell) = \frac{m^2}{\sigma_\ell}\varrho^m \binom{m+k-1}{m} \sum_{j=0}^{k-1} (-1)^j \binom{k-1}{j} \underbrace{\int_1^{\infty} \frac{\mathrm{d}y}{((\varrho-1)+y-x/\sigma_\ell)^{m+1}y^{m+j+1}}}_{I_1(x;m,\varrho,\sigma_\ell;j)\big|_1^\infty}. \tag{3.22}$$

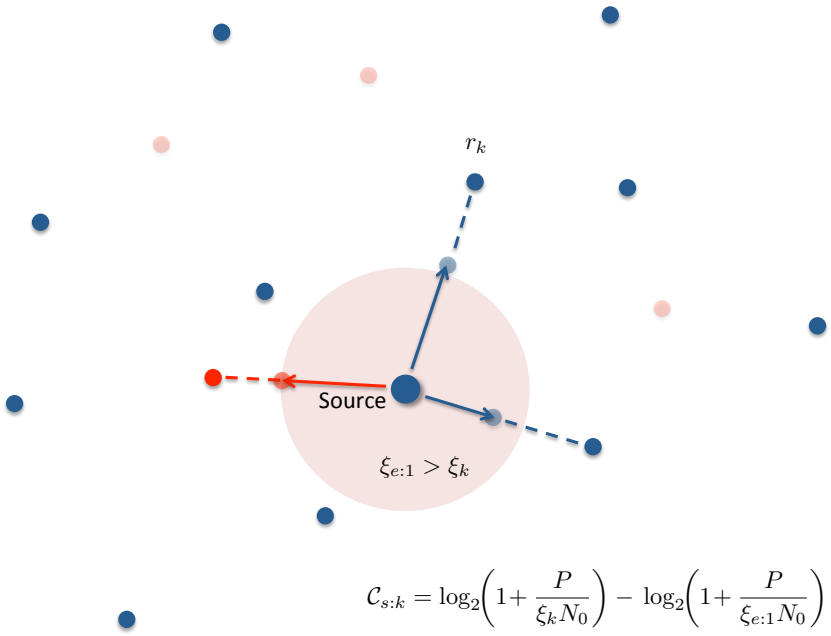



Figure 3.5: Regularized secrecy neighborhood in $\mathcal{S}$-Graph

The above integral has the solution [68, pp.28, Eq. (1.2.6.3)]

$$I_1(x;m,\varrho,\sigma_\ell;j)\Big|_1^\infty=\sum_{v=0}^{2m+j}(-1)^{v+1}\binom{2m+j}{v}f(x;m,\varrho,\sigma_\ell;j,v), \tag{3.23}$$

where

$$f(x;m,\varrho,\sigma_\ell;j,v)\triangleq\begin{cases}\dfrac{-\ln(\varrho-x/\sigma_\ell)}{((\varrho-1)-x/\sigma_\ell)^{2m+j+1}} & \text{if } v=m+j,\\ \dfrac{1-(\varrho-x/\sigma_\ell)^{m+j-v}}{(m+j-v)((\varrho-1)-x/\sigma_\ell)^{2m+j+1}} & \text{if } v\neq m+j,\end{cases} \tag{3.24}$$

such that the following closed-form expression for the distribution of the pathloss difference $\Delta$ is obtained:

$$p_\Delta(x;k,m,\varrho,\sigma_\ell)=\frac{m^2\varrho^m}{\sigma_\ell}\binom{m+k-1}{m}\sum_{j=0}^{k-1}\binom{k-1}{j}\sum_{v=0}^{2m+j}(-1)^{j+v+1}\binom{2m+j}{v}f(x;m,\varrho,\sigma_\ell;j,v). \tag{3.25}$$

From the above, the probability that $\mathcal{C}_{s:k}>0$ under the environmental conditions described by set of parameters $\{m,\varrho,\sigma_\ell\}$ becomes

$$\Pr{}_{\text{Naka}}(i,m,\varrho)=m^2\varrho^m\binom{m+k-1}{m}\sum_{j=0}^{k-1}\binom{k-1}{j}\sum_{v=0}^{2m+j}(-1)^{j+v+1}\binom{2m+j}{v} \times\underbrace{\int_\varrho^\infty f(\sigma_\ell(\varrho-y);m,\varrho,\sigma_\ell;j,v)\,\mathrm{d}y}_{I_2(\varrho;m;j,v)\big|_\varrho^\infty}. \tag{3.26}$$

The latter integral assumes three distinct forms depending on the relationship between the indexes $v$ and $j$, and the parameter $m$, dealt with separately in the sequel.

***Case 1:*** $v<m+j$

Here $I_2(\varrho;m;j,v)\big|_\varrho^\infty$ reduces to [68, pp. 27, Eq. (1.2.5.6)]

$$I_2(\varrho;m;j,v)\big|_\varrho^\infty\xrightarrow[v<m+j]{}\frac{1}{m+j-v}\left[\frac{1}{(2m+j)(\varrho-1)^{2m+j}}-\underbrace{\int_\varrho^\infty\frac{x^{m+j-v}}{(x-1)^{2m+j+1}}\,\mathrm{d}x}_{I_3(\varrho;m;m+j-v,2m+j)\big|_\varrho^\infty}\right]. \tag{3.27}$$

The solution of the latter integral is given by

$$I_3(\varrho;m;p,q)\Big|_{\varrho}^{\infty} \triangleq \int_{\varrho}^{\infty} \frac{x^p}{(x-1)^{q+1}}\,\mathrm{d}x = \sum_{t=0}^{p} \binom{p}{t} \frac{(\varrho-1)^{t-q}}{q-t}, \tag{3.28}$$

which yields

$$I_2(\varrho;m;j,v)\Big|_{\varrho}^{\infty} \xrightarrow[v<m+j]{} \frac{-1}{m+j-v} \sum_{t=1}^{m+j-v} \binom{m+j-v}{t} \frac{(\varrho-1)^{t-2m-j}}{2m+j-t}. \tag{3.29}$$

***Case 2:*** $v = m + j$

In this case $I_2(\varrho;m;j,v)\big|_{\varrho}^{\infty}$ evaluates to [67, pp. 235, Eq. (2.727.1.8)]

$$I_2(\varrho;m;j,v)\Big|_{\varrho}^{\infty} \xrightarrow[v=m+j]{} \frac{-1}{2m+j} \left[ \frac{\ln \varrho}{(\varrho-1)^{2m+j}} + \underbrace{\int_{\varrho}^{\infty} \frac{\mathrm{d}x}{x(x-1)^{2m+j}}}_{I_4(\varrho;m;1,2m+j)\big|_{\varrho}^{\infty}} \right], \tag{3.30}$$

where the integral $I_4(\varrho;m;p,q)\big|_{\varrho}^{\infty}$ is a particular case of [68, pp. 28, Eq. (1.2.6.3)]

$$I_4(\varrho;m;p,q)\big|_{\varrho}^{\infty} \triangleq \int_{\varrho}^{\infty} \frac{\mathrm{d}x}{x^p(x-1)^q} = \sum_{t=0}^{p+q-2} (-1)^{p+q+t} \binom{p+q-2}{t} g(\varrho;p,t), \tag{3.31}$$

with

$$g(\varrho;p,t) \triangleq \begin{cases} -\ln\left(\dfrac{\varrho-1}{\varrho}\right) & \text{if } t = p-1, \\ \dfrac{\left(\dfrac{\varrho}{\varrho-1}\right)^{t-p+1} - 1}{t-p+1} & \text{if } t \neq p-1. \end{cases} \tag{3.32}$$

In particular, from Eq. (3.31), we obtain

$$I_4(\varrho;m;1,2m+j)\big|_{\varrho}^{\infty} = \sum_{t=0}^{2m+j-1} (-1)^{2m+j+t+1} \binom{2m+j-1}{t} g(\varrho;1,2m+j). \tag{3.33}$$

$$\Pr_{\text{Naka}}(k,m,\varrho) = m^2\varrho^m \binom{m+k-1}{m} \sum_{j=0}^{k-1} \binom{k-1}{j} \sum_{v=0}^{2m+j} (-1)^{j+v+1} \binom{2m+j}{v} \times \tag{3.36}$$

$$\times \left\{ \begin{array}{ll} \dfrac{-1}{m+j-v} \displaystyle\sum_{t=1}^{m+j-v} \dfrac{\binom{m+j-v}{t}}{(2m+j-t)(\varrho-1)^{2m+j-t}} & \text{if } v < m+j \\ \dfrac{-\ln\varrho}{(2m+j)(\varrho-1)^{2m+j}} + \displaystyle\sum_{t=0}^{2m+j-1} \dfrac{(-1)^{2m+j+t+1}}{(2m+j)} \binom{2m+j-1}{t} g(\varrho;1,2m+j) & \text{if } v = m+j \\ \dfrac{(2m+j)^{-1}}{(m+j-v)(\varrho-1)^{2m+j}} + \displaystyle\sum_{t=0}^{m+v-1} \dfrac{(-1)^{m+v+t+1}}{m+j-v} \binom{m+v-1}{t} g(\varrho;v-m-j,2m+j+1) & \text{if } v > m+j \end{array} \right\}$$

***Case 3:*** $v > m+j$

Finally, in this case $I_2(\varrho;m;j,v)\big|_{\varrho}^{\infty}$ can be written as [68, pp. 27, Eq. (1.2.5.6)]

$$I_2(\varrho;m;j,v)\big|_{\varrho}^{\infty} \xrightarrow[v>m+j]{} \frac{1}{m+j-v} \left[ \frac{1}{(2m+j)(\varrho-1)^{2m+j}} - \underbrace{\int_{\varrho}^{\infty} \frac{1}{x^{v-m-j}(x-1)^{2m+j+1}}\,\mathrm{d}x}_{I_4(\varrho;m;v-m-j,2m+j+1)\big|_{\varrho}^{\infty}} \right]. \tag{3.34}$$

The integral appearing in Eq. (3.34) is similar to $I_4(\varrho;m;1,2m+j)\big|_{\varrho}^{\infty}$ and has the solution [68, pp. 28, Eq. (1.2.6.3)]

$$I_4(\varrho;m;v-m-j,2m+j+1)\Big|_{\varrho}^{\infty} = \sum_{t=0}^{m+v-1} (-1)^{m+v+t+1} \binom{m+v-1}{t} g(\varrho;v-m-j,2m+j+1). \tag{3.35}$$

The closed-form expression for $p_{\text{Naka}}(i,m,\varrho,\sigma_\ell)$ given in equation (3.36) at the top of page follows immediately from equations (3.26) through (3.35).

### *Special Cases of Interest*

Before we proceed to the scenario of multiple eavesdroppers, let us consider some particular cases of interest within the single eavesdropper scenario, extracting from Eq. (3.36) specified and simplified expressions that allow us to gain insight into unicast links under the corresponding conditions.

**Low Relative Intensity Ratios**

The worst case in terms of the relative intensity ratio that can be analyzed with our results is $\varrho = 1$, since Eq. (3.32), and consequently Eq. (3.36), are not defined for $\varrho < 1$. Notice, however, that this "limitation" of the analysis is not very substantial. Indeed, given the assumption that the source finds a single eavesdropper in its vicinity under the eavesdropper density $\lambda_e$, and that the density of legitimate nodes is smaller than the latter (*i.e.*, $\varrho \triangleq \frac{\lambda_\ell}{\lambda_e} < 1 \Rightarrow \lambda_\ell < \lambda_e$), the likelihood that the source finds a legitimate node in its vicinity diminishes with $\varrho$.

Although Eq. (3.36) cannot be directly evaluated for $\varrho = 1$, its limit at $\varrho \to 1$ does exist. Omitting the derivation which is laborious and rather mechanical, in this special case, we have

$$\Pr_{\text{Naka}}(k, m) = \binom{2m-1}{m}\binom{k+2m-1}{k+m-1}^{-1}. \tag{3.37}$$

Plots of Eq. (3.37) are shown in Fig. 3.6 and Fig. 3.7, which also includes curves obtained with Eq. (3.2). These figures show that the nearest node experiences no change in secrecy capacity as a result of fading. However, further nodes *benefit* from fading. In other words, AGWN is the *worst* possible case, as far as the capacity of unicasts on the $\mathcal{S}$-Graph is concerned!

This counter-intuitive result can be explained as follows. Since the densities of both networks are identical, and the single eavesdropper is the nearest eavesdropper, the legitimate node and eavesdropper are in equal footing in terms of which one experiences the smallest path loss. Therefore, on average, fading affect both these receive equally, and consequently, the secrecy capacity is not affected by fading.

However, farther nodes ($k > 1$) are *not* at equal footing comparing to the single/nearest eavesdropper. In fact, under AWGN, noise is the only factor that enables a legitimate node with a statistical disposition to be located further than the eavesdropper to experience a lower path loss smaller then the latter. Consequently, the secrecy capacity of unicast channels on the $\mathcal{S}$-Graph decreases rapidly with $r$ in the AWGN case. In contrast, under fading, the occurrence of a large channel gain may render the path loss to a further node lower than that to the eavesdropper, improving the secrecy capacity. We remark that this result, namely, that fading helps increase the probability of non-zero secrecy capacity of (sufficiently) *farther* nodes holds also when $\varrho > 1$. This can be inferred, for instance, from Eq. (3.38) which is depicted in figures 3.6 and 3.7 and, in the limit for $\varrho \to 1$ captures a special case of Eq. (3.37) with $m = 1$.

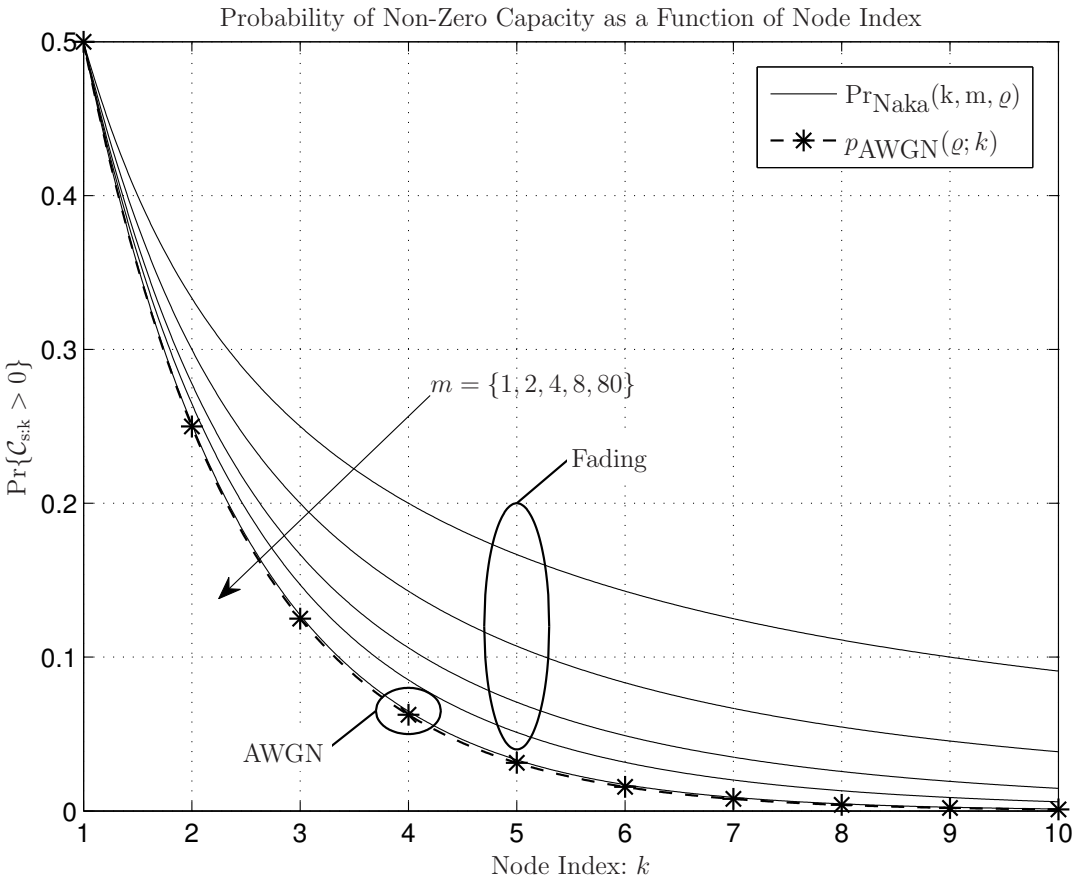



Figure 3.6: Effect of fading onto $\Pr\{\mathcal{C}_{s:k} > 0\}$ in the case of unitary relative intensity ratio ($\varrho$=1).

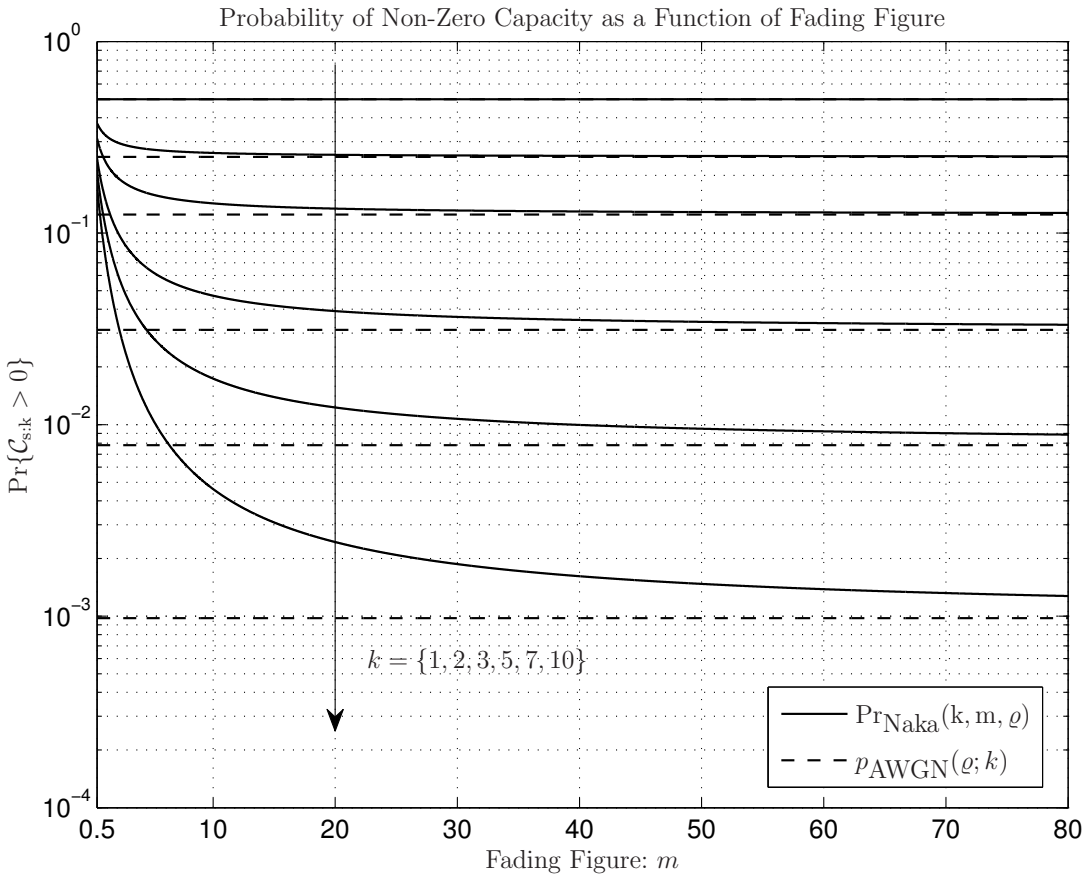



Figure 3.7: Effect of distance onto $\Pr\{\mathcal{C}_{s:k} > 0\}$ in the case of unitary relative intensity ratio ($\varrho$=1).

### Rayleigh Fading

Stimulated by the results above, which indicate a *positive* effect of fading over the secrecy capacity of $\mathcal{S}$-unicast channels, we turn our attention to the worst (terrestrial) fading case under the Nakagami-$m$ model, *i.e.*, Rayleigh ($m = 1$).

While in this case no unified simple expression for $\Pr\{\mathcal{C}_{s:k} > 0\}$ exists, with $m = 1$, Eq. (3.36) reduces to the closed-form expression

$$\Pr_{\text{Rayleigh}}(k, \varrho) = \frac{P_k(\varrho)}{(\varrho - 1)^k} - \frac{\varrho^k \log \varrho^k}{(\varrho - 1)^{k+1}}, \tag{3.38}$$

where $P_k(\varrho)$ are polynomials of degree $k$ on $\varrho$, a few of which are listed in Table 3.1.

Plots of $\Pr\{\mathcal{C}_{s:k} > 0\}$ under Rayleigh fading obtained from Eq. (3.38) are compared in Fig. 3.8 and Fig. 3.9 to the corresponding probabilities under AWGN, as per Eq. (3.2). The results show that care must be exercised when attempting to carry conclusions drawn for networks exposed to low intensity ratio ($\rho = 1$), over to networks with larger intensity ratios ($\rho > 1$).

Specifically, it is found that in the presence of fading, the larger the $\varrho$, the farther must a legitimate node be in order to experience an increase in $\Pr\{\mathcal{C}_{s:k} > 0\}$ relative to that under AWGN conditions. In other words, in networks subject to a low relative intensity ratio, fading only helps nodes sufficiently far from the source.

Given the above, one can therefore speak of a *critical relative intensity ratio*, hereafter denoted by $\varrho^*$, as the value of $\varrho$ such that $p_{\text{Rayleigh}}(k, \varrho) = p_{\text{AWGN}}(k, \varrho)$, that is

$$\varrho^* = \left\{ \varrho \,\middle|\, \frac{P_k(\varrho)}{(\varrho - 1)^k} - \frac{\varrho^k \log \varrho^k}{(\varrho - 1)^{k+1}} - \left(\frac{\varrho}{\varrho + 1}\right)^k = 0 \right\}. \tag{3.39}$$

Unfortunately, due to the presence of the logarithm, simple closed-form solutions of Eq. (3.39) cannot be found. A plot of the critical density as a function of the node index $k$ is, however, shown in Fig. 3.10. Curiously, it is found that the relationship between the critical relative intensity ratio and the node index is very well approximated by the following linear model

$$\varrho^* = \frac{11}{9}k - \frac{2}{9}. \tag{3.40}$$

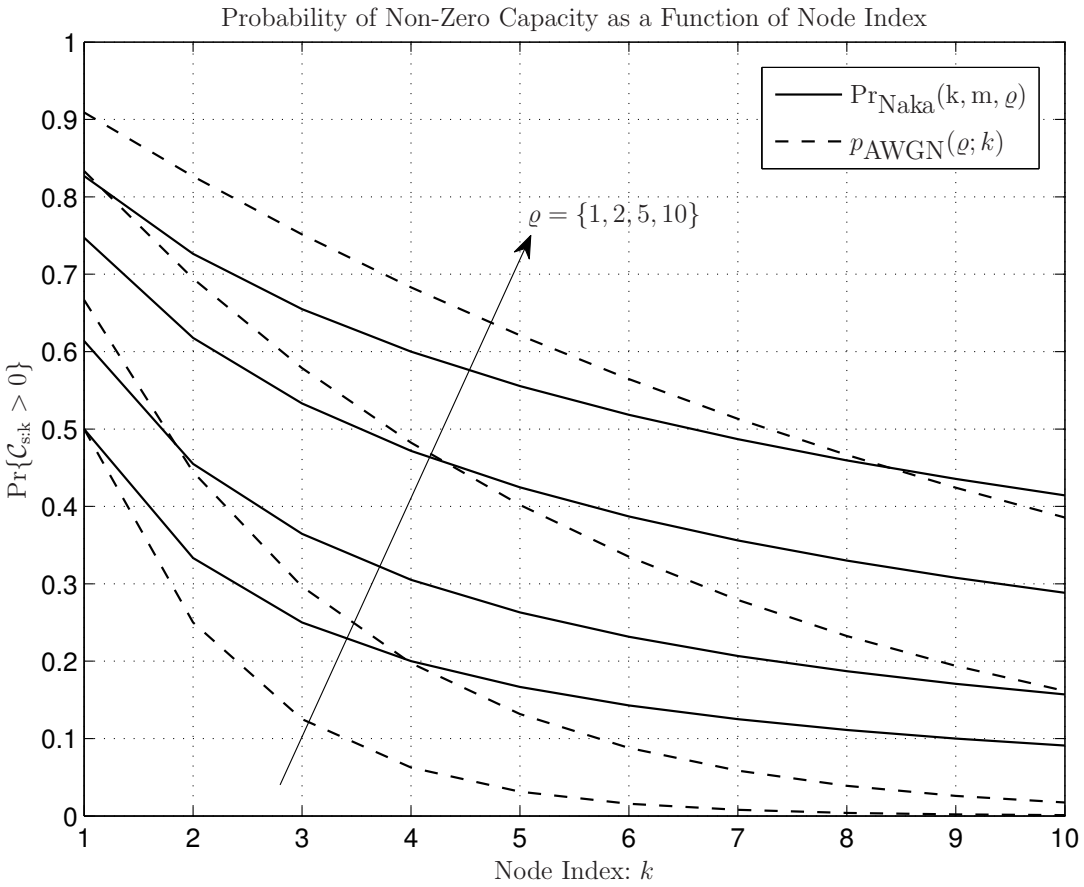



Figure 3.8: Effect of distance onto $\Pr\{\mathcal{C}_{s:k} > 0\}$ in the case of Rayleigh fading ($m = 1$).

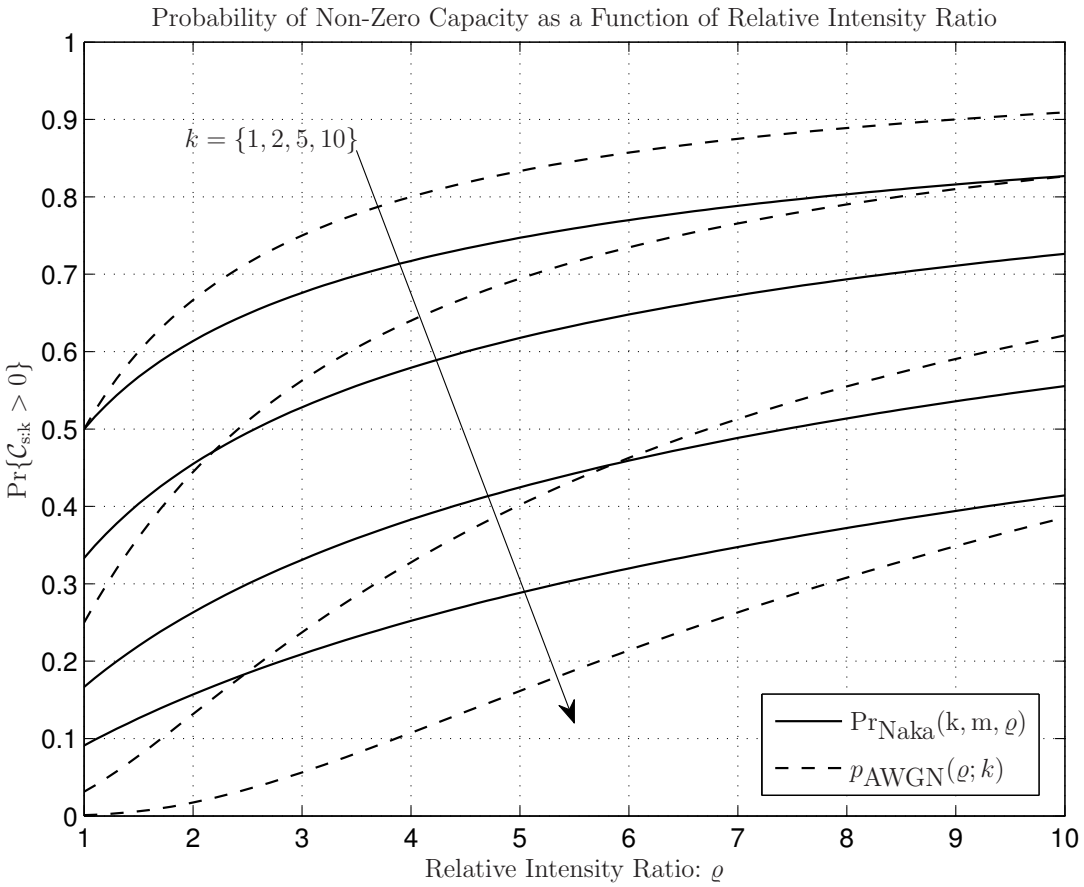



Figure 3.9: Effect of relative intensity ratio onto $\Pr\{\mathcal{C}_{s:k} > 0\}$ in the case of Rayleigh fading ($m = 1$).

Table 3.1: Polynomial terms in Eq. (3.38)

| $k$ | Polynomials in $\varrho$ |
|---|---|
| 1 | $\varrho$ |
| 2 | $\varrho + \varrho^2$ |
| 3 | $-\frac{1}{2}\varrho + \frac{5}{2}\varrho^2 + \varrho^3$ |
| 4 | $\frac{1}{3}\varrho - \frac{5}{3}\varrho^2 + \frac{13}{3}\varrho^3 + \varrho^4$ |
| 5 | $-\frac{1}{4}\varrho + \frac{17}{12}\varrho^2 - \frac{43}{12}\varrho^3 + \frac{77}{12}\varrho^4 + \varrho^5$ |
| 6 | $\frac{1}{5}\varrho - \frac{13}{10}\varrho^2 + \frac{37}{10}\varrho^3 - \frac{63}{10}\varrho^4 + \frac{87}{10}\varrho^5 + \varrho^6$ |
| 7 | $-\frac{1}{6}\varrho + \frac{37}{30}\varrho^2 - \frac{241}{60}\varrho^3 + \frac{153}{20}\varrho^4 - \frac{197}{20}\varrho^5 + \frac{223}{20}\varrho^6 + \varrho^7$ |
| 8 | $\frac{1}{7}\varrho - \frac{25}{21}\varrho^2 + \frac{463}{105}\varrho^3 - \frac{1007}{105}\varrho^4 + \frac{481}{35}\varrho^5 - \frac{499}{35}\varrho^6 + \frac{481}{35}\varrho^7 + \varrho^8$ |
| 9 | $-\frac{1}{8}\varrho + \frac{65}{56}\varrho^2 - \frac{271}{56}\varrho^3 + \frac{3349}{280}\varrho^4 - \frac{5471}{280}\varrho^5 + \frac{6289}{280}\varrho^6 - \frac{5471}{280}\varrho^7 + \frac{4609}{280}\varrho^8 + \varrho^9$ |
| 10 | $\frac{1}{9}\varrho - \frac{41}{36}\varrho^2 + \frac{1333}{252}\varrho^3 - \frac{3707}{252}\varrho^4 + \frac{6877}{252}\varrho^5 - \frac{8999}{252}\varrho^6 + \frac{8641}{252}\varrho^7 - \frac{6479}{252}\varrho^8 + \frac{4861}{252}\varrho^9 + \varrho^{10}$ |

Note: $m = 1$, arbitary $\varrho$

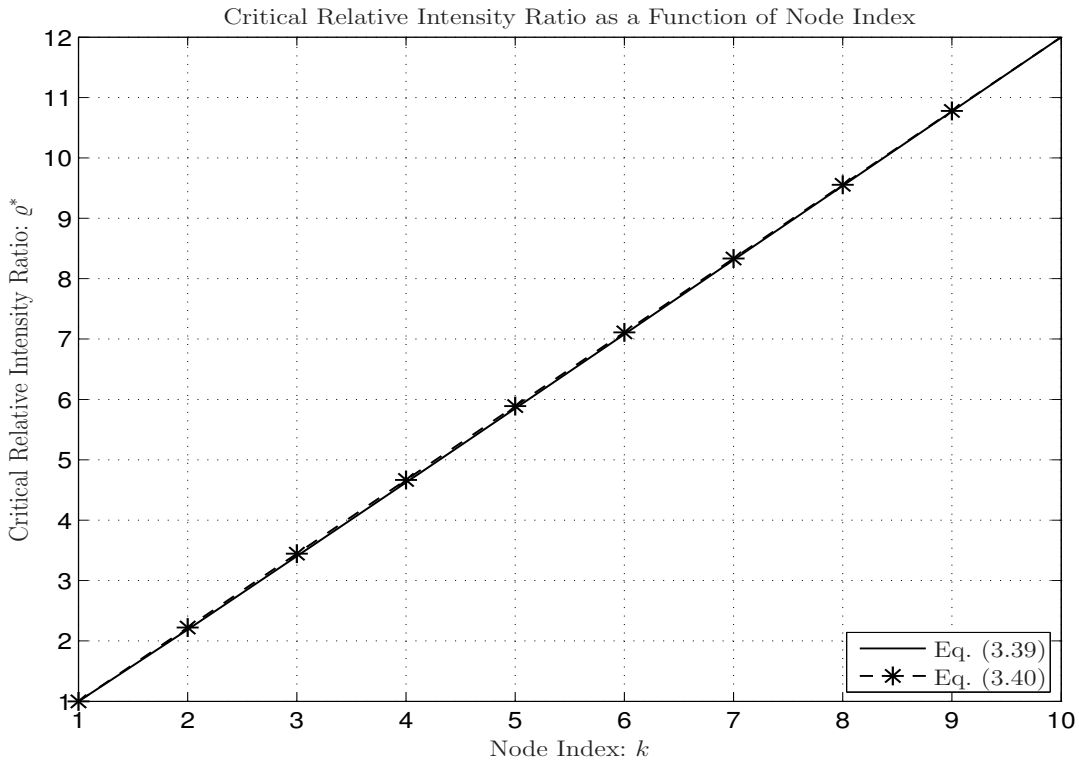



Figure 3.10: Critical relative intensity ratio as a function of the node index (distance) in the case of Rayleigh fading.

## 3.4 Connection Outage

Before we conclude this chapter, let us briefly address another issue. In order to compute the secrecy transmission capacity [24] of a random network subject to fading, one would require not only the secrecy outage but also the connection outage, which measures the probability that a node can communicate with a source in the first place. This expression is, to the best of our knowledge, still unknown, but can be easily calculated employing the model here utilised.

Denote the transmission rate as $R_t$, then the connection outage in AWGN can be computed using Eq. (3.4) as

$$\mathcal{P}_{\text{co}}(R_t) = \Pr\{\log_2\left(1+\tfrac{\rho}{\xi_k}\right) < R_t\} \overset{(a)}{=} \frac{\Gamma(k, \pi\lambda_\ell[\frac{\rho}{(2^{R_t}-1)}]^\delta)}{\Gamma(k)}, \tag{3.41}$$

where (a) follows from [67, Eq. (3.381)].

The PDF of connection outage as a function of transmission rate can be obtained by taking derivative of the Eq. (3.41)

$$f(R_t) = \frac{(\pi\lambda_\ell)^k \rho^{\delta k}}{\Gamma(k)} \frac{\delta \cdot \log 2 \cdot 2^{R_t}}{(2^{R_t}-1)^{\delta k+1}} \exp\left(-\pi\lambda_\ell \left(\frac{\rho}{2^{R_t}-1}\right)^\delta\right). \tag{3.42}$$

A similar result is given in [29] by using Erlang distribution. Compared to the latter, the derivation above is more general, since any path loss coefficient $\alpha$ (embedded in $\delta$) is admissible.

Next, consider the distribution of the *path gains*. The PDF of Nakagami-$m$ fading model is expressed by [12]

$$f(x) = \frac{m^m x^{m-1} exp(-mx)}{\Gamma(m)}. \tag{3.43}$$

A geometry-inclusive fading model for wireless networks in the case of $\delta = 1$ was studied in [12], where distance and fading uncertainties are combined in the *path loss process with fading*. In contrast, the results to follow here apply for generalized values of $\delta$, with network dimension $d = 2$.

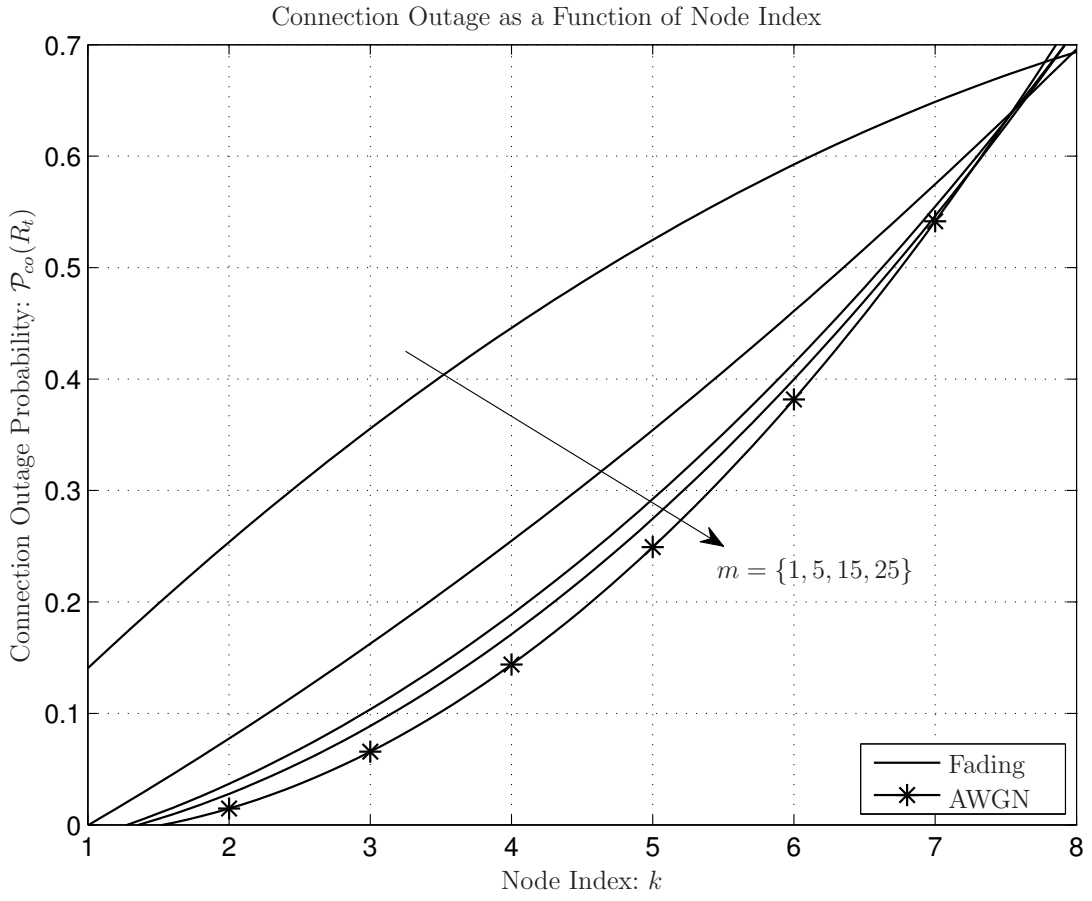



Figure 3.11: Connection outage probability $\mathcal{P}_{co}$ as a function of node index under Nakagami-$m$ fading for various $m$, with $R_t = 1$, $\lambda_\ell = 2$ and $\alpha = 4$ .

$$\mathcal{P}_{\text{co}}(R_t) = 1 + \frac{\Gamma(\frac{1}{2}+\frac{k}{2}+m)\,{}_2F_2(\frac{k}{2}+\frac{1}{2}, \frac{1}{2}+\frac{k}{2}+m, \frac{3}{2}, \frac{3}{2}+\frac{k}{2}, \frac{(\pi\lambda_\ell)^2}{4mu})}{(\pi\lambda_\ell)^{-k-1}\cdot(k+1)(mu)^{\frac{k}{2}+\frac{3}{2}}\Gamma(m)\Gamma(k)} - \frac{\Gamma(\frac{k}{2}+m)\,{}_2F_2(\frac{k}{2}, \frac{k}{2}+m, \frac{1}{2}, 1+\frac{k}{2}, \frac{(\pi\lambda_\ell)^2}{4mu})}{(\pi\lambda_\ell)^{-k}\cdot k\cdot(mu)^{\frac{k}{2}}\Gamma(m)\Gamma(k)}. \tag{3.45}$$

The channel gain $\zeta$ is the function of independent variables $|h|^2$ and $r^\alpha$. Then, the distribution of $\zeta$ can be expressed by

$$\begin{aligned} f_{\zeta_k}(x) =& \int_0^\infty y \frac{m^m (yx)^{m-1} e^{-mxy}}{\Gamma(m)} \frac{(\pi\lambda_\ell)^k y^{\frac{2}{\alpha}(k-\frac{\alpha}{2})} e^{-\pi\lambda_\ell y^{\frac{2}{\alpha}}}}{\frac{\alpha}{2}\Gamma(k)} \mathrm{d}y, \\ =& \frac{B}{x^{\frac{2k}{\alpha}+2}} \Big[ mx\Gamma(m+\tfrac{2k}{\alpha})\,{}_1F_1\left(m+\tfrac{2k}{\alpha}, \tfrac{1}{2}, \tfrac{(\pi\lambda_\ell)^2}{4mx}\right) + \\ & \sqrt{mx}(-\pi\lambda_\ell)\Gamma\big(m+\tfrac{2k}{\alpha}+\tfrac{1}{2}\big)\,{}_1F_1\Big(m+\tfrac{2k}{\alpha}+\tfrac{1}{2}, \tfrac{3}{2}, \tfrac{(\pi\lambda_\ell)^2}{4mx}\Big)\Big], \end{aligned} \tag{3.39}$$

where $B = \frac{(2\pi\lambda_\ell)^k}{\alpha\Gamma(m)\Gamma(k)m^{\frac{2k}{\alpha}+1}}$.

When the wireless transmission is under Nakagami-$m$ fading, and the path gain which depends on channel fading and stochastic distances between communicating pairs, the connection outage for $\alpha = 4$ can be computed as

$$\begin{aligned} \mathcal{P}_{\text{co}}(R_t) &= \Pr\left\{\log_2(1+\rho\zeta_k) \le R_t\right\}, \\ &= \frac{2m^m(\pi\lambda_\ell)^k}{\alpha\cdot\Gamma(k)\Gamma(m)} \int_0^\infty x^{\frac{1}{2}(k-2)} e^{-\pi\lambda_\ell x^{\frac{1}{2}}} \int_0^{ux} y^{m-1} e^{-my} \mathrm{d}y\, \mathrm{d}x, \end{aligned} \tag{3.40}$$

where $u = \frac{2^{R_t}-1}{\rho}$.

The above integral has been evaluated using [69, Eq. (2.10.3.9)], yielding the closed form expression given in Eq. (3.45) on the top of this page. Notice that Eq. (3.45) generalizes Eq. (3.41), in the sense that for $m \to \infty$ the two expressions should coincide. This is illustrated in Fig. 3.11.

## 3.5 Conclusions

In this chapter, we investigated the secrecy outage of unicast channels in random networks exposed to randomly located single eavesdropper, obtaining original expressions which include uncertainty in terms of the location of legitimate nodes relative to the eavesdropper, and fading. In particular, we conducted a detailed analysis of the impact of Nakagami-$m$ block fading and of the density of legitimate nodes relative to that of eavesdroppers. The results indicate that depending on those conditions, fading may result in an increase in the probability of a non-zero secrecy capacity of unicast channels, compared to that available under AWGN. The findings are described in detail in our articles [19, 70, 71].

Specifically, we have have added following contributions to this chapter

- Obtained the expression for probability of non-zero secrecy outage of unicast channel under AWGN channel [19].
- Derived the expression of probability of non-zero secrecy outage of unicast channel in presence of single eavesdropper under Nakagami-$m$ fading channel [19, 70].
- Derived a new compact expression for connection outage probability under fading channel [71].

# Chapter 4

# Single Antenna Systems in Unicast Channels: Multiple Eavesdroppers

**Summary:**

*In this chapter, we offer a characterization of the impact of noise, path loss, density and fading onto the secrecy capacity achieved between a pair of legitimate nodes of a network in the possible presence of randomly located eavesdroppers. We derive the probability of non-zero capacity for the case of an unknown number of eavesdroppers per neighborhood.*

Reprinted from Proc. IEEE Personal Indoor Mobile Radio Communication, Satyanarayana Vuppala, Giuseppe Abreu, Secrecy Outage in Random Wireless Networks subjected to Fading, pp 441-445, Copyright (2013), with permission IEEE.

## 4.1 Introduction

The results investigated in Chapter 3 only cover a portion of the situations faced by a unicasting source on the $\mathcal{S}$-Graph. Specifically, the number of eavesdroppers in the vicinity of the source is not always one, but rather a Poisson random variable with intensity given by the footprint of the source times the density of eavesdroppers.

In the cases when the number of neighboring eavesdroppers is larger than one, and their corresponding path losses or path gains are affected by fading, the secrecy capacity of the unicasting channel is not determined by the nearest eavesdropper, but rather by the eavesdropper with the *minimum* path loss or *maximum* path gain amongst those present (see Fig. 4.1). In other words, the $k$-th unicast channel will experience a non-zero secrecy capacity iff

$$\Delta \triangleq \xi_k - \min\{\xi_{e:1}, \cdots, \xi_{e:K}\} \leq 0, \tag{4.1}$$

$$\Delta \triangleq \max\{\zeta_{\mathrm{e}:1}, \cdots, \zeta_{\mathrm{e}:K}\} - \zeta_k \ \geq 0, \tag{4.2}$$

where $K$ is a Poisson random variable; $\xi_{e:k}$ and $\zeta_{\mathrm{e}:k}$ are path losses and path gains of corresponding $k$-th eavesdropper respectively.

In following sections, we have derived the best eavesdropper distribution in two different approaches. In first approach, we used path loss distribution in order to find the best eavesdropper distribution. With this approach, we derived the closed-form solutions for the secrecy outage probability. However, in some cases it is easier to work with path gains instead of path losses. To this point, in second approach, we used path gains to obtain the best eavesdropper distribution.

## 4.2 Nakagami Fading Case: Approach 1

For notational convenience[1], let us denote the lower extreme order statistics appearing in Eq. (4.1) simply by $\bar{\xi}_e$, that is $\bar{\xi}_e \triangleq \min\{\xi_{e:1}, \cdots, \xi_{e:K}\}$. In order to derive the probability $\Pr\{\mathcal{C}_{s:k} > 0\}$, the distribution of $\bar{\xi}_e$ is required. Deriving such a distribution exactly is, however, a formidable task since the number of eavesdroppers $K$ is *random* and *unknown*, and the path losses $\xi_{e:k}$'s are *non-identically* distributed random variates.

[1] Adding a "$K$" to the notation is not consistent since $K$ is random and, more importantly, one finds that $\bar{\xi}_e$ is in fact not strongly dependent on $K$.

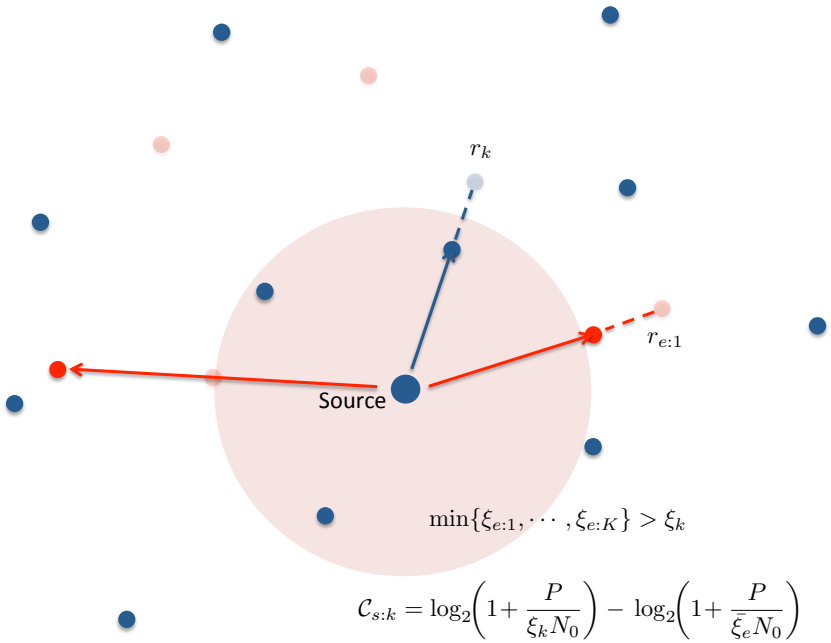



Figure 4.1: $\mathcal{S}$-Graph in Fading

Fortunately, an accurate approximation[2] of such a distribution can nevertheless be derived as follows. First, ignoring the mild correlation amongst $\xi_{e:k}$'s and for given $m$ and $\sigma_e$, we obviously have

$$\min\{\xi_{e:1}, \xi_{e:2}, \cdots, \xi_{e:K}\} \leq \min\{\xi_{e:1}, \xi_{e:2}\}, \ \forall\ K \geq 2. \tag{4.3}$$

Relying on such a bounding approach, the first major problem – namely the randomness of $K$ – can be avoided. Recalling that $\xi_{e:1} \sim p_{\xi_e}(x; k, m, \sigma_e)$, with $p_{\xi_e}(x; k, m, \sigma_e)$ as given in Eq. (3.16), the exact distribution of $\min\{\xi_{e:1}, \xi_{e:2}\}$ can be obtained through the theory of ordered statistics [72, pp. 96, Eq. (5.2.1)] yielding

$$\begin{aligned} p_{\bar{\xi}_e}(x; m, \sigma_e) = p_{\xi_e}(x; 1, m, \sigma_e) + p_{\xi_e}(x; 2, m, \sigma_e) - P_{\xi_e}(x; 1, m, \sigma_e) \cdot p_{\xi_e}(x; 2, m, \sigma_e) \\ - P_{\xi_e}(x; 2, m, \sigma_e) \cdot p_{\xi_e}(x; 1, m, \sigma_e), \end{aligned} \tag{4.4}$$

where $P_{\xi_e}(x; k, m, \sigma_e)$ denotes the cumulative distribution corresponding to $p_{\xi_e}(x; k, m, \sigma_e)$, whose closed-form is given by [12, Eq. (6)]

$$P_{\xi_e}(x; 1, m, \sigma_e) = 1 - \left(\frac{\sigma_e}{x + \sigma_e}\right)^m, \tag{4.5}$$

$$P_{\xi_e}(x; 2, m, \sigma_e) = m\left(\frac{\sigma_e}{x + \sigma_e}\right)^{m+1} - (m+1)\left(\frac{\sigma_e}{x + \sigma_e}\right)^m + 1. \tag{4.6}$$

Secondly, we invoke the general result of extreme value theory [73], which determines that the minimum of a number of random variates is well modeled by one of the distributions of the Weibull family [72]. Consequently, we may fit a Weibull model to the exact distribution given in Eq. (4.4), that is

$$p_{\bar{\xi}_e}(x; \mu_e) \approx \frac{1}{\mu_e} e^{-x/\mu_e}, \tag{4.7}$$

where the parameter $\mu$ is the *average least path loss* at the eavesdroppers, *i.e.*, $\mu_e \triangleq \mathbb{E}[\bar{\xi}_e]$.

[2]The result (to follow soon) is an approximation because the slight correlation amongst path losses $\xi_{e:k}$'s will be ignored for mathematical tractability.

The expectation of $\bar{\xi}_e$ can be calculated from the definition and Eq. (4.4), yielding

$$\mathbb{E}[\bar{\xi}_e] \triangleq \int_0^\infty x \cdot p_{\bar{\xi}_e}(x;m,\sigma_e)\,\mathrm{d}x = \underbrace{\int_0^\infty x \cdot p_{\xi_e}(x;1,m,\sigma_e)\,\mathrm{d}x}_{I_5(\sigma_e;m)\big|_0^\infty} + \underbrace{\int_0^\infty x \cdot p_{\xi_e}(x;2,m,\sigma_e)\,\mathrm{d}x}_{I_6(\sigma_e;m)\big|_0^\infty} - \underbrace{\int_0^\infty x \cdot P_{\xi_e}(x;1,m,\sigma_e)\cdot p_{\xi_e}(x;2,m,\sigma_e)\,\mathrm{d}x}_{I_7(\sigma_e;m)\big|_0^\infty} - \underbrace{\int_0^\infty x P_{\xi_e}(x;2,m,\sigma_e)\cdot p_{\xi_e}(x;1,m,\sigma_e)\,\mathrm{d}x}_{I_8(\sigma_e;m)\big|_0^\infty}, \tag{4.8}$$

where the closed-form solutions of the integrals $I_5(\sigma_e;m)\big|_0^\infty$ and $I_6(\sigma_e;m)\big|_0^\infty$ exist and are respectively given by [68, pp. 27, Eq. (1.2.5.9) and Eq. (1.2.5.10)]

$$I_5(\sigma_e;m)\big|_0^\infty = m\,\sigma_e^m \int_0^\infty \frac{x}{(\sigma_e+x)^{m+1}}\,\mathrm{d}x = \frac{\sigma_e}{m-1}, \tag{4.9}$$

$$I_6(\sigma_e;m)\big|_0^\infty = m\,(m+1)\,\sigma_e^m \int_0^\infty \frac{x^2}{(\sigma_e+x)^{m+2}}\,\mathrm{d}x = \frac{2\sigma_e}{m-1}. \tag{4.10}$$

In order to find a solution for integral first rewrite $I_7(\sigma_e;m)\big|_0^\infty$ as

$$I_7(\sigma_e;m)\big|_0^\infty = m(m+1)\sigma_e^m \underbrace{\int_0^\infty \frac{x^2}{(\sigma_e+x)^{m+2}}\,\mathrm{d}x}_{I_{7A}(\sigma_e;m)\big|_0^\infty} - m(m+1)\sigma_e^{2m} \underbrace{\int_0^\infty \frac{x^2}{(\sigma_e+x)^{2m+2}}\,\mathrm{d}x}_{I_{7B}(\sigma_e;m)\big|_0^\infty}, \tag{4.11}$$

Identifying that $I_{7A}(\sigma_e;m)\big|_0^\infty$ and $I_{7B}(\sigma_e;m)\big|_0^\infty$ are particular cases of [68, pp. 27, Eq. (1.2.5.10)]

$$I_{7A}(\sigma_e;m)\big|_0^\infty = \frac{1}{(m-1)\sigma_e^{m-1}} - \frac{2}{m\sigma_e^{m-1}} + \frac{1}{(m+1)\sigma_e^{m-1}}, \tag{4.12}$$

$$I_{7B}(\sigma_e;m)\big|_0^\infty = \frac{1}{(2m-1)\sigma_e^{2m-1}} - \frac{1}{m\sigma_e^{2m-1}} + \frac{1}{(2m+1)\sigma_e^{2m-1}}, \tag{4.13}$$

we obtain

$$I_7(\sigma_e;m)\big|_0^\infty = \frac{\sigma_e(7m^2-1)}{(m-1)(2m-1)(2m+1)}. \tag{4.14}$$

Likewise, $I_8(\sigma_e;m)\big|_0^\infty$ can be rewritten as

$$I_8(\sigma_e;m)\big|_0^\infty = \underbrace{\int_0^\infty \frac{m^2\sigma_e^{2m+1}x}{(\sigma_e+x)^{2m+2}}\,\mathrm{d}x}_{I_{8A}(\sigma_e;m)\big|_0^\infty} - \underbrace{\int_0^\infty \frac{m(m+1)\sigma_e^{2m}x}{(\sigma_e+x)^{2m+1}}\,\mathrm{d}x}_{I_{8B}(\sigma_e;m)\big|_0^\infty} + \underbrace{m\sigma_e^m \int_0^\infty \frac{x}{(\sigma_e+x)^{m+1}}\,\mathrm{d}x}_{I_{8C}(\sigma_e;m)\big|_0^\infty}, \tag{4.15}$$

where [68, pp. 27, Eq. (1.2.5.9)]

$$I_{8A}(\sigma_e;m)\big|_0^\infty = \frac{1}{2m\sigma_e^{2m}} - \frac{1}{(2m+1)\sigma_e^{2m}}, \tag{4.16}$$

$$I_{8B}(\sigma_e;m)\big|_0^\infty = \frac{1}{(2m-1)\sigma_e^{2m-1}} - \frac{1}{2m\sigma_e^{2m-1}}, \tag{4.17}$$

$$I_{8C}(\sigma_e;m)\big|_0^\infty = \frac{1}{m(m-1)\sigma_e^{m-1}}, \tag{4.18}$$

which yields

$$I_8(\sigma_e;m)\big|_0^\infty = \frac{\sigma_e(4m^2+3m-1)}{2(m-1)(2m-1)(2m+1)}. \tag{4.19}$$

Finally, combining equations (4.8) to (4.19), we obtain

$$\mu_e = \mathbb{E}[\bar{\xi}_e] \leq \frac{3\sigma_e}{(4m-2)}, \tag{4.20}$$

where the inequality sign indicates that, in deriving Eq. (4.20), the correlation between $\xi_{e:1}$ and $\xi_{e:2}$ was ignored, which implies that the result is a *lower bound* on the true value of $\mathbb{E}[\min\{\xi_{e:1},\xi_{e:2}\}]$.

Recall also the correlation between $\xi_{e:1}$ and $\xi_{e:2}$ originates from the ordination of the two eavesdroppers according to their distances to the source [12]. While such distances scale with the density of eavesdroppers, captured by $\sigma_e$, the scaling factor is obviously the same for the closer and farther eavesdroppers. The same argument holds in supporting the fact that fading does not affect the looseness of the bound shown in equation (4.20).

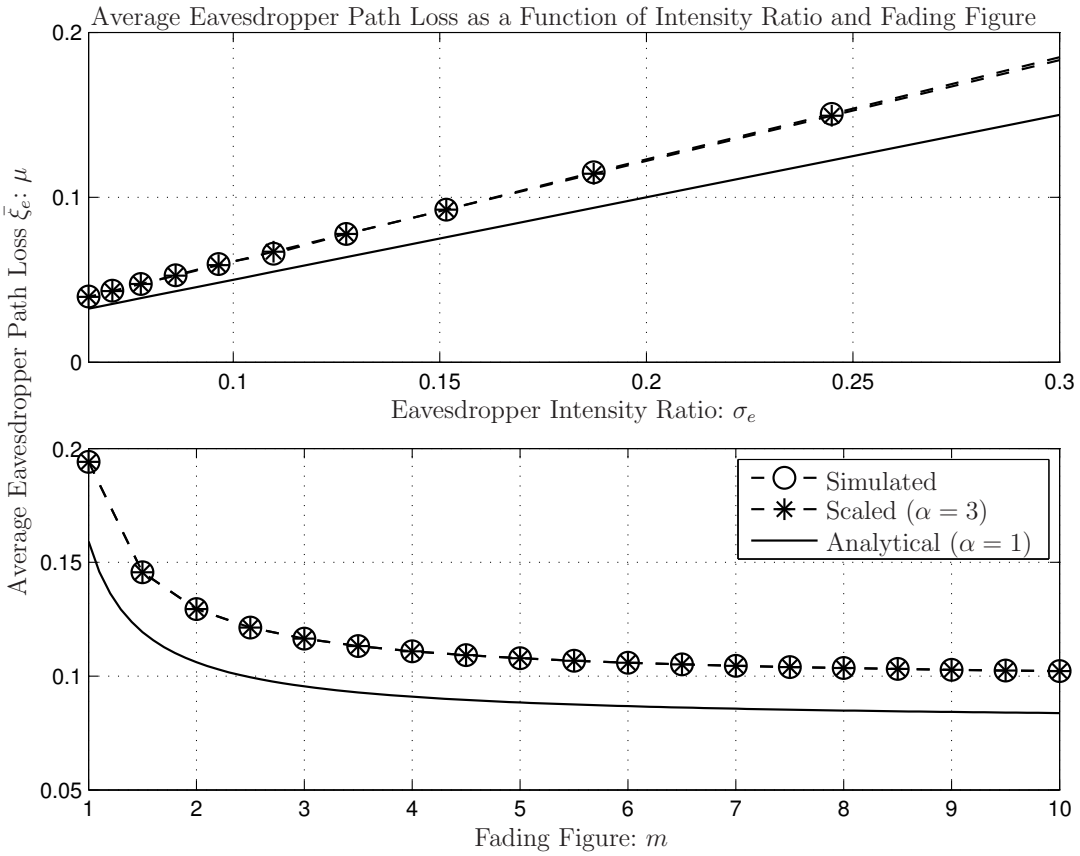



Figure 4.2: Average eavesdropper path loss as a function of intensity ratio and $m$.

Consequently, it is expected that the error between $\mu_e$ as obtained from Eq. (4.20) and the true value of $\mathbb{E}[\min\{\xi_{e:1}, \xi_{e:2}\}]$ is *independent* of $\sigma_e$ or $m$. In other words, we may write

$$\mu_e = \alpha \frac{3\sigma_e}{(4m-2)}, \tag{4.21}$$

where $\alpha$ is a scaling factor *constant* with respect to $\sigma_e$ and $m$.

This fact is indeed corroborated by the results shown in Fig. 4.2, where a plot of Eq. (4.20) is compared against the empirical evaluations of $\mathbb{E}[\min\{\xi_{e:1}, \xi_{e:2}\}]$ obtained via simulation, overlaid with a fitted version of Eq. (4.21). From such fitting we obtain the scaling factor $\alpha = 6/5$, thus

$$\mu_e \approx \frac{18\sigma_e}{5(4m-2)}. \tag{4.22}$$

Using Eq. (4.7), we finally obtain the following exponential model for the distribution of $\bar{\xi}_e$

$$p_{\bar{\xi}_e}(x; m, \sigma_e) = \frac{5(4m-2)}{18\sigma_e} e^{-\frac{5(4m-2)x}{18\sigma_e}}, \tag{4.23}$$

Figures 4.3 and 4.4 illustrate the accuracy of the above model. In Fig. 4.3, the empirical distributions obtained with $K = 2$ and $K = 6$ are shown to be nearly identical and be equally well fitted to Eq. (4.23). In turn, Fig. 4.4 which depicts the Kullback-Leibler divergence between Eq. (4.23) and empirical distributions obtained for various values of $K$ and $m$, which we denote $D_\Delta(i, m, \sigma_e)$, demonstrates that the accuracy of the model in fact improves with $K$ and $m$.

Using the latter model for $p_{\bar{\xi}_e}(x; m, \sigma_e)$, the distribution of the path loss difference $\Delta$ becomes

$$\begin{aligned}
p_\Delta(x; k, m, \sigma_e, \sigma_\ell) &= \int_{-x}^{\infty} p_{\bar{\xi}_e}(\tau; m, \sigma_e) \cdot p_\xi(x+\tau; k, m, \sigma_\ell)\, \mathrm{d}\tau, \qquad (4.24)\\
&\xrightarrow[\text{Eq.(3.16) into (4.7)}]{} \frac{5A_\ell(4m-2)}{18\sigma_e} \int_{-x}^{\infty} \frac{e^{-\frac{5(4m-2)\tau}{18\sigma_e}} (x+\tau)^{k-1}}{(\sigma_\ell + x + \tau)^{m+i}}\, \mathrm{d}\tau,\\
&\xrightarrow[z \triangleq x+\tau]{} \frac{5A_\ell(4m-2)}{18\sigma_e} \int_{0}^{\infty} e^{-\frac{5(4m-2)(z-x)}{18\sigma_e}} \frac{z^{k-1}}{(\sigma_\ell + z)^{m+k}}\, \mathrm{d}z,\\
&\xrightarrow[y \triangleq 1+\frac{z}{\sigma_\ell}]{} \frac{5m(4m-2)}{18\sigma_e} \binom{m+k-1}{m} e^{\frac{5(4m-2)(\sigma_\ell+x)}{18\sigma_e}} \int_{1}^{\infty} \frac{e^{-\frac{5(4m-2)y}{18\varrho}} (y-1)^{k-1}}{y^{m+i}}\, \mathrm{d}y.
\end{aligned}$$

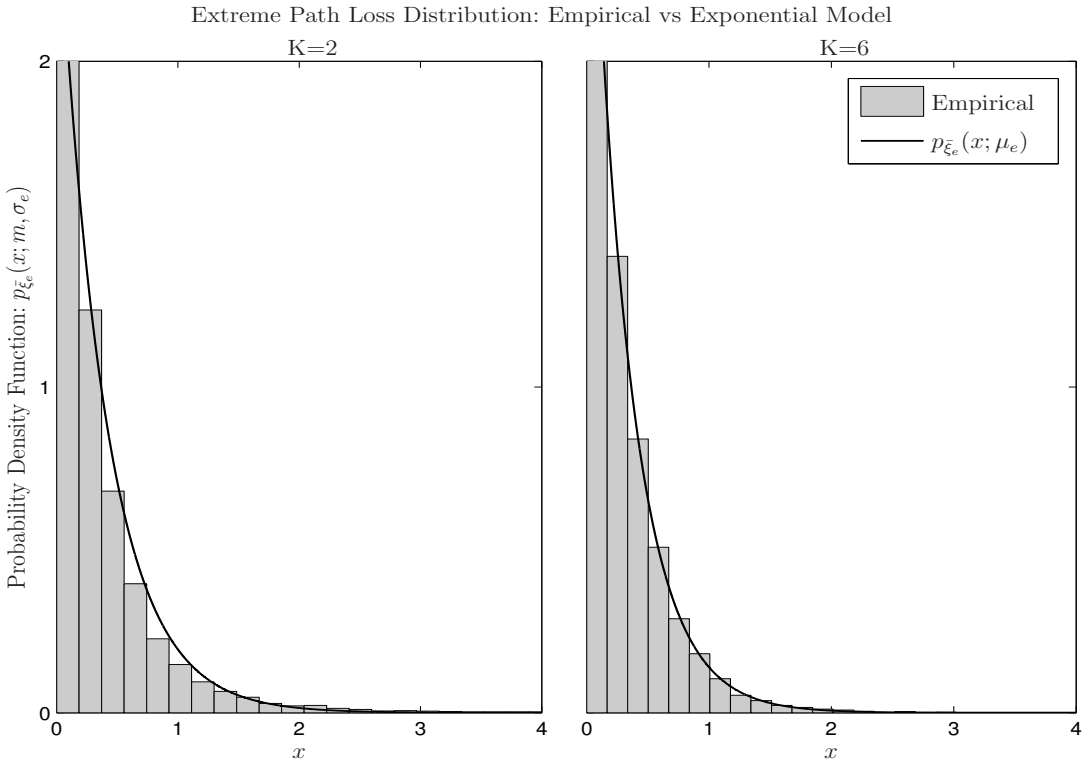
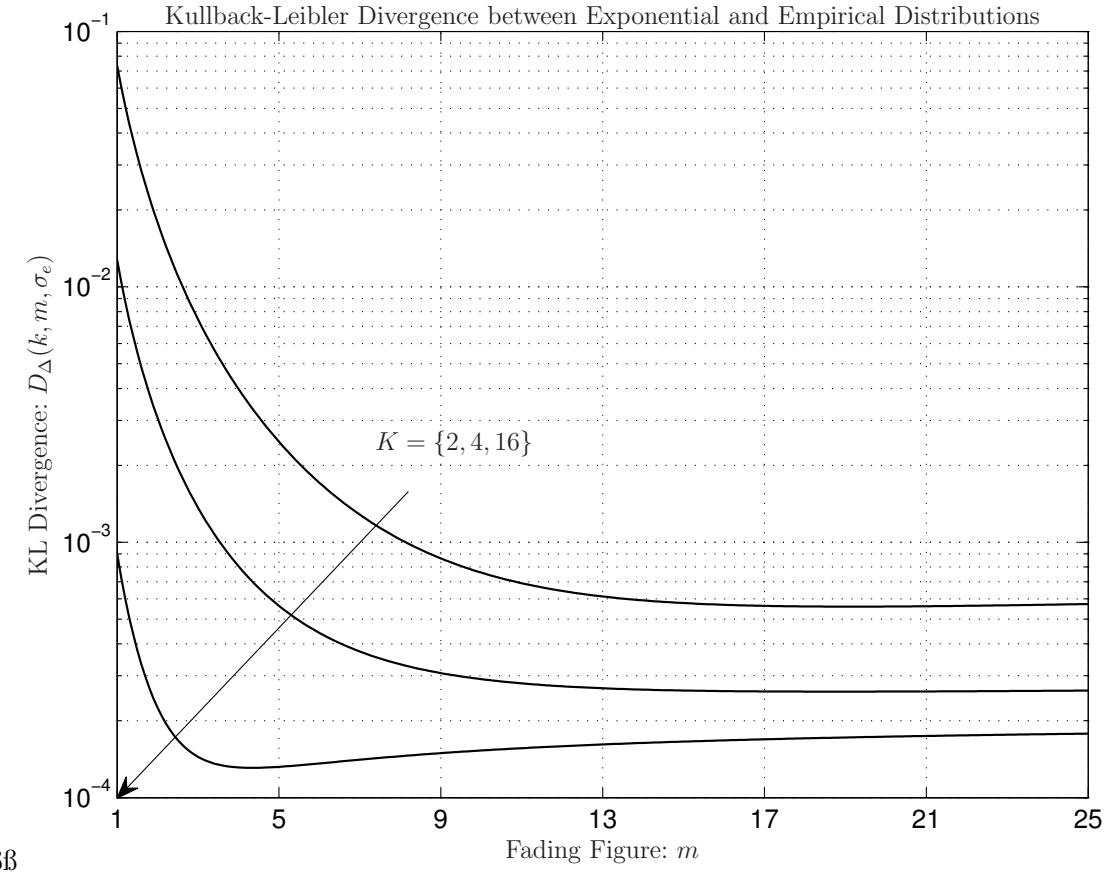



Figure 4.3: Illustration of the accuracy of the exponential model for the extreme path loss distribution with various $K$'s.




ßß

Figure 4.4: Kullback-Leibler divergence between exponential distribution and its empirical distributions as a function of $m$ and for various $K$'s.

Expanding the term $(y-1)^{k-1}$ and invoking the Binomial Theorem, we obtain

$$p_{\Delta}(x;k,\sigma_{\ell},\sigma_e)=\frac{5m(4m-2)}{18\sigma_e}\binom{m+k-1}{m}\times \sum_{j=0}^{k-1}(-1)^j\binom{k-1}{j}e^{\frac{5(4m-2)(\sigma_{\ell}+x)}{18\sigma_e}}\int_1^{\infty}\frac{e^{-\frac{5(4m-2)\sigma_{\ell}y}{18\sigma_e}}}{y^{j+m+1}}\,\mathrm{d}y, \tag{4.25}$$

where the last integral is a generalized Exponential Integral $E_{\nu}(x)$ [74, pp. 228, Eq. (5.1.4)].

Integrating $p_{\Delta}(x;k,m,\sigma_e,\sigma_{\ell})$, we obtain the probability that a non-zero secrecy capacity between the source and the $k$-th node exists (in the presence of a randomly located multiple eavesdroppers), namely

$$p_{\text{Naka:Multi}}(k,m,\varrho)=\int_{-\infty}^{0}p_{\Delta}(x;k,m,\sigma_{\ell},\sigma_e)\,\mathrm{d}x= \tag{4.26}$$

$$\frac{5m(4m-2)}{18\sigma_e}\binom{m+k-1}{m}\sum_{j=0}^{k-1}(-1)^j\binom{k-1}{j}e^{\frac{5(4m-2)}{18\varrho}}E_{m+j+1}\left(\tfrac{5(4m-2)}{18\varrho}\right)\underbrace{\int_{-\infty}^{0}e^{\frac{5(4m-2)x}{18\sigma_e}}\,\mathrm{d}x}_{=\frac{18\sigma_e}{5(4m-2)}}=$$

$$m\binom{m+k-1}{m}\sum_{j=0}^{k-1}(-1)^j\binom{i-1}{j}e^{\frac{5(4m-2)}{18\varrho}}E_{m+j+1}\left(\tfrac{5(4m-2)}{18\varrho}\right),$$

where we have slightly extended the notation in order to highlight the fact that the result is obtained under the assumption that multiple eavesdroppers may be present.

The term $e^{\frac{5(4m-2)}{18\varrho}}E_{m+j+1}\left(\frac{5(4m-2)}{18\varrho}\right)$ appearing in Eq. (4.26) can be accurately bounded by very simple rational functions, specifically [74, pp. 229, Eq. (5.1.19)]

$$\frac{1}{m+j+\frac{5(4m-2)}{18\varrho}+1}\leq e^{\frac{5(4m-2)}{18\varrho}}E_{m+j+1}\left(\tfrac{5(4m-2)}{18\varrho}\right)\leq\frac{1}{m+j+\frac{5(4m-2)}{18\varrho}}. \tag{4.27}$$

Replacing the latter bounds into Eq. (4.26), and using the relation [68, pp.498, Eq. (4.2.2.44)]

$$\sum_{j=0}^{n} \frac{(-1)^j}{j+\beta}\binom{n}{j} = \frac{1}{\beta}\binom{n+\beta}{n}^{-1}, \tag{4.28}$$

we obtain the bounds

$$p_{\text{Naka:Multi}}(k,m,\varrho) \;\leq\; \frac{m\binom{m+k-1}{m}}{(m+\frac{5(4m-2)}{18\varrho})\binom{m+\frac{5(4m-2)}{18\varrho}+k-1}{k-1}}, \tag{4.29a}$$

$$p_{\text{Naka:Multi}}(k,m,\varrho) \;\geq\; \frac{m\binom{m+k-1}{m}}{(m+\frac{5(4m-2)}{18\varrho}+1)\binom{m+\frac{5(4m-2)}{18\varrho}+k}{k-1}}, \tag{4.29b}$$

which after further simplification reduce to

$$p_{\text{Naka:Multi}}(k,m,\varrho) \leq \underbrace{\prod_{k=0}^{k-1} \frac{m+k}{m+\frac{5(4m-2)}{18\varrho}+k}}_{p^{U}_{\text{Naka:Multi}}(k,m,\varrho)}, \tag{4.30a}$$

$$p_{\text{Naka:Multi}}(k,m,\varrho) \geq \underbrace{\prod_{k=0}^{k-1} \frac{m+k}{m+\frac{5(4m-2)}{18\varrho}+k+1}}_{p^{L}_{\text{Naka:Multi}}(k,m,\varrho)}. \tag{4.30b}$$

The above bounds can also be shown to be accurate by means of their divergence with respect to the exact solution (4.26). To this end, let us denote the Kullback-Leibler Divergence [75] between Eq. (4.26) and the bounds offered in (4.30a) and (4.30b), respectively, by $D^{U}_{\text{Naka:Multi}}(k,m,\varrho)$ and $D^{L}_{\text{Naka:Multi}}(k,m,\varrho)$. Plots of these functions are shown in Fig. 4.5, which clearly shows that the upper bound is generally tighter than the lower bound, but that for the large values of fading figure $m$ both bounds are equivalent.

A comparison of the probability of non-zero secrecy capacity under Rayleigh fading with multiple eavesdroppers as predicted by Eq. (4.26), against the $\Pr\{\mathcal{C}_{s:k} > 0\}$ in AWGN according to Eq. (3.2) is shown in Fig. 4.6. It is found that, like in the case of a single eavesdropper, fading favors the unicast channels, since the curves for $\Pr\{\mathcal{C}_{s:k} > 0\}$ under fading approach that for the AWGN case from below. We omit further plots, but similar results are found also for $\varrho > 1$.

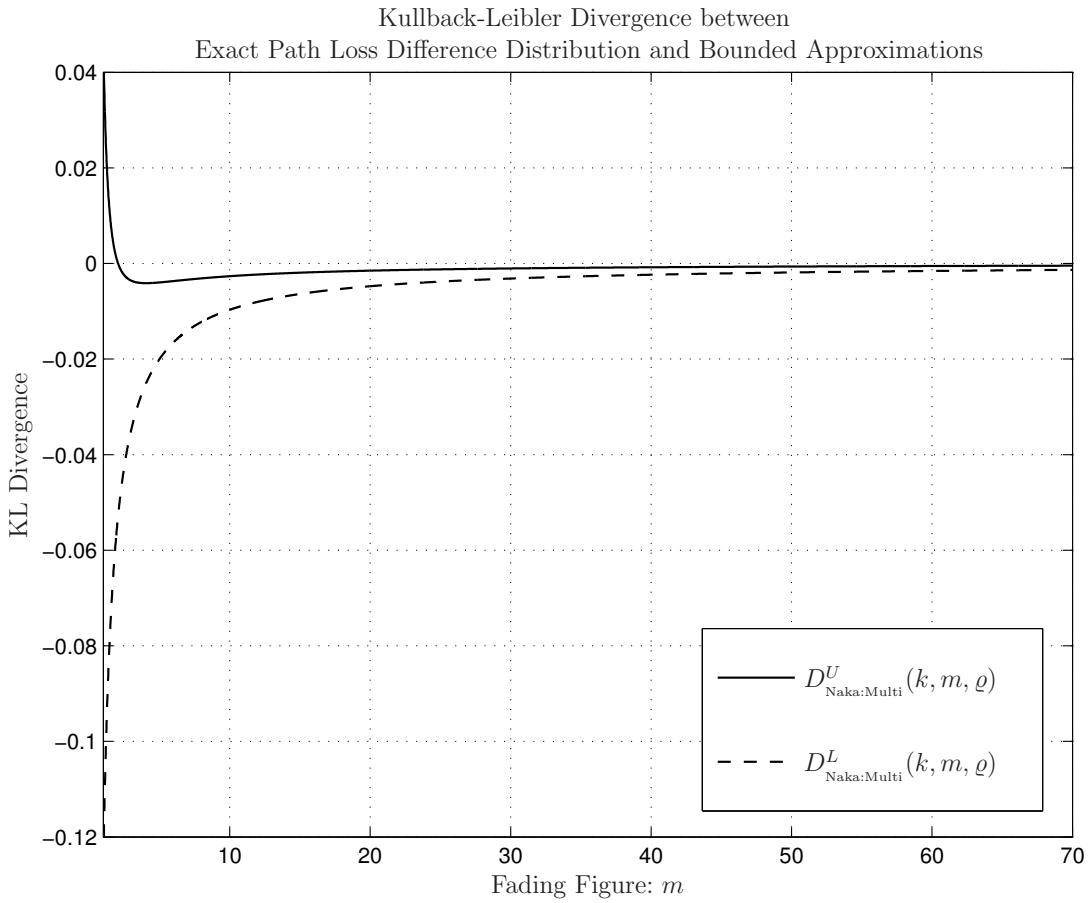



Figure 4.5: Kullback-Leibler divergence between exponential distribution and its empirical distributions as a function of $m$ and for various $K$'s.

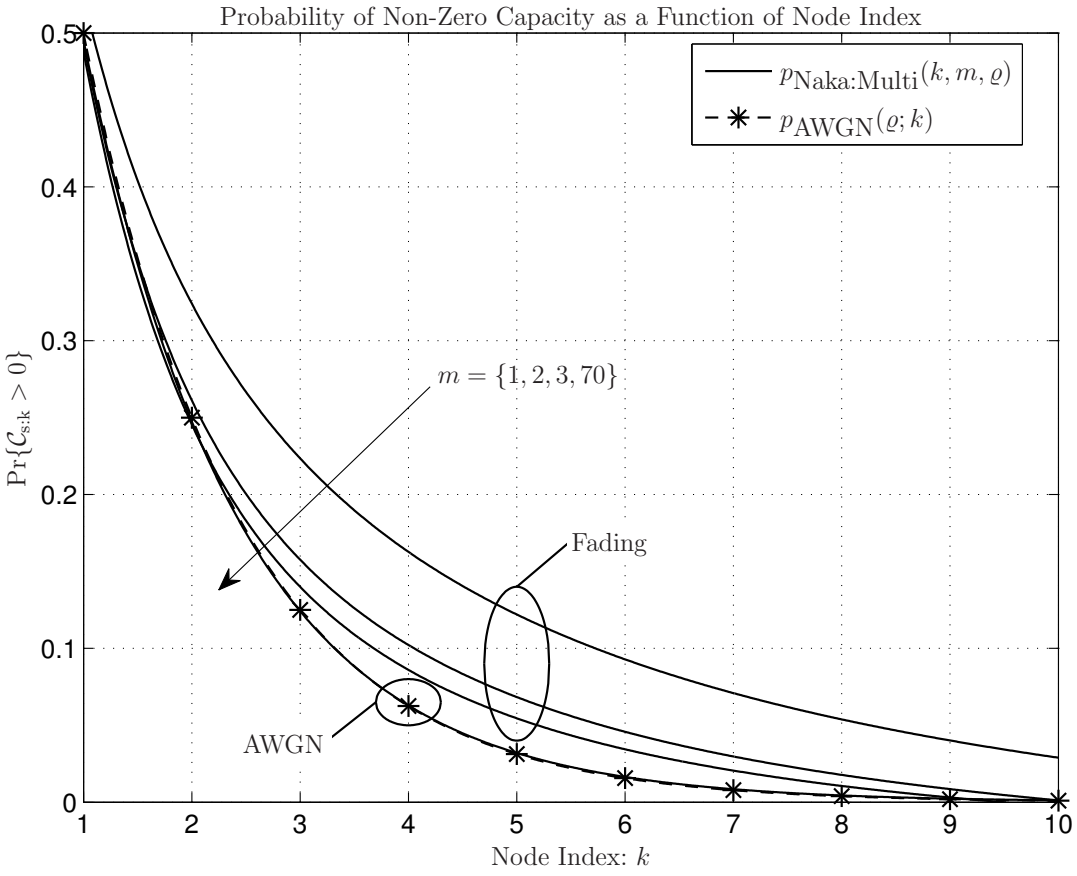



Figure 4.6: Effect of distance (node index) onto $\Pr\{\mathcal{C}_{s:k} > 0\}$ in the case of unitary relative intensity ratio ($\varrho$=1).

It has be shown [9] that in the wire-tap channel – which can be considered as special case of Scenario 2 – the probability $\Pr\{\mathcal{C}_{s:k} > 0\}$ can be improved in an *average* sense by quasi-static fading. In comparison to that result, the analysis presented above offers evidence that such an improvement is also theoretically possible under more relaxed assumptions, specifically, without the quasi-stationarity condition, despite of knowledge on the location of the eavesdropper, and even if more than one eavesdroppers are present.

## 4.3 Nakagami Fading Case: Approach 2

Our interest is to characterize the secrecy outage of the ordered (*i.e.*, uniquely identified) nodes, the distributions of interest concerning the legitimate network are those corresponding to the path gains of each $k$-th node – hereafter denoted $\zeta_k$.

**Path Gain Distributions of the $k$-th Legitimate Node**

A geometry-inclusive fading model for wireless networks, where distance and fading uncertainties are combined was developed in [12], where for the case of channels with a path loss exponent $\alpha = 2$, the distribution of the *path loss* associated with random pairs of a Poisson network subjected to Nakagami-$m$ fading, namely $\xi \triangleq r^2/|h|^2$, was derived. In light of secrecy capacity formulation, however, it will prove convenient to work instead with the distribution of the corresponding *path gains*. To this end, recall that [12]

$$\psi \sim |h|^2 \sim f(x;m) \triangleq \frac{m^m x^{m-1} e^{-mx}}{\Gamma(m)}, \tag{4.31}$$

$$r_k^2 \sim q(x;k,\lambda) \triangleq e^{-\pi\lambda x}\frac{(\pi\lambda x)^k}{x\Gamma(k)}, \tag{4.32}$$

which straightforwardly yields

$$\begin{aligned} p_{\zeta_k}(x;k,m,\lambda) = \int_0^\infty f(xy;m)\cdot q(y;k,\lambda)\,\mathrm{d}y &= \frac{m^m(\pi\lambda)^k}{\Gamma(m)\Gamma(k)}\int_0^\infty (xy)^{m-1}e^{-mxy}y^k e^{-\pi\lambda y}\,\mathrm{d}y, \\ &= \frac{\Gamma(m+k)m^m(\pi\lambda)^k(x)^{m-1}}{\Gamma(m)\Gamma(k)(mx+\pi\lambda)^{m+k}}. \end{aligned} \tag{4.33}$$

From equation (4.33), the distribution of the path gain to the $k$-th closest legitimate node is given by

$$p_{\zeta_k}(x;k,m,\eta_\ell) = A(k;m,\eta_\ell)\cdot\frac{x^{m-1}}{(\eta_\ell\, x+1)^{m+k}}, \tag{4.34}$$

where the auxiliary function $A(k;m,\eta)$ is defined as

$$A(k;m,\eta) \triangleq \frac{\Gamma(m+k)\eta^m}{\Gamma(m)\Gamma(k)}, \tag{4.35}$$

while $\eta_\ell$ is the *intensity ratio* of the *legitimate network*, so denominated in allusion to its absorbing two the *fading intensity* $m$ and the *intensity* of the Poisson point process $\lambda$ into a single quantity, namely

$$\eta \triangleq m/(\lambda\pi). \tag{4.36}$$

In consistence with the above-introduced notation, the intensity ratio of the *eavesdropping network* will be henceforth denoted by $\eta_{\mathrm{e}}$.

***Path Gain Distribution of "Best" Eavesdropper***

Fortunately an accurate approximation[3] of such a distribution can nevertheless be derived as follows. First, ignoring the mild correlation amongst $\zeta_{\mathrm{e}:k}$'s we have

$$\bar{\zeta}_{\mathrm{e}} \leq \frac{\max\{\psi_1,\psi_2\cdots\psi_K\}}{\min\{\xi_1,\xi_2\cdots\xi_K\}}, \tag{4.37}$$

where, $\psi_k$ and $\xi_k$ follow a Nakagami-$m$ fading model and the pathloss model given in [12], respectively.

One difficulty in evaluating the bound in inequality (4.37) is to determine a reasonable range for the Poisson variate $K$. Indeed, since all $\psi_k$'s are equivalent and independent, while $\xi_k$'s are statistically increasing, the maximum eavesdropper path gain $\bar{\zeta}_{\mathrm{e}}$ must converge. In other words, it is to be expected that a sufficiently large $K$ can be taken beyond which the likelihood that $\zeta_{\mathrm{e}:K} > \zeta_{\mathrm{e}:k=\{1,\cdots,K-1\}}$ vanishes.

In contrast, for a given legitimate path gain $\zeta_{\ell:k}$ what determines the secrecy capacity of a channel subjected to fading is not any specific eavesdropper, but rather the

[3]The result to be given soon is an approximation due to the fact that the path gains $\zeta_{\mathrm{e}:k}$'s are also correlated (albeit only slightly so), which will be ignored for analytical purposes.

eavesdropper with the *maximum*[4] (instantaneous) path gain amongst those present. Consequently, concerning the eavesdropping network and assuming that the communicating pair is exposed to an *unknown* number $K$ of eavesdroppers, the distribution of interest is an *extreme value distribution*, namely, the statistics of the quantity

$$\bar{\zeta}_{\mathrm{e}} \triangleq \max\{\zeta_{\mathrm{e}:1}, \cdots, \zeta_{\mathrm{e}:K}\}. \tag{4.38}$$

We will henceforth refer to the eavesdropper whose path gain is largest, such that $\zeta_{\mathrm{e}} = \bar{\zeta}_{\mathrm{e}}$, as the "*best*" eavesdropper. Let us also remark that the subindex $K$ is not added to the notation of $\bar{\zeta}_{\mathrm{e}}$ in anticipation to the fact that best eavesdropper path gain will be found not to depend strongly on $K$.

Deriving the distribution of $\bar{\zeta}_{\mathrm{e}}$ directly from equations (4.38) and (4.34) is, however, a formidable task since the number of eavesdroppers $K$ is *random* and *unknown*, and the path gains $\zeta_{\mathrm{e}:k}$'s are *non-identically* distributed variates. Indeed, to the best of our knowledge, von Mises-like conditions [72] to determine the domain of attraction of an extreme value distribution of a random set of non-identical variates does not exist.

We are therefore interested a sufficiently large $K$ such that

$$P(1;K) \cap P(2;K) \cdots P(K-1;K) \leq \varepsilon, \tag{4.39}$$

where the quantity $\varepsilon$ is chosen to be $\ll 1$ and we have implicitly defined,

$$\begin{aligned} P(k;K) &\triangleq \Pr\{\zeta_{\mathrm{e}:K} > \zeta_{\mathrm{e}:k}\} \\ &= \int_0^\infty p_{\zeta_{\mathrm{e}:k}}(x;k,m,\eta_{\mathrm{e}}) \underbrace{\int_x^\infty p_{\zeta_{\mathrm{e}:K}}(z;K,m,\eta_{\mathrm{e}})\, \mathrm{d}z}_{I_1(z;K,m,\eta_{\mathrm{e}})\big|_x^\infty}\, \mathrm{d}x. \end{aligned} \tag{4.40}$$

The indefinite form of the integral $I_1(z;K,m,\eta_\ell)$ appearing in Eq. (4.40) evaluates to [68, pp.30, Eq. (1.2.5.5)]

$$I_1(z;K,m,\eta_{\mathrm{e}}) = \frac{A(K;m,\eta_{\mathrm{e}})}{\eta_{\mathrm{e}}^{m+K}} \sum_{j=0}^{m-1} \binom{m-1}{j} \frac{(-1)^j \left(x+\frac{1}{\eta_{\mathrm{e}}}\right)^{-(K+j)}}{\eta_{\mathrm{e}}^j (K+j)}.$$

[4]It is here implicitly assumed that eavesdroppers do *not* form collusions. The case with collusion will be discussed in next chapter.

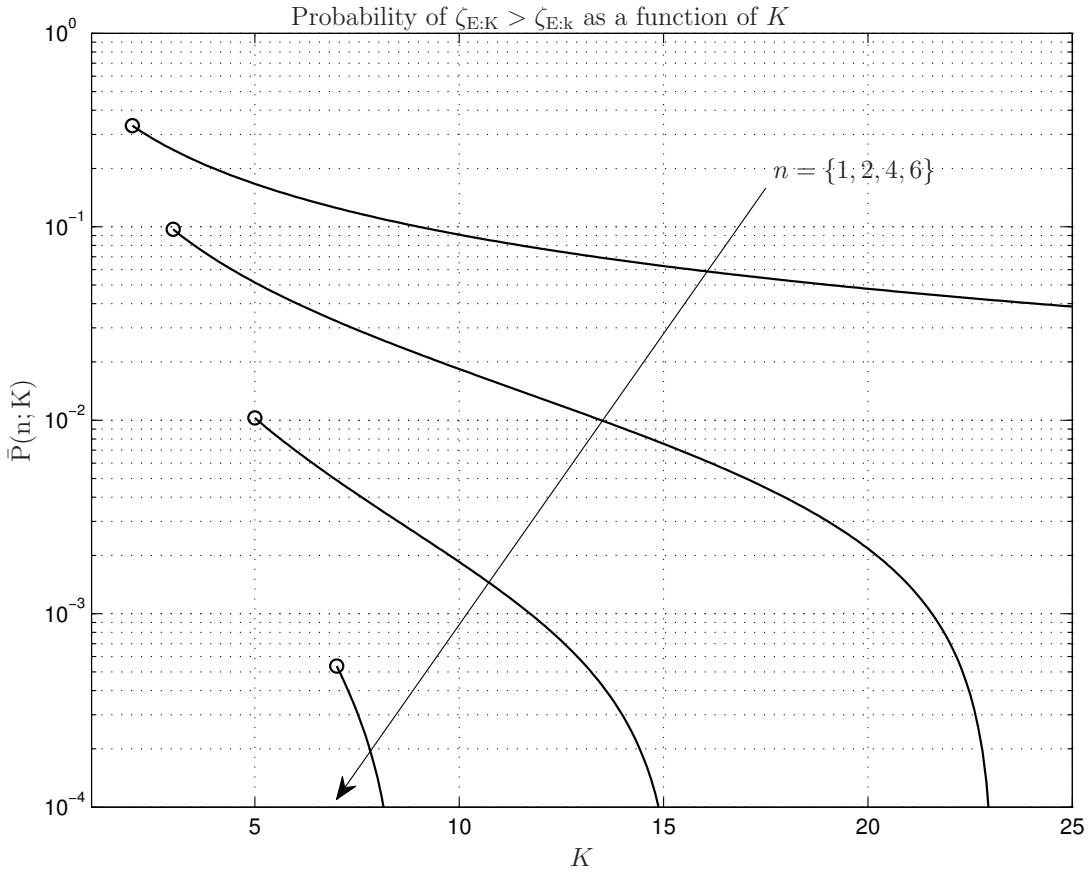



Figure 4.7: Probability that the furthest $K$-th eavesdropper has the largest path gain than all other $K - 1$ eavesdroppers.

Therefore,

$$P(k;K) = \frac{A(K;m,\eta_{\mathrm{e}})\Gamma(m+k)}{\Gamma(m)\Gamma(k)} \sum_{j=0}^{m-1} \binom{m-1}{j} \tfrac{(-1)^j}{(K+j)} \int_0^{\infty} \frac{x^{m-1}{\eta_{\mathrm{e}}}^{-(m+k+K+j)}}{(x+\frac{1}{\eta_{\mathrm{e}}})^{m+k+K+j}}. \quad (4.41)$$

The last integral finally simplifies to [68, pp.30, Eq. (1.2.5.30)]

$$P(k;K) = \frac{\Gamma(m+k)\Gamma(m+K)}{\Gamma(m)\Gamma(k)\Gamma(m)\Gamma(K)} \sum_{j=0}^{m-1} \tfrac{(-1)^j}{K+j} \sum_{t=0}^{m-1} \binom{m-1}{t} \tfrac{(-1)^t}{k+K+j+t}. \quad (4.42)$$

From equations (4.39) and (4.42) the range of values of $\varepsilon$ can be determined. Specifically, recognize that $P(K-1;K) > P(K-2;K) > \cdots$ and let us define a truncation of the product on the lefthand side of inequality (4.39)

$$\bar{P}(n;K) \triangleq \prod_{k=1}^{n} P(K-n;K), \quad n \leq K-1. \quad (4.43)$$

Clearly the function $\bar{P}(n;K)$ is strictly and fast descending, as illustrated in Fig. 4.7, such that the largest possible value of $\varepsilon$ is given by $\bar{P}(1;K) = P(K-1;K)$. But since $P(K-1;K)$ is also fast decreasing, it follows that the likelihood that the furthest amongst $K$ eavesdroppers has the largest path gain becomes negligible even for a relatively small $K$. For instance, according to Fig. 4.7 it is found that $\varepsilon < 0.0001$ for $K = 10$. Hereafter we will therefore take $K = 10$.

With an adequate truncation of the sets $\{\psi_1, \psi_2 \cdots \psi_K\}$ and $\{\xi_1, \xi_2 \cdots \xi_K\}$ well defined, we may proceed to compute the numerator of the ratio in Eq. (4.37). Assuming that $\psi_k$'s are independently and identically distributed [12] with CDF and PDF is given by

$$F(x;m) = \frac{\gamma(m,mx)}{\Gamma(m)}, \quad (4.44)$$

$$f(x;m) = \frac{m^m x^{m-1} e^{-mx}}{\Gamma(m)}. \quad (4.45)$$

The von-Mises condition [76], [72] associated with the quantity $\bar{\psi} \triangleq \max\{\psi_1, \psi_2 \cdots \psi_K\}$ are then

$$\lim_{x\to\infty} \frac{d}{dx}\left[\frac{1-F(x;m)}{f(x;m)}\right] = 0, \tag{4.46}$$

which indicates that $\bar{\psi}$ follows a Gumbel Distribution with parametes

$$\mu = F^{-1}(1-\tfrac{1}{K}), \tag{4.47}$$

$$\sigma = F^{-1}(1-\tfrac{1}{Ke}) - \mu. \tag{4.48}$$

Explicitly,

$$\bar{\psi} \sim \mathrm{Pr}_{\bar{\psi}}(x;\mu,\sigma) \triangleq \frac{1}{\sigma} e^{\left(-e^{-\frac{x-\mu}{\sigma}} - \frac{x-\mu}{\sigma}\right)}. \tag{4.49}$$

The accuracy of the Gumbel model of equation (4.49) is illustrated in Fig. 4.8 by comparison with the empirical distribution obtained with $K = 10$.

Finally, returning to inequality (4.37) and recalling that the path losses $\xi_k$ are ordered, it follows that $\bar{\xi} = \xi_1$, such that the distribution of the denominator is given in Eq. (4.32), with $k = 1$.

We now define for our analysis $\tau \triangleq \mu/\sigma$, where $\mu$ and $\sigma$ vary from 1 to 2 and from 0.1 to 1 respectively, while $m$ goes from 0.5 to 100 and $K = 10$.

From the above, the CDF and PDF of $\bar{\zeta}_{\mathrm{e}}$ can now be computed, yielding respectively

$$P_{\bar{\zeta}_{\mathrm{e}}}(x;\lambda,\mu,\sigma) = \int_0^\infty q(z;1,\lambda) F_{\bar{\psi}}(zx;\mu,\sigma)\mathrm{d}x = \pi\lambda \int_0^\infty \frac{e^{-e^{-\frac{(zx-\mu)}{\sigma}}}}{e^{\pi\lambda z}}\mathrm{d}z, \tag{4.50}$$

$$\xrightarrow[t\triangleq e^{-\frac{(zx-\mu)}{\sigma}}]{} \frac{\pi\lambda\sigma}{x} e^{-\frac{\pi\lambda\mu}{x}} \int_0^{e^\tau} \frac{e^{\frac{\pi\lambda\sigma\log(t)-t}{x}}}{t}\mathrm{d}t = \frac{\pi\lambda\sigma}{x} e^{-\frac{\pi\lambda\mu}{x}} \gamma(\tfrac{\pi\lambda\sigma}{x}, e^\tau),$$

and

$$p_{\bar{\zeta}_{\mathrm{e}}}(x;\lambda,\mu,\sigma) = \frac{(\pi\lambda\mu - x)}{x^2} P_{\bar{\zeta}_{\mathrm{e}}}(x;\lambda,\mu,\sigma) + \underbrace{\frac{\pi\lambda\sigma}{x} e^{-\frac{\pi\lambda\mu}{x}} \gamma'(\tfrac{\pi\lambda\sigma}{x}, e^\tau)}_{H(x;\lambda,\mu,\sigma)}. \tag{4.51}$$

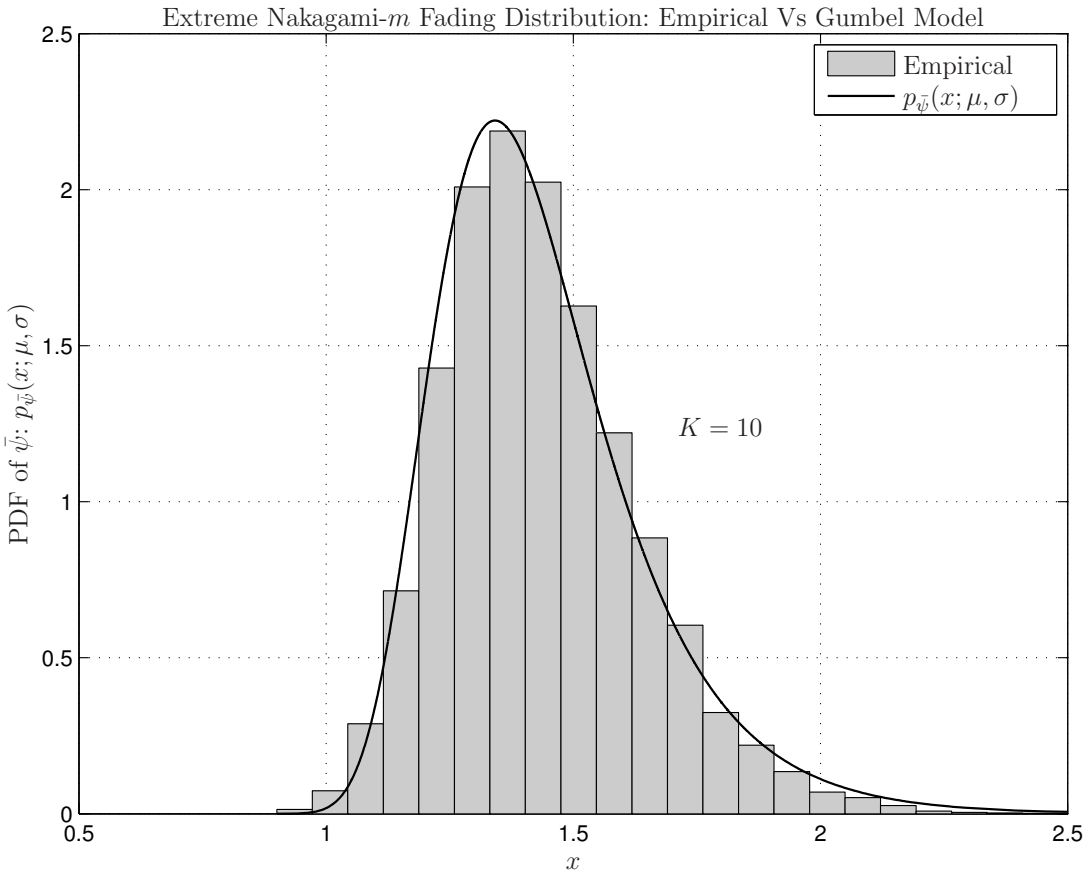



Figure 4.8: Illustration of the accuracy of the gumbel model for the extreme nakagami-$m$ distribution for a given $K$.

**Simplified Path Gain Distribution of "Best" Eavesdropper**

Due to the presence of the lower incomplete gamma and its derivative, the best eavesdropper path gain distribution given by Eq. (4.51) is hard to manipulate. It will prove convenient, therefore, to replace this function by a simpler model. To this end, we invoke the general result of extreme value theory [73], which determines that the maximum of a number of random variates can be well approximated one of the distributions of the generalized extreme value family [72].

We seek therefore to find a two-parameter Generalized Extreme value (GEV) approximation of $p_{\bar{\zeta}_\mathrm{e}}(x;\lambda,\mu,\sigma)$ in the form

$$p_{\bar{\zeta}_\mathrm{e}}(x;\nu,\theta) \approx \frac{1}{\theta}\left(\tfrac{x-\nu+\theta}{\theta}\right)^{-2} e^{-\left(\frac{x-\nu+\theta}{\theta}\right)^{-1}}, \tag{4.52}$$

where the parameters $\nu$ and $\theta$ are the location and scale parameters, respectively.
The above GEV model can parameterized using the median and mode of our earlier result given in Eq. (4.51). Specifically, the median is given by

$$\mathrm{med}(\bar{\zeta}_\mathrm{e}) \triangleq P^{-1}_{\bar{\zeta}_\mathrm{e}}(1/2), \tag{4.53}$$

while the mode can be calculated from

$$\mathrm{mod}(\bar{\zeta}_\mathrm{e}) \triangleq \left\{ x \;\middle|\; \frac{\mathrm{d}}{\mathrm{d}x} p_{\bar{\zeta}_\mathrm{e}}(x;\lambda,\mu,\sigma) = 0 \right\}. \tag{4.54}$$

Differentiating $p_{\bar{\zeta}_\mathrm{e}}(x;\lambda,\mu,\sigma)$ yields

$$\begin{aligned} p'_{\bar{\zeta}_\mathrm{e}}(x;\lambda,\mu,\sigma) &= \frac{(\pi\lambda\mu - x)}{x^2} p_{\bar{\zeta}_\mathrm{e}}(x;\lambda,\mu,\sigma) + H'(x;\lambda,\mu,\sigma) - \frac{(2\pi\lambda\mu - z)}{x^3} P_{\bar{\zeta}_\mathrm{e}}(x;\lambda,\mu,\sigma), \\ &= \frac{(\pi\lambda\mu - x)}{x^2} p_{\bar{\zeta}_\mathrm{e}}(x;\lambda,\mu,\sigma) - \frac{(2\pi\lambda\mu - x)}{x^3} P_{\bar{\zeta}_\mathrm{e}}(x;\lambda,\mu,\sigma) + \\ &\qquad \frac{(\pi\lambda\mu - x)}{x^2} H(x;\lambda,\mu,\sigma) + \frac{\pi\lambda\sigma}{x} e^{-\frac{\pi\lambda\mu}{x}} \gamma''(\tfrac{\pi\lambda\sigma}{x}, e^\tau). \end{aligned} \tag{4.55}$$

Equating to zero and simplifying gives

$$\begin{aligned} 0 \;&= \frac{(\pi\lambda\mu - x)}{x^2}\left( -\frac{\gamma(\frac{\pi\lambda\sigma}{x}, e^\tau)}{x} + \frac{\pi\lambda\mu}{x^2}\gamma(\tfrac{\pi\lambda\sigma}{x}, e^\tau)) \right) - \\ &\frac{(2\pi\lambda\mu - x)}{x^3}\gamma(\tfrac{\pi\lambda\sigma}{x}, e^\tau) + \frac{(\pi\lambda\mu - x)}{x^2}\gamma'(\tfrac{\pi\lambda\sigma}{x}, e^\tau) + \frac{(\pi\lambda\mu - x)}{x^2}\gamma'(\tfrac{\pi\lambda\sigma}{x}, e^\tau) + \gamma''(\tfrac{\pi\lambda\sigma}{x}, e^\tau), \\ &= \frac{\gamma''(\frac{\pi\lambda\sigma}{x}, e^\tau)}{\gamma(\frac{\pi\lambda\sigma}{x}, e^\tau)} x^4 - \frac{2\gamma'(\frac{\pi\lambda\sigma}{x}, e^\tau)}{\gamma(\frac{\pi\lambda\sigma}{x}, e^\tau)} x^3 + \left( 2 + \frac{2\pi\lambda\mu\gamma'(\frac{\pi\lambda\sigma}{x}, e^\tau)}{\gamma(\frac{\pi\lambda\sigma}{x}, e^\tau)} \right) x^2 - (4\pi\lambda\mu)x + (\pi\lambda\mu)^2. \end{aligned} \tag{4.56}$$

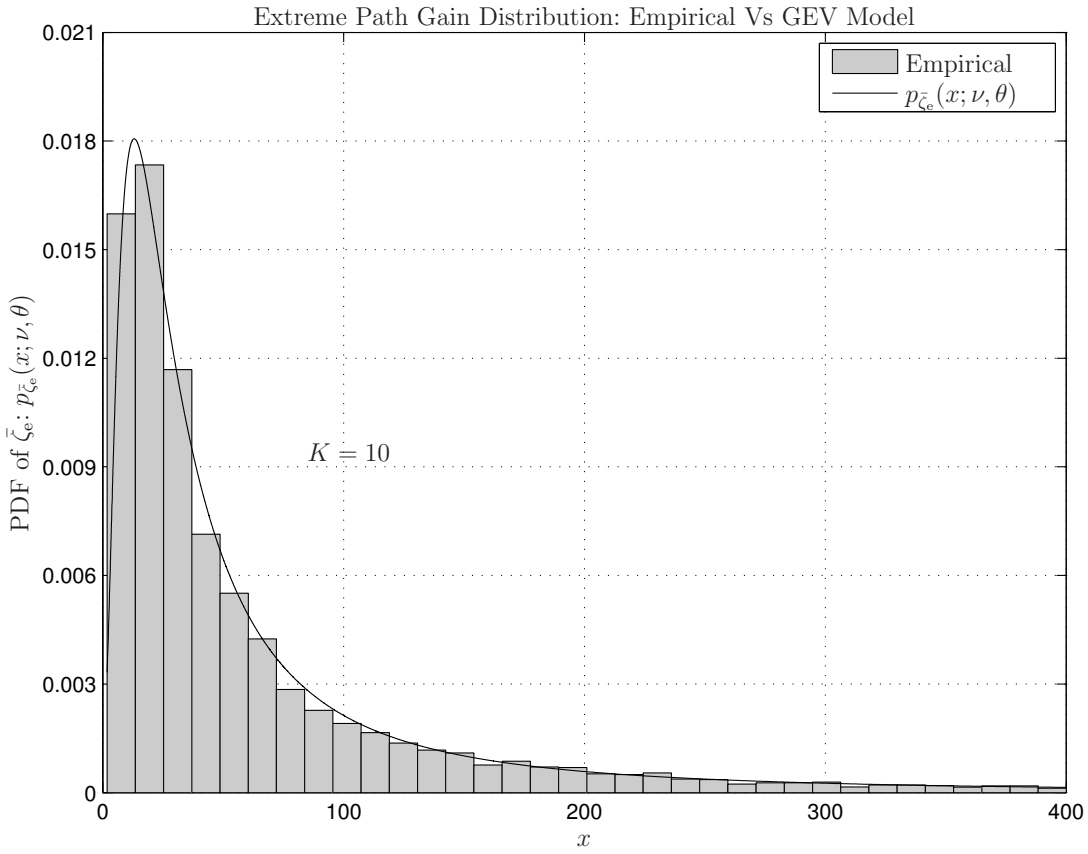



Figure 4.9: Illustration of the accuracy of the GEV model for the extreme path gain distribution for a given $K$.

Solving the above equation numerically, $\mathrm{mod}(\bar{\zeta}_{\mathrm{e}})$ can be calculated, such that the GEV model can be parameterized using

$$\theta = \frac{\mathrm{med}(\bar{\zeta}_{\mathrm{e}}) - \mathrm{mod}(\bar{\zeta}_{\mathrm{e}})}{(2 - \ln 2)} \ln 4, \tag{4.57}$$

$$\nu = \mathrm{med}(\bar{\zeta}_{\mathrm{e}}) + \tfrac{\theta}{2}. \tag{4.58}$$

The accuracy of the GEV model is illustrated in Fig. 4.9 via comparison with an empirical distribution obtained with $K = 10$.

With possession of accurate models for the distributions of the numerator and denominator of the ration in inequality (4.37), the secrecy non-outage probability between the source and $k$-th node (in the presence of a randomly located multiple eavesdroppers) can be calculated.

Referring back to Eq. (3.14), defining the function $\beta(\kappa) \triangleq 2^{R_s}(\rho^{-1} + \kappa) - \rho^{-1}$ and replacing $\zeta_{\mathrm{e}}$ with $\bar{\zeta}_{\mathrm{e}}$ we obtain

$$\begin{aligned} \tilde{\mathcal{P}}_{\mathrm{out}}(R_s) &= \Pr\left\{\zeta_k > \beta(\bar{\zeta}_{\mathrm{e}})\right\}, \\ &= \int_0^{\infty} p_{\bar{\zeta}_{\mathrm{e}}}(x;\nu,\theta) \cdot \Bigg( \underbrace{\int_{\beta(x)}^{\infty} p_{\zeta_k}(z;k,m,\eta_\ell)\,\mathrm{d}z}_{I_1(z;k,m,\eta_\ell)\big|_{\beta(x)}^{\infty}} \Bigg) \mathrm{d}x, \end{aligned} \tag{4.59}$$

where, the indefinite form of the integral $I_1(z;k,m,\eta_\ell)$ evaluates to [68, pp.30, Eq. (1.2.5.5)]

$$I_1(z;k,m,\eta_\ell) = \frac{A(k;m,\eta_\ell)}{\eta_\ell^{m+k}} \sum_{j=0}^{m-1} \binom{m-1}{j} \frac{\left[\beta(x)+\frac{1}{\eta_\ell}\right]^{-(k+j)}}{(k+j)(-\eta_\ell)^j}. \tag{4.60}$$

Therefore, by defining $\varpi \triangleq (2^{R_s}(\nu-\theta+\rho^{-1})-\rho^{-1}+\frac{1}{\eta_\ell})$, the following equation is obtained by straightforward calculation from (4.59)

$$\tilde{\mathcal{P}}_{\text{out}}(R_s) = \frac{A(k;m,\eta_\ell)}{\theta\eta_\ell^{m+k}} \sum_{j=0}^{m-1} \binom{m-1}{j} \frac{(-\frac{1}{\eta_\ell})^j}{(k+j)} \int_0^\infty \frac{\left(\frac{x-\nu+\theta}{\theta}\right)^{-2} e^{-\left(\frac{x-\nu+\theta}{\theta}\right)^{-1}}}{\left[\beta(x)+\frac{1}{\eta_\ell}\right]^{(k+j)}} \,\mathrm{d}x, \tag{4.61}$$

$$\xrightarrow[t\triangleq\frac{\theta}{x-\nu+\theta}]{} \frac{A(k;m,\eta_\ell)}{\theta\eta_\ell^{m+k}} \sum_{j=0}^{m-1} \binom{m-1}{j} \frac{(-\frac{1}{\eta_\ell})^j}{(k+j)} \times \int_0^{\frac{\theta}{\theta-\nu}} \frac{e^{-t}}{\left[2^{R_s}\theta + t\underbrace{(2^{R_s}(\nu-\theta+\rho^{-1})-\rho^{-1}+\frac{1}{\eta_\ell})}_{\varpi}\right]^{(k+j)}} \,\mathrm{d}t,$$

$$\xrightarrow[y\triangleq 2^{R_s}\theta+t\varpi]{} \frac{A(k;m,\eta_\ell)}{\theta\eta_\ell^{m+k}} \sum_{j=0}^{m-1} \binom{m-1}{j} \frac{(-\frac{1}{\eta_\ell})^j e^{\frac{2^{R_s}\theta}{\varpi}}}{\varpi^{k+j+1}(k+j)} \int_{2^{R_s}\theta}^{2^{R_s}\theta+\varpi\frac{\theta}{\theta-\nu}} \frac{e^{-\frac{y}{\varpi}}(y-2^{R_s}\theta)^{k+j}}{y^{k+j}} \,\mathrm{d}y,$$

$$= \frac{A(k;m,\eta_\ell)}{\theta\eta_\ell^{m+k}} \sum_{j=0}^{m-1} \binom{m-1}{j} \frac{(-\frac{1}{\eta_\ell})^j e^{\frac{2^{R_s}\theta}{\varpi}}}{\varpi^{k+j+1}(k+j)} \sum_{t=0}^{m-1} \binom{k+j}{t} (-2^{R_s}\theta)^t \int_{2^{R_s}\theta}^{2^{R_s}\theta+\varpi\frac{\theta}{\theta-\nu}} \frac{e^{-\frac{y}{\varpi}}}{y^t} \,\mathrm{d}y,$$

$$= \frac{A(k;m,\eta_\ell)}{\theta\eta_\ell^{m+k}} e^{\frac{2^{R_s}\theta}{\varpi}} \sum_{j=0}^{m-1} \binom{m-1}{j} \frac{(-\frac{1}{\eta_\ell})^j}{\varpi^{k+j+1}(k+j)} \sum_{t=0}^{k+j} \binom{k+j}{t} (-2^{R_s}\theta)^t \times \left[(2^{R_s}\theta)^{1-t} E_t(\tfrac{2^{R_s}\theta}{\varpi}) - (2^{R_s}\theta+\varpi\tfrac{\theta}{\theta-\nu})^{1-t} E_t(\tfrac{2^{R_s}\theta}{\varpi}+\tfrac{\theta}{\theta-\nu})\right].$$

Finally, the secrecy outage probability can be obtained by substituting Eq. (4.61) into Eq. (3.14). Plots of the secrecy outage obtained with the above expressions are shown in Figures 4.10 and 4.11. The results in Fig. 4.10 are somewhat intuitive. Namely, Fig. 4.10 indicates that it is hard to ensure a low secrecy outage for nodes further from the source and for high rates. The results in Fig. 4.11, however, are less intuitive, as the achievable secrecy non-outage is largely independent on the reference SNR $\rho$, *even for a fixed rate*! Since $\rho$ is fundamentally controlled by the source's transmit power, the conclusion is that at least to the closest source, it is possible to communicate secretly in the presence of a numerous, and unknown number of eavesdroppers, using very low power (for instance half the power of background noise).

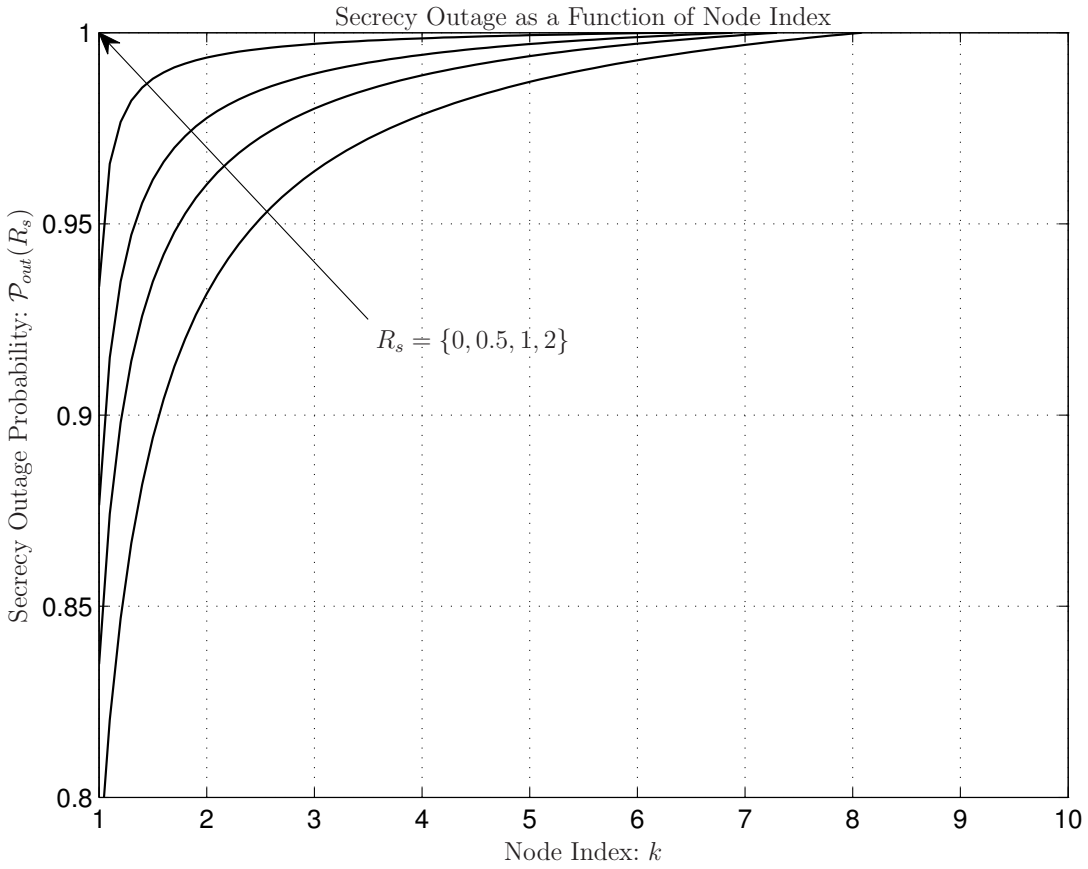



Figure 4.10: Secrecy outage as a function of node index in the case of Rayleigh fading ($m = 1$) and for various rates, with unitary reference SNR ($\rho = 1$).

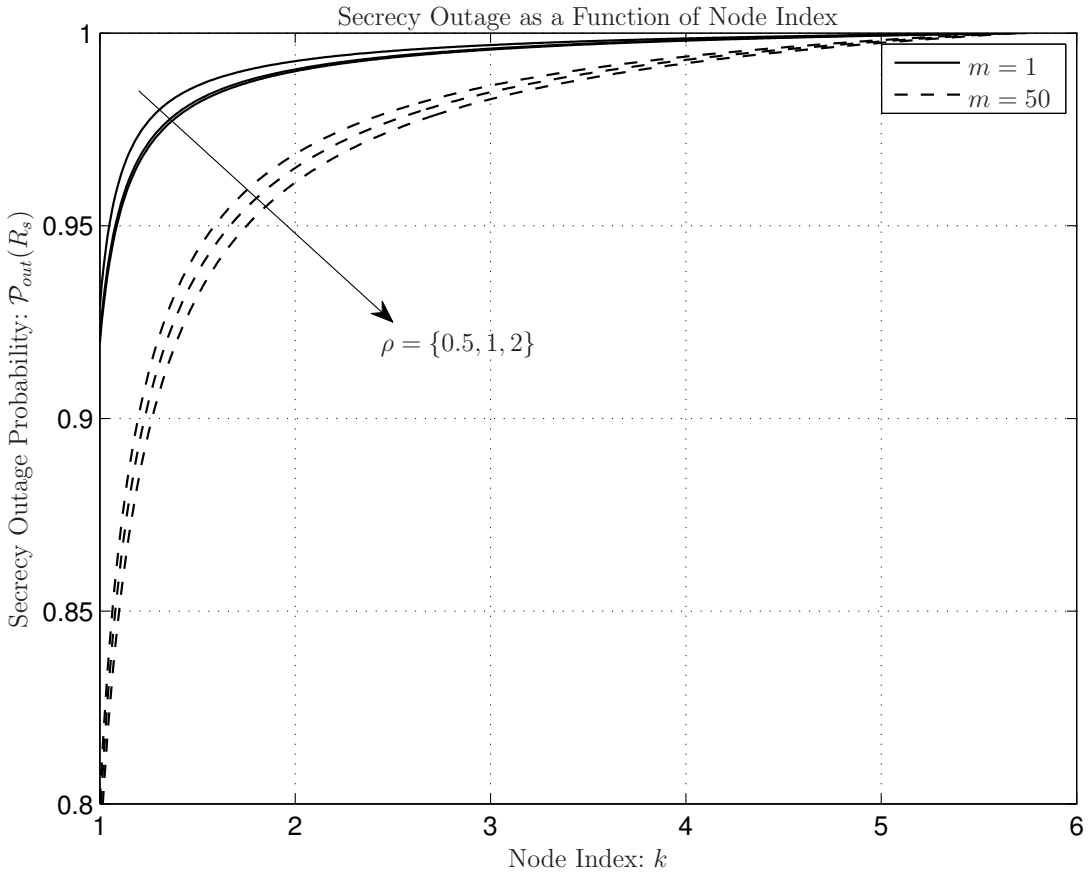



Figure 4.11: Secrecy outage as a function of node index and for various reference SNR's ($\rho = \{0.5, 1, 5, 25\}$), with unitary rate ($R_s = 1$).

## 4.4 Many Eavesdroppers and Legitimate nodes

Let us consider the case where the source is able to identify which of its neighbors has the best path loss as depicted in Fig. 4.12, subsequently unicasting to that node. This case relates to the scenario studied in [9,10], in the sense that the selection of the device with the "best channel" can either occur in terms of the "best node" at a given time thanks to the quasi-stationarity of the channel – as assumed in [9] – or in terms of the "best time" – as assumed in [10].

In the context of our analytical framework, this assumption implies that secrecy capacity of unicast channel in question is governed by the statistics of the *minimum* path loss amongst the present. In other words, the unicast channel will experience non zero secrecy capacity iff

$$\Delta \triangleq \min\{\xi_1, \cdots, \xi_K\} - \min\{\xi_{e:1}, \cdots, \xi_{e:K}\} = \bar{\xi}_\ell - \bar{\xi}_e \leq 0, \tag{4.62}$$

where we have implicitly defined $\bar{\xi}_\ell \triangleq \min\{\xi_{\ell:1}, \cdots, \xi_{\ell:K_\ell}\}$.

The distribution of above the path loss difference $\Delta$ then becomes

$$\begin{aligned} p_\Delta(x; m, \sigma_e, \sigma_\ell) &= \int_{-x}^{\infty} p_{\bar{\xi}_e}(\tau; \sigma_e) \cdot p_{\bar{\xi}_\ell}(x+\tau; \sigma_\ell)\, \mathrm{d}\tau, \\ &\xrightarrow[\text{subst. eq. (4.23)}]{} \frac{25(4m-2)^2}{324\sigma_e\sigma_\ell} e^{-\frac{5x(4m-2)}{18\sigma_\ell}} \int_{-x}^{\infty} e^{-\frac{5\tau(4m-2)(\sigma_e+\sigma_\ell)}{18\sigma_e\sigma_\ell}}\, \mathrm{d}\tau, \\ &= \frac{5(4m-2)}{18(\sigma_e+\sigma_\ell)} e^{\frac{5x(4m-2)}{18\sigma_e}}, \end{aligned} \tag{4.63}$$

where the $\bar{\xi}_\ell$ is distributed according to the Eq. (4.23), only with $\sigma_\ell$ replacing $\sigma_e$, as can be shown via steps identical to those used to derive the distribution of $\bar{\xi}_e$.
Finally, the probability that a non-zero secrecy capacity between the source and the *best* node exists (in the presence of a randomly located multiple eavesdroppers) is given by

$$p_{\text{Naka:Multi}}(\varrho) = \int_{-\infty}^{0} p_\Delta(x; m, \sigma_e, \sigma_\ell)\, \mathrm{d}x = \frac{5(4m-2)}{18(\sigma_e+\sigma_\ell)} \underbrace{\int_{-\infty}^{0} e^{\frac{5(4m-2)x}{18\sigma_e}}\, \mathrm{d}x}_{=\frac{18\sigma_e}{5(4m-2)}} = \frac{\sigma_e}{\sigma_e+\sigma_\ell} = \frac{\varrho}{\varrho+1}. \tag{4.64}$$

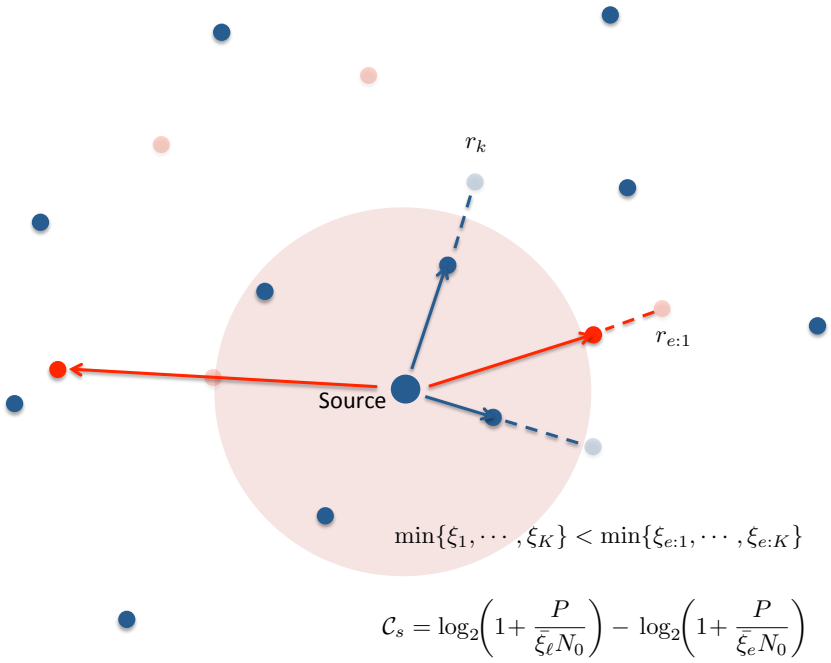



Figure 4.12: Regular secrecy neighborhoods

Notice that the expression given in Eq. (4.64) is precisely the same as the probability of non-zero capacity found for the *nearest* node in the AWGN channel [29], which is particularly interesting since the result is *independent* of the fading figure $m$. The result that $\Pr\{\mathcal{C}_{s:k} > 0\}$ is *independent* of the fading figure $m$ is intuitively acceptable for $k = 1$ (nearest node), since in the AWGN channel the best node is always the nearest.

We have, however, also consistently verified empirically that in fact the expression $\left(\frac{\varrho}{\varrho+1}\right)^k$ accurately describes the non-zero secrecy capacity probability to the $k$-th best node in the presence of *any* fading channel[5]. This results from the fact that the expression

$$p_{\Delta}(x; k, m, \sigma_e, \sigma_\ell) = \frac{5(4m-2)}{18(\sigma_e + \sigma_\ell)} \left(\frac{\varrho}{\varrho+1}\right)^{k-1} \cdot e^{\frac{5x(4m-2)}{18\sigma_e}}, \tag{4.65}$$

turns out to be a very accurate (if heuristic) generalization of Eq. (4.63) to the case when the unicast link in question is the one to the $k$-th best legitimate node. The accuracy of Eq. (4.65) is illustrated in Fig. 4.13, once again relying on the Kullback-Leibler divergence between the expression and corresponding empirical distributions, denoted $D_{\Delta:\text{Multi}}(k, m, \sigma_e, \sigma_\ell)$. In addition to the empirically observed accuracy, this "*conjecture*" is strengthened by the fact that it is in line with the previous finding that the *out degree* of an $\mathcal{S}$-graph is fading invariant [14].

## 4.5 Conclusions

In this chapter, we derived the original expressions for the secrecy outage of unicast channels in random networks in presence of randomly located eavesdroppers under Nakagami-$m$ fading. In particular, we conducted a detailed analysis of the impact of Nakagami-$m$ block fading and of the density of legitimate nodes relative to that of eavesdroppers, including the derivation of expressions for the case when an unknown number of eavesdroppers are present.

[5]This can be easily observed empirically, but hard to prove rigorously due to the difficulty in deriving the distributions of the $k$-th best path losses.

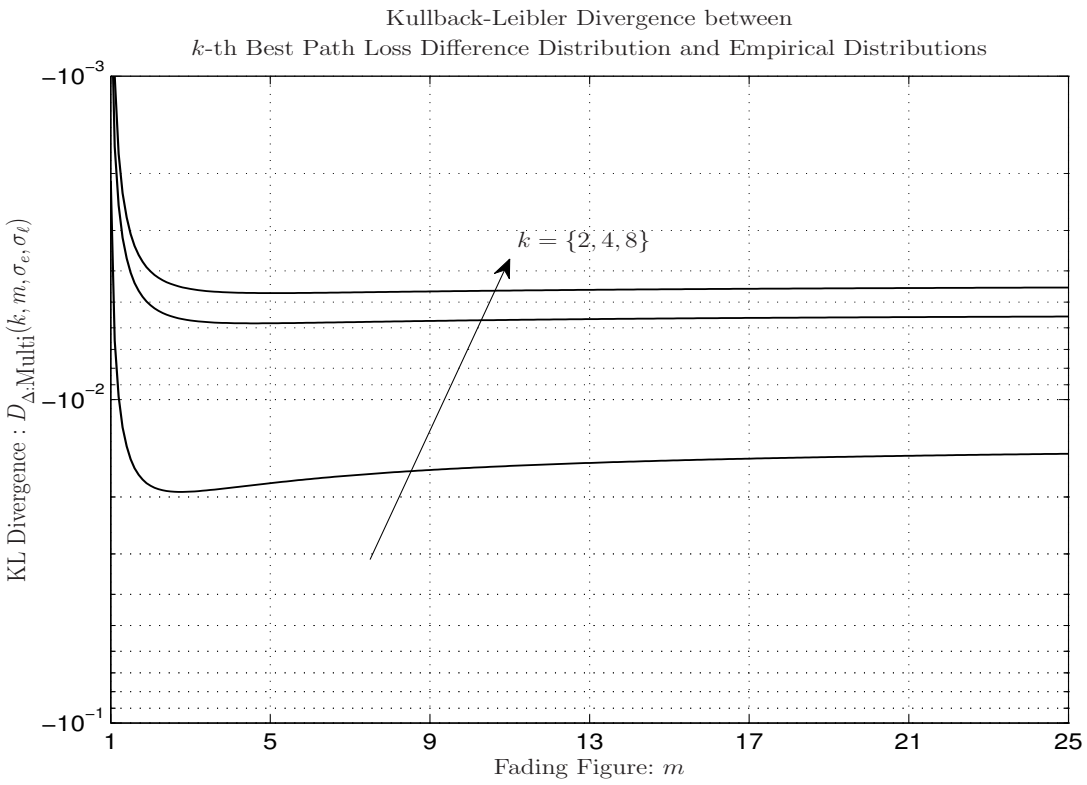



Figure 4.13: Kullback-Leibler Divergence between $k$-th best node path loss difference distribution and its empirical distributions as function of $m$.

The results indicate that depending on those conditions, fading may result in an increase in the probability of a non-zero secrecy capacity of unicast channels, compared to that available under AWGN. The results corroborate and extend the findings in related articles such as [12, 14, 29].

An interesting outcome of the analysis is that the uncertainty on the number of eavesdropper does not play a significant role. Another interesting result is that under the aforementioned conditions, secret communication at a given rate is possible (albeit subjected to outage), with very low transmit power. Specifically, it is found that the secrecy outage is not strongly dependent on the source's transmit power. We recently accomplished all these results in [19, 20].

- Derived the expression of probability of non-zero secrecy outage of unicast channel in presence of multiple eavesdroppers under Nakagami-$m$ fading channel.
- Obtained the best path gain distribution of eavesdroppers and consequently we compute probability of non-zero secrecy capacity of unicast channels in presence of multiple eavesdroppers under Nakagami-$m$ fading channel [19, 20].
- Derived the probability that a non-zero secrecy capacity between the source and the *best* node exists (in the presence of a randomly located multiple eavesdroppers) [19].

# Chapter 5

# Correlation and Collusion

**Summary:**

*In this chapter, we derive the asymptotic (high SNR ratio) expressions for the secrecy outage probability of random networks under correlated Nakagami-m fading channels. Numerical results show that correlated fading has an important effect on security, which may be either beneficial or harmful, depending on the secrecy outage constraints. The aggregate eavesdroppers' path gain is modeled and consequently secrecy outage probability under collusion of eavesdroppers is derived.*

Reprinted from Proc. Asilomar Conference on Signals, Systems and Computers, Satyanarayana Vuppala, Giuseppe Abreu, Secrecy transmission capacity of random networks, pp 743-747, Copyright (2013), with permission IEEE.

## 5.1 Introduction

In Chapter 3 and 4, we have investigated the secrecy capacity of unicast channels under different scenarios of randomly located eavesdroppers. We obtained closed-form solutions in terms of the location of legitimate nodes relative to eavesdroppers, the number of eavesdroppers, and the impact of Nakagami-$m$ block fading.

In those and other similar works, however, secrecy metrics (*e.g.*, capacity, transmission capacity and outage) were calculated under the assumptions that the legitimate and eavesdropping channels are mutually *independent* and without considering the collusion among eavesdroppers. One hand, *channel correlation* is frequently observed in practical wireless environments due to the unavailability of line-of-sight paths, poor scattering, and proximity between legitimate receivers and eavesdroppers. The previous works where the impact of correlation in the secrecy of random networks is comparatively small, but the issue has not entirely escaped the attention of the community. For instance, the secrecy capacity and secrecy outage capacity of point-to-point system subjected to correlated fading channels were studied in [77] and [78], respectively.

In this chapter, we contribute to this discussion by deriving asymptotic (high signal-to-noise ratio) expressions for the secrecy outage probability of random networks under correlated Nakagami-$m$ fading channels. Our findings indicate that correlation acts non-uniformly, increasing secrecy rate when secrecy outage is larger than 50%, but reducing secrecy rate when secrecy outage is less than 50%.

On the other hand, *cooperation* among the legitimate and eavesdropper nodes is certain to play a role, one of recent works on the role of cooperation in network secrecy is worthy of mention [79]. We consider the case that if cooperation is an important part of the system used by legitimate nodes to communicate, it must be assumed that the same strategy will be exploited by intruders as well. Indeed, it can be said that ignoring cooperation amongst eavesdroppers when addressing the question of achievable secrecy outage and average secrecy capacity of random networks is contradictory to Wyner's original notion of "wire tapping".

Optimal cooperation amongst eavesdroppers is referred to as collusion, since that in light of the secrecy capacity expression given by Eq. (3.1), the optimum outcome of eavesdropping cooperation is aggregate of the power of all eavesdropping signals. The number of articles considering the impact of eavesdroppers' collusion in random

networks is again comparatively small, but the issue has been occasionally considered. For instance, the secrecy capacity of a single legitimate link with length $r_\ell$ in the presence of colluding eavesdroppers under an AWGN channel model was studied in [29], and the probability of non-zero secrecy capacity with multiple antenna transmission schemes in Rayleigh fading channels was analyzed in [30].

In this chapter, we derive the closed-form asymptotic expressions for the secrecy rate distribution, average secrecy rate, secrecy outage probability and secrecy transmission capacity of random networks with Nakagami-$m$ fading channel and colluding eavesdroppers.

## 5.2 Correlation

An indirect way to generalize the assumption of uniformity that is implied by a PPP is to incorporate spatial correlation into the model. Indeed, clusterization [80] – a mechanism that is often used to approximate other point processes via PPPs [53] – can be seen as a particular case of correlation, since it ultimately consists of correlation of the random distances from a source to group of clusterized nodes, which in turn as *per* Eq. (3.1) affects the legitimate and eavesdropping SNRs and thus the secrecy capacity.

However, to the best of our knowledge, no previous work exists on the secrecy capacity and outage capacity of random wireless networks with channel correlation.

First, let us rewrite the secrecy outage probability of unicast link for correlated fading channels at high SNR regime as

$$\mathcal{P}_{\text{out}}(R_s) = \Pr\left\{ \log_2 \left( \frac{\rho^{-1} + \frac{|h_k|^2}{r_k^\alpha}}{\rho^{-1} + \frac{|h_e|^2}{r_e^\alpha}} \right) < R_s \right\} \leq \Pr\left\{ \log_2 \left( \frac{|h_k|^2}{|h_e|^2} \frac{r_e^\alpha}{r_k^\alpha} \right) < R_s \right\}. \quad (5.1)$$

Denote $x_k = |h_k|^2$ and $x_e = |h_e|^2$, where both channels are subjected to Nakagami-$m$ fading. Then, the joint distribution of $x_k$ and $x_e$ is a bivariate gamma distribution given by [81]

$$f_{x_k,x_e}(x_0,x_1) = \frac{m^{m+1}(x_0x_1)^{\frac{m-1}{2}}}{\Gamma(m)(1-\rho)\rho^{\frac{m-1}{2}}} \exp\left\{ -\frac{m(x_0+x_1)}{1-\rho} \right\} I_{m-1}\left( \frac{2\sqrt{\rho}m}{1-\rho}\sqrt{x_0x_1} \right), \; x_0, x_1 > 0, \quad (5.2)$$

where $\rho$ is the correlation coefficient and $I_{m-1}(x)$ is the modified Bessel function of order $m-1$.

The ratio of channel fading envelopes can be calculated as a function of their joint distribution by

$$\begin{aligned} f_{\frac{x_k}{x_e}}(z) &= \int_0^\infty y f_{x_k,x_e}(zy,y)\mathrm{d}y, \\ &= \frac{2^{2m-1}\Gamma(m+\frac{1}{2})(1-\rho)^m}{\sqrt{\pi}\Gamma(m)} \frac{z^{m-1}(z+1)}{[(z+1)^2-4\rho z]^{m+\frac{1}{2}}}. \end{aligned} \tag{5.3}$$

As the distances of legitimate nodes and eavesdroppers are mutually independent, similarly the distribution of their ratio $\frac{r_e^\alpha}{r_l^\alpha}$ can be obtained as

$$f_{\frac{r_e^\alpha}{r_l^\alpha}}(z) = \int_0^\infty y f_{r_e,r_l}(zy,y)\mathrm{d}y \overset{(f)}{=} \frac{\delta k A_\mathrm{e} A_\ell^k z^{\delta-1}}{(A_\mathrm{e} z^\delta + A_\ell)^{k+1}}, \tag{5.4}$$

where, $(f)$ follows from [67, Eq. (3.351.3)].

Denote $\gamma = \frac{|h_l|^2}{|h_e|^2}\frac{r_e^\alpha}{r_l^\alpha}$, the PDF of $\gamma$ can be acquired from the product of these two ratios. Distribution of $\gamma$ for correlated fading channels can be derived as

$$\begin{aligned} f_\gamma(y) &= \int_0^\infty f_{\frac{|h_k|^2}{|h_e|^2},\frac{r_e^\alpha}{r_l^\alpha}}\left(z,\frac{y}{z}\right)\frac{1}{z}\mathrm{d}z = \int_0^\infty f_{\frac{|h_k|^2}{|h_e|^2}}(z)\cdot f_{\frac{r_e^\alpha}{r_l^\alpha}}\left(\frac{y}{z}\right)\frac{1}{z}\mathrm{d}z, \\ &= \delta\cdot k\cdot A_\mathrm{e} A_\ell^k \frac{2^{2m-1}\Gamma(m+\frac{1}{2})(1-\rho)^m}{\sqrt{\pi}\Gamma(m)} \\ &\quad \times \int_0^\infty \frac{z^{\delta k+m-1}(z+1)y^{\delta-1}}{[(z+1)^2-4\rho z]^{m+\frac{1}{2}}(A_\ell z^\delta + A_\mathrm{e} y^\delta)^{k+1}} dz. \end{aligned} \tag{5.5}$$

Then, secrecy outage probability under correlated fading channels can be calculated by the following equation

$$\begin{aligned} \mathcal{P}_{\mathrm{out}}(R_s) &= \Pr\{\log_2(\gamma) < R_s\} = \int_0^{2^{R_s}} f_\gamma(y)\mathrm{d}y, \\ &= \frac{2^{2m-1}\Gamma(m+\frac{1}{2})(1-\rho)^m}{\sqrt{\pi}\Gamma(m)} \int_0^\infty \frac{z^{\delta k+m-1}(z+1)}{[(z+1)^2-4\rho z]^{m+\frac{1}{2}}} s\left[\frac{1}{z^{\delta k}} - \frac{1}{(z^\delta + \frac{A_\mathrm{e}}{A_\mathrm{e}}\times 2^{R_s})^k}\right]\mathrm{d}z. \end{aligned} \tag{5.6}$$

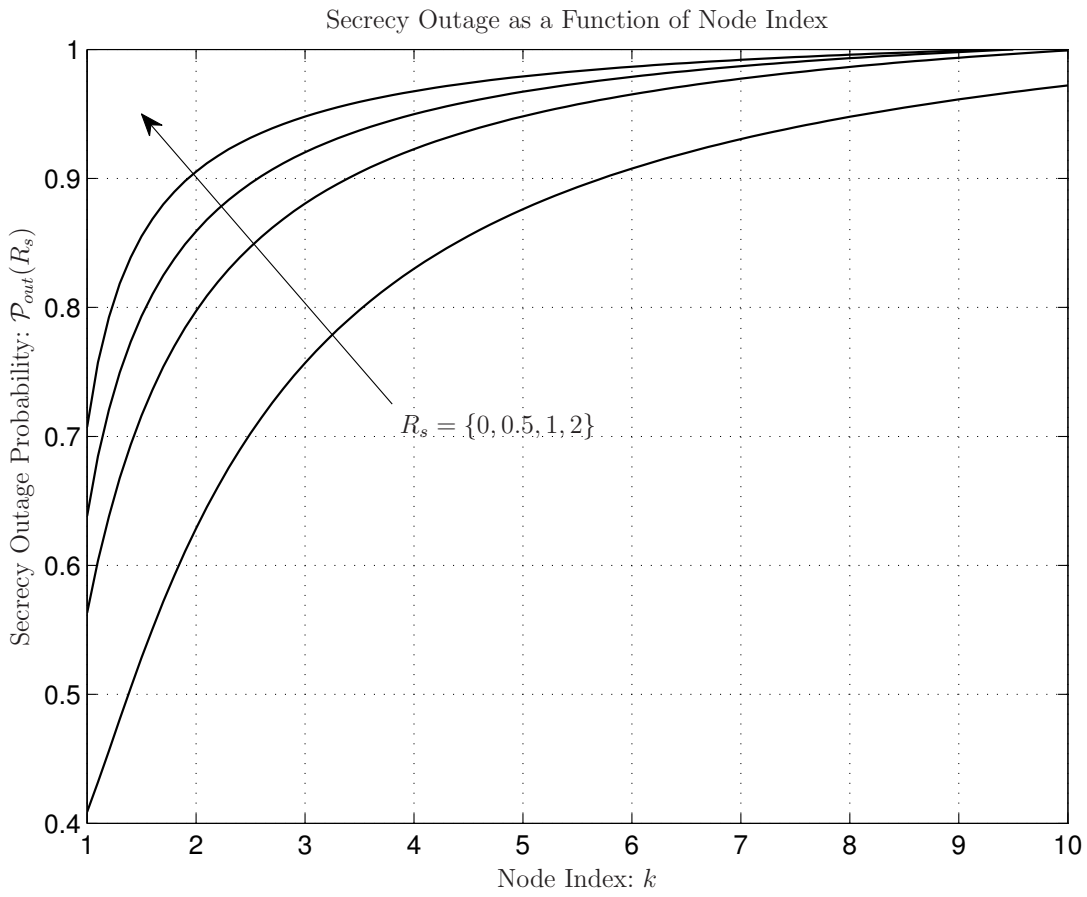
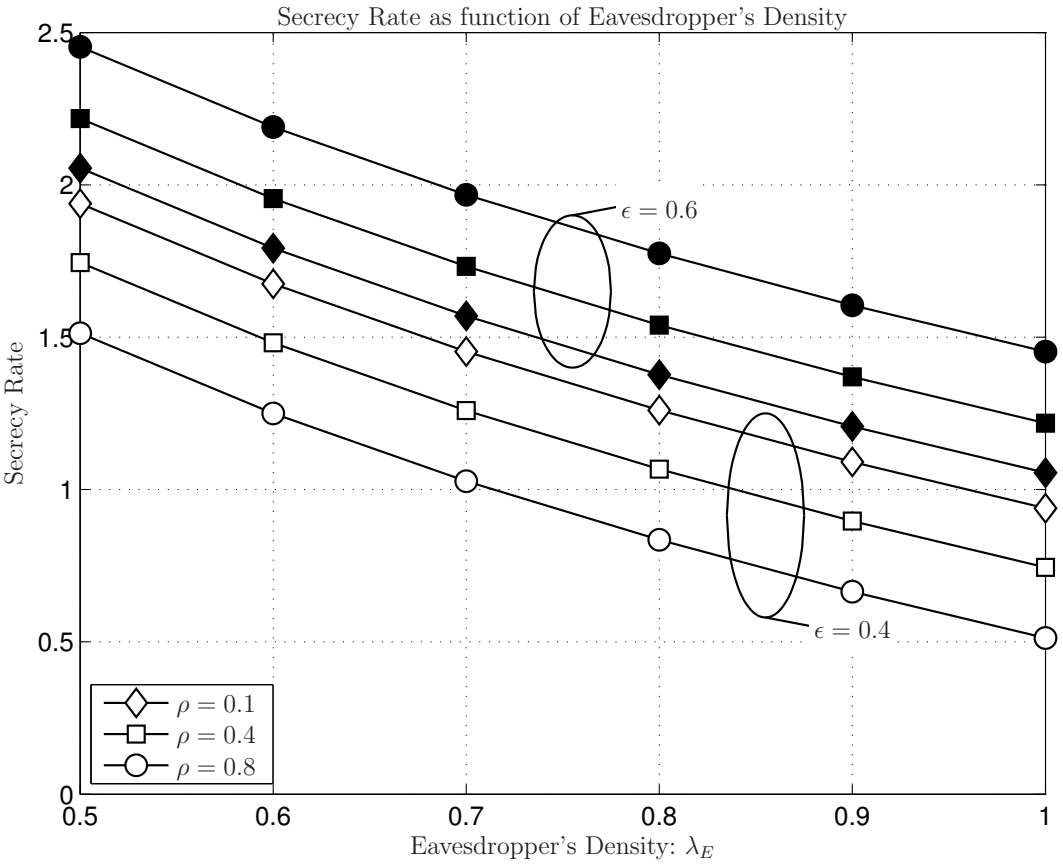



Figure 5.1: Secrecy outage probability $\mathcal{P}_{\text{out}}$ as a function of node index under Nakagami-m fading for various secrecy rates, with $\lambda_\ell = \lambda_{\text{e}} = 1$ and $m = 1$.




,

Figure 5.2: Secrecy rate as a function of eavesdroppers' intensity, with $\lambda_\ell = 2$, $\alpha = 2$, $m = 1$, $k = 1$.

The impact of correlation on the secrecy outage of different nodes under Nakagami-$m$ fading can be observed in Fig. 5.1, where we show plots of $\mathcal{P}_{\text{out}}$ as a function of node index for a constant channel correlation coefficient $\rho = 0.9$. The figure displays various curves for various secrecy rates, with $\lambda_\ell = \lambda_{\text{e}} = 1$, $\alpha = 2$ and $m = 1$. Compared to Fig. 4.10, no particular new insight is gained, as it is found that for any given secrecy rate $R_s$, nodes farther away have higher outage than nodes closer to the source, as expected.

Consider however the minimum secrecy rate $R_s$ achieved under a certain outage $\epsilon$, as a function of the density of eavesdroppers $\lambda_{\text{e}}$, which can be obtained by numerically inverting Eq. (5.6). The results are shown in Fig. 5.2. This time it can be seen that, surprisingly, the secrecy rate increases with the correlation if the secrecy outage is higher then 50%, but decreases otherwise. Since, as shown in Fig. 5.1, farther nodes have higher outage, we conclude from both figure together that correlation helps farther nodes and harms nearer ones.

## 5.3 Collusion

Before describing collusion, let us briefly summarise the aspects of interference, which is another key parameter in characterizing the network-wide secrecy throughput of large scale networks. If undesigned, interference is an aggregated sum of undesired signals due to concurrent transmissions, that may cause severe throughput degradation. Interference can affect the secrecy of a random network if it reduces the SINR at legitimate nodes. For the sake of completeness, in this thesis we will deal the interference aggregation in next chapter. It is somewhat naive to assume that interference aggregates randomly.

Instead, a more modern approach is to formulate optimisation problems around the aggregation of interference [82], which can be in turn seen as a form of cooperation. But since cooperation is certain to play a role, one of our recent works on the role of cooperation in network secrecy is worthy of mention [79].

Since the optimal cooperation amongst eavesdroppers is referred to as collusion, therefore the secrecy capacity of a unicast link in the presence of colluding eavesdroppers can be written as [29]

$$C_s = \max\left\{ \log_2\left(1+\varrho\frac{|h_\ell|^2}{r_\ell^\alpha}\right) - \log_2\left(1+\varrho\sum_{k=1}^{\infty}\frac{|h_{\text{e}:k}|^2}{r_{\text{e}:k}^\alpha}\right), 0\right\}, \tag{5.7}$$

where $h_{\mathrm{e}:k}$ and $r_{\mathrm{e}:k}$ are the fading envelope and the distance associated with the channel between the source and the $k$-th eavesdropper.

It follows that the secrecy rate of a unicast link in the presence of colluding eavesdroppers can be written as [29]

$$R_s = \log_2\!\left(1+\varrho\frac{|h_\ell|^2}{r_\ell^\alpha}\right) - \log_2\!\left(1+\varrho\sum_{k=1}^{\infty}\frac{|h_{\mathrm{e}:k}|^2}{r_{\mathrm{e}:k}^\alpha}\right) = \log_2\!\left(\frac{\varrho^{-1}+\zeta_\ell}{\varrho^{-1}+\hat{\zeta}_{\mathrm{e}}}\right), \tag{5.8}$$

where we have implicitly defined the quantities $\zeta_\ell \triangleq \frac{|h_\ell|^2}{r_\ell^\alpha}$ and $\hat{\zeta}_{\mathrm{e}} \triangleq \sum_{k=1}^{\infty}\frac{|h_{\mathrm{e}:k}|^2}{r_{\mathrm{e}:k}^\alpha}$, which denote the channel gains of the legitimate node, and the *equivalent* channel gain of the collusion of eavesdroppers, respectively.

Clearly, the difficulty in evaluating Eq. (5.8) is to determine the distribution of the ratio $\frac{\varrho^{-1}+\zeta_\ell}{\varrho^{-1}+\hat{\zeta}_{\mathrm{e}}}$, which in turn requires the evaluation of the distribution of $\zeta_E$. The latter is the subject of Section 5.3.1. For now, however, let us just highlight that we will hereafter follow related literature [46, 77] and consider the particular case of an asymptotic reference SNR regime, where $\varrho \to \infty$, such that

$$R_s \to \log_2\!\left(\frac{\zeta_\ell}{\hat{\zeta}_{\mathrm{e}}}\right). \tag{5.9}$$

From equations (5.7) through (5.9), it is clear that in the asymptotically large SNR regime, the secrecy capacity is determined by the channel gain ratio, rather the actual received power. We may also add that the asymptotic assumption does not detract value from the analysis, as the proportionality between the legitimate-to-eavesdropper channel advantage and inherent secrecy is indeed at the core of the information-theoretic perspective of secrecy capacity first brought to life in the pioneering works on the topic [6–8].

Returning to our discussion, it will be shown that the distribution of an asymptote of $R_s$ under eavesdropper collusion can be found, in possession of which other results can be obtained, including the *average secrecy rate* $\bar{R}_s \triangleq \mathbb{E}[R_s]$.

Finally, in possession of $\bar{R}_s$, the secrecy transmission capacity [24] of the network can be determined. This metric is of interest since the characterization of the secrecy capacity of every individual unicast link in a large random network is impractical.

Mathematically, the secrecy transmission capacity is defined by

$$\tau \triangleq \bar{R}_s(1-\mathcal{P}_{\text{co}})\lambda_\ell, \tag{5.10}$$

### 5.3.1 Aggregate Eavesdroppers' Path Gain

As discussed in the preceding section, the distribution of the equivalent aggregate eavesdropper path gain $\hat{\zeta}_{\text{e}}$ is needed in order to characterize the secrecy rate of random networks with colluding eavesdroppers. For future notation convenience, let us define the variable $X_{\text{e}:k} \triangleq |h_{\text{e}:k}|^2$, such that we have

$$\hat{\zeta}_{\text{e}} = \sum_{k=1}^{\infty} X_{\text{e}:k} \cdot r_{\text{e}:k}^{-\alpha}, \tag{5.11}$$

where $r_{\text{e}:k}$'s are in ascending order, without loss of generality.

Before we proceed, let us briefly analyze Eq. (5.11) qualitatively. First, it must be pointed out that the path loss model itself – implied by the presence of the terms $r_{\text{e}:k}^{-\alpha}$ – only applies for $r_{\text{e}:1}$, since the wireless channel does not amplify transmit power [59]. Secondly, recalling the definition of secrecy capacity as in Eq. (3.1) and given that one can only speak of a secrecy rate under the condition that the link is not in secrecy outage, it must be clear that none of the terms $X_{\text{e}:k} \cdot r_{\text{e}:k}^{-\alpha}$ can be larger than $|h_\ell|^2/r_\ell^\alpha$. This non-outage condition therefore imposes an even stronger constraint on the minimum distance that can be held by eavesdroppers for the analysis hereafter to apply. Specifically, in an AWGN channel the non-outage condition obviously implies the boundary condition $r_{\text{e}:1} > r_\ell$. As for the fading case, it has been shown [19] that even without eavesdropping collusion fading reduces the secrecy rate achievable by communicating pairs of shorter distances, which in turn implies that the minimum distance required to satisfy a non-outage condition under fading and colluding eavesdroppers is larger than $r_\ell$.

In light of the above, it will be hereafter assumed that $r_{\text{e}:1} > r_{\min}$, which will be further referred to as the guard zone distance (see Fig. 5.3). Under this model and by force of Campbell's theorem, the characteristic function of $\hat{\zeta}_{\text{e}}$ can be computed by [59, 60]

$$\phi_{\hat{\zeta}_{\text{e}}}(w) = \exp\left(-2\pi\lambda_{\text{e}} \int_X \int_{r_{\min}}^{\infty} r \cdot [1 - e^{jwxr^{-\alpha}}] \cdot f_X(x)\, \mathrm{d}r\mathrm{d}x\right), \tag{5.12}$$

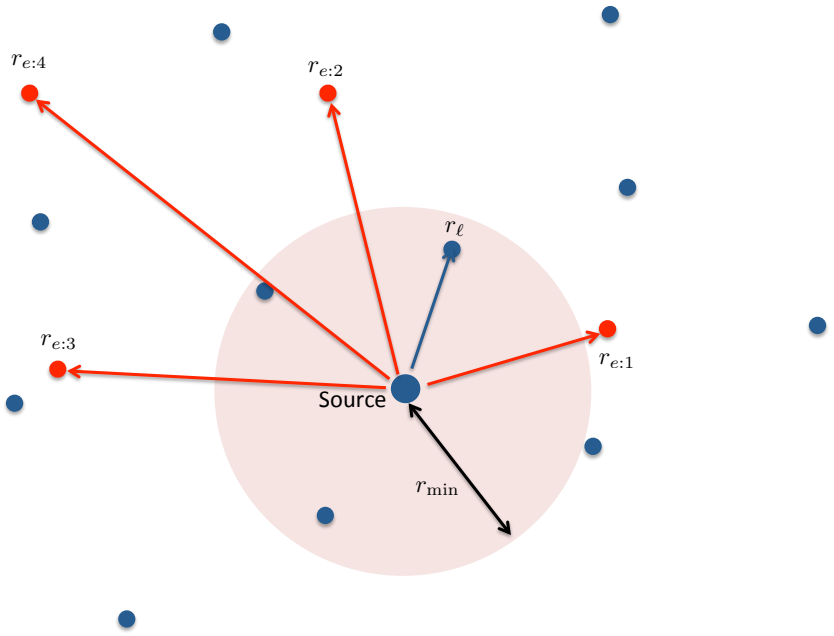



Figure 5.3: Illustration of a legitimate pair neighborhood with guard zone distance $r_{\min}$ and a pool of colluding eavesdroppers.

Unfortunately neither Eq. (5.12) nor its inverse Laplace transform admit a closed form, except for the specific case of Rayleigh fading [24]. We can, however, employ Eq. (5.12) to obtain closed forms of the corresponding cumulants. Specifically, the $n$-th cumulant of $\phi(w)$ can is given by

$$\kappa(n) = \frac{1}{j^n} \frac{\mathrm{d}^n \log \phi(w)}{\mathrm{d}w^n}\Big|_{w=0}. \tag{5.13}$$

The $n$-th cumulant of $\phi_{\hat{\zeta}_\mathrm{e}}(w)$ can be

$$\kappa_{\hat{\zeta}_\mathrm{e}}(n) = 2\pi\lambda_\mathrm{e} \int\limits_X \int\limits_{r_\mathrm{min}}^{\infty} x^n r^{1-n\alpha} f_X(x) \mathrm{d}r\mathrm{d}x = \frac{2\pi\lambda_\mathrm{e} r_\mathrm{min}^{2-n\alpha}}{(n\alpha-2)} \cdot \frac{\Gamma(m+n)}{m^n \Gamma(m)}, \tag{5.14}$$

where for notational simplicity we omit the dependence of $\kappa$ on the $m$ and $\lambda_\mathrm{e}$.

Based on this exact cumulant expression, various models for the distribution of the equivalent aggregate eavesdropper gain can be built, some of which are discussed in the sequel.

#### 5.3.1.1 Modeling $\hat{\zeta}_\mathrm{e}$ via Edgeworth Asymptotic Expansion

The Edgeworth series is the optimum asymptotic expansion to approximate a probability distribution in terms of its cumulants [83], in the sense that it minimizes the error between the cumulants of the reconstructed distribution and the original (exact) cumulants themselves.

Given the complete sequence of cumulants $\{\kappa_{\hat{\zeta}_\mathrm{e}}(n)\} = \{\kappa_{\hat{\zeta}_\mathrm{e}}(1), \kappa_{\hat{\zeta}_\mathrm{e}}(2), \cdots\}$, the Edgeworth expansion is given by

$$f_{\hat{\zeta}_\mathrm{e}}(x; \{\kappa_{\hat{\zeta}_\mathrm{e}}(n)\}) = \mathcal{N}(x) \left\{ 1 + \sum_{k=1}^{\infty} k_{\hat{\zeta}_\mathrm{e}}^{k/2}(2) \sum_{\{i_t\}} He_{k+2I}(x) \prod_{t=1}^{k} \tfrac{1}{i_t!} \left( \frac{S_{t+2}}{(t+2)!} \right)^{i_t} \right\}, \tag{5.15}$$

where $S_n \triangleq \kappa_{\hat{\zeta}_\mathrm{e}}(n) / k_{\hat{\zeta}_\mathrm{e}}^{n-1}(2)$ are normalized cumulants, $\mathcal{N}(x)$ denotes the Standard Normal distribution, $He_n(x)$ is the $n$-th order Chebyshev-Hermite polynomial, and the sum taken over the set $\{i_t\}$ means that for each $k$, the indexes $i_t$'s are the non-negative integer solutions of the $k$-th order Diophantine equation

$$i_1 + 2\, i_2 + \cdots + k, \tag{5.16}$$

with

$$i_1 + i_2 + \cdots + i_k = I. \tag{5.17}$$

A comparison between an empirical distribution obtained via simulations with $\lambda_e = 1$ and $m = 1$ and the Edgeworth model using the first 5 cumulants is shown in Fig. 5.4. It can be seen that the model is relatively accurate but, despite the asymptotic optimality, does suffer the effect of the truncation of the first unbounded summation in (5.15), which is unavoidable in practice. This, together with the analytical intractability of the model, prompts us to consider a simpler (and in fact more accurate) model, as discussed in the sequel.

#### 5.3.1.2 Modeling $\hat{\zeta}_e$ as a Gamma Variate

In order to obtain a more tractable and accurate model for the distribution of $\hat{\zeta}_e$, start by noticing that for the specific case of $\alpha = 2$, the terms $X_{e:k} \cdot r_{e:k}^{-\alpha}$ in Eq. (5.11) are given by the square of the ratio of two Nakagami-$m$ variates. But it has been recently shown [84] that the ratio of Nakagami variates is itself well approximated by a Nakagami variate, from which it follows that for $\alpha = 2$ each term $X_{e:k} \cdot r_{e:k}^{-\alpha}$ is (approximately) a Gamma variate. And since the sum of Gamma variates is also a Gamma variate, we conclude the that for specific case of $\alpha = 2$ the distribution of the equivalent aggregate eavesdropper path gain $\hat{\zeta}_e$ can be well approximated by a Gamma distribution.

Motivated by this fact, we consider a gamma model for $\hat{\zeta}_e$ also for other values of $\alpha$. Specifically, we consider the model

$$f_{\hat{\zeta}_e}^{(\Gamma)}(x; \nu, \theta) = \frac{x^{\nu-1} e^{-\frac{x}{\theta}}}{\theta^{\nu} \Gamma(\nu)}, \tag{5.18}$$

where the parameters $\nu$ and $\theta$ are given by

$$\nu = \frac{\kappa_{\hat{\zeta}_e}^2(1)}{\kappa_{\hat{\zeta}_e}(2)}, \quad \text{and} \quad \theta = \frac{\kappa_{\hat{\zeta}_e}(2)}{\kappa_{\hat{\zeta}_e}(1)}. \tag{5.19}$$

The accuracy of the Gamma model is illustrated in figures 5.4, 5.5 and 5.6. First, in Fig. 5.4, the empirical PDF of $\hat{\zeta}_e$ for $\alpha = 4$, with $m = 1$ and $\lambda_e = 1$ is compared against the Gamma distribution given in equation (5.18).

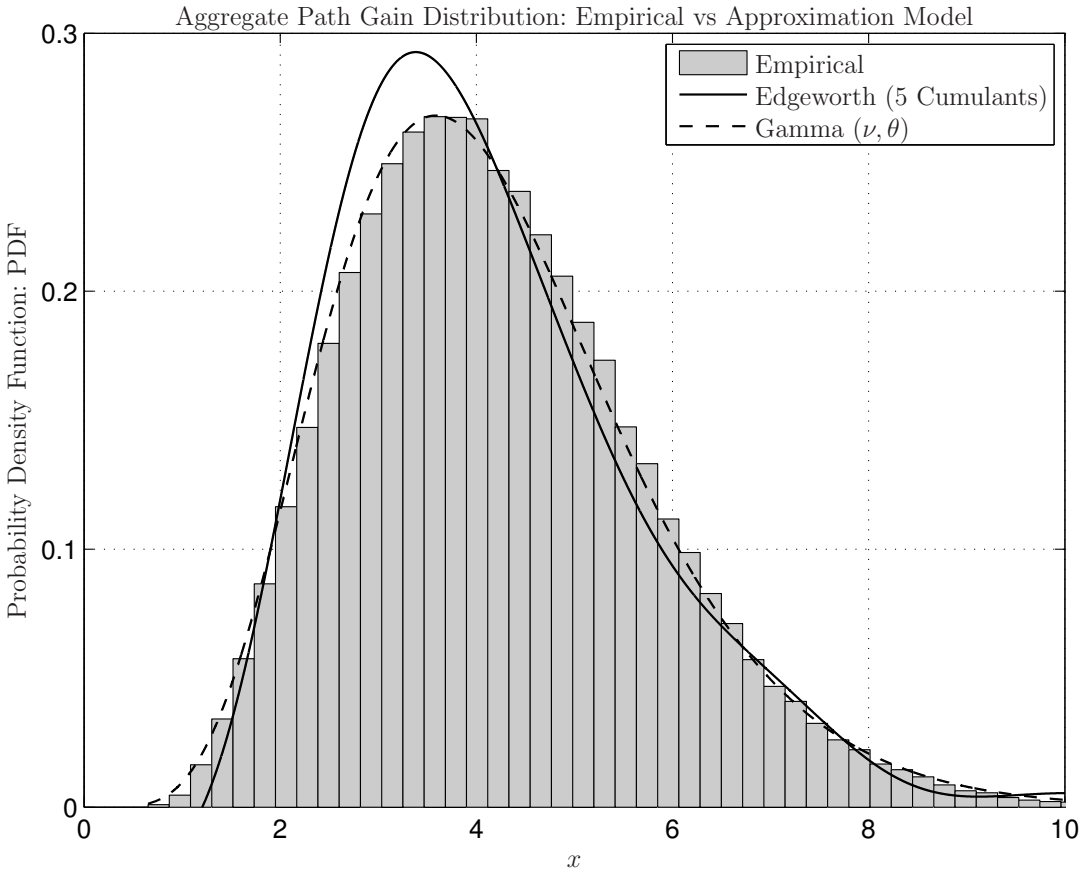



Figure 5.4: Edgeworth and Gamma models Vs Empirical ($\alpha = 4$, $m = 1$).

The results indicate that in fact the Gamma approximation is very accurate also $\alpha = 4$, visibly superior to that provided by the Edgeworth expansion with 5 cumulants.

Next, in figures 5.5 and 5.6, the accuracy of the Gamma model under various parameterizations is demonstrated by means of their Kullback-Leibler divergences to corresponding empirical distributions. Altogether, the results again confirm that the Gamma model is indeed highly accurate across a wide range of channel and network conditions, as measured by the parameters $\alpha$, $m$ and $\lambda_{\mathrm{e}}$.

#### 5.3.1.3 On the Convergence of $\hat{\zeta}_{\mathrm{e}}$

Before moving to the derivation secrecy performance metrics using the model described above, let us briefly address the convergence of the infinite sum involved in evaluating $\hat{\zeta}_{\mathrm{e}}$, as per Eq. (5.11). First, it can be stated that by force of Eq. (5.14), the sum in Eq. (5.11) is absolutely convergent for all $\alpha > 2/n$, since the cumulants of $\hat{\zeta}_{\mathrm{e}}$ are finite under the latter condition. Still, the rate of convergence of the sum required to calculate $\hat{\zeta}_{\mathrm{e}}$ is of relevance when validating the models described above.

In particular, it is of interest to know whether $\hat{\zeta}_{\mathrm{e}}$ can be accurately evaluated by truncating the sum at a sufficiently large number of terms $K$, and how large must $K$ be. Here, we refer to Fig. 5.7, where plots of truncated approximations of $\hat{\zeta}_{\mathrm{e}}$ as a function of $m$ and for various value of the parameters $\alpha$ and $\lambda_{\mathrm{e}}$ are shown. The plots 5.7 indicate that for the purpose of simulations, the sum can be truncated at $K$ with negligible sacrifice in accuracy.

### 5.3.2 Asymptotic Expressions

The distributions obtained above could obviously be used also to model aggregate interference originating from simultaneous transmissions by multiple legitimate users. However, under the assumption that legitimate pairs communicate in a completely uncoordinated fashion, such aggregate interference affects both legitimate nodes and eavesdroppers alike, as considered for instance in [24].

In that case, equations (5.8) and (5.9) could be revised to

$$R'_s = \log_2\left(\frac{\varrho'^{-1} + \zeta_\ell}{\varrho'^{-1} + \hat{\zeta}_{\mathrm{e}}}\right) \underset{\varrho' \to \infty}{\longrightarrow} \log_2\left(\frac{\zeta_\ell}{\hat{\zeta}_{\mathrm{e}}}\right), \tag{5.20}$$

with $\varrho' \triangleq P/(N_0 + I_\ell)$, where $I_\ell$ denotes the aggregate interference of legitimate nodes.

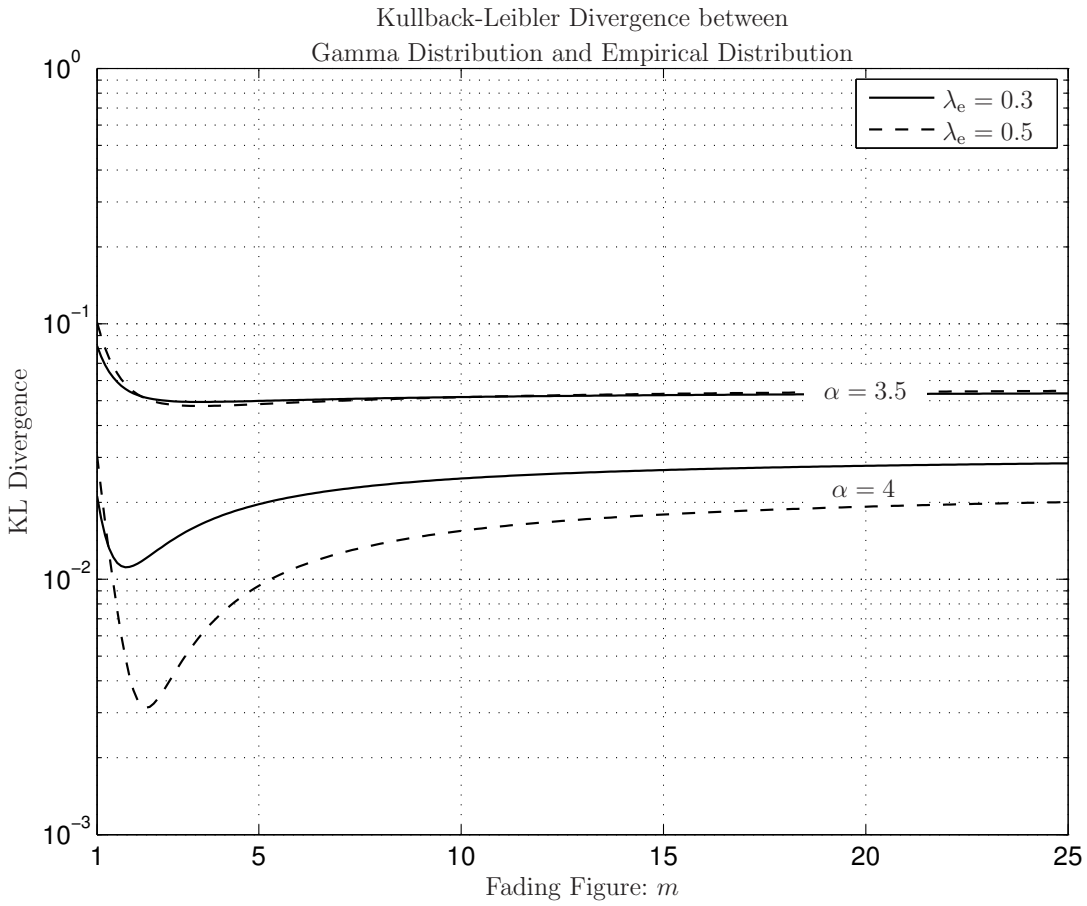



Figure 5.5: Divergence between empirical and Gamma distributions for various path loss exponents $\alpha$, eavesdropper density $\lambda_e$ and fading figure $m$.

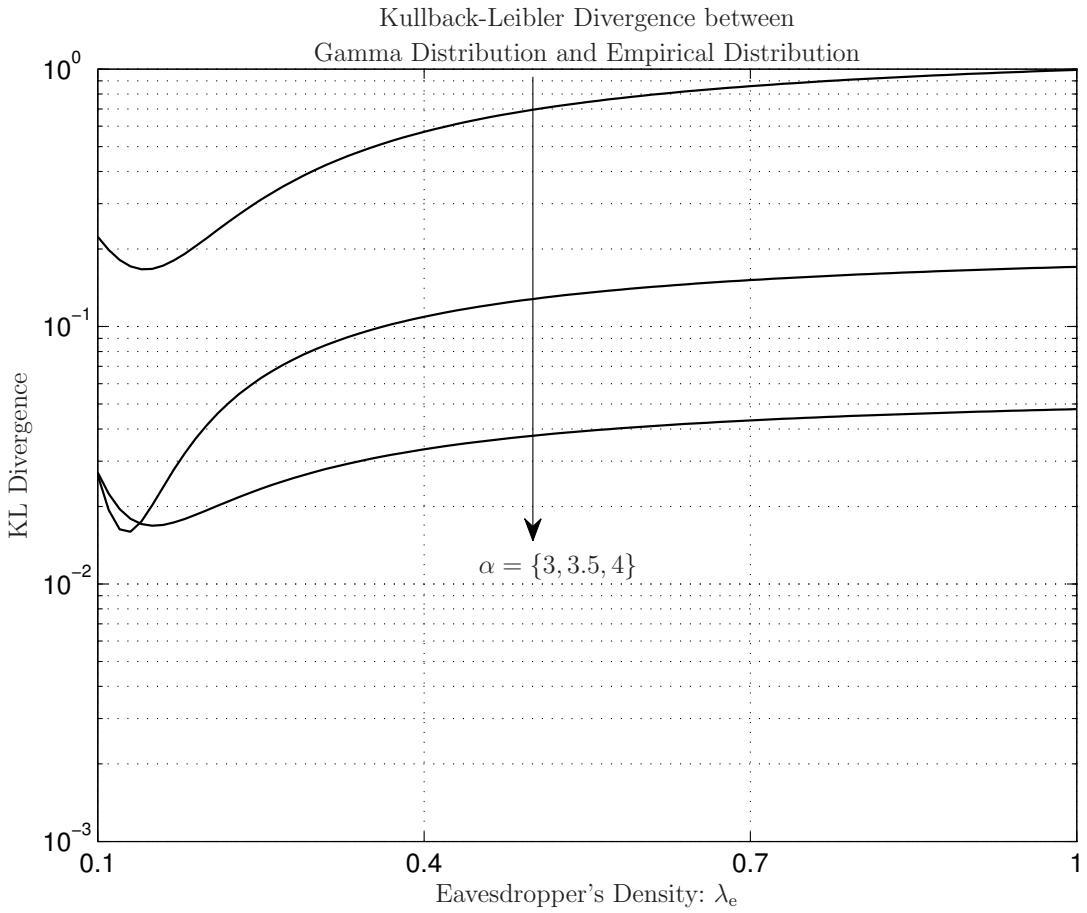



Figure 5.6: Divergence between empirical and Gamma distributions for various path loss exponents $\alpha$, eavesdropper density $\lambda_e$ and fading figure $m$.

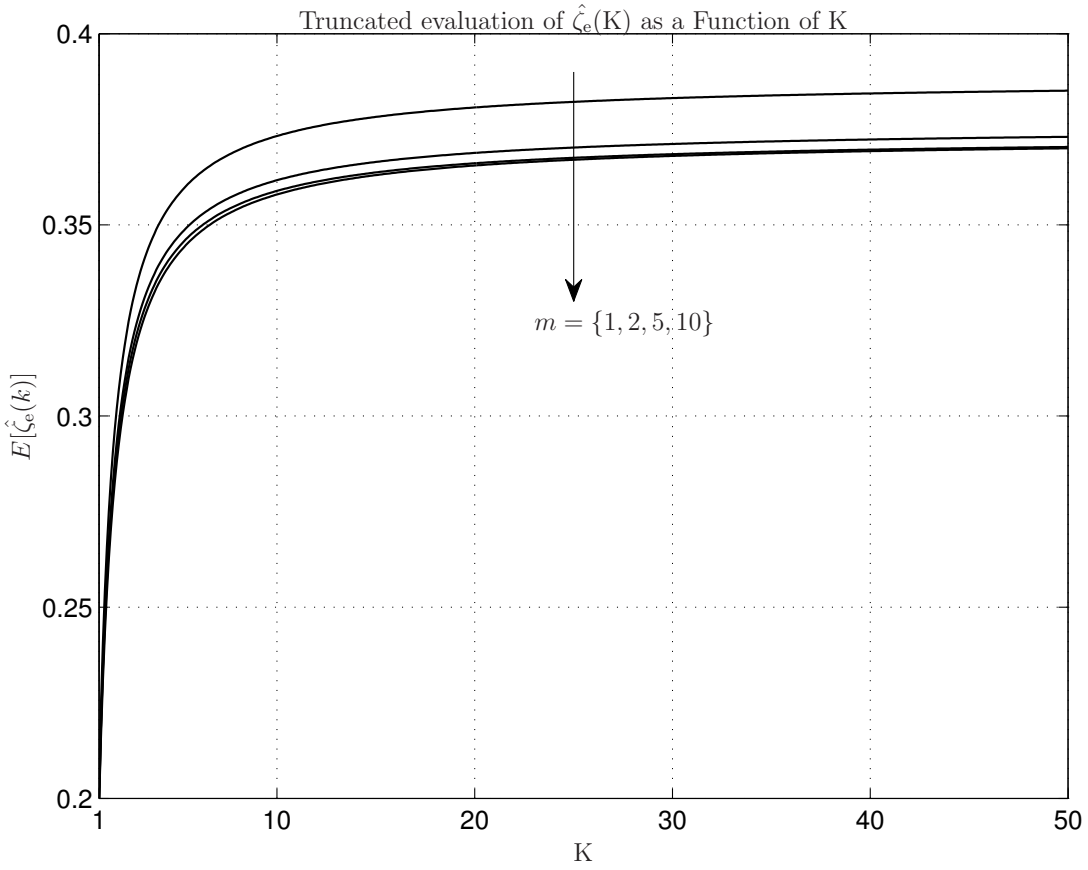



Figure 5.7: Truncated evaluation of $\hat{\zeta}_e(K)$ under different channel conditions.

Comparing equations (5.8) and (5.9) with (5.20), it is evident that no fundamental distinction between them exits, in the sense that our assumption of an asymptotic SNR simply translates to an equivalent assumption of an asymptotic SINR.

In related literature, the latter assumption is sometimes also referred to as *low-outage* regime [85, 86]. In the sequel, we will therefore follow related literature and focus on the case of low-outage networks, where aggregate interference is negligible.

Notice also that some form of interference control is required to optimise throughput (reduce outage) in random networks, which is usually implemented in the form of a self-managed channel access mechanism [87, 88] that improves on the classic ALOHA [89].

But since throughput maximisation mechanisms ultimately lead to significantly lower densities of *active* nodes compared to the actual density of the network [90], it can be said that the analysis to follow is in line with low-outage/high-throughput regime characterisation, particularly in cases of small $\lambda_\ell$.

With an accurate model for the distribution of $\hat{\zeta}_\mathrm{e}$, we are ready to characterize the secrecy rate, secrecy outage probabilities and secrecy transmission capacity of random networks subjected to Nakagami fading and colluding eavesdroppers.

It is convenient to start with the secrecy outage probability. Let $Z = \zeta_\ell / \hat{\zeta}_\mathrm{e}$, denote the ratio of legitimate versus (colluding) eavesdroppers path gains. From equation (5.18) and the Nakagami distribution, we have

$$\begin{aligned} F(z; r_\ell, m, \alpha, \lambda_\mathrm{e}) &= \Pr\{Z < z\}, \\ &= \int_0^\infty \frac{x^{\nu-1}\exp(-\frac{x}{\theta})}{\theta^\nu \Gamma(\nu)} \int_0^{z r_\ell^\alpha x} \frac{m^m y^{m-1}\exp(-my)}{\Gamma(m)}\,\mathrm{d}y\,\mathrm{d}x, \\ &= \frac{1}{\theta^\nu \Gamma(m)\Gamma(\nu)} \int_0^\infty x^{\nu-1} e^{-\frac{x}{\theta}} [\Gamma(\nu) - \Gamma(\nu, \tfrac{z m r_\ell^\alpha x}{\theta})]\,\mathrm{d}x, \\ &= 1 - \frac{\Gamma(\nu+m)\,{}_2F_1\left(\nu, \nu+m, 1+\nu; -\dfrac{1}{m\theta r_\ell^\alpha z}\right)}{(m\,\theta\, r_\ell^\alpha\, z)^\nu \Gamma(m)\Gamma(\nu)\nu}, \end{aligned} \tag{5.21}$$

where the dependence on $\lambda_\mathrm{e}$ is implied by the dependence of $\nu$ and $\theta$ on $\lambda_\mathrm{e}$.

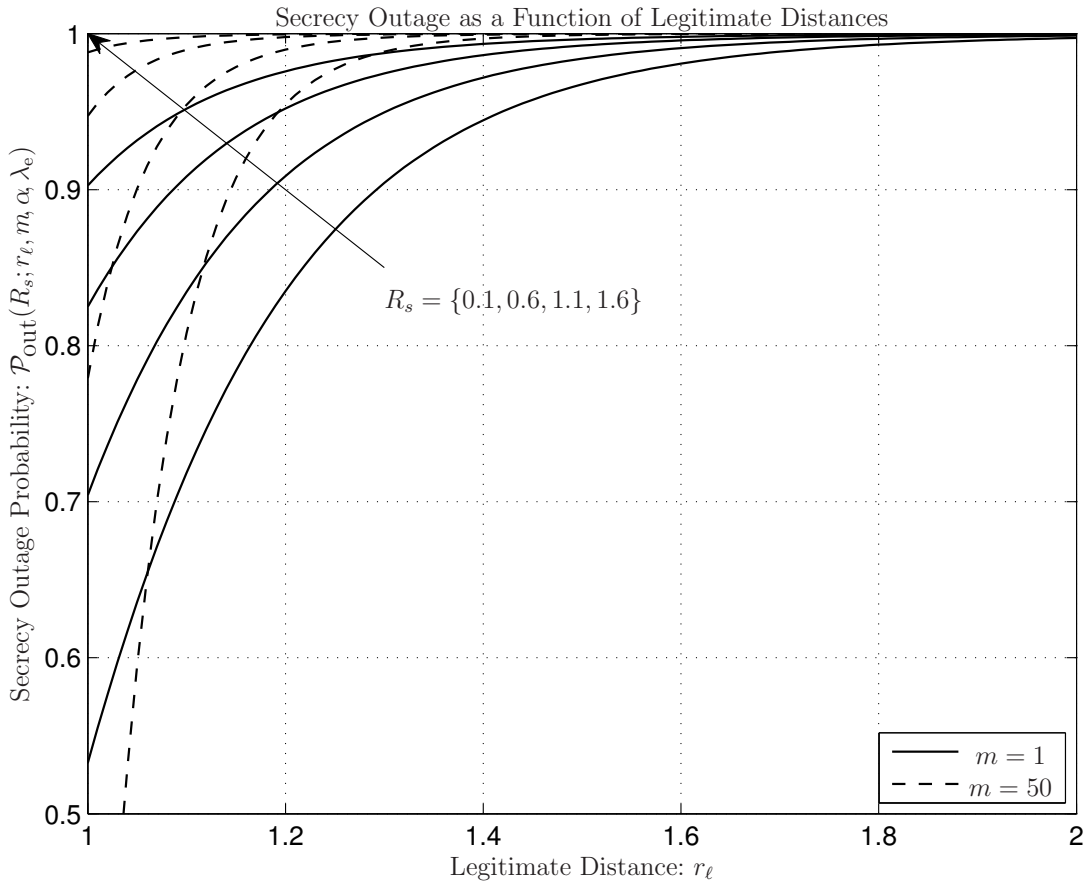



Figure 5.8: Secrecy outage probability as a function of legitimate distance in the case of Rayleigh fading ($m = 1$) and for various rates, with $\lambda_e = 1$ and $r_{\min} = 1$.

Then, from Eq. (3.14), and using the asymptotic relation of Eq. (5.9), we obtain straightforwardly

$$\mathcal{P}_{\text{out}}(R_s; r_\ell, m, \alpha, \lambda_{\text{e}}) = 1 - \frac{\Gamma(\nu+m)\,{}_2F_1\!\left(\nu, \nu+m, 1+\nu; -\dfrac{1}{m\,\theta\, r_\ell^{\alpha}\, 2^{R_s}}\right)}{(m\,\theta\, r_\ell^{\alpha}\, 2^{R_s})^{\nu}\Gamma(m)\Gamma(\nu)\nu}. \tag{5.22}$$

The distribution of the secrecy rate $R_s$ is then obtained by derivation of the expression in Eq. (5.22), yielding [91]

$$f_{R_s}(z; r_\ell, m, \alpha, \lambda_{\text{e}}) = \frac{\Gamma(\nu+m)(-1)^{\nu-1}\log(2)}{\Gamma(m)\Gamma(\nu)(m\theta r^{\alpha} 2^z)^{\nu}}\,{}_3F_2\!\left(\nu+1, \nu, \nu+m, \nu, 1+\nu; -\frac{1}{m\,\theta\, r_\ell^{\alpha}\, 2^z}\right). \tag{5.23}$$

Likewise, the average secrecy rate $\bar{R}_s$ can then be easily derived by averaging the rate $\log(\frac{\zeta_\ell}{\hat{\zeta}_{\text{e}}})$ over the distribution of the ratio $\zeta_\ell/\hat{\zeta}_{\text{e}}$, namely

$$\begin{aligned}
\bar{R}_s &= \int_1^{\infty} \log(z) F(z; r_\ell, m, \alpha, \lambda_{\text{e}})\,\mathrm{d}z, \qquad (5.24)\\
&= -\log(z) F(z; r_\ell, m, \alpha, \lambda_{\text{e}})\big|_1^{\infty} + \int_1^{\infty} \frac{F(z; r_\ell, m, \alpha, \lambda_{\text{e}})}{z}\mathrm{d}z,\\
&= \frac{(mr^{\alpha})^{-\nu}\Gamma(\nu+m)}{\nu\theta^{\nu}\Gamma(m)\Gamma(\nu)} \int_1^{\infty} \frac{{}_2F_1\!\left(\nu, \nu+m, 1+\nu; -\dfrac{1}{z\,m\,\theta\, r_\ell^{\alpha}}\right)}{z^{\nu+1}}\mathrm{d}z,\\
&= \frac{(mr^{\alpha})^{-\nu}\Gamma(\nu+m)}{\nu^2\theta^{\nu}\Gamma(m)\Gamma(\nu)}\,{}_3F_2\!\left(\nu, \nu, \nu+m, 1+\nu, 1+\nu; -\frac{1}{m\,\theta\, r_\ell^{\alpha}}\right).
\end{aligned}$$

With the expressions derived in this section, we can study the availability of secrecy in random networks in the presence of colluding eavesdroppers, and the effect of fading thereby. First, consider the secrecy outage probability. Plots of $\mathcal{P}_{\text{out}}(R; r_\ell, m, \alpha, \lambda_{\text{e}})$, shown in Fig. 5.8, indicate fading increases the likelihood of secrecy outage for nodes closer to the source, but reduces it for nodes further away. This result is similar to that observed in the case of non-colluding eavesdroppers [19].

Considering both results together, the general impact of fading seems to be one of "distributing" secrecy outage amongst the nodes in the neighborhood of a source. One could infer from the latter that a similar behavior is to be found when studying the secrecy transmission capacity, and that is indeed what Fig. 5.9 illustrates.

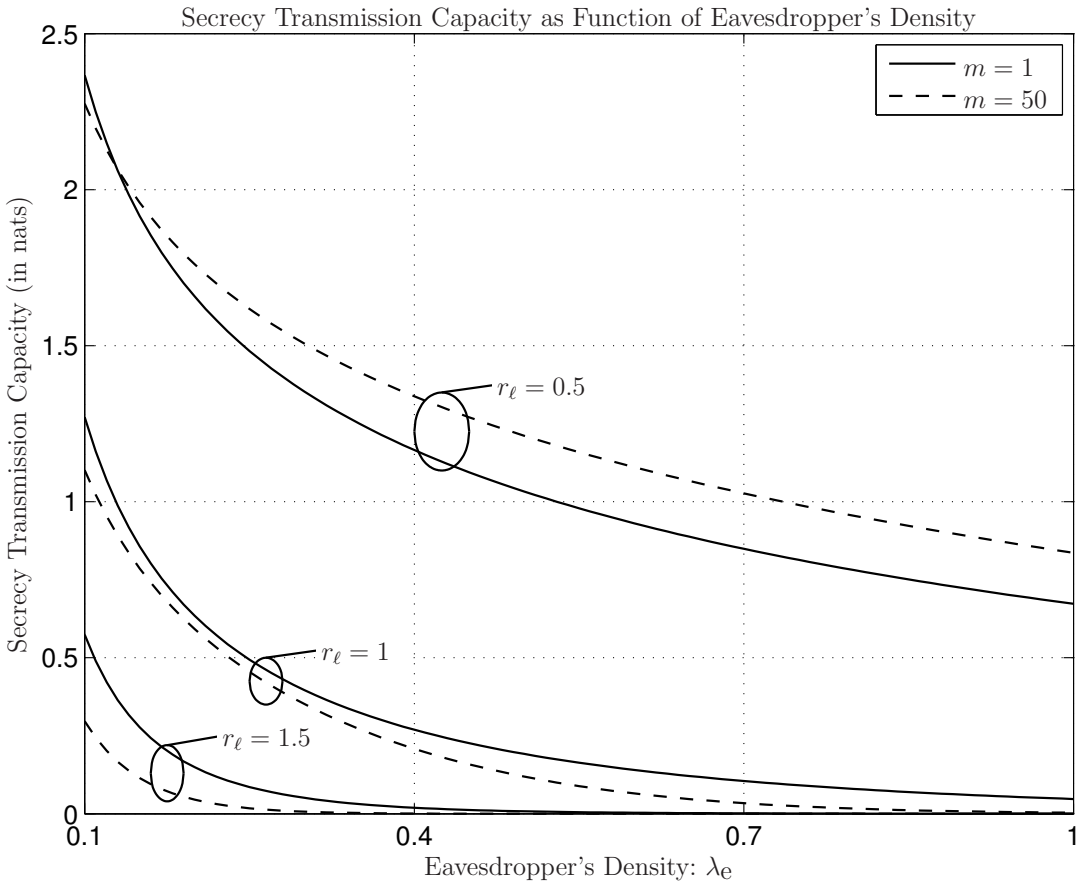



Figure 5.9: Secrecy transmission capacity as a function of eavesdropper's density and for various legitimate distances $r_\ell$, with $\mathcal{P}_{\text{co}} = 0.5$ and $\lambda_\ell = 1$.

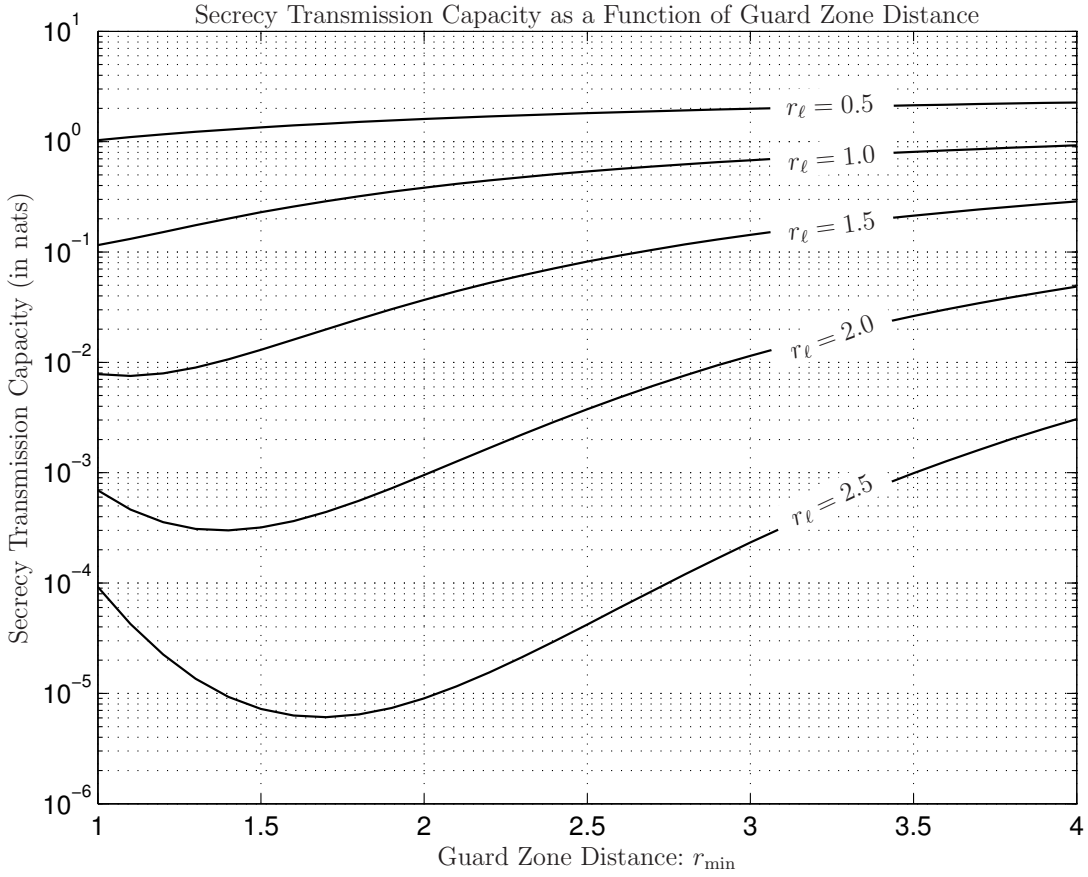



Figure 5.10: Secrecy transmission capacity as a function of guard zone distances in the case of Rayleigh fading ($m = 1$) and for various legitimate distances $r_\ell$, with $\mathcal{P}_{\text{co}} = 0.5$ and $\lambda_\ell = 1$.

Specifically, the figure shows that albeit the secrecy transmission capacity obviously increases absolutely as the legitimate pair grows closer, a relatively decrease (compared to AWGN conditions) is experienced by nearer nodes, while a relative increase in capacity is experienced by further nodes.

This general "rule-of-thumb" description of the impact of fading is confirmed once again by the results in Fig. 5.10, which however also indicates that exceptions do occur. Specifically, it found that if the guard zone does not include the legitimate pair (*i.e.*, if $r_{\min} < r_\ell$), then fading can also hurt the secrecy capacity of nodes at further distances.

Setting aside the impact of fading, all the results combined also indicate that information theoretical secrecy (in the Wyner sense) is only significant in random networks with colluding eavesdroppers, if a guard zone of reasonable size exists, and if the legitimate pair is within it.

## 5.4 Conclusions

In Section 5.2, we studied the impact of correlated fading on the secrecy outage of random networks. By analyzing secrecy outage expression, it is found that the impact of channel correlation is selective, *i.e.*, it improves secrecy rate when secrecy outage is larger than 50%, and decreases it when secrecy outage is less than 50%.

In Section 5.3, our expressions are valid for the high SNR regime with negligible interference, also known as the *low-outage* regime. An interesting outcome of the analysis is that the uncertainty on the number of eavesdroppers does not play a significant role. Another interesting result is that under the worst conditions, such as fading and colluding eavesdroppers, secret communication at a given rate is possible (albeit subjected to outage). Specifically, it is shown that the guard zone distance plays a crucial role in determining the secrecy capacity.

Specifically, we have have added following contributions to this chapter

- Obtained the expression for probability of secrecy outage of unicast channel under mutually correlated fading channels [71] and colluding eavesdroppers [92].
- Approximated the aggregate path gain distribution of colluding eavesdroppers and consequently, derived the expressions for secrecy outage probability with guard zone distance [92].

# Chapter 6

# Interference

**Summary:**

*In this chapter, we investigate the secrecy outage in wireless networks under various channel models. To derive the expression of secrecy outage, we model the interference impact of legitimate users by incorporating two propagation channel models in wireless networks that influence the secrecy capacity. We offer original and highly accurate expressions for the aggregate interference with fading and shadowing, which can also be used to obtain other analytical results.*

## 6.1 Introduction

In Chapter 5, we have investigated the impact of correlation and collusion among eavesdroppers on the secrecy outage of unicast links in single antenna systems. In particular, we derived the closed-form asymptotic expressions for the secrecy rate distribution, average secrecy rate, secrecy outage probability and secrecy transmission capacity of random networks with correlated Nakagami-$m$ fading channels and colluding eavesdroppers.

In this direction, Zhou *et al.* [24] derived the expression of secrecy outage probability, similar to the results in [9], but from the context of random networks under Rayleigh fading. More recently, Shu *et al.* [42] analyzed the effect of interference on the secrecy capacity of random networks with cognitivity. However, the fading and the interference protection thresholds as described in [59, 60], were not considered in [42].

In this chapter, we investigate secrecy outage in cognitive wireless networks taking into account interference, fading and shadowing. In particular, we investigate secrecy outage in wireless networks by considering Gamma and Log-normal approximation for interference characterization. Two transmission scenarios, i.e. Nakagami-m fading channel model and shadowed fading channel model are considered to evaluate the impact of interference, fading and shadowing onto the secrecy.

## 6.2 Aggregate Interference

Consider that primary user (source) wishes to unicast to a legitimate receiver $\ell$ in the presence of an eavesdropper located at the unknown distance $r_{\mathrm{e}}$ with interference from other users, subjected to path loss governed by the exponent $\alpha$. Then, the *secrecy capacity* in bits/sec/Hz of the unicast channel[1] under the assumption that eavesdroppers do not collude, is [8, 9]

$$\begin{aligned} C_s &= \max\left\{\log_2\left(1+\frac{|h_\ell|^2 P}{r_\ell^\alpha I_{\mathrm{s}}}\right)-\log_2\left(1+\frac{|h_{\mathrm{e}}|^2 P}{r_{\mathrm{e}}^\alpha I_{\mathrm{s}}}\right), 0\right\}, \\ &= \max\{\log_2\left(1+\Upsilon_\ell\right)-\log_2\left(1+\Upsilon_{\mathrm{e}}\right), 0\}, \end{aligned} \tag{6.1}$$

[1] We assume that interference, $I_{\mathrm{s}}$ dominates noise power, i.e when the system is interference limited, then the thermal noise is negligible.

where $I_{\mathrm{s}}$ denotes the aggregate interference power of all the secondary users; and we have implicitly defined $\Upsilon_{\ell} \triangleq \frac{|h_{\ell}|^2 P}{r_{\ell}^{\alpha} I_{\mathrm{s}}}$ and $\Upsilon_{\mathrm{e}} \triangleq \frac{|h_{\mathrm{e}}|^2 P}{r_{\mathrm{e}}^{\alpha} I_{\mathrm{s}}}$, which denote the signal-to-interference ratio's (SIR) of legitimate node and eavesdropper, respectively.

If the capacity of the channel from the primary user to any eavesdroppers is above the rate $R_{\ell}$, *i.e.*, $\log_2(1+\Upsilon_{\mathrm{e}}) > R_{\ell}$, the security of the message is compromised. The probability of this event is known as secrecy outage probability [24] which is denoted by $\mathcal{P}_{\mathrm{out}}(R_{\ell})$. To facilitate our analysis, we compute the secrecy outage probability for the nearest eavesdropper as

$$\mathcal{P}_{\mathrm{out}}(R_{\ell}) = \int_0^{\infty} \Pr\{\Upsilon_e(r) > \beta_{\ell}\} f_{r_{\mathrm{e}}}(r) \mathrm{d}r, \tag{6.2}$$

where $\beta_{\ell} = 2^{R_{\ell}} - 1$.

Each secondary user of cognitive sensor networks must sense the channel before it starts using the spectrum, in order to not cause harmful interference to the primary channel. To satisfy this constraint, the secondary users should rely on some of the sensing techniques as specified in [59] and [60]. The activity of secondary user is thus conditioned on not receiving a beacon signal from any primary user. For convenience, we define the auxiliary variable $X \triangleq |h|^2$, such that a secondary user is active if

$$\frac{PX}{r^{\alpha}} \leq \delta \rightarrow r^{-\alpha} X \leq \bar{\xi}, \tag{6.3}$$

where $\bar{\xi} = \frac{\delta}{P}$ is the normalized activating threshold.

**Channel Model**

We consider path loss and fading of the wireless channel, which are assumed to be independent over the network. The pathloss is usually modeled as $l(r) = r^{-\alpha}$, while the fading under Nakagami-$m$ channel as [12]

$$X \sim f_X(x; m) \triangleq \frac{m^m x^{m-1} e^{-mx}}{\Gamma(m)}, \tag{6.4}$$

where $m$ is the fading parameter and $\Gamma(m)$ is the upper incomplete gamma function.

If the received fading envelope at receiver is also affected by shadowing, then the composition of Nakagami-$m$ fading and Log-Normal (LN) shadowing has a Gamma-LN

distribution whose PDF is given by

$$f_X(x;m,\mu_p,\sigma_p)=\int_0^\infty \left(\frac{m}{z}\right)^m x^{m-1}e^{-\frac{m}{z}x}\Gamma(m)\frac{\varrho}{\sqrt{2\pi}\mu_{\Omega_p}z}\exp\left(-\frac{(\varrho\log z-\mu_{\Omega_p})^2}{2\sigma^2_{\Omega_p}}\right)\mathrm{d}z, \quad (6.5)$$

where $\Omega_p$ is the mean squared-envelope, $\mu_{\Omega_p}$ and $\sigma_{\Omega_p}$ are mean and standard deviation of $\Omega_p$ respectively, and $\varrho=\log(10)/10$.

Since the closed form solution for composite Gamma-LN distribution is hard to obtain, we use the approximation of equation (6.5) with a single LN distribution[2] as given in [93]

$$X\sim f_X(x;\mu_{dB},\sigma_{dB})=\frac{1}{\sqrt{2\pi}\mu_{dB}x}\exp\left(-\frac{(\log x-\mu_{dB})^2}{2\sigma^2_{dB}}\right), \quad (6.6)$$

$$\mu_{dB}=\varrho[\psi(m)-\log(m)]+\mu_{\Omega_p},\sigma_{dB}=\varrho^2\zeta(2,m)\sigma^2_{\Omega_p}, \quad (6.7)$$

where $\psi(m)$ is the Euler psi function and $\zeta(2,m)$ is the generalized Riemann zeta function.

Clearly, the difficulty in evaluating Eq. (6.2) is determining the distribution of $\Upsilon_e$, which in turn requires the evaluation of the distribution of aggregate interference $I_{\mathrm{s}}$. The latter is the subject of next section, in which we characterized the distribution of interference using cumulants approach.

The normalized interference generated by all the users at the receiver is

$$I_{\mathrm{s}}=\sum_{k=1}^{\infty}X_{\mathrm{s}:k}\cdot r_{\mathrm{s}:k}^{-\alpha}, \quad (6.8)$$

where $X_{\mathrm{s}:k}$ and $r_{\mathrm{s}:k}$ are the squared fading envelope and the distance from the source to the $k$-th secondary user, respectively.

We also assume that no user is located closer than $r_{min}$ to the primary receiver, which is a reasonable assumption in practical scenarios. For sake of simplicity, we consider $r_{min}=1$ throughout our discussion. Similar to the characterisation of aggregate collusion, here also we employ cumulants technique in order to model various distributions of interest.

[2]By slight abuse of notation, we reuse $X$ to denote composite distribution of Nakagami-$m$ fading and LN Shadowing.

Again, by force of Campbell's theorem, the characteristic function of $I_{\mathrm{s}}$ can be computed by [59, 60] as similar to the Eq. (5.12).

$$\phi_{I_{\mathrm{s}}}(w) = \exp\left(-2\pi\lambda_{\mathrm{s}} \int_{X} \int_{r_{min}}^{\infty} [1-\exp(jwxr^{-\alpha})] f_X(x) r \mathrm{d}r\mathrm{d}x\right), \tag{6.9}$$

where $j$ is the imaginary unit. Due to the constraint on secondary transmissions as specified in Eq. (6.3), Eq. (6.9) can be re-written as

$$\phi_{I_{\mathrm{s}}}(w) = \exp\left(-2\pi\lambda_{\mathrm{s}} \int_{X} \int_{r_{min}}^{\infty} [1-\exp(jwxr^{-\alpha})] \mathbf{1}\{r^{-\alpha}x\} f_X(x) r \mathrm{d}r\mathrm{d}x\right). \tag{6.10}$$

Unfortunately neither Eq. (6.10) nor its inverse Laplace transform admit a closed form, except for the specific case of Rayleigh fading [24]. We can, however, employ Eq. (6.10) to obtain closed forms of the corresponding cumulants. The $n$-th cumulant of $\phi(w)$ can be expressed as

$$\kappa_{I_{\mathrm{s}}}(n) = \frac{1}{j^n} \frac{\mathrm{d}^n \log \phi_{I_{\mathrm{s}}}(w)}{\mathrm{d}w^n}\Big|_{w=0} \tag{6.11}$$

Substitute (6.10) into (6.11), the $n$-th cumulant expressed as

$$\kappa_{I_{\mathrm{s}}}(n) = 2\pi\lambda_{\mathrm{s}} \int_{0}^{\infty} \int_{\max\{1,(x/\bar{\xi})^{1/b}\}}^{\infty} x^n r^{1-nb} f_X(x) \mathrm{d}r\mathrm{d}x. \tag{6.12}$$

After series of integral caluculations (please refer [59, 60] for detailed derivations),

$$\kappa_{I_{\mathrm{s}}}(n) = \frac{2\pi\lambda_{\mathrm{s}}}{nb-2} \left[E_X^l(n, \bar{\xi}) + \bar{\xi}^{n-\frac{2}{b}} E_X^u(\tfrac{2}{b}, \bar{\xi})\right], \tag{6.13}$$

where $E_X^l(n, \bar{\xi})$ and $E_X^u(\frac{2}{b}, \bar{\xi})$ are $n$-th order lower and upper partial moments of $X$ respectively. The closed form expressions of $\kappa_{I_{\mathrm{s}}}(n)$ under Nakagami-$m$ and Log-Normal distributions are provided in [59].

Based on the Eq. (6.13) exact cumulant expression, various models for the distribution of the equivalent aggregate interference can be built, some of which are discussed in the sequel. Before we proceed, let us recap the Edgeworth series, which is the

optimum asymptotic expansion to approximate a probability distribution in terms of its cumulants [83] in the sense that it minimizes the error between the cumulants of the reconstructed distribution and the original (exact) cumulants themselves. Due to analytical intractability of this model, prompts us to consider a simpler (and in fact more accurate) models.

### 6.2.1 Modeling $I_{\mathrm{s}}$ as a Gamma Variate

In order to obtain a more tractable and accurate model for the distribution of $I_{\mathrm{s}}$, start by noticing that for the specific case of $\alpha = 2$, the terms $X_{\mathrm{s}:k} \cdot r_{\mathrm{s}:k}^{-\alpha}$ in Eq. (6.8) are given by the square of the ratio of two Nakagami-$m$ variates. But it has been recently shown [84] that the ratio of Nakagami variates is itself well approximated by a Nakagami variate, from which it follows that for $\alpha = 2$ each term $X_{\mathrm{s}:k} \cdot r_{\mathrm{s}:k}^{-\alpha}$ is (approximately) a Gamma variate. And since the sum of Gamma variates is also a Gamma variate, we conclude that for specific case of $\alpha = 2$ the distribution of the equivalent aggregate interference $I_{\mathrm{s}}$ can be well approximated by a Gamma distribution.

Motivated by this fact, we consider a gamma model for $I_{\mathrm{s}}$ also for other values of $\alpha$. Specifically, we consider the model

$$f_{I_{\mathrm{s}}}^{(\Gamma)}(x;\nu,\theta) = \frac{x^{\nu-1}e^{-\frac{x}{\theta}}}{\theta^{\nu}\Gamma(\nu)}, \tag{6.14}$$

where the parameters $\nu$ and $\theta$ are given by

$$\nu = \frac{\kappa_{I_{\mathrm{s}}}^2(1)}{\kappa_{I_{\mathrm{s}}}(2)}, \theta = \frac{\kappa_{I_{\mathrm{s}}}(2)}{\kappa_{I_{\mathrm{s}}}(1)}. \tag{6.15}$$

### 6.2.2 Modeling $I_{\mathrm{s}}$ as a Log-Normal Variate

Considering the fact that the $I_{\mathrm{s}}$ is heavy-tailed and positively skewed random variable, we consider another approximation model for interference characterization, that is Log-Normal distribution approximation. By doing so, we obtain the following expressions relating cumulants to parameters of LN distribution

$$f_{I_{\mathrm{s}}}^{(L)}(x;\mu,\sigma) = \frac{1}{\sqrt{2\pi}\mu x}\exp\left(-\frac{(\log x-\mu)^2}{2\sigma^2}\right), \tag{6.16}$$

where the parameters $\mu$ and $\sigma$ are given by

$$\mu = \log\left(\frac{\kappa_{I_{\mathrm{s}}}^2(1)}{\sqrt{\kappa_{I_{\mathrm{s}}}^2 1) + \kappa_{I_{\mathrm{s}}}^2(2)}}\right), \sigma^2 = \log\left(1+\frac{\kappa_{I_{\mathrm{s}}}(2)}{\kappa_{I_{\mathrm{s}}}^2(1)}\right). \tag{6.17}$$

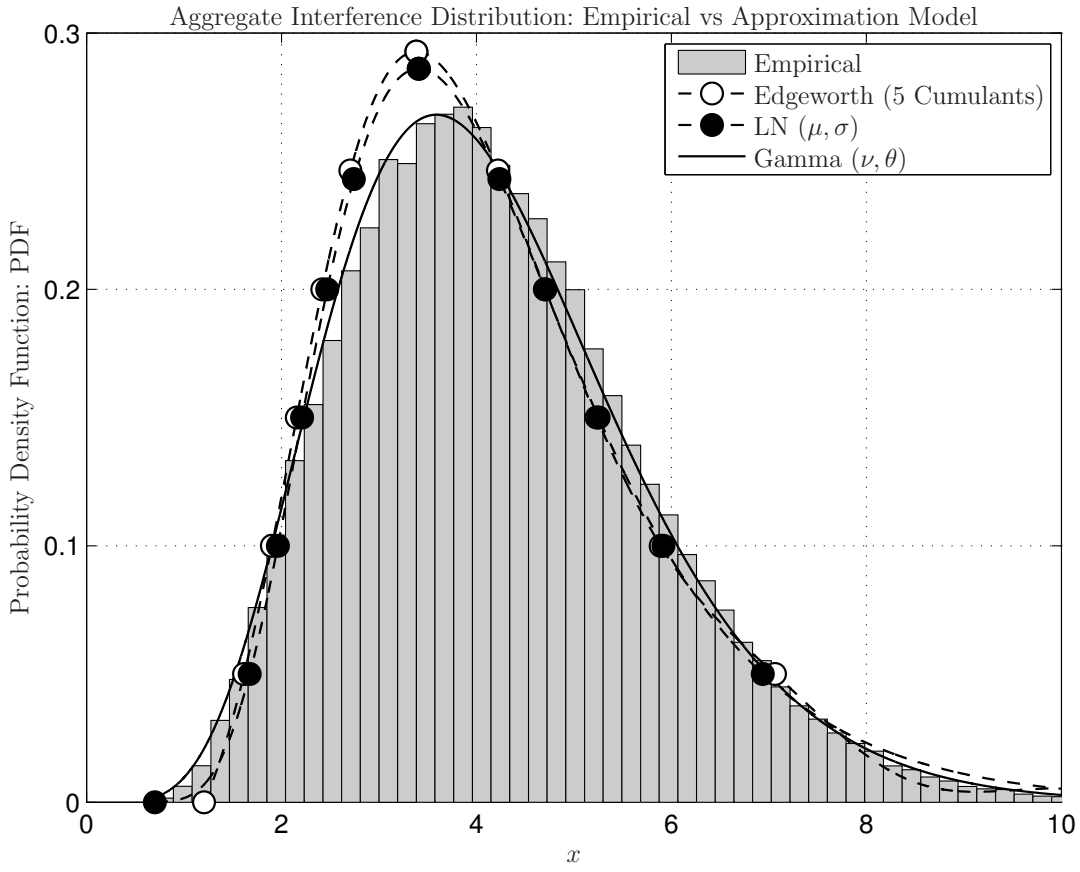



Figure 6.1: Edgeworth, Gamma and Log-Normal models compared to empirical distribution ($\alpha = 4$, $m = 1$, $\lambda_s = 1$).

The accuracy of the Gamma model and LN model is illustrated in Fig. 6.1. The empirical PDF of $I_{\rm s}$ for $\alpha = 4$, with $m = 1$ (Rayleigh fading) and $\lambda_{\rm s} = 1$ is compared against the Gamma distribution and LN distribution given in equations (6.14) and (6.16), respectively. The results indicate that in fact both approximations are very accurate and superior to that provided by the Edgeworth expansion with 5 cumulants.

## 6.3 Secrecy Outage

In this section, we aim to characterize the secrecy outage by considering the approximation models from sections 6.2.1 and 6.2.2. We obtain probability of secrecy outage under two different channel models, one under Nakagami-$m$ fading and the other under the combination of Nakagami-$m$ fading and LN shadowing. To derive the secrecy outage probability, for the first phenomenon, we use gamma approximation model for interference characterization, while for the latter case we use LN approximation.

### 6.3.1 Nakagami-$m$ Fading Channel Model

As discussed in the previous section, to derive secrecy outage probability, $\Pr\{\Upsilon_{\rm e}(r) > \beta_\ell\}$ needs to be computed beforehand. Now, when the received signal $X_{\rm e}$ at eavesdropper is a Gamma random variable with $\nu_{\rm e}(= m)$ and $\theta_{\rm e}(= \frac{1}{m})$ and interference is modeled with another gamma random variable with $\nu_{\rm s}$ and $\theta_{\rm s}$ as discussed in section 6.2.1, the $\Pr\{\Upsilon_{\rm e}(r) > \beta_\ell\}$ is given as in [61]

$$\Pr\{\Upsilon_{\rm e}(r) > \beta_e\} = \frac{\Gamma(\nu_{\rm e}+\nu_{\rm s})}{\Gamma(\nu_{\rm e})}\left(\frac{\theta_e}{r^2\beta_e\theta_{\rm s}}\right)^{\nu_{\rm s}} \times {}_2F_1\left(\nu_{\rm s}, \nu_{\rm e}+\nu_{\rm s}, 1+\nu_{\rm s}, -\frac{\theta_e}{r^2\beta_e\theta_{\rm s}}\right). \quad (6.18)$$

Consequently, the secrecy outage probability calculated from Eq. (6.2) is

$$\begin{aligned}
&\mathcal{P}_{\rm out}(\beta_\ell; r, \nu_{\rm e}, \theta_{\rm e}, \nu_{\rm s}, \theta_{\rm s}) \qquad (6.19)\\
&= \frac{2\pi\lambda_e\Gamma(\nu_{\rm e}+\nu_{\rm s})}{\Gamma(\nu_{\rm e})}\left(\frac{\theta_e}{\beta_e\theta_{\rm s}}\right)^{\nu_{\rm s}} \int_0^\infty \frac{re^{-\pi\lambda_e r^2}}{(r^2)^{\nu_{\rm s}}} {}_2F_1\left(\nu_{\rm s}, \nu_{\rm e}+\nu_{\rm s}, 1+\nu_{\rm s}, -\frac{\theta_e}{r^2\beta_e\theta_{\rm s}}\right) {\rm d}r,\\
&= \frac{\pi\lambda_e\Gamma(\nu_{\rm e}+\nu_{\rm s})}{\Gamma(\nu_{\rm e})}\left(\frac{\theta_e}{\beta_e\theta_{\rm s}}\right)^{\nu_{\rm s}} \left\{\left(\frac{\theta_e}{\beta_e\theta_{\rm s}}\right)^{1-\nu_{\rm s}} \Gamma\left(\begin{matrix}1+\nu_{\rm s}, \nu_{\rm s}-1, 1, \nu_{\rm e}+1\\ \nu_{\rm s}, \nu_{\rm e}+\nu_{\rm s}, 2\end{matrix}\right) \times \right.\\
&\left. {}_2F_2\left(1, \nu_{\rm e}+1, 2-\nu_{\rm s}, \nu_{\rm s}; \frac{\lambda_e\pi\theta_e}{\beta_e\theta_{\rm s}}\right) + (\pi\lambda_e)^{\nu_{\rm s}-1}\Gamma(1-\nu_{\rm s}) {}_2F_2\left(\nu_{\rm s}, \nu_{\rm e}+\nu_{\rm s}, 1+\nu_{\rm s}, \nu_{\rm s}; \frac{\lambda_e\pi\theta_e}{\beta_e\theta_{\rm s}}\right)\right\},
\end{aligned}$$

where the last integral follows from the table of integrals in [68, pp.268, Eq. (2.21.2.6)].

### 6.3.2 Shadowed Fading Channel Model

In the scenario of shadowed fading channel model, the received signal $X_{\mathrm{e}}$ is LN with $\mu_{\mathrm{e}}$ and $\sigma_{\mathrm{e}}$ as discussed in the channel model. Meanwhile, the aggregate interference is another LN with $\mu_{\mathrm{s}}$ and $\sigma_{\mathrm{s}}$ as mentioned in Section 6.2.2. By the multiplicative reproductive productive property of LN random variables, the secrecy outage is given as

$$\Pr\{\Upsilon_e(r) > \beta_\ell\} = Q\left[\frac{\beta_\ell r^2 - \mu}{\sigma}\right], \tag{6.20}$$

where $\mu = \mu_{\mathrm{s}} - \mu_{\mathrm{e}}$ and $\sigma = \sqrt{\sigma_{\mathrm{s}}^2 + \sigma_{\mathrm{e}}^2}$.

Combining Eq. (6.2), and Eq. (6.20), we obtain secrecy outage probability straightforwardly,

$$\begin{aligned}
\mathcal{P}_{\mathrm{out}}(\beta_\ell; r, \mu, \sigma) &= \int_0^\infty Q\left[\frac{\beta_\ell r^2 - \mu}{\sigma}\right] f_{r_{\mathrm{e}}}(r)\mathrm{d}r, \qquad (6.21)\\
&= \pi\lambda_e \int_0^\infty \mathrm{erfc}\left[\frac{\beta_\ell r^2 - \mu}{\sqrt{2}\sigma}\right] e^{-\pi\lambda_e r^2} r\mathrm{d}r,\\
&= \frac{\pi\lambda_e\sigma}{\sqrt{2}r_{\mathrm{e}}} e^{-\frac{\pi\lambda_e\mu}{r_{\mathrm{e}}}} \int_{-\mu/\sqrt{2}\sigma}^\infty \mathrm{erfc}[z] e^{-\frac{\pi\lambda_e\sqrt{2}z\sigma}{r_{\mathrm{e}}}} \mathrm{d}z,\\
&= -\frac{e^{-\frac{\pi\lambda_e\mu}{\beta_\ell}}}{2} e^{\left(\frac{\pi\lambda_e\sigma\sqrt{2}}{2\beta_\ell}\right)^2} \mathrm{erfc}\left(\frac{\pi\lambda_e\sigma}{\sqrt{2}\beta_\ell} - \frac{\mu}{\sqrt{2}\sigma}\right) + \left(1 + \mathrm{erf}\left(\frac{\mu}{\sqrt{2}\sigma}\right)\right)/2,
\end{aligned}$$

where $\mathrm{erf}(x)$ and $\mathrm{erfc}(x)$ are error functions.

Plots of secrecy outage probabilities from the expressions (6.19) and (6.21) are shown in figures 6.2 and 6.3. Fig. 6.2 is drawn under the composite Nakagami-$m$ fading and LN shadowing channel model with the parameters $\mu_{\mathrm{e}} = 0$, $\sigma_{\mathrm{e}} = 6$, $\alpha = 4$ and for various $m$ and $\mu_{\mathrm{s}}, \sigma_{\mathrm{s}}$ are calculated from Eq. (6.17). Fig. 6.2 indicates that probability of secrecy outage decreases with the increase in eavesdropper's equivocation rate, and the secrecy outage decreases with the increase in density of eavesdroppers.

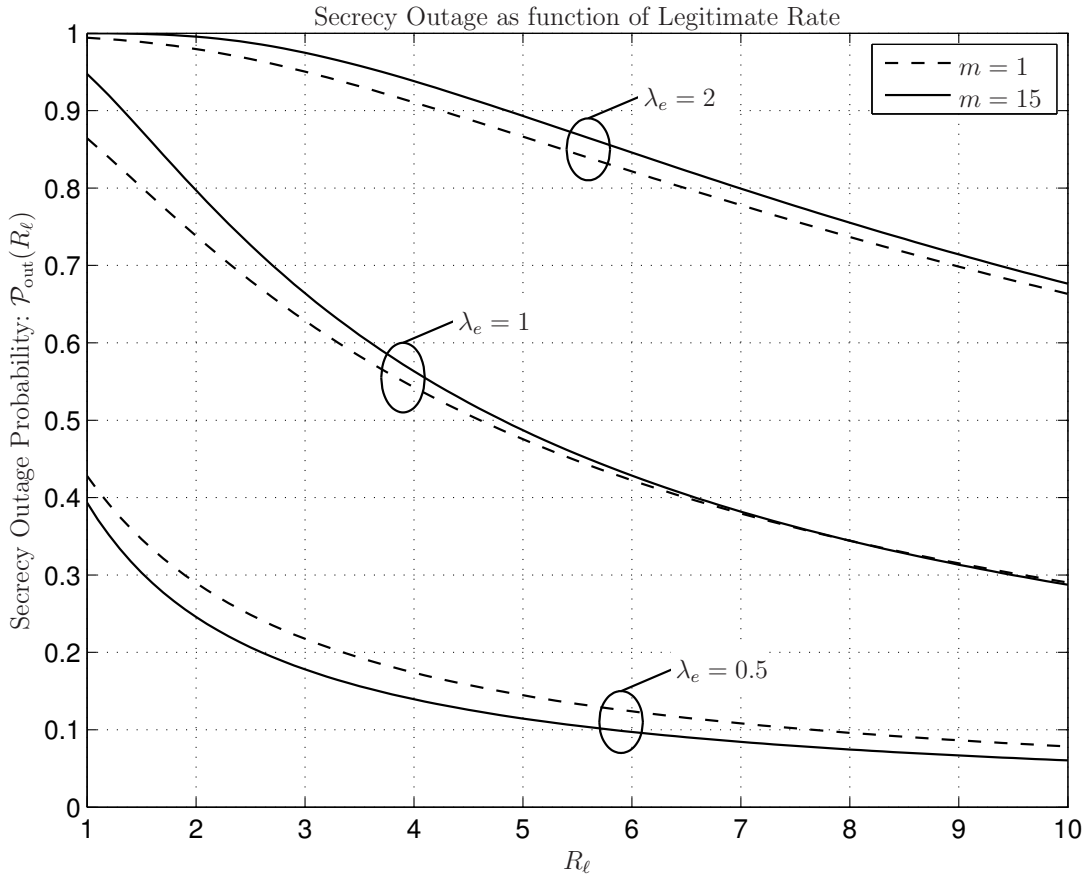



Figure 6.2: Secrecy outage as a function of eavesdropper's equivocation rate ($\beta_\ell$) for the case of $m = 1$ and $m = 15$, respectively.

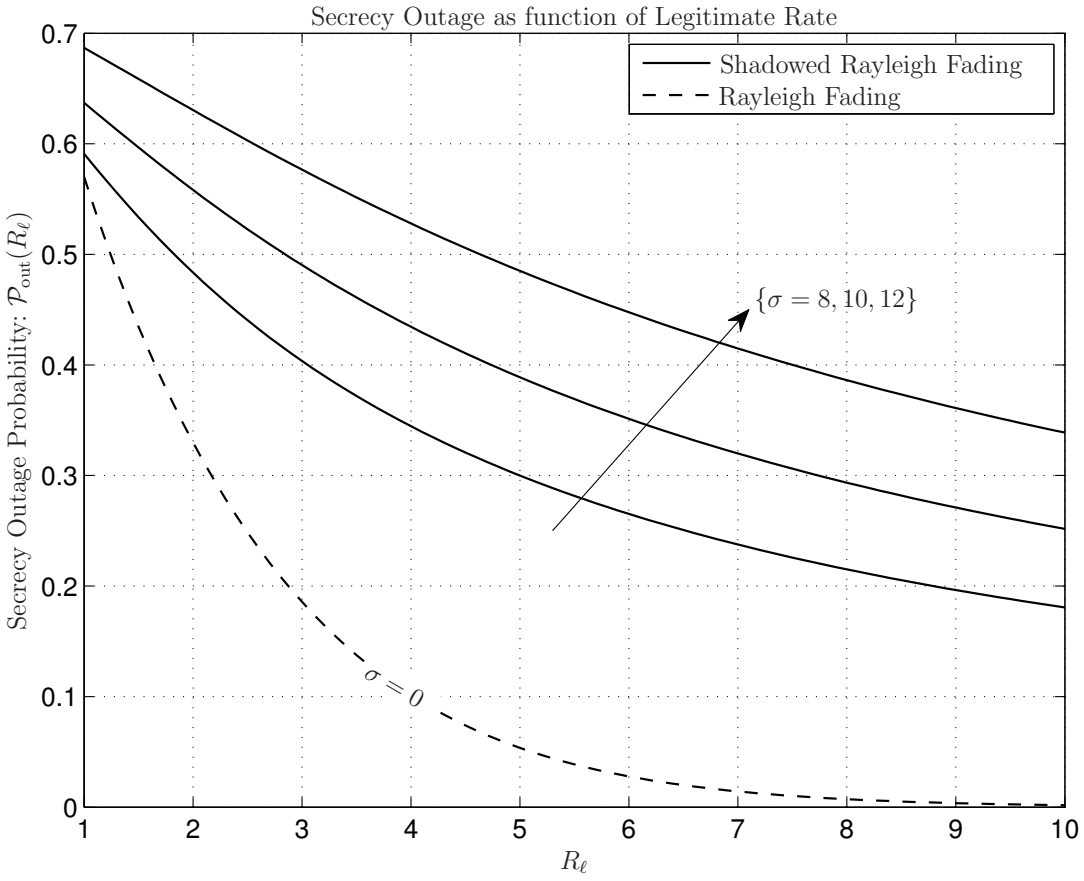



Figure 6.3: Secrecy outage as a function of eavesdropper's equivocation rate ($\beta_\ell$) for the case of $m = 1$.

The results in Fig. 6.2, however, are intuitive as the intensity of fading has little impact on the secrecy outage. Rather, the density of eavesdroppers has the most significant impact on secrecy outage, followed by the equivocation ratio.

In Fig. 6.3, comparison of the plots of secrecy outage probability under the two phenomenon - Nakagami-$m$ fading and composite Nakagami-$m$ fading-LN Shadowing are shown with the parameters $\mu_{\mathrm{e}} = 0$, $\alpha = 4$ with various $\sigma_{\mathrm{e}}$ and $\mu_{\mathrm{s}}, \sigma_{\mathrm{s}}$ calculated from Eq. (6.17). It is illustrated from the figure that, the secrecy outage probability increases while the value of $\sigma_e$ increases and secrecy outage is lesser in the case of Nakagami-$m$ fading as compared to the composite case. We can also comprehend from the figure that the secrecy capacity can still be mainatined at lower equivocation rates. On the other hand, it is found that the presence of shadowing is an even stronger factor that can quickly increase the secrecy outage.

## 6.4 Conclusions

We offered original and accurate expressions for the aggregate interference with fading and shadowing, which can also be used to obtain other analytical results. In particular, we conducted a detailed analysis of the secrecy outage under the impact of Nakagami-$m$ fading, shadowing and density of eavesdroppers. The conclusions attained from our analysis can be specified as - the secrecy capacity can be maintained at lower equivocation rates, the impact of shadowing is severe as it increases the secrecy outage quickly and eavesdropper's density impacts secrecy outage the most which is closely followed by the equivocation ratio. Recently, we have submitted these results in [94].

We list our contributions of this chapter as below

- Section 6.1: We approximated the aggregate interference with Gamma and Log-Normal random variables.
- Section 6.2: We derived the secrecy outage probability under Nakagami fading channel and Log-Normal fading channels [94].

# Chapter 7

# Multiple Antenna Systems

**Summary:**

*In this chapter, we derive the closed-form expressions for the secrecy outage probability of random networks under Nakagami-m fading channel with multiple antennas and in the presence of randomly located eavesdroppers. We also further analyse the alternative (conditional) secrecy outage probability [95] which helps to compare the cost incurred to achieve secrecy by measuring the probability that a transmitted signal fails to achieve perfect security. In addition, various transmission factors such as number of antennas, fading coefficient, and node density are analyzed to assess their impact on the secrecy outage probability of the random network.*

## 7.1 Introduction

Although there is an increasing tendency of research on intrinsic secrecy in random wireless network, most current works focus on systems with single antenna and mainly study prorogation without fading or with Rayleigh fading [24]. Nakagami-$m$ fading matches some empirical fading conditions which are more or less severe than that of Rayleigh fading and has the advantage of including Rayleigh fading as a special case [47]. The study of secrecy capacity and secrecy outage under Nakagami-$m$ fading was investigated in [96] by considering point to point transmission. Recently, in [19], the authors analyzed the secrecy outage probability of random networks under Nakagami-$m$ fading channel with PPP distributed eavesdroppers.

Most of the above works [14,19,24,29] considered the single antenna node case. Previous works on the impact of multiple antennas in random networks with secrecy is not vast, but there are few works done in this domain. For instance, authors studied secure connectivity of wireless random networks with multi-antenna transmission in Rayleigh fading channels with directional antenna and eigen-beamforming schemes in [30]. More recently, in [97], authors have computed the secrecy rate under a regularized channel inversion precoding in a Rayleigh fading channel.

In this chapter, we derived closed-form expressions for the secrecy outage probability of random networks in the presence of randomly located eavesdroppers. The contributions of this work are two-fold

- Unlike the works of [14,19] and [24], which considered the case with single antenna, we study the secrecy outage of random networks with multiple antennas; To generalize the pathloss model, this chapter study Nakagami-$m$ fading by taking Rayleigh fading as a special case which is commonly analyzed as in [30], [97];
- To analyse the cost incurred to achieve secrecy, we study the alternative (conditional) secrecy outage probability [95] which helps to compare the cost incurred to achieve secrecy by measuring the probability that a transmitted signal fails to achieve perfect security.

### System Model

Consider a random network in an unbounded Euclidean space of dimension $d$, modeled by a stationary PPP [64] of intensity $\lambda$ in $\mathbb{R}^d$. Let the aforementioned model be

applied to two overlaid networks of *legitimate* nodes and *eavesdroppers*, respectively, with corresponding densities $\lambda_\ell$ and $\lambda_\mathrm{e}$, and their correspondent PPP are denoted as $\Phi_\ell$ and $\Phi_\mathrm{e}$, respectively. Let the location of a given source define the origin of the space, without lack of generality. Consider that the source wishes to unicast to a legitimate node $\ell$, located at a distance $r_\ell$, in the presence of an eavesdropper located at the unknown distance $r_\mathrm{e}$, both subjected to Nakagami-$m$ fading and path loss governed by the exponent $\alpha$. The source node uses an N antenna uniform linear array (ULA) for signal transmission. All the legitimate nodes and eavesdroppers are each equipped with single antenna. The channel coefficients from source node to legitimate receivers and eavesdropper are denoted as $h_\ell$ and $h_\mathrm{e}$, respectively. The signals received at legitimate receiver and eavesdropper can be presented as

$$\begin{aligned} Y_\ell &= \sqrt{P}\mathbf{u}\mathbf{v}_\ell h_\ell r_\ell^{-\frac{\alpha}{2}} x + n_\ell, \\ Y_\mathrm{e} &= \sqrt{P}\mathbf{u}\mathbf{v}_\mathrm{e} h_\mathrm{e} r_\mathrm{e}^{-\frac{\alpha}{2}} x + n_\mathrm{e}, \end{aligned} \tag{7.1}$$

where, $P$ is the transmission power; $\mathbf{u}$ is the normalized transmit beamforming vector; $x$ is the information signal with $\mathbb{E}\{|x|^2\} = 1$; $n_\ell$ and $n_\mathrm{e}$ are the AWGN; $\mathbf{v}_i = [1, e^{j\pi\cos\theta_i}, \cdots, e^{j\pi(N-1)\cos\theta_i}]^T$ is the antenna manifold vector.

We assume that the CSI of legitimate channel is available at the source node by using feedback. The transmitting beamforming vector to maximize signal-to-noise-ratio (SNR) at legitimate receiver can be achieved by, $\mathbf{u} = \frac{\mathbf{v}_\ell}{\sqrt{N}}$. The random path gains of the channels between the source and a given legitimate node and eavesdropper can be given as $\zeta_\ell \triangleq N|h_\ell|^2/r_\ell^\alpha$ and $\zeta_\mathrm{e} \triangleq \omega(\theta)|h_\mathrm{e}|^2/r_\mathrm{e}^\alpha$, where $\omega(\theta) = \frac{1}{N}|\mathbf{v}_\ell^H\mathbf{v}_\mathrm{e}|^2$. Then, the *secrecy capacity* of the unicast channel, is [8, 9]

$$\mathcal{C}_s = \max\{0, \log_2(1+\zeta_\ell\rho) - \log_2(1+\zeta_\mathrm{e}\rho)\}, \tag{7.2}$$

Consequently, the probability that the secrecy capacity of the legitimate channel is above a given threshold $R_s \geq 0$ is defined as [24]

$$\tilde{\mathcal{P}}_\mathrm{out}(R_s) \triangleq \Pr\{\mathcal{C}_s > R_s\} = \Pr\left\{\log_2\left(\tfrac{1+\zeta_\ell\rho}{1+\zeta_\mathrm{e}\rho}\right) > R_s\right\}. \tag{7.3}$$

From (7.2), the *secrecy outage probability* $\Pr\{\mathcal{C}_s > R_s\}$ can be rewritten as

$$\mathcal{P}_\mathrm{out}(R_s) \triangleq \Pr\{\mathcal{C}_s \leq R_s\} = 1 - \Pr\{\mathcal{C}_s > R_s\}. \tag{7.4}$$

By considering the alternative secrecy outage probability as described in [95], the source node might be able to choose two rates, i.e. the transmission rate $R$ and the secrecy rate $R_s$. For any transmitted signal, the legitimate node will be able to decode if the channel capacity is greater than the transmission rate, $C_\ell > R$, to achieve perfect secrecy. The alternative secrecy outage probability can be expressed in terms of conditional probability as $\mathcal{P}_{\text{out}}(R_s) = \Pr\{C_s < R_s | C_\ell > R\}$.

Besides the outage probabilities themselves, we shall hereafter also consider as a figure of merit the *conditional secrecy outage probability*, which by force of the Bayes rule is defined as

$$\mathcal{P}_{\text{out}}^{\text{co}} = \Pr\{C_s < R_s, C_\ell > R\}/\Pr\{C_\ell > R\}. \tag{7.5}$$

The interpretation of Eq. (7.5) is the likelihood that the channel is in outage for secrecy, although not in outage for communications. Or in other words, what is the chance that secret communication cannot take place at a desired rate, given that the legitimate channel can sustain a prescribed rate of communication.

Denote $\mathcal{P}_{\text{out}}^{S} = \Pr\{C_s < R_s, C_\ell > R\}$ and $\mathcal{P}_{\text{out}}^{T} = \Pr\{C_\ell > R\}$, conditional secrecy outage probability can be written as

$$\mathcal{P}_{\text{out}}^{\text{co}} = \frac{\mathcal{P}_{\text{out}}^{S}}{\mathcal{P}_{\text{out}}^{T}}. \tag{7.6}$$

## 7.2 Path Gain Distributions

### 7.2.1 Path Gain Distribution of the Legitimate Node

Since our interest is to characterize the secrecy outage of a particular node, the distributions of interest concerning the legitimate network are those corresponding to the path gains of each legitimate node $\zeta_\ell$. In this chapter, we consider the path gain distribution of legitimate nodes $\zeta_\ell = N|h_\ell|^2/r_\ell^\alpha$. Recall that the probability distribution function of Nakagami-m fading [12]

$$h \sim f(x, m) = \tfrac{2m^m}{\Gamma(m)} x^{2m-1} e^{-mx^2}. \tag{7.7}$$

The cumulative density function for the path gain distribution of legitimate nodes can be derived as

$$F_{\zeta_\ell}(z; m, r_\ell, \alpha, N) = \Pr(N|h_\ell|^2 r_\ell^{-\alpha} < z), \tag{7.8}$$
$$= \int_0^{\sqrt{\frac{z}{N}} r_\ell^{\alpha/2}} f(x, m)\mathrm{d}x = \frac{\Gamma(m) - \Gamma(m, \frac{m \cdot z \cdot r_\ell^\alpha}{N})}{\Gamma(m)}.$$

By taking the derivative of Eq. (7.8), the probability density function of the path gain can be expressed as

$$f_{\zeta_\ell}(z; m, r_\ell, \alpha, N) = \frac{m^m r_\ell^{m\cdot\alpha} z^{m-1} e^{-\frac{z\cdot m\cdot r_\ell^\alpha}{N}}}{N^m \Gamma(m)}. \tag{7.9}$$

### 7.2.2 Path Gain Distribution of the "Best" Eavesdropper

In order to obtain an expression for the secrecy outage probability Eq. (7.4) and conditional secrecy outage probability Eq. (7.5), the distribution of the path gain $\zeta_\mathrm{e}$ need to be derived. Before we proceed to do so, however, some qualitative comments are in order. In contrast, for a given legitimate path gain $\zeta_\ell$ what determines the secrecy capacity of a channel subjected to fading is not any specific eavesdropper, but rather the eavesdropper with the *maximum*(instantaneous) path gain amongst those present. The distribution of interest, *i.e* the path gain distribution of the best eavesdropper ($\bar{\zeta}_\mathrm{e}$) can be derived using PGFL of PPP as (for $\alpha = 2$)

$$\begin{aligned} F_{\bar{\zeta}_\mathrm{e}}(z) &= \Pr\{\bar{\zeta}_\mathrm{e} < z\} = \mathbb{E}_{\Phi_E}[\Pr\{\max_{\mathrm{e}\in\phi}(\zeta_\mathrm{e}) < z|\Phi_E\}], \\ &= \mathbb{E}_{\Phi_E}\left[\prod_{\mathrm{e}\in\Phi_E} \Pr\{\zeta_\mathrm{e} < z|\Phi_E\}\right] = \mathbb{E}_{\Phi_E}\left[\prod_{\mathrm{e}\in\Phi_E}\left(1 - \frac{\Gamma(m, \frac{m\cdot z\cdot r_\mathrm{e}^2}{\omega(\theta)})}{\Gamma(m)}\right)\right], \\ &= \exp\left(-\lambda_\mathrm{e}\int_0^{2\pi}\int_0^{\infty} r_\mathrm{e}\cdot\frac{\Gamma(m, \frac{m\cdot z\cdot r_\mathrm{e}^2}{\omega(\theta)})}{\Gamma(m)}\mathrm{d}r_\mathrm{e}\ \mathrm{d}\theta\right), \\ &= \exp\left(-\lambda_\mathrm{e}\int_0^{2\pi}\frac{\omega(\theta)}{2z}\mathrm{d}\theta\right) = \exp\left(-\tfrac{\lambda_\mathrm{e}\Theta}{2z}\right), \end{aligned} \tag{7.10}$$

where $\Theta = \int_0^{2\pi}\omega(\theta)\mathrm{d}\theta$.

## 7.3 Secrecy Outage

### 7.3.1 Secrecy Outage Probability

With possession of path gain distributions of the legitimate and best eavesdropper channels, the secrecy outage probability between the source and legitimate node (in the presence of randomly located multiple eavesdroppers) can be written from Eq. (7.4) as

$$\mathcal{P}_{\text{out}}(R_s) = \int_0^\infty \int_{\beta(y)}^\infty f_{\bar{\zeta}_\text{e}}(x) f_{\zeta_\ell}(y) \mathrm{d}x \, \mathrm{d}y = \int_0^\infty (1 - F_{\bar{\zeta}_\text{e}}(\theta(y))) f_{\zeta_\ell}(y) \mathrm{d}y, \tag{7.11}$$

where $\theta(y) = 2^{R_s}[(\rho^{-1} + y) - \rho^{-1}]$.

Considering the case with $\alpha = 2, R_s = 0$, that is, the secrecy outage probability can be derived as

$$\begin{aligned} \mathcal{P}_{\text{out}}(R_s) &= \frac{m^m r_\ell^{2m}}{N^m \Gamma(m)} \int_0^\infty y^{m-1} e^{-\frac{y \cdot m \cdot r_\ell^2}{N}} \exp\left(-\tfrac{\lambda_\text{e}\Theta}{2y}\right) \mathrm{d}y, \\ &= 1 - \frac{2(m \cdot r_\ell)^m}{\Gamma(m)} \left(\frac{\lambda_\text{e}\Theta}{2N \cdot m}\right)^{\frac{m}{2}} \text{BesselK}\left[-\text{m}, \sqrt{\tfrac{2\text{m}r_\ell^2 \lambda_\text{e}\Theta}{\text{N}}}\right], \end{aligned} \tag{7.12}$$

where BesselK[a, b] is the modified Bessel function of the second kind.

### 7.3.2 Conditional Secrecy Outage Probability

In order to obtain the closed-form expression for the conditional secrecy outage probability, we need to evaluate numerator and denominator of Eq. (7.6).

First, Let us consider the denominator. The outage probability between the source node and legitimate node is calculated with path gain distribution as derived in Section 7.2 by taking $R = R_s$

$$\mathcal{P}_{\text{out}}^T = \frac{\Gamma(m, \frac{\beta \cdot m \cdot r_\ell^2}{N})}{\Gamma(m)}, \tag{7.13}$$

where $\beta = \frac{2^{R_s}-1}{\rho}$.

Now, we derive the numerator $\mathcal{P}_{\text{out}}^{S}$ as

$$\begin{aligned}\mathcal{P}_{\text{out}}^{S} &= \Pr\{\log_2\left(\tfrac{1+\zeta_\ell\rho}{1+\bar{\zeta}_\text{e}\rho}\right) < R_s, \log_2\left(1+\zeta_\ell\rho\right) > R_s\}, \\ &= \Pr\{\bar{\zeta}_\text{e} > \tfrac{\zeta_\ell-\beta}{T}, \zeta_\ell > \beta\} = \int_{\beta}^{\infty}\int_{\frac{y-\beta}{T}}^{\infty} f_{\bar{\zeta}_\text{e}}(x) f_{\zeta_\ell}(y)\mathrm{d}x\,\mathrm{d}y, \\ &= \int_{\beta}^{\infty}(1-F_{\bar{\zeta}_\text{e}}(\tfrac{y-\beta}{T}))f_{\zeta_\ell}(y)\mathrm{d}y.\end{aligned} \tag{7.14}$$

By substituting Eq. (7.10) into Eq. (7.14)

$$\begin{aligned}\mathcal{P}_{\text{out}}^{S} &= \frac{m^m r_\ell^{2m}}{N^m\Gamma(m)}\int_{\beta}^{\infty} y^{m-1}e^{-\frac{y\cdot m\cdot r_\ell^2}{N}}(1-\exp\left(-\tfrac{2^{R_s}\lambda_\text{e}\Theta}{2(y-\beta)}\right))\mathrm{d}y, \\ &= \frac{\Gamma(m,\frac{\beta\cdot m\cdot r_\ell^2}{N})}{\Gamma(m)} - \frac{m^m r_\ell^{2m}}{N^m\Gamma(m)}\int_{\beta}^{\infty} y^{m-1}e^{-\frac{y\cdot m\cdot r_\ell^2}{N}}\exp\left(-\frac{\lambda_\text{e}\Theta}{2\left(\frac{y-\beta}{2^{R_s}}\right)}\right)\mathrm{d}y, \\ &= \frac{\Gamma(m,\frac{\beta\cdot m\cdot r_\ell^2}{N})}{\Gamma(m)} - \frac{m^m r_\ell^{2m}(2^{R_s})^m}{N^m\Gamma(m)}\int_{\beta}^{\infty}(z+\tfrac{\beta}{2^{R_s}})^{m-1}e^{-\frac{(z\cdot 2^{R_s}+\beta)\cdot m\cdot r_\ell^2}{N}}\exp\left(-\tfrac{\lambda_\text{e}\Theta}{2z}\right)\mathrm{d}z.\end{aligned} \tag{7.15}$$

Consequently, conditional secrecy outage probability is computed as

$$\begin{aligned}\mathcal{P}_{\text{out}}^{\text{co}} &= 1 - \frac{m^m r_\ell^{2m}(2^{R_s})^m}{N^m\Gamma(m)}e^{-\frac{\beta\cdot m\cdot r_\ell^2}{N}}\sum_{j=0}^{m-1}\binom{m-1}{j}\left(\tfrac{\beta}{2^{R_s}}\right)^j \\ &\qquad\times\int_{\beta}^{\infty} z^{m-1-j}e^{-\frac{z\cdot 2^{R_s}\cdot m\cdot r_\ell^2}{N}}\exp\left(-\tfrac{\lambda_\text{e}\Theta}{2z}\right)\mathrm{d}z, \\ &= 1 - e^{-\frac{\beta\cdot m\cdot r_\ell^2}{N}}\sum_{j=0}^{m-1}\binom{m-1}{j}2^{1+\frac{j-m}{2}}\cdot\beta^j\cdot 2^{R_s\cdot\frac{m-j}{2}}\cdot m^{\frac{m+j}{2}} \\ &\qquad\times r_\ell^{m+j}(\lambda_\text{e}\Theta)^{\frac{m-j}{2}}\text{BesselK}\left[\text{j}-\text{m}, \sqrt{\tfrac{2^{\text{Rs}+1}\text{m}r_\ell^2\lambda_\text{e}\Theta}{\text{N}}}\right].\end{aligned} \tag{7.16}$$

With the expressions derived in the previous section we can study the availability of secrecy in random wireless networks in the presence of randomly distributed eavesdroppers, and the effect of fading thereby.

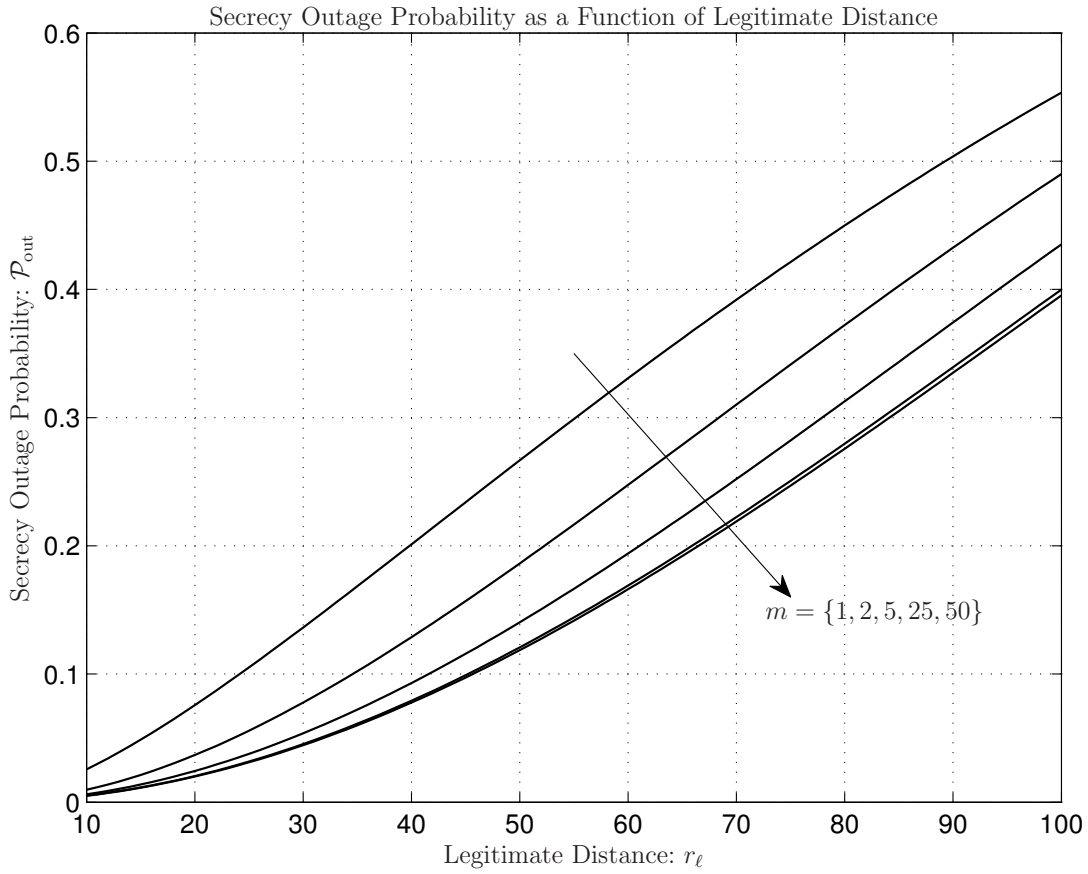



Figure 7.1: Secrecy outage probability as a function of legitimate distance for various fading figure $m$, with $\lambda_{\text{e}} = 0.0001$, $\theta = 90$ and $N = 5$.

First, we consider the secrecy outage probability $\mathcal{P}_{\text{out}}(R_s)$ as a function of legitimate distance as shown in Fig. 7.1. In this figure, we consider the impact of fading on the secrecy outage probability. On one hand, comparing with Rayleigh fading, $m = 1$, Nakagami-m fading contribute to enhance the secrecy of the network and the multiple antenna at the source node can better explore the channel diversity using beamforming. Also as the value of $m$ increases (fading decreases), the secrecy outage probability is relatively improved and approaches a lower bound similar to the channel with Gaussian fading. On the other hand, legitimate nodes far from transmitter will have higher secrecy outage probability.

In order to assess the effect of legitimate density on secrecy outage probability in comparison with eavesdropper density, we defined a new parameter $\lambda_\ell^{\min}(= 1/\pi r^2)$ which is the density at which no other legitimate node exists around the source node. In Fig. 7.2, we studied the secrecy outage probability as a function of fading parameter, number of antennas and density ratio between legitimate nodes and eavesdroppers.

Similar to previous results in Fig. 7.1, Fig. 7.2 suggests that as fading figure increases and the number of transmit antennas increases, the secrecy outage decreases. Besides, Fig. 7.2 shows that density ratio of legitimate and eavesdroppers has impact on the secrecy outage. For the case with higher density of eavesdropper, there is higher probability of secrecy outage, since the eavesdropper is more likely to exist in a smaller region around the source node and consequently have smaller path loss compared to legitimate nodes.

Fig. 7.3 displays various curves for different secrecy rates. As expected, the increase of required secrecy rate leads to higher probability of secrecy outage. The interesting point is that, the use of multiple antenna can significantly increase the security of the wireless network. As with more antennas, the transmitter can explore the transmission diversity and focus more signal power on the legitimate receiver by adopting beamforming.

It is illustrated from the Fig. 7.4 that, the conditional secrecy outage probability increases while the value of $\lambda_{\text{e}}$ increases. No particular insight is gained from this figure, as it is found that for any given $\lambda_{\text{e}}$, nodes further away have higher outage than nodes closer to the source, as expected. Setting aside the impact of fading, all the results combined also indicate that information theoretical secrecy is significant in random wireless networks with multiple transmit antennas at the source node, if the legitimate node is closer to source node with lesser eavesdropper density.

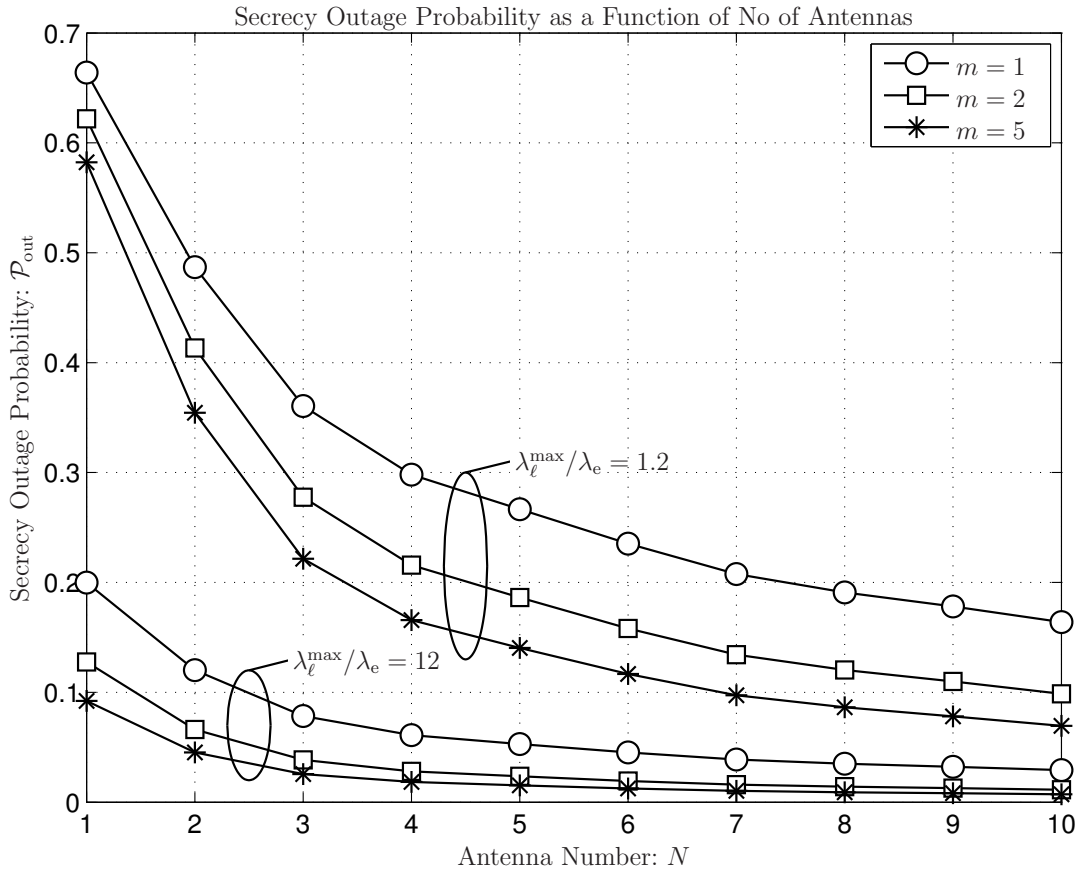



Figure 7.2: Secrecy outage probability as a function of eavesdropper density for various fading figure $m$ and different $\lambda_{\text{e}}$, with $r_\ell = 50m$ and $\theta = 90$.

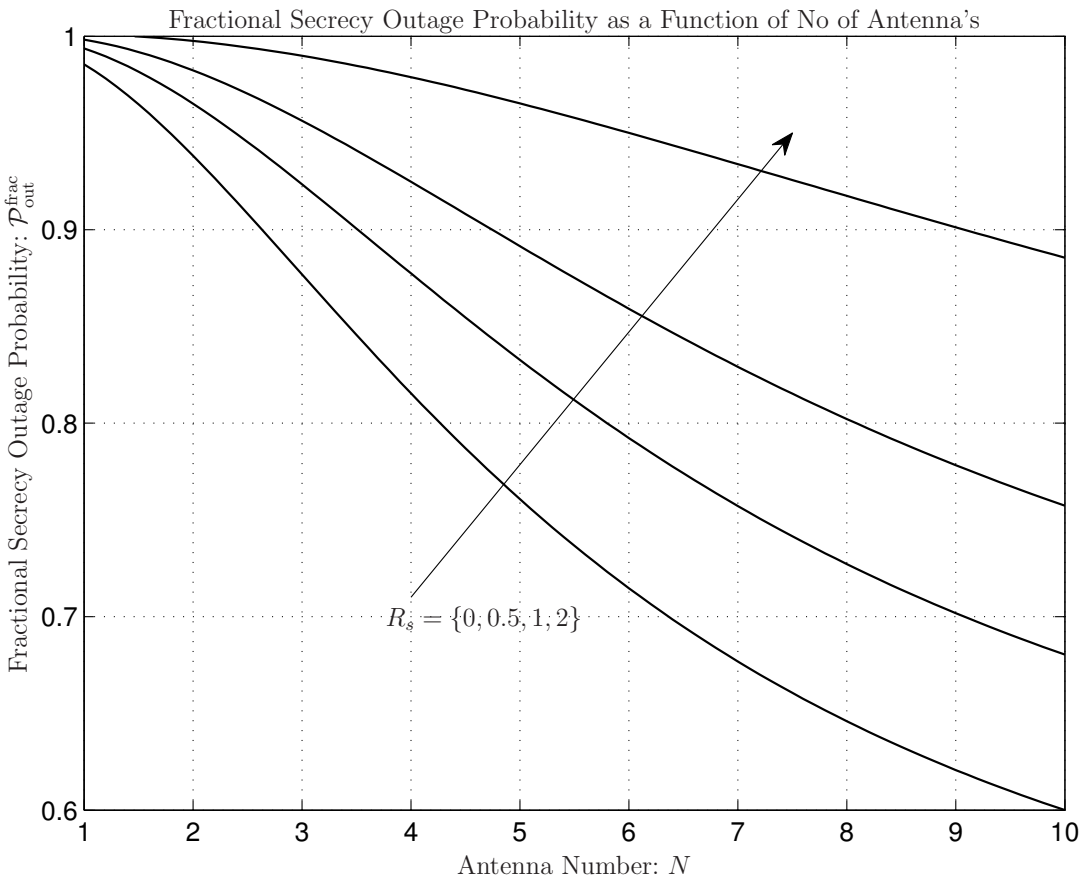



Figure 7.3: Conditional secrecy outage probability as a function of number of transmit antenna for various $R_s$, with $\lambda_{\text{e}} = 0.001$, $r_\ell = 50m$, and $\theta = 90$.

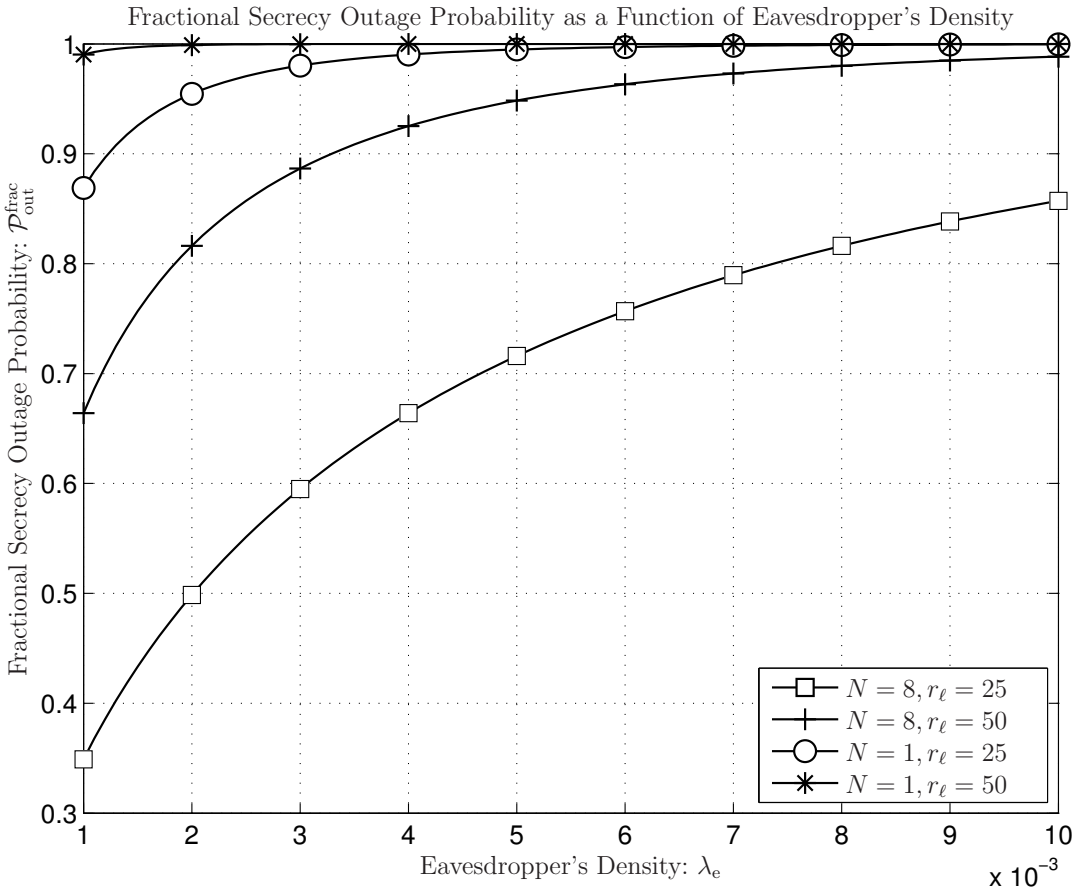



Figure 7.4: Conditional secrecy outage probability as a function of eavesdropper's density for various number of transmit antenna and different $r_\ell$, with $m = 1$ and $\theta = 90$.

## 7.4 Conclusions

In this chapter, we studied the secrecy metrics of random wireless networks under Nakagami-$m$ fading with multiple antennas. The path gain distributions of the legitimate nodes and that of the best eavesdropper are derived. Using these results, the secrecy outage probability $\mathcal{P}_{\text{out}}$ is derived. The secrecy outage probability and transmission outage are further combined to analyse the conditional secrecy outage of the random network. The impact of transmission factors, including number of transmit antennas, fading figure, legitimate node distance and node density are studied and analyzed in numerical results. We recently submitted our findings to [98]. Our results show that the increase in the number of antennas at the source node and increase in the fading figure can both lead to decrease in secrecy outage probability, while the increase of eavesdropper's density degrades the secrecy communication.

In particular, we list our contributions of this chapter as below

- We derived the path gain distribution of the legitimate node.
- Using the above result, we derived the best path gain distribution of eavesdroppers using PGFL of PPP.
- We computed the secrecy outage probability and the conditional secrecy outage probability under Nakagami fading channel [98].

# Chapter 8

# Generalizing Topologies

**Summary:**

*The study of the inherent secrecy capacity of wireless networks of random topologies is currently of great interest to the communication and information theory communities. Indeed, a good amount of work exists on the secrecy analysis of random networks, the majority of which relies on PPPs to model the spatial distribution of devices. It has been recently demonstrated, however, that MHCPPs are also suited to characterize the random location of users and base-stations of cellular systems. In this chapter, we therefore offer an analysis of the secrecy outage probability of random networks under the MHCPP model, with the objective of shedding some light on the security limitations/capabilities inherent encountered in cellular systems.*

## 8.1 Introduction

Although there is an increasing tendency of research on intrinsic secrecy in random wireless networks, most of current works focus on systems with PPP based deployments. Literature on the impact of realistic topologies, described by more alternative point process models that generalize the PPP in the analysis of random networks is not vast, but the issue has not entirely escaped the attention of the community. Recently [45, 49, 55, 99], focus has started to shift so as to address the somewhat "naive" assumption of uniformity, found in all aforementioned works. To clarify, it has been shown that the PPPs cannot accurately model the majority of wireless systems of interest, including cellular [45, 99] and WiFi [49] networks. More recently [100, 101], the inaccuracy of PPP as a model of BS locations on different tiers of heterogeneous cellular systems was again demonstrated. All in all, it is now established fact that as far the the topological models for random networks is concerned, the PPP alone is not sufficient, such that alternative models need be considered. Following this recent trend, specifically, we will study the inherent secrecy in random networks, with the particular aim of quantifying the impact of generalized topological models.

In order to illustrate the importance of network topology on the conditions determining the secrecy capacity of corresponding network, consider the example of typical residential WiFi networks. From a security standpoint, these networks are characterised by the clusterization on a home-by-home basis, *i.e.*, devices within the house are typically considered legitimate users, while devices outside premises play the role of possible eavesdroppers. As a result, the assumption of a random but statistically uniform spatial distribution of BS's and users (as implied by a PPP model) is clearly unrealistic, motivating studies conducted under a more general model such as done in [44] and [48].

Likewise, in cellular networks, the distribution of BSs follow terrain, as well as regulatory (city-plan), demand and space availability conditions, and therefore are far from (statistically) uniform. Furthermore, devices in urban areas served by pico and femto cells may be clustered together, for instance in and around shopping malls and train-stations), while devices in less populated areas served by macro cells are more sparsely located.

Such conditions are clearly distinct from the random and uniformly distributed network assumptions that lead to a Poison number of nodes per unit area – *i.e.*, the PPP model – commonly adopted in current literature [9,46]. In response to the limitations of the PPP

model, recent work has appeared which focuses on the impact of topological models onto the accuracy of analytical results obtained for random networks [45,49,55,99–101].

To elaborate, in [49], HCPPs were proposed to model networks with carrier-sensing multiple access (CSMA), and in [45] the coverage probability of cellular systems analysed under the PPP, HCPP and Strauss Process (SP) models were compared against field data, which demonstrated that indeed HCPP Type I and SP lead to significantly more accurate results then the PPP model commonly used earlier. Motivated by such recent results, we consider the MHCPP Type I model in order to model the distribution of BSs in the analysis to follow.

Before proceeding to the system model, let us mention some properties of point process (PP). For stationary PP ($\Phi_p$), the average sum of a function can be expressed in terms of second order product densities. Without loss of generality, we take the node to lie at the origin $o$ (but excluding that point), the average sum of any integrable function $f(x)$ using Campbell's theorem can be expressed as [99]

$$\mathbb{E}_o^! \left[ \sum_{x \in \Phi} f(x) \right] = \frac{1}{\lambda_p} \int_{\mathbb{R}^2} \varrho^{(2)}(x) f(x) \, \mathrm{d}x, \tag{8.1}$$

where the notation $\mathbb{E}_o^!$ signifies that the expectation is taken around the origin but excluding it; $\lambda_p$ denotes the density of the stationary PP; $\varrho^{(2)}(x)$ is the second order density of the PP; and $\mathbb{R}^2$ is the two-dimensional Euclidean space.

Since we model the distribution of BS's in our network with a MHCPP, it is worthwhile to mention here some properties of this PP. In the MHCPP, all the points obtained from a stationary PPP of intensity $\lambda_p$ are retained only if they are at distance at least $d$ from all other points. The intensity of the resulting MHCPP is $\lambda = \lambda_p \exp(-\lambda_p \pi d^2)$. Consequently, the second order product of the resulting PP is [53]

$$\varrho^{(2)}(x) = 2\pi\lambda^2 \exp(2\pi\lambda_p d^2) \cdot x \cdot \exp(-\lambda_p V_d(x)), \tag{8.2}$$

where $V_d(x)$ is the area of the union of two disks of radius $d$ whose centres are separated by $x$, which is given by

$$V_d(x) = \begin{cases} 2\pi d^2 - 2d^2 \mathrm{acos}\left(\frac{x}{2d}\right) + x\sqrt{d^2 - \frac{x^2}{4}} & \text{if } x < 2d, \\ 2\pi d^2 & \text{if } x \geq 2d. \end{cases} \tag{8.3}$$

## 8.2 Secrecy Outage

Consider the downlink cellular network in an unbounded Euclidean space of dimension two, where the mobile stations (MSs) occupy random locations with uniform probability, such that their spatial distribution can be modelled by an independent homogenous PPP $\Phi_{\text{MS}}$ [64].

On the other hand, BSs are assumed to be randomly distributed also with uniform probability, *except* for the fact that a *minimum distance* (hard-core distance) $d$ between BSs is observed, such that BSs are spatially distributed according to a two-dimensional MHCPP $\Phi_{\text{BS}}$ of intensity $\lambda_{\text{BS}}$.

Let a fraction of the MSs randomly chosen from $\Phi_{\text{MS}}$ be eavesdroppers, which define a PPP of density $\lambda_{\text{e}}$ embedded within $\Phi_{\text{MS}}$. All the legitimate nodes and eavesdroppers are equipped with single antenna each, and without loss of generality, we add a typical (target) MS at the origin of the coordinate system (Palm's point). It is also assumed that the target MS is interference-free.

The downlink cellular network model described above is consistent with the one in [46]. Under this model, the *secrecy capacity* of the downlink AWGN channel to the target in this cellular system is given by [8, 9]

$$\mathcal{C}_s = \max\left\{0, \log_2\left(1+\frac{\rho}{r_{\text{BS}}^{\alpha}}\right) - \log_2\left(1+\frac{\rho}{r_e^{\alpha}}\right)\right\}, \tag{8.4}$$

where, $r_{\text{BS}}$ is the distance between the target MS and the serving BS; $r_{\text{e}}$ is the distance between target MS and the nearest eavesdropper; and $\alpha$ is the path loss exponent, which is hereafter treated as a general parameter as it may assume different values depending on propagation conditions.

Notice that in the AWGN case, the nearest eavesdropper is certain to experience the smallest path loss amongst non-legitimate nodes.

For now, let us just highlight that we will hereafter follow related literature [46] and consider the particular case of an asymptotic reference SNR regime, where $\rho \to \infty$,

such that

$$\begin{aligned}\tilde{\mathcal{P}}_{\text{out}}(R_s) &= \Pr\left\{\log_2\left(1+\frac{\rho}{r_\ell^\alpha}\right)-\log_2\left(1+\frac{\rho}{r_{\text{e}}^\alpha}\right)>R_s\right\},\\ &= \Pr\left\{\log_2\left(\frac{\rho^{-1}+r_\ell^{-\alpha}}{\rho^{-1}+r_{\text{e}}^{-\alpha}}\right)>R_s\right\},\\ &= \Pr\left\{\log_2\left(\frac{r_{\text{e}}^\alpha}{r_\ell^\alpha}\right)>R_s\right\} = \Pr\left\{r_{\text{e}}>2^{R_s/\alpha}\cdot r_\ell\right\}.\end{aligned} \tag{8.5}$$

For comparison purposes, we shall also follow [46] and analyse the secrecy non-outage probability under the assumption that the serving BS has perfect knowledge of the location of the nearest eavesdropper, and for two different scenarios, namely:

**Nearest BS:** The BS nearest to the target MS is selected to serve it;

**Optimal BS:** The BS that yields the best secrecy performance at the target MS is selected.

### Distance Distributions

In order to characterize the secrecy outage probability of cellular networks, one needs to compute the distributions of the distances between the nearest eavesdropper and both the BS, and the target MS. Since the MSs follow a homogenous PPP, we obtain the distribution of the distances between the nearest eavesdropper and the target MS as [99]

$$f_{r_{\text{e}}}(r) = 2\pi r\lambda_{\text{e}}e^{-\pi\lambda_{\text{e}}r^2}. \tag{8.6}$$

In order to calculate the secrecy outage probability of a channel between the target node and the nearest BS, however, we also need to derive the distribution of the distances $r_{\text{BS}}$. But since BSs are distributed according to an MHCPP, the distribution of the distance between the target and the nearest BS – hereafter referred to as the nearest BS distribution and denoted $r_{\text{BS}}^*$– is not known in closed form. Fortunately, an approximate method to derive the distribution of $r_{\text{BS}}^*$ was proposed in [48], yielding

$$f_{r_{\text{BS}}^*}(r) = \frac{2r}{d^2}(1-e^{-\pi d^2\lambda_{\text{BS}}})\times\begin{cases}1 & \text{if } 2r<d,\\ e^{-\hat{\lambda}M(r,d)} & \text{if } 2r\geq d,\end{cases} \tag{8.7}$$

where $\hat{\lambda}$ is the virtual density of the area $M(r,d)$, which is defined by [48]

$$M(r,d) \triangleq \pi r^2 - r^2 \text{acos}\left(\tfrac{2r^2-d^2}{2r^2}\right) - d^2 \text{acos}\left(\tfrac{d}{2r}\right) + \tfrac{d}{2}\sqrt{4r^2-d^2}. \tag{8.8}$$

We conclude this Section by remarking that under the conventional PPP model, the standard approach to finding the secrecy outage probability for the case when the BS is optimally selected would be to first obtain the distribution of the distance between the target node and an arbitrary $k$-th nearest BS. As can be inferred from Eq. (8.7), however, deriving the corresponding distribution under an MHCPP is an intractable problem. Fortunately, as shall be shown in Section 8.2.2, an elegant alternative to the latter approach exists, which circumvents that problem.

We therefore do *not* require any further distance distribution besides the ones offered above.

### 8.2.1 Secrecy Outage Probability: Nearest BS Case

As a consequence of Eq. (8.7), the secrecy outage probability for the case when the nearest BS is selected depends on whether the target MS is inside or outside the region around a BS defined by the hard core distance $d$

Part 1 - MS inside Hard Core Region: $r < d/2$

$$\begin{aligned}\tilde{\mathcal{P}}_{\text{out}}(R_s) &= \int_0^{\infty}\int_0^{2^{R_s/\alpha}x} f_{r_{\text{e}}}(y)\cdot f_{r^*_{\text{BS}}}(x)\,\text{d}y\,\text{d}x,\\ &= \frac{2(1-e^{-\pi\lambda_{\text{BS}}d^2})}{d^2}\int_0^{\infty} x\cdot e^{-\pi\lambda_{\text{e}}2^{2R_s/\alpha}x^2}\text{d}x = \frac{1-e^{-\pi\lambda_{\text{BS}}d^2}}{\pi\cdot\lambda_{\text{e}}\cdot 2^{2R_s/\alpha}\cdot d^2}.\end{aligned} \tag{8.9}$$

Part 2 - MS inside Hard Core Region: $r \geq d/2$

$$\begin{aligned}\tilde{\mathcal{P}}_{\text{out}}(R_s) &= \int_0^{\infty}\int_0^{2^{R_s/\alpha}x} f_{r_{\text{e}}}(y)\cdot f_{r^*_{\text{BS}}}(x)\,\text{d}y\,\text{d}x,\\ &= \frac{2(1-e^{-\pi\lambda_{\text{BS}}d^2})}{d^2}\int_0^{\infty} x\cdot e^{-\pi\lambda_{\text{e}}2^{2R_s/\alpha}x^2}\cdot e^{-\hat{\lambda}M(x,d)}\text{d}x.\end{aligned} \tag{8.10}$$

Unfortunately the above integral doesn't have closed form solution, however, we can compute the required secrecy outage probability numerically.

### 8.2.2 Secrecy Outage Probability: Optimal BS Case

In this scenario, initially we consider that all BS can act as a potential candidate to serve as a typical MS. However, the BS with the maximum secrecy rate will be selected. Based on these assumption, the secrecy capacity Eq. in (8.4) can be re-written as (high SNR regime)

$$R_s = \max\left\{\max_{\mathrm{BS}\in\Phi_{\mathrm{BS}}}\left\{\log_2\!\left(\frac{1}{r_{\mathrm{BS}}^{\alpha}}\right) - \log_2\!\left(\frac{1}{r_{\mathrm{e}}^{\alpha}}\right)\right\}, 0\right\}. \tag{8.11}$$

The secrecy outage probability can be derived as

$$\begin{aligned}
\mathcal{P}_{\mathrm{out}}(R_s) &= \Pr\{C_s \le R_s\}, \qquad (8.12)\\
&= \Pr[\text{All BS can not provide secrecy rate larger than } R_s],\\
&= \mathbb{E}_{\Phi_{\mathrm{e}}}\left[\mathbb{E}_{\Phi_{\mathrm{BS}}}\left[\prod_{x\in\Phi_{\mathrm{BS}}} 1\{\Phi_{\mathrm{e}}\cap B(x,2^{R_s/\alpha}x)\neq 0\}\right]\right],\\
&= \mathbb{E}_{\Phi_{\mathrm{e}}}\left[\mathbb{E}_{\Phi_{\mathrm{BS}}}\left[\prod_{x\in\Phi_{\mathrm{BS}}}\Big[1-1\{\Phi_{\mathrm{e}}\cap B(x,2^{R_s/\alpha}x)=0\}\Big]\right]\right],\\
&= \mathbb{E}_{\Phi_{\mathrm{e}}}\left[\mathbb{E}_{\Phi_{\mathrm{BS}}}\left[e^{-\sum\limits_{x\in\Phi_{\mathrm{BS}}} 1\{\Phi_{\mathrm{e}}\cap B(x,2^{R_s/\alpha}x)=0\}}\right]\right],\\
&\overset{a}{\ge} \mathbb{E}_{\Phi_{\mathrm{e}}}\left[e^{\mathbb{E}_{\Phi_{\mathrm{BS}}}\left[-\sum\limits_{x\in\Phi_{\mathrm{BS}}} 1\{\Phi_{\mathrm{e}}\cap B(x,2^{R_s/\alpha}x)=0\}\right]}\right],\\
&\overset{b}{=} \mathbb{E}_{\Phi_{\mathrm{e}}}\left[\exp\left[-\lambda_{\mathrm{BS}}\int_{d}^{\infty}\varrho^{(2)}(x)1\{\Phi_{\mathrm{e}}\cap B(x,2^{R_s/\alpha}x)=0\}\mathrm{d}x\right]\right],\\
&\overset{c}{\ge} \exp\left[-\lambda_{\mathrm{BS}}\int_{d}^{\infty}\varrho^{(2)}(x)\Pr\{\Phi_{\mathrm{e}}(B(x,2^{R_s/\alpha}x))=0\}\mathrm{d}x\right],
\end{aligned}$$

where step $(a)$ follows from [99, Conjecture 1], and step $(b)$ is obtained using the Eq. (8.1), and step $(c)$ follows from Jensen's inequality.

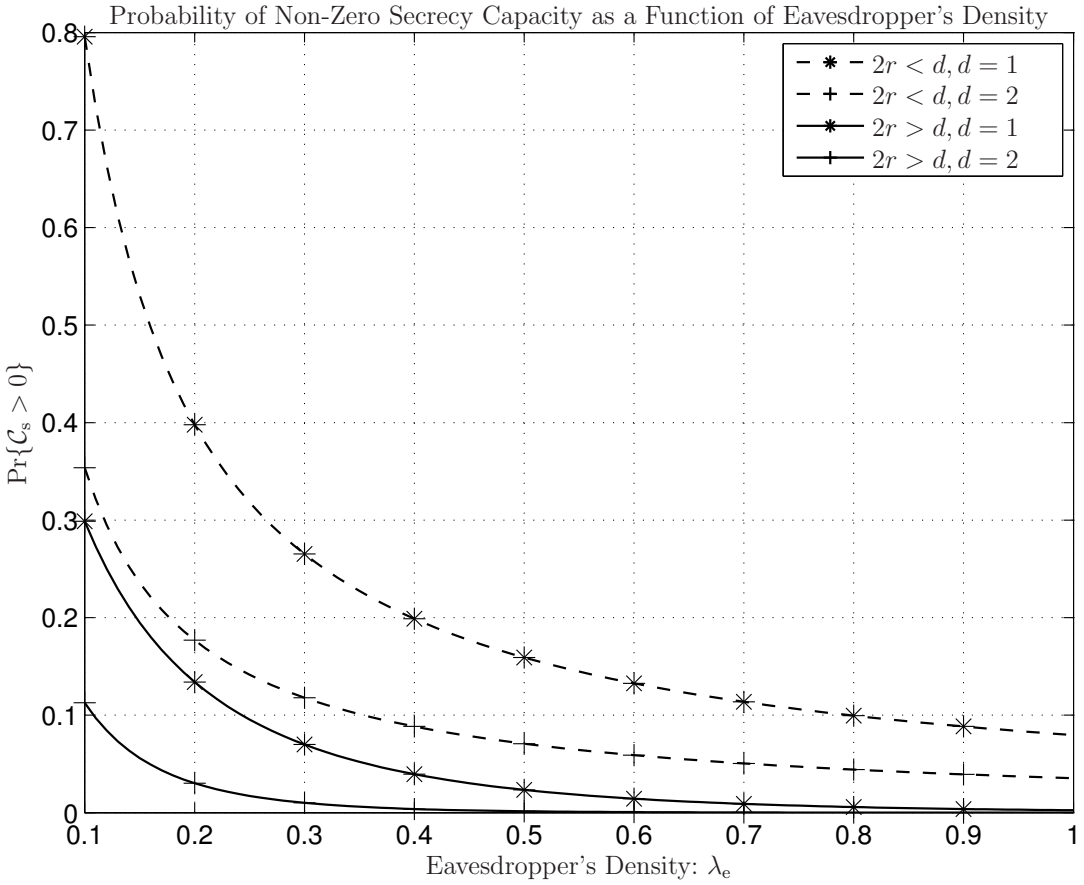



Figure 8.1: Probability of achieving a non-zero secrecy capacity, expressed as a function of the density of eavesdropper's in the scenario 8.2.1 (Case 1: Part 1 and 2), with $\alpha = 2$ and $\lambda_{\mathrm{BS}} = 1$.

Now, the secrecy outage probability can be written as

$$\begin{aligned}\mathcal{P}_{\text{out}}(R_s) &= \Pr\{C_s \leq R_s\}, \\ &= \exp\left[-\lambda_{\text{BS}}\left(\int_d^{\infty} \varrho^{(2)}(x) e^{-\pi\lambda_{\text{e}} 2^{2R_s/\alpha} x^2} \mathrm{d}x\right)\right], \\ &= \exp\left[-\lambda_{\text{BS}}\left(\int_d^{2d} \varrho^{(2)}(x) e^{-\pi\lambda_{\text{e}} 2^{2R_s/\alpha} x^2} \mathrm{d}x + \int_{2d}^{\infty} \varrho^{(2)}(x) e^{-\pi\lambda_{\text{e}} 2^{2R_s/\alpha} x^2} \mathrm{d}x\right)\right].\end{aligned} \tag{8.13}$$

However, it can be obtained straightforwardly by substituting the Eq. (8.2) in the last expression.

Fig. 8.1 illustrate the two cases of selecting nearest BS on the secrecy non-outage probability. A comparison of the probability of non-zero secrecy capacity with nearest eavesdropper under the two cases, which are determined by Eq. (8.9) and Eq. (8.10), against the $\tilde{\mathcal{P}}_{\text{out}}(0) = \Pr\{C_s > 0\}$ is shown. It is found that the secrecy non-outage probability decreases with the increase of $\lambda_{\text{e}}$.

Next, we evaluate the effect of BS placements on the secrecy non-outage probability. Fig. 8.2 shows the $\tilde{\mathcal{P}}_{\text{out}}(0)$ as a function of BS density. For a given $\lambda_{\text{BS}}$, we notice that the secrecy non-outage probability decreases with $d$. It can be explained by the fact that as the resulting topologies become more and more regular and the serving BS nodes are moving away from the intended MSs.

Another interesting point to note is that the secrecy non-outage probability is almost constant for higher values of $d$. Again, this can be addressed by the fact that MHCPP becomes more regular by increasing $\lambda_{\text{BS}}$, for higher values of $d$.

Fig. 8.3 shows the plots of the secrecy non-outage probability as a function of $\lambda_{\text{e}}$ for the case of optimal serving BS. Similar to Fig. 8.1, it is observed that the secrecy non-outage probability decreases with an increase in $\lambda_{\text{e}}$. It is also depicted that the secrecy non-outage probability decreases for higher values of $d$.

In summary, from all the figures, it is noticed that for sufficiently large $d$ the achievable secrecy capacity is very low. This counter-intuitive result can be explained as follows. Since BS nodes are sparsely placed for higher values of $d$, distance between BS and intended MS increases, consequently decreasing secrecy capacity.

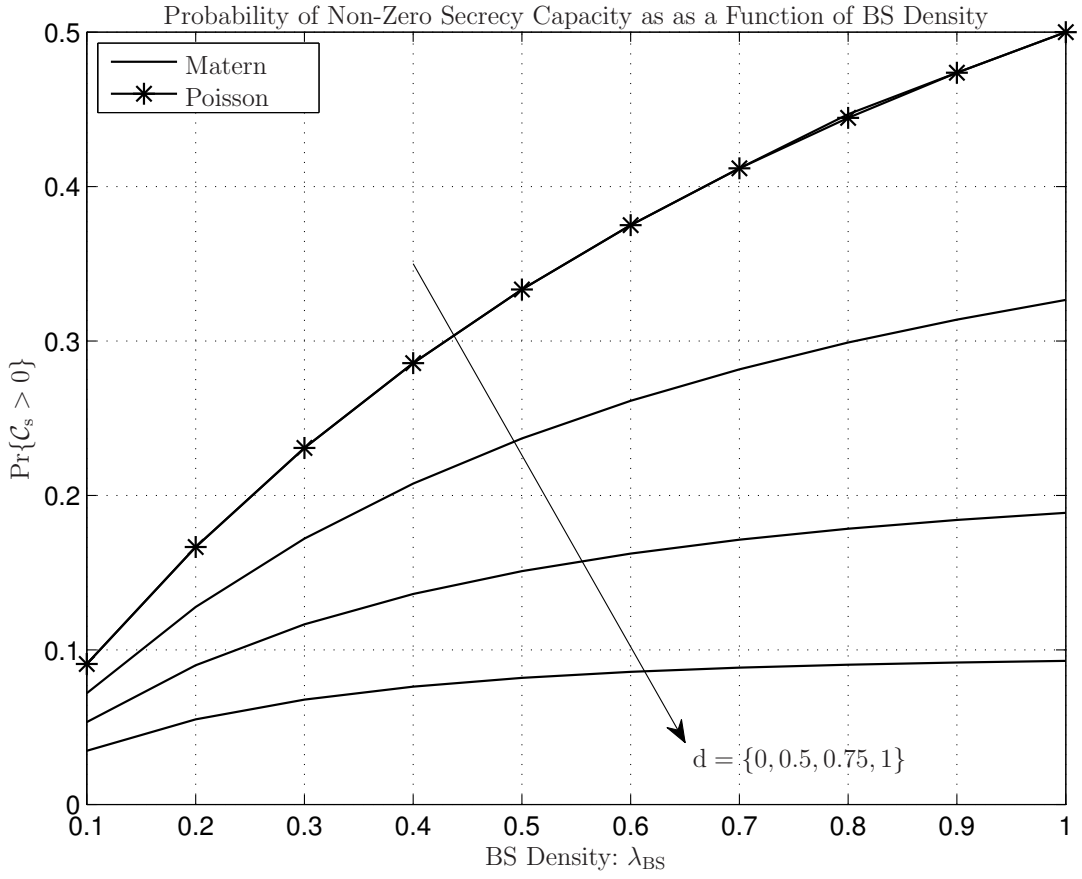



Figure 8.2: Probability of achieving a non-zero secrecy capacity, expressed as a function of the density of BS's in the scenario 8.2.1 (Case 1: Part 2), with $\alpha = 2$ and $\lambda_e = 1$.

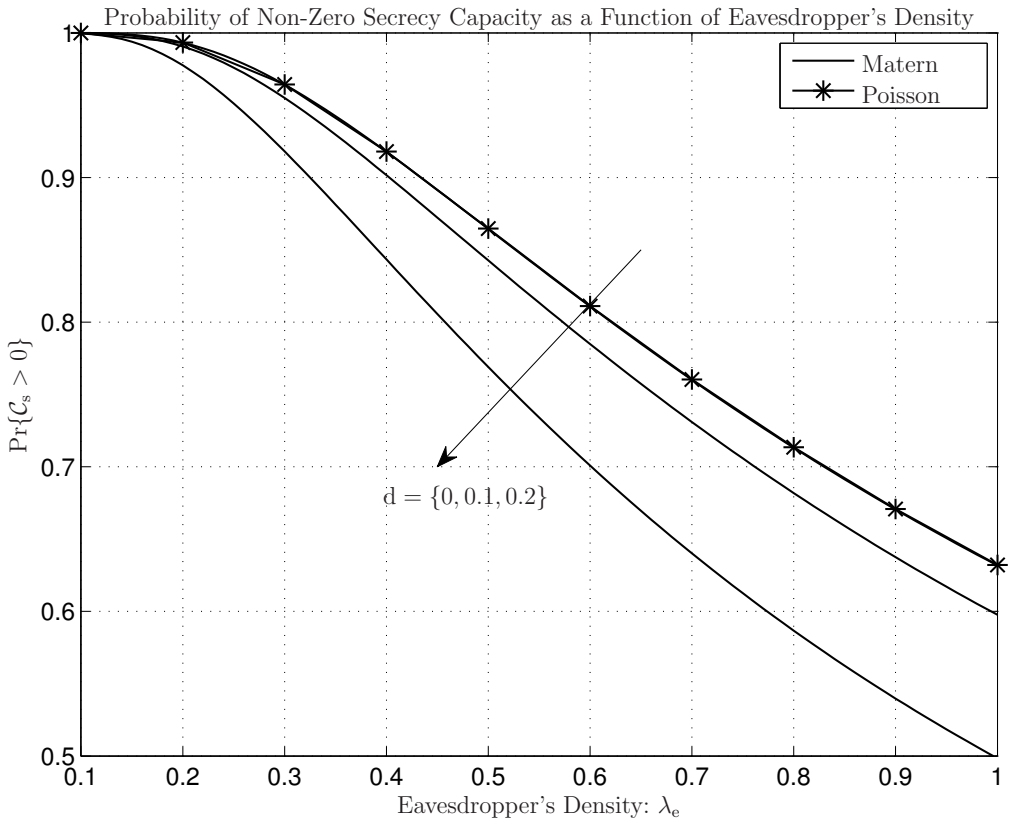



Figure 8.3: Probability of achieving a non-zero secrecy capacity, expressed as a function of eavesdropper's density in the scenario 8.2.2 (Case 2), with $\alpha = 4$ and $\lambda_{\mathrm{BS}} = 1$.

## 8.3 Conclusions

In this chapter, we studied the secrecy characteristics of cellular wireless networks by employing MHCPP. Using the distance distributions of the BS nodes and that of the nearest eavesdropper, the secrecy outage probability $\mathcal{P}_{\text{out}}$ is derived. Our results, which are submitted in [102], show that the increase in the matern hard-core distance $d$ and decrease in the BS density can both lead to decrease in secrecy outage probability.

In particular, we list our contributions of this chapter as below

- We modelled the downlink cellular network with MHCPP.
- We derived expressions for the secrecy outage probability of nearest BS serving scenario in downlink communications [102].
- We also derived the secrecy outage probability of downlink optimal BS serving scenario [102].

# Chapter 9

# Conclusions and Future Directions

## 9.1 Conclusions

In this thesis, we studied the secrecy metrics of random wireless networks under Nakagami-$m$ fading in single and multiple antennas systems. The path loss and path gain distributions of the legitimate nodes and that of the best eavesdropper are derived. Using these results, the secrecy outage probability $\mathcal{P}_{\text{out}}$ is derived under different scenarios. Namely, we have obtained the secrecy outage probability when the legitimate and eavesdropper channels are correlated and for the case of colluding eavesdroppers. We also characterized the secrecy outage probability by taking interference into account. Later on, we have extended our results to cellular networks by employing MCHPP.

Our results are intuitive, namely they indicate that it is hard to ensure a low secrecy outage for nodes farther from the source and for high rates. It is also shown that the achievable secrecy non-outage is largely independent on the reference SNR $\rho$, *even for a fixed rate*! Since $\rho$ is fundamentally controlled by the source's transmit power, the conclusion is that at least to the closest source, it is possible to communicate secretly in the presence of a numerous, and unknown number of eavesdroppers, using very low power (for instance half the power of background noise).

The impact of other transmission factors, including number of transmit antennas, fading figure, legitimate node distance and node density are studied and analyzed. We

published and recently submitted our findings to [19, 20, 70, 71, 79, 92, 94, 98, 102, 103]. Our results show that the increase in the number of antennas at the source node and increase in the fading figure can both lead to decrease in secrecy outage probability, while the increase of eavesdropper's density degrades the secrecy communication.

## 9.2 Future Directions

We will investigate various figures of merit to measure the secrecy in random networks – such as the node degree of secrecy graphs, the secrecy outage probability, the unicast secrecy capacity and the secrecy transmission capacity – employing stochastic geometric models that have recently emerging to enable the study of point processes beyond the Poissonian case.

Two specific approaches that can be envisioned at this state is to consider the such HCPP and SP models, which have been already studied in the context of communication throughput [44, 45, 54, 99] but not yet in the context of wireless secrecy. To go further into details, to the best of our knowledge the distance distributions of pairs of nodes under the HCPP or SP have not yet been derived. Such distributions are of vital importance to characterise the secrecy of random networks.

The derivation of such distributions for the HCPP and SP models and their application to the evaluation of secrecy metrics will therefore be an outcome of our future work.

Despite the successful application of Stochastic Geometry in the analysis of wireless systems from a network perspective, demonstrated by recent literature [38], a wave of self-criticism has started to permeate the communication theory community in recognition to the lack of accuracy of the underlying assumptions that are typically adopted. In order to be able to handle networks of truly general topologies, the supplementation of Stochastic Geometric models is therefore crucial.

In our future works, we will attempt to develop alternatives to stochastic geometry in the study of secrecy in random networks, by incorporating other ideas such as order statistics, random walks and graph theory. To offer a concrete example, in one of our results [20] we employed order statistics to obtain an expression of the secrecy outage and the secrecy capacity of unicast links in random networks with PPP models. Since order statistics are only weakly dependent on distributions – in the sense that they are typically determined mostly by the tails rather then the modes – it is foreseeable that those results can be extended to non-PPP as well.

# Own Publications

## Journals:

- Satyanarayana Vuppala, Giuseppe Abreu, "Unicasting on the Secrecy Graph", IEEE Transactions on Information Forensics and Security, pp 1469-1481, Vol. 8, No. 9, Sept. 2013.

- Satyanarayana Vuppala, Giuseppe Abreu,"Secrecy Outage Analysis in Cellular Networks",' submitted to IEEE Wireless Communications Letters. (under review)

## Conferences:

### Authored Papers:

- Satyanarayana Vuppala, W. Liu, Giuseppe Abreu and T Ratnarajah, "Secrecy Outage of Nakagami-m MISO Channels with Randomly Located Receivers," IEEE Global Conference on Signal and Information Processing (GlobalSIP), Atlanta, Georgia, USA, December 3-5, 2014. (Accepted)

- Satyanarayana Vuppala, W. Liu, T Ratnarajah and Giuseppe Abreu, "Secrecy Outage Analysis of Cognitive Wireless Sensor Networks," IEEE Fourty-Eigth Asilomar Conference Conference on Signals, Systems, and Computers, Pacific Grove, CA, Nov. 2014. (Best paper award nominee)

- Satyanarayana Vuppala and Giuseppe Abreu, "Secrecy Transmission Capacity of Random Networks", Proc. IEEE Fourty-Seventh Asilomar Conference Conference on Signals, Systems, and Computers, Pacific Grove, CA, Nov. 2013. (Invited paper)

- Satyanarayana Vuppala, Giuseppe Abreu, "Secrecy Outage in Random Wireless Networks subjected to Fading", Proc. IEEE Personal Indoor Mobile Radio Communication, London, UK, Sept 8-11, 2013, pp. 441 – 445.

- Satyanaranaya Vuppala and Giuseppe Abreu, "Analysis of Secure Unicast Links in Stochastic Wireless Networks", Proc. IEEE International Conference on Communications, Budapest, Hungary, June 9-13, 2013, pp 1588-1593.

- Satyanaranaya Vuppala and Giuseppe Abreu, "Unicasting on the S-Graph", Proc. IEEE Fourty-Sixth Asilomar Conference Conference on Signals, Systems, and Computers, Pacific Grove, CA, 4-7 Nov. 2012, pp.1891 - 1895. (Best paper award nominee)

## Co-authored Papers:

- W. Liu, Satyanarayana Vuppala, Giuseppe Abreu and T Ratnarajah, "Secrecy Outage in Correlated Nakagami-m Fading Channels," IEEE Personal Indoor Mobile Radio Communication, Sept. 2014. (Accepted)

# Bibliography


[1] H. Imai, G. Hanaoka, U. Maurer, and Y. Zheng, "Information theoretic security," Special Issue of the IEEE Transactions on Information Theory, 2008.

[2] "Wireless physical layer security," Special Issue of the EURASIP Journal on Wireless Communications and Networking, 2009.

[3] M. Bloch, M. Debbah, Y. L. abd Yasutada Oohama, and A. Thangaraj, "Physical-layer security," Special Issue of the IEEE Journal of Communications and Networks, 2012.

[4] W. Saad, W. Saad, L. Lai, Wing-Kin, H. V. Poor, and A. L. Swindlehurst, "Signal processing techniques for wireless physical layer security," Special Issue of the IEEE Journal on Selected Areas on Communications, 2013.

[5] T. Q. Duong, D. B. da Costa, K. J. Kim, K.-H. S. Liu, and V. N. Q. Bao, "Secure physical layer communications," Special Issue of the IET Communications, 2014.

[6] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355 –1367, Oct. 1975.

[7] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339 – 348, May 1978.

[8] L. Y. Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451 – 456, Jul. 1978.

[9] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2515 – 2534, Jun. 2008.

[10] P. K. Gopala, L. Lai, and H. El-Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 10, pp. 4687 – 4698, Oct. 2008.

[11] Y. Liang, V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2470 – 2492, Jun. 2008.

[12] M. Haenggi, "A geometric interpretation of fading in wireless networks: Theory and applications," *IEEE Trans. Inform. Theory*, vol. 54, no. 12, pp. 5500 – 5510, Dec. 2008.

[13] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousee, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE Journal on Selected Areas in Communications.*, vol. 27, no. 7, pp. 1029 – 1046, Sep. 2009.

[14] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—part I: Connectivity," *IEEE Trans. Information Forensics and Security*, vol. 7, no. 1, pp. 125 – 138, Feb. 2012.

[15] P. Gupta and P. Kumar, "The capacity of wireless networks," *IEEE Trans. Information Theory.*, vol. 46, no. 2, pp. 388– 404, 2000.

[16] S. S. Karande, Z. Wang, H. R. Sadjadpour, and J. J. Garcia-Luna-Aceves, "Optimal unicast capacity of random geometric graphs: Impact of multipacket transmission and receptions," *IEEE Trans. on Selected Areas in Comm,.*, vol. 27, no. 7, pp. 1180 – 1191, Sep. 2009.

[17] M. Franceschetti, O. Dousse, D. N. C. Tse, and P. Thiran, "Closing the gap in the capacity of wireless networks via percolation theory," *IEEE Trans. Information Theory.*, vol. 53, no. 3, pp. 1009 – 1018, 2007.

[18] S. Weber, J. G. Andrews, and N. Jindal, "An overview of the trans- mission capacity of wireless networks," *IEEE Trans. Communications.*, vol. 58, no. 12, Dec. 2010.

[19] S. Vuppala and G. Abreu, "Unicasting on the secrecy graph," *IEEE Trans. Information Forensics and Security*, vol. 8, no. 9, pp. 1469 – 1481, Sep. 2013.

[20] ——, "Secrecy outage in random wireless networks subjected to fading," in *Proc. IEEE Personal Indoor Mobile Radio Communication*, London, UK., Sept8-11 2013, pp. 441 – 445.

[21] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Information Theory.*, vol. 58, no. 5, pp. 3000 – 3015, May. 2012.

[22] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank, "The effect of eavesdroppers on network connectivity: A secrecy graph approach," *IEEE Trans. Information Forensics and Security*, vol. 6, no. 3, pp. 712 – 724, Sep. 2011.

[23] J. Zhang, L. Fu, and X. Wang, "Asymptotic analysis on secrecy capacity in large-scale wireless networks," *IEEE/ACM Transactions on Networking*, vol. 22, no. 1, pp. 66–79, Feb. 2014.

[24] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Comm.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

[25] M. Grossglauser and D. N. C. Tse, "Mobility increases the capacity of ad-hoc wireless networks," *IEEE Trans. on Networking.*, vol. 10, no. 4, pp. 477 – 486, Aug. 2002.

[26] J. N. Laneman, "Cooperative diversity in wireless networks: Algorithms and Architectures," Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge, U.S.A., Sep. 2002. [Online]. Available: http://allegro.mit.edu/pubs/posted/doctoral/2002-laneman-phd.pdf

[27] A. Khisti, U. Erez, and G. W. Wornell, "A capacity theorem for cooperative multicasting in large wireless networks," in *Proc. IEEE Allerton Conference on Communications, Control and Computing*, Illinois, U.S.A, October 2004.

[28] A. Bletsas, H. Shin, and M. Z. Win, "Cooperative communications with outage-optimal opportunistic relaying," *IEEE Trans. Wireless Commun.*, vol. 6, no. 9, pp. 3450–3460, 2007.

[29] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—part II: Maximum rate and collusion," *IEEE Trans. Information Forensics and Security.*, vol. 7, no. 1, pp. 139 – 147, Feb. 2012.

[30] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. on Networking.*, vol. 10, no. 2, pp. 425 – 430, Feb. 2011.

[31] M. Mirmohseni and P. Papadimitratos, "Colluding eavesdroppers in large cooperative wireless networks," in *Proc. IEEE 2nd Iran Workshop on Communication and Information Theory (IWCIT)*, May 2014.

[32] P. C. Pinto and M. Z. Win, "Communication in a Poisson field of interferers – part i: Interference distribution and error probability," *IEEE Trans. Wireless Commun.*, (to appear).

[33] W. Znaidi, M. Minier, and J. Babau, "An ontology of attacks in wireless sensors networks," *INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE (INRIA)*, October 2008.

[34] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in *Wireless Network Security.* Springer US, 2007.

[35] T. Dierks and E. Rescorla, "The transport layer security (TLS) protocol version 1.1," RFC 4346, April 2006.

[36] S. Kent and R. Atkinson, "IP encapsulating security payload (ESP)," RFC 4346, April 1998.

[37] W. Diffie and M. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on*, vol. 22, no. 6, pp. 644 – 654, nov 1976.

[38] M. Haenggi, *Stochastic Geometry for Wireless Networks.* Cambridge University Press, 2012.

[39] S. Bornholdt and H. G. Schuster, *Handbook of Graphs and Networks: From the Genome to the Internet.* Wiley, 2003.

[40] P. C. Pinto and M. Z. Win, "Percolation and connectivity in the intrinsically secure communications graph," *IEEE Trans. Inform. Theory*, vol. 58, no. 3, pp. 1716 – 1730, Mar. 2012.

[41] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE International Symposium on Information Theory*, Toronto, ON., Jul.6-11 2008, pp. 539–543.

[42] Z. Shu, Y. L. Yang, Y. Qian, and R. Q. Hu, "Impact of interference on secrecy capacity in a cognitive radio network," in *Proc. IEEE Global Telecommunications Conference (Globecom'11)*, 2011.

[43] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inform. Theory*, vol. 58, no. 5, pp. 3000 – 3015, 2012.

[44] H. Q. Nguyen, F. Baccelli, and D. Kofman, "A stochastic geometry analysis of dense ieee 802.11 networks," in *IEEE International International Conference on Computer Communications*, 2007, p. 11991207.

[45] A.Guo and M. Haenggi, "Spatial stochastic models and metrics for the structure of base stations in cellular networks," *IEEE Trans. Wireless Comm.*, vol. 12, no. 11, pp. 5800 – 5812, Nov. 2013.

[46] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: Physical layer security in cellular networks: Physical layer security in cellular networks:a stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2776–2787, June 2013.

[47] N. Beaulieu and C. Cheng, "Efficient nakagami-m fading channel simulation," *Vehicular Technology, IEEE Transactions on*, vol. 54, no. 2, pp. 413–424, March 2005.

[48] G. Alfano, M. Garetto, and E. Leonardi, "New insights into the stochastic geometry analysis of dense csma networks," in *INFOCOM, 2011 Proceedings IEEE*, 2011, pp. 2642–2650.

[49] H. ElSawy, E. Hossain, and M. Haenggi, "A modified hard core point process for analysis of random csma wireless networks in general fading environments," *IEEE Trans. Commun.*, vol. 61, no. 4, pp. 1520 – 1534, April 2013.

[50] S. Kadhe, S. Jaggi, M. Bakshi, and A. Sprintson, "Reliable, deniable, and hidable communication over multipath networks," arXiv:1401.4451, 2014.

[51] G. Rahmatollahi and G. Abreu, "Closed-form hop-count distributions in random networks with arbitrary routing," *IEEE Trans. Communications.*, vol. 60, no. 2, pp. 429–444, Feb. 2012.

[52] C. Cooper and A. Frieze, "Random walks on random graphs," in *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 3, 2009, pp. 95–106.

[53] M. Haenggi, "Mean interference in hard-core wireless networks," *IEEE Commun. Lett.*, vol. 15, no. 8, pp. 792–794, Aug. 2011.

[54] J. G. Andrews, R. K. Ganti, M. Haenggi, N. Jindal, and S. Weber, "A primer on spatial modeling and analysis in wireless networks," *IEEE Commun. Mag.*, vol. 48, no. 11, pp. 156–163, Nov. 2010.

[55] H. ElSawy, E. Hossain, and M. Haenggi, "Stochastic geometry for modeling, analysis, and design of multi-tier and congnitive cellular wireless networks:a survey," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 3, pp. 996 – 1019, July 2013.

[56] E. S. Sousa and J. A. Silvester, "Optimum transmission ranges in a direct-sequence spread spectrum multihop packet radion network," *IEEE J. Select. Areas Commun.*, vol. 8, no. 5, pp. 762–771, Jun. 1990.

[57] J. Venkataraman, M. Haenggi, and O. Collins, "Shot noise models for outage and throughput analyses in wireless ad hoc networks," in *IEEE Military Communications Conference (MILCOM),Washington, DC*, Oct. 2006, pp. 1–7.

[58] J.F.C.Kingman, *Poisson processes*. New York: Oxford Univ. Press, 1993.

[59] A. Ghasemi and E. S. Sousa, "Interference aggregation in spectrum-sensing cognitive wireless networks," *IEEE Journal on Selected topics in Signal Processing.*, vol. 2, no. 1, pp. 41 – 56, Feb. 2008.

[60] A. Rabbachin, T. Q. S. Quek, H. Shin, and M. Z. Win, "Cognitive network interference," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 2, pp. 480 – 493, Feb. 2011.

[61] R. W. Heath, M. Kountouris, and T. Bai, "Modeling heterogeneous network interference using poisson point processes," *IEEE Transactions on Signal Processing*, vol. 61, no. 16, pp. 4114 – 4126, Aug. 2013.

[62] R. K. Ganti, F. Baccelli, and J. G. Andrews, "Series expansion for interference in wireless networks," *IEEE Trans. Inform. Theory*, vol. 58, no. 4, pp. 2194 – 2205, 2012.

[63] M. Franceschetti and R. Meester, *Random Networks for Communication: from Statistical Physics to Information Systems.* Cambridge University Press,, 2007.

[64] D. Daley and D. V. Jones, *An introduction to the theory of point processes.* NewYork: Springer, 1988.

[65] ——, *An introduction to the theory of point processes 2.* Dordrecht: Springer, 2005.

[66] M. Haenggi, "On distances in uniformly random networks," *IEEE Trans. Information Theory.*, vol. 51, no. 10, pp. 3584 – 3586, Oct. 2005.

[67] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 6th ed. Academic Press, Jul. 2000.

[68] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integrals and Series - Elementary Functions*, ser. (in Russian). Moscow Fizmatlit, 2003, vol. 1.

[69] ——, *Integrals and Series - Elementary Functions*, ser. (in Russian). Moscow Fizmatlit, 1983, vol. 2.

[70] S. Vuppala and G. Abreu, "Unicasting on the $\mathcal{S}$-graph," in *IEEE Fourty-Sixth Asilomar Conference Conference on Signals, Systems, and Computers*, 2012.

[71] W. Liu, S. Vuppala, G. Abreu, and T. Ratnarajah, "Secrecy outage in correlated nakagami fading," accepted to IEEE Personal Indoor Mobile Radio Communication, Sept. 2014.

[72] H. A. David and H. N. Nagaraja, *Order Statistics.* Wiley, 2003.

[73] E. Castillo, *Extreme value theory in engineering.* Academic Press, 1988.

[74] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, 10th ed. Dover Publications, 1965.

[75] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New York, NY: Wiley-Interscience, 2006.

[76] G. Song and Y. G. Li, "Asymptotic throughput analysis for channel-aware scheduling," *IEEE Trans. Commun.*, vol. 54, no. 10, pp. 1827 – 1834, Oct. 2006.

[77] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated ergodic fading channels at high snr," *IEEE Trans. Inform. Theory*, vol. 57, no. 4, pp. 1975–1983, April 2011.

[78] J. Zhu, X. Jiang, O. Takahashi, and N. Shiratori, "Effects of channel correlation on outage secrecy capacity," *Journal of Information Processing*, vol. 21, no. 4, pp. 640–649, Oct. 2013.

[79] S. Vuppala and G. Abreu, "Secrecy transmission capacity of random networks," in *IEEE Fourty-Seventh Asilomar Conference Conference on Signals, Systems, and Computers*, 2013.

[80] S. Akoum and R. W. Heath, "Interference coordination: Random clustering and adaptive limited feedback," *IEEE Trans. Signal Processing*, vol. 61, no. 7, pp. 1822–1834, Apr. 2013.

[81] C. Candan and U. Orguner, "The moment function for the ratio of correlated generalized gamma variables," *Statistics and Probability Letters*, vol. 83, no. 10, pp. 2353 – 2356, 2013.

[82] A. Rabbachin, M. Z. Win, and A. Conti, "Interference engineering for network secrecy in nakagami fading channels," in *Proc. IEEE International Conference on Communications*, 2013.

[83] S. Binnikov and R. Moessner, "Expansions for nearly Gaussian distributions," *Astron. Astrophys. Suppl. Ser.*, no. 130, pp. 193–205, Oct. 1998.

[84] E. Mekić, M. Stefanović, P. Spalević, N. Sekulović, and A. Stanković, "Statistical analysis of ratio of random variables and its application in performance analysis of multihop wireless transmissions," *Mathematical Problems in Engineering*, 2012.

[85] R. K. Ganti, J. G. Andrews, and M. Haenggi, "High-sir transmission capacity of wireless networks with general fading and node distribution," *IEEE Trans. Inform. Theory*, vol. 57, no. 5, pp. 3100 – 3116, May 2011.

[86] K. Gulati, R. K. Ganti, J. G. Andrews, B. L. Evans, and S. Srikanteswara, "Characterizing decentralized wireless networks with temporal correlation in the low outage regime," *IEEE Trans. Wireless Comm.*, vol. 11, no. 9, pp. 3122 – 3125, Sep 2012.

[87] A. Karnik and A. Kumar, "Distributed optimal self-organization in ad hoc wireless sensor networks," *IEEE Trans. on Networking.*, vol. 15, no. 5, pp. 1035 – 1045, 2007.

[88] J. Liu, A. L. Stolyar, M. Chiang, and H. V. Poor, "Queue back-pressure random access in multihop wireless networks: Optimality and stability," *IEEE Trans. Inform. Theory*, vol. 55, no. 9, pp. 4087 – 4098, 2009.

[89] N. Abramson, "The ALOHA system - Another alternative for computer communications," in *Proc. IEEE Joint Computer Conference*, 1970.

[90] P. Nardelli and G. T. F. de Abreu, "On hopping strategies for autonomous wireless networks," in *IEEE Global Conference on Communications (Globecomm'09)*, 2009.

[91] "Derivatives of Hypergeometric2F1 Function," http://functions.wolfram.com/HypergeometricFunctions/Hypergeometric2F1/20/02/05/0003/, 2001.

[92] S. Vuppala and G. Abreu, "Asymptotic secrecy analysis of random networks with colluding eavesdroppers," submitted to IEEE/ACM Trans. on Networking.

[93] C. H. M. de Lima, M. Bennis, and M. Latva-aho, "Coordination mechanisms for self-organizing femtocells in two-tier coexistence scenarios," *IEEE Transactions on Wireless Communications*, vol. 11, no. 6, pp. 2212 – 2223, June 2012.

[94] S. Vuppala, W. Liu, , T. Ratnarajah, and G. Abreu, "Secrecy outage analysis of cognitive wireless sensor networks," June 2014, accepted to IEEE Fourty-Eigth Asilo- mar Conference Conference on Signals, Systems, and Computers, Pacific Grove, CA, Nov. 2014.

[95] X. Zhou, M. McKay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *Communications Letters, IEEE*, vol. 15, no. 3, pp. 302–304, March 2011.

[96] M. Sarkar and T. Ratnarajah, "Secure wireless multicasting through nakagamim fading MISO channel," in *Proc. IEEE* $45^{\text{th}}$ *Asilomar Conference on Signals, Systems and Computers*, Nov 2011, pp. 300–304.

[97] G. Geraci, S. Singh, J. G. Andrews, J.Yuan, and I. B. Collings, "Secrecy rates in broadcast channels with confidential messages and external eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2931–2943, May 2014.

[98] S. Vuppala, W. Liu, , G. Abreu, and T. Ratnarajah, "Secrecy outage of Nakagami-m miso channels with randomly located receivers," submitted to IEEE International Conference on Communications, London, UK, June, 2015.

[99] A. M. Ibrahim, T. ElBatt, and A. El-Keyi, "Covergae probabilty analysis for wireless networks using point processes," in *Proc. IEEE* $24^th$ *International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'13)*, 2013, pp. 1002–1007.

[100] Y. Zhou, Z. Zhao, Q. Ying, R. Li, X. Zhou, and H. Zhang, "Two-tier spatial modeling of base stations in cellular networks," arXiv:1404.1142v2, Aug. 2014.

[101] Q. Ying, Z. Zhao, Y. Zhou, R. Li, X. Zhou, and H. Zhang, "Characterizing spatial patterns of base stations in cellular networks," arXiv:1404.1143v2, Jun. 2014.

[102] S. Vuppala and G. Abreu, "Secrecy outage analysis in cellular networks," Aug. 2014, submitted to IEEE Wireless Communication Letters.

[103] ——, "Analysis of secure unicast links in stochastic wireless networks," in *Proc. IEEE International Conference on Communications (ICC)*, Budapest, Hungary, June 9-13 2013, pp. 1588 – 1593.