MONASH University

Enhancing Security in Random Wireless Network with the Aid of Friendly Jammers

by

Jishan E Giti

B. Sc. in Electrical & Electronic Engineering

M. Sc. in Electrical & Electronic Engineering

A thesis submitted for the degree of Doctor of Philosophy at
Monash University in
Faculty of Information Technology

October, 2020

This thesis is dedicated to my beloved mother,
Prof. Dr. Selina Parween
(1954-2020)
for inspiring me to have a PhD.

Copyright Notice

Abstract

An active or adaptive eavesdropper is an adversary that can act as both an illegitimate receiver and hostile jammer, rendering any communication between parties unsecured. An active eavesdropper is considered to be full-duplex (FD) while an adaptive eavesdropper is a half-duplex (HD) node. This project investigates the strengthening of physical layer security in wireless communication and proposes the use of friendly jammers to counter hostile jamming from adaptive eavesdroppers, which has not been studied before in literature. By exploiting their half-duplex nature the friendly jammers deceive the eavesdroppers to be passive listeners with source-like deceptive friendly jamming signals. The effectiveness of security strength at physical layer is often measured by secrecy capacity (SC) and secrecy outage probability (SOP) measures.

First, we investigate the impact of employing friendly jammers in improving secured communication for a relay-aided half-duplex system for single as well as multiple antenna channels. We show that the use of friendly jammer as a means to strengthen physical layer security is highly effective as demonstrated through increased SC and decreased SOP by a large margin. Numerical results, obtained through computer simulations, under different scenarios of varying jamming power and average main channel gain to average eavesdropper channel gain ratio demonstrate the effectiveness of friendly jammer in providing physical layer security. However, the scenario considered here is rather simplistic which assumes that the location of eavesdropper(s) and its channel state information (CSI) is known to the transmitter.

Next we investigate an extended and more complex but practically deployable scenario where eavesdroppers are randomly located, and the transmitter has a secrecy protected zone enforced. The destinations, eavesdroppers and friendly jammers are distributed according to homogeneous Poisson point process (HPPP). The network geometry of the random wireless network causes complex manipulation for the derivation for the secrecy parameters. The secrecy capacity is evaluated for different friendly jamming parameters and radii of the secrecy protected zone. Illustrative numerical results demonstrates that the friendly jammers can enhance the secrecy capacity of a random wireless network.

The friendly jammers are found prominently effective when the secrecy protected zone is very small and/or the node intensity of the destinations is low. We then consider full-duplex eavesdroppers in this scenario replacing the half-duplex ones.

We derived both SC and SOP for the relay-aided networks and SC for the random wireless networks. The mathematical derivations of SC and SOP, and their numerical performance analysis of our proposed system support the benefits of employing friendly jammers. The research work is very helpful understanding the security of the systems in classical wireless system models as well as random wireless models. The regular relay-aided cellular or radio networks fall under the category of classical models, and random wireless networks have found applications in wireless sensor networks, self-driving cars, health-care monitoring and so on. Therefore, this thesis has broad aspects on various types of wireless applications.

Declaration

I, Jishan E Giti, hereby declare that this thesis contains no material which has been accepted for the award of any other degree or diploma at any university or equivalent institution and that, to the best of my knowledge and belief, this thesis contains no material previously published or written by another person, except where due reference is made in the text of the thesis. All primary sources of help have been acknowledged where necessary.

Signature: Date: 13/10/2020

Acknowledgements

First and foremost, I would like to express my deepest gratitude to my supervisors, Dr. Amin Sakzad, Prof. Joarder Kamruzzaman, Prof. Bala Srinivasan and Dr. Raj Gaire, for guiding me throughout my PhD studies. I learned a lot and grew up to be a better researcher with their advice and persuasion. It was an excellent opportunity for me to work with such knowledgeable supervisors.

I would like to thank all members of my panel committee, namely Ron Steinfeld, Vincent Lee and Xingliang Yuan, for their feedback and support during my candidature. I express my gratitude to my former mentor Prof. Md. Zahurul Islam Sarkar, Dept. of EEE, Rajshahi University of Engineering & and Technology (RUET) for introducing me to the world of information-theoretic security.

I would also like to thank Monash University for providing me financial support during my PhD, in the form of Monash International Postgraduate Research Scholarship and Monash Graduate Scholarship. I sincerely thank CSIRO for granting me a top-up scholarship, thus encouraging me to enhance my research ability.

Furthermore, I would like to thank my fellow PhD students, including Sameen, Fatima, Komal, Yathi, Bo, Shams, Paula and Kelvin, for their moral supports. A special thank goes to amazing Danette Deriane and Helen Cridland along with the former and current FIT GRS team for helping me with all the necessary information about my candidature and also giving mental support time-to-time. I would also like to thank Ms. Julie Holden for assisting us with her GSAS/ALS sessions about how to represent our research orally or written.

Finally, I would like to express gratitude towards my biggest strength, my family. My husband, Shah Ariful Hoque Chowdhury, was always there to support me mentally, if not physically by my side throughout the PhD while managing his own PhD studies. I cannot give enough thanks to my parents, Md. Lutfur Rahman and late Prof. Selina Parween, for always supporting me and inspiring me to dream a dream. My elder brother Md. Toufiqur Rahman and his lovely wife Marzia Quddus are very supportive

and shower me with love more than enough. My PhD journey was not going to this smooth without any of their support.

Publications

1. **Journal Papers**

   (a) J. E. Giti, A. Sakzad, B. Srinivasan, J. Kamruzzaman and R. Gaire, "Secrecy Capacity against Adaptive Eavesdroppers in a Random Wireless Network using Friendly Jammers and Protected Zone", *Journal of Network and Computer Applications*, Elsevier, ISSN:1084-8045E-ISSN:1095-8592. DOI: https://doi.org/10.1016/j.jnca.2020.102698.

   Status: Published

2. **Conference Papers**

   (a) J. E. Giti, B. Srinivasan and J. Kamruzzaman, "Impact of Friendly Jammers on Secrecy Multicast Capacity in Presence of Adaptive Eavesdroppers", *IEEE GLOBECOM 2017 Workshops: 5th IEEE GLOBECOM Workshop on Trusted Communications with Physical Layer Security*, Singapore, 4-8 December, 2017.

   Status: Published

   (b) J. E. Giti, A. Sakzad, B. Srinivasan, J. Kamruzzaman and R. Gaire, "Friendly Jammer against an Adaptive Eavesdropper in a Relay-aided Network", *The 16^{th} International Wireless Communications & Mobile Computing (IWCMC) Conference*, Limassol, Cyprus, 15-19 June, 2020.

   Status: Published

Contents

List of Figures

List of Tables

List of Abbreviations

A/D	Analog-to-Digital
AF	Amplify-and-forward
AN	Artificial Noise
AWGN	Additive white Gaussian noise
CDF	Cumulative Distribution Function
CJ	Cooperative Jamming
CoF	Compute-and-forward
COP	Connection Outage Probability
CSI	Channel State Information
DF	Decode-and-forward
DL	Deep Learning
FD	Full-duplex
FJ	Friendly Jammer
GPS	Global Positioning System
HD	Half-duplex
HPPP	Homogeneous Poisson Point Process
IoT	Internet-of-things
IPZ	Interference Protected Zone
LT	Laplace Transform
MER	Average Main Channel Gain to Average Eavesdropper Channel Gain Ratio
MIMO	Multiple-Input Multiple-Output
MISO	Multiple-Input Single-Output
OSI	Open Systems Interconnection
PDF	Probability Density Function
SC	Secrecy Capacity
SGZ	Secrecy Guard Zone
SI	Self-interference
SIMO	Single-Input Multiple-Output
SISO	Single-Input Single-Output
SINR	Signal-to-Interference-plus-Noise Ratio

SNR	Signal-to-Noise Ratio
SOP	Secrecy Outage Probability
SPZ	Secrecy Protected Zone
WSN	Wireless Sensor Network

Chapter 1

Introduction

1.1 Overview and Challenges

The demand for wireless communication is increasing day by day. The broadcasting nature of the wireless medium continuously puts it under the threat of eavesdropping and jamming [1]. Sometimes encryption-decryption method alone is not sufficient for proper information theoretic security and not all wireless devices are suitable for computationally complex cryptography. Traditionally, cryptographic protocols are used alone to secure the wireless communications; however, this is considered to be an upper layer issue and is independent of the physical layer, thereby does not guarantee a complete security [2,3]. Since physical layer security has become a huge matter of concern, significant research works have been done in recent times to enhance the security of wireless communication. Also, a short battery lifetime with high energy drain and complex computational process are matters of huge concerns for many portable wireless devices which cannot afford the cryptographic methods. The traditional cryptography requires additional resources for key generation and management [4–6]. In networks with low-complexity devices, key distribution for symmetric cryptosystems and the high computational complexity of asymmetric cryptosystems raise issues due to lack of infra-structure [1, 7]. Encryption methods assume that an eavesdropper is incapable of breaking the encryption due to limitations in its capacity. With the growth of computational power, this assumption may not hold for every network. The physical layer security requires low computational complexity and does not assume any limitation for the eavesdropper's computational abilities, thus becoming a much appreciated method considered among researchers.

Emerging applications like internet-of-things (IoT), smart cities and autonomous vehicles on road show the rise to support 5G and beyond and wireless local area network

(WLAN) to meet the data communication need [8]. As a result, assessing security risks, i.e., security auditing has become a huge concern for various organisations [9]. The strong security requirement by these applications has generated huge attention among researchers to work on physical layer security. Physical layer security, in combination with the cryptographic solution at the upper layer, promises enhanced security assurance to these applications.

1.2 Preliminaries

1.2.1 Wireless Communication Model

A simple wireless communication can be portrayed by Fig. 1.1. Here, a source transmits signal to a destination over the wireless channel. The open nature of the wireless

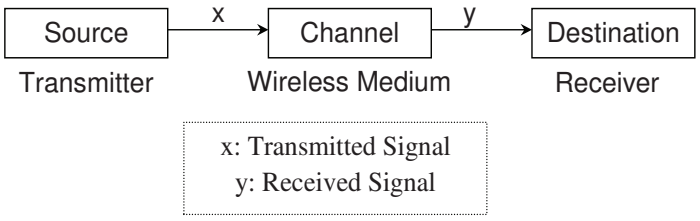


FIGURE 1.1: A simple wireless network.

medium causes various problems to hamper the quality of the transmission due to multipath fading, path-loss and shadowing, and also causes security breach in the form of eavesdropping and jamming. Due to these problems the received signal y at the destination is different from the transmited signal x from the source as shown in Fig. 1.1. The received signal includes the effects of fading, noise and also the interference from other sources or adversaries residing in the network. Throughout this thesis, the jamming intentionally done by an adversary to degrade the legitimate transmission is recognised as the hostile jamming.

1.2.2 Physical Layer

In wireless communication, the physical layer is the wireless medium or channel which handles the data transmissions between the users. Due to the nature of radio propagation and broadcasting, this physical layer suffers from channel fading, shadowing, eavesdropping and even jamming. This is why wireless networks requires adaptive and integrated protocols for all layers of the open systems interconnection (OSI) model of telecommunication. The OSI model is a concept that discusses the interoperability

for various communication protocols from physical layer to application layer and vice versa [10]. Though physical layer is the bottom layer of this model, its vulnerable characteristics pushes the designers to hire experts from communications, signal processing, network theory and as well as physical layer security backgrounds [11].

1.2.3 Physical Layer Security

Physical layer security stands for a secure physical layer so that the eavesdropping can be prevented without any upper layer data encryption. By securing the physical layer along with other layers, a total information-theoretic security can be achieved. In wireless communication, the physical layer security is ensured by exploiting the characteristics of channel fading and noise. It is implemented using signal processing, communication, and coding techniques. The target is to degrade the eavesdropping channel so that the eavesdropper cannot learn a single bit of information transmitted by the source. Unlike cryptographical approaches this information-theoretic security does not rely on computationally hard assumptions [7]. This approach eliminates the key management issue [12] which results in significantly lower complexity in resource savings. Also, the physical layer security can be used to augment the security provided by the existing cryptosystems with an additional level of protection for information transmission or to achieve key agreement including key generation and distribution for the remote terminals [13, 14].

1.2.4 Fading and Shadowing

In wireless medium, when the signal quality degrades over long distances even without the presence of large amount of noise, it is called fading. A channel with this characteristic is called a fading channel. This phenomenon happens due to the constructive and destructive combination of randomly delayed, reflected, scattered and diffracted signal components [10, 15]. The fading occurs from both natural and man-made causes such as rain, snow, fog, multiple transmission links, tall buildings and so on. As a result, the amplitude or phase of the signal is affected and signal loss happens. The rapid fluctuation in signal amplitude and phase over a small distance is called the small-scale fading, or simply the fading. Researchers regularly work with various types of channel models describing the statistical behaviour of the fading such as Rayleigh, Rician, log-normal fading channels and so on. The characteristics of the fading in a channel can be also classified as a slow or fast fading depending on whether the amplitude or phase change (fading) is roughly constant over the period of use or not, respectively. The system models used in this thesis deal with slow Rayleigh fading which can be characterised by

the following expression of probability density function (PDF) [15],

$$p_\gamma(\gamma) = \frac{1}{\overline{\gamma}} \exp\left(-\frac{\gamma}{\overline{\gamma}}\right), \tag{1.1}$$

where, γ and $\overline{\gamma}$ denote the instantaneous and average signal-to-noise ratio (SNR) of the channel, respectively.

Shadowing causes fluctuations in the received signal power due to objects obstructing the propagation path between a transmitter and a receiver. For example, a tall building or a mountain can cause the shadowing effect of the transmission, and the receiver may lose the connection with the transmitter. Shadowing falls under the category of large-scale fading.

1.2.5 SNR and SINR

Both signal-to-noise ratio (SNR) and signal-to-interference-plus-noise ratio (SINR) are measures of signal levels compared to background noise levels. In case of SINR, the signal level is compared to both noise and interference levels of the network. The expressions for SNR and SINR are, respectively, given below.

$$SNR = \frac{P}{N}$$
$$SINR = \frac{P}{I+N},$$

where, P, N and I denote the average power of signal, noise and interference, respectively. In wireless communication, SNR and SINR are used to measure the quality of wireless connection. As wireless communication suffers from attenuation due to path loss and interference from other sources or jammers, maintaining a good SNR or SINR is very important.

In case of fading channels, the noise in SNR or SINR cannot be considered to be simple thermal noise. The fading characteristics also need to be considered along with the noise. As a result, researchers proposed an appropriate measure as average SNR including the effect of the fading and can be expressed as [15],

$$\overline{\gamma} \triangleq \int_0^\infty \gamma p_\gamma(\gamma) d\gamma, \tag{1.2}$$

where, $p_\gamma(\gamma)$ is obtained from the expression of PDF in (1.1), $\gamma = \frac{\alpha^2 E_s}{N_0}$ is the instantaneous SNR per symbol with α, E_s and N_0 being the fading amplitude or signal power modulator, energy per symbol and noise power spectral density, respectively.

1.2.6 Eavesdropping and Jamming

The broadcasting nature of wireless medium makes it vulnerable to eavesdropping. The eavesdroppers try to listen to the transmission by being near to the legitimate entities whether the legitimate entity is a source, destination or a relay. Mostly, eavesdroppers are silent nodes that just listen to transmission, and these nodes are hard to locate [16]. These types of eavesdroppers are known as passive eavesdroppers. On the other hand, some eavesdroppers can carry out active attacks on wireless networks to intentionally disrupt transmission. An eavesdropper who maliciously attacks the network is called an active eavesdropper [16–18].

The most known active attack is jamming the network by an adversary. The entity who causes the jamming to degrade the quality of a communication is called a jammer. In this thesis, the jamming by an adversary is denoted as *hostile jamming* and the jammer is called a *hostile jammer*. In contrast, the jamming *against* an adversary is called *friendly jamming* and the jammer is called a *friendly jammer*. Fig. 1.2 summarises some common

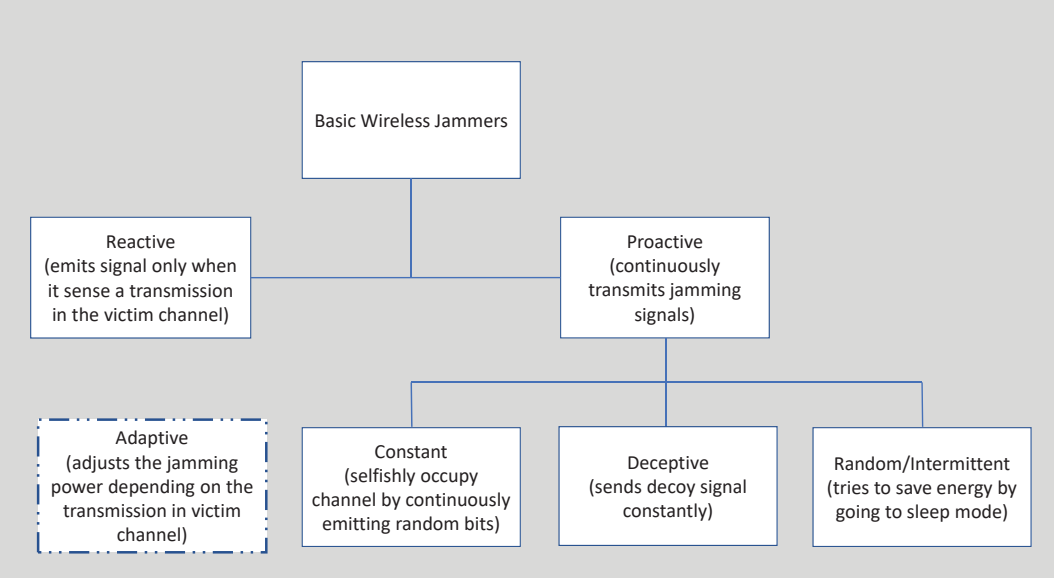


FIGURE 1.2: Some common types of jammers (hostile or friendly) based on the nature of jamming signal.

types of jammers found in the literature. This classification can be applicable to both hostile and friendly jammers. Sometimes, hostile jamming comes from an eavesdropper. The jamming signal, to infiltrate the legitimate transmission, may consists of just noise or can be an exploited version of the source signal tampered by the eavesdropper. For the latter case, the jammer may also be known as an *adaptive jammer* [19] though some researchers have used the term adaptive jammer for a jammer with adjustable jamming power [20].

As discussed above, an eavesdropper capable of carrying out active attack is an active eavesdropper. However, many researchers opted for different terms for an eavesdropper depending on whether it can simultaneously listen and jam or not. If an eavesdropper is *half-duplex* (HD) in nature then it is called an *adaptive eavesdropper*, which either listens or jams depending on the channel conditions [21]. On the other hand, a *full-duplex* (FD) eavesdropper can simultaneously listen and jam, and is strictly called an *active eavesdropper* [22]. In this thesis, we consider an adaptive eavesdropper as a half-duplex eavesdropper whereas an active eavesdropper as a full-duplex one.

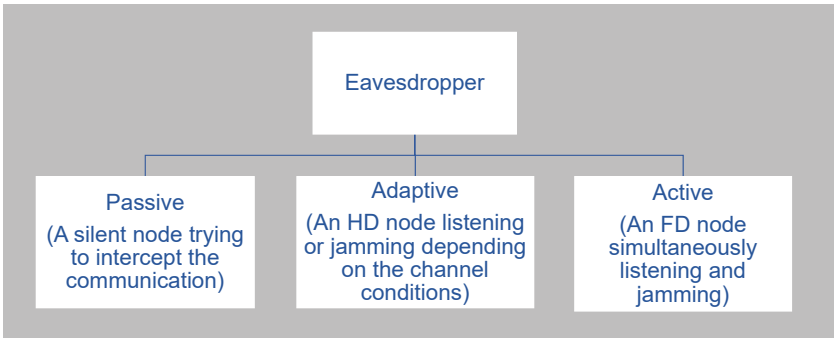


FIGURE 1.3: Types of eavesdroppers used in this thesis.

Fig. 1.3 summarises the types of eavesdroppers discussed in this thesis. The thesis mostly deals with adaptive eavesdroppers as their HD nature is exploitable by friendly jammers to stop them from hostile jamming. In reception mode, these eavesdroppers are just like passive ones. Chapter 5 provides insights about the use of friendly jammers against the active (FD) eavesdroppers.

1.2.7 Friendly Jamming

If a jamming signal does not affect the quality of the legitimate transmission, then the jamming can be considered as friendly jamming. Jamming against eavesdroppers by source, relay, destination or hired nodes can be found in the literature. Some researchers, as explained next, coined the term 'friendly jamming' if the jamming is beneficial to the system secrecy. When a helper node is hired to interfere with the eavesdroppers in exchange of currency or energy, that node is called a friendly jammer [23, 24]. The source, relay and destination based jammings are based on energy distribution for both transmission and jamming. Sometimes the relays can be untrusted and behave like eavesdroppers themselves. Destination based jamming is useful if the eavesdropper is located near the destination. However, for a single-antenna destination it cannot be possible to receive the source signal and jam the eavesdropper simultaneously. Jamming by source, relay and destination also introduce strong self-interference (SI) which is

again an extra thing to consider for the legitimate receivers [25]. On the other hand, the friendly jammers do not deal with the problem of SI and source can choose to pay them in currency for their services if the source has enough resources.

A friendly jammer is considered to be the part of a legitimate system and the entities of the system can be given a chance to decode the friendly jamming from their received signal. However, while dealing with multiple friendly jammers and/or legitimate receivers, the friendly jammers can use zero-forcing (ZF) precoding. The ZF precoding uses null spaces of the channel matrices between the jammers and the legitimate receivers to infiltrate with jamming. Mathematically speaking, if we design the jamming signal ($\mathbf{x}_J$) as a normalized signal onto the null space of the channel vector $\mathbf{j}_D$ between the jammer and the group of N destinations [26, 27], we have,

$$\mathbf{j}_D \mathbf{x}_J = \sum_{i=1}^{N} (j_{Di} \times x_J) = 0 \tag{1.3}$$

However, the eavesdropper cannot decode the jamming signal and suffers from the interference caused by it. This thesis investigates the use of friendly jammers in various types of wireless networks against various types of eavesdroppers.

1.2.8 Networks Categories by Antenna Number

The wireless networks can be categorised into four different types depending on the antenna numbers at the transmitter and receiver. The types are as follows,

(i) Single-input-single-output (SISO): Both the transmitter and the receiver have single antenna.

(ii) Single-input-Multiple-output (SIMO): The transmitter is equipped with single antenna but the receiver has multiple antennas.

(iii) Multiple-input-single-output (MISO): The transmitter has multiple antennas but the receiver is equipped with single antenna.

(iv) Multiple-input-Multiple-output (MIMO): Both the transmitter and the receiver have Multiple antennas.

These types are discussed in the literature under the topic of antenna diversity. If an entity is equipped with multiple antennas it creates multiple independent links for wireless communication. As a result, multiple antennas are useful for more reliable communication, higher secrecy capacity, beamforming and so on [28–30]. However, employing antenna diversity may not be cost-effective for all devices.

1.2.9 Secrecy Capacity

The secrecy capacity is the difference between the capacity of the legitimate channel (also known as the main channel) and that of the eavesdropping channel. As Wyner [31] proved that secrecy is only possible if the eavesdropper has a degraded channel compared to the main channel, the secrecy capacity should have a positive value. The expression of secrecy capacity can be given as,

$$C_s = [C_{main} - C_{eavesdropper}]^+. \tag{1.4}$$

where, C_s is the secrecy capacity in bits/Hz/sec, C_ℓ is the capacity of channel ℓ, and $[\cdot]^+ = max(\cdot, 0)$. In case of multiple destinations and multiple eavesdroppers as shown in Fig. 1.4, C_{main} is the minimum of the capacities found at all the destinations, and $C_{eavesdropper}$ is the maximum of the capacities found at all the eavesdroppers.

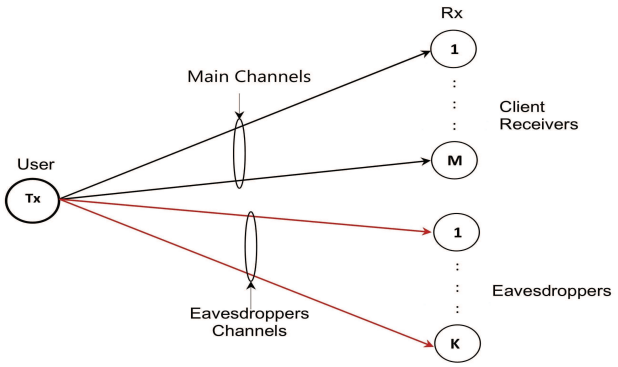


FIGURE 1.4: Channels in a wireless network with eavesdroppers.

Now, Shannon's capacity theorem [32] states that the capacity of a channel with a bandwidth of B Hz can be given as,

$$C = \mathrm{B}\log_2(1 + \mathrm{SNR}).$$

The main and eavesdropper channel capacities are calculated using this theorem to obtain the secrecy capacity. The theorem is derived with the help of following expression for secrecy capacity,

$$C_s = \max_{f(x)} \mathcal{I}(x; y) \tag{1.5}$$
$$\text{with } \mathcal{I}(x; y) = h(y) - h(y|x),$$

where, *f(x)* is the input distribution or the probability density function (pdf) of transmitted signal x, $\mathcal{I}(x;y)$ denotes the mutual information between x and the received signal y, and $h(\cdot)$ denotes the entropy or the uncertainty of information. This idea prompted researchers to derive secrecy capacity for various fading channels for SISO, SIMO, MISO and MIMO networks [13, 29, 33, 34].

1.2.10 Secrecy Outage Probability (SOP)

It is the probability that the secrecy is compromised. According to Parada and Blahut [33], the secure communication can be guaranteed temporarily if the eavesdropper's channel is worse than the main channel. Later on, Barros and Rodrigues proposed secrecy outage probability to characterise secrecy capacity in terms of outage probability if the source does not know the eavesdropper's channel [35]. The secrecy outage probability can be expressed in terms of secrecy capacity obtained by (1.4) as,

$$P_{out} = Pr(C_s < R_s), \tag{1.6}$$

where, $R_s > 0$ is the target secrecy rate. The significance of this definition is that when the secrecy rate is set to R_s, confidential communication will be ensured only if $C_s > R_s$, otherwise secure transmission will not be guaranteed. However, this definition does not necessarily imply a lack of secrecy since the outage event may also happen due to lack of reliability [7]. The lack of reliability is the case when the legitimate receivers fail to decode the transmitted message correctly.

1.2.11 Secrecy Zones

Secrecy zones are created to keep the surroundings of transmitters free from eavesdroppers. Generally, eavesdroppers try to be near the source for eavesdropping purpose thus achieving higher eavesdropping capacity. As a result, the secrecy capacity decreases as eavesdropper's distance from the transmitter increases due to secrecy zones. If the transmitter has the resources to identify an eavesdropper in its surrounding, then the transmitter either ceases the transmission to save power or tries to deactivate the eavesdropper. If the transmitter stops transmission when there is an eavesdropper inside a certain area surrounding the transmitter, then the area is called a secrecy guard zone (SGZ) [36]. On the other hand, if the transmitter deactivates the eavesdroppers then the zone is known as secrecy protected zone (SPZ). Before starting the transmission the source constructs a secrecy protected zone by scanning and removing nearby eavesdroppers with the help of various detecting devices such as a metal detector, x-ray detector,

evolved heat detector and so on [37, 38]. The destinations in [39] are found to use similar methods to introduce interference protected zones (IPZ) around themselves to avoid nearby interference from cooperating nodes.

1.2.12 Random Wireless Network

For large scale wireless networks, the source, destination, eavesdroppers and other nodes are located at random places. This types of scattered nodes are found in heterogeneous cellular networks, wireless sensor networks, internet-of-things (IoT) based networks, smart cities and so on [40]. The distribution of distances between the nodes is an important factor to know since the randomness of node locations causes randomness in the path-loss and SINR levels. The aggregated interference at each node depends on this distribution. We also need to estimate the higher moments of the distribution, since the energy required by the source for the transmission over distance D can be assumed proportional to D^{α} with α being the path-loss constant [41]. Many researchers opted for the Poisson point process to characterise the distribution of the node distances. A well accepted model for non-mobile nodes in wireless network is the homogeneous Poisson point process (HPPP) model [42]. We have used this model for our random wireless network and a brief description of the distribution of the distances between two nodes in a circular coverage area is given in Chapter 4.

1.3 Motivation and Objectives

The relevant previous works in the current lierature and research gap are described in Chapter 2. The existing literature motivated us to investigate use of friendly jammers against hostile jamming when the hostile jamming is coming from the adaptive or active eavesdroppers. The hostile jamming causes a drop in the legitimate channel capacity and additional eavesdropping causes a rise in eavesdropper's channel capacity. As a result, the system suffers from a low secrecy capacity and a high secrecy outage probability. Most researchers have chosen passive eavesdroppers as adversary and even when dealing with adaptive eavesdroppers they do not exploit the half-duplex nature of the eavesdroppers to avoid the hostile jamming. The objectives of the thesis are as follows:

(i) To investigate if the friendly jammers are capable of enhancing the security of a relay-aided radio network where the source has the knowledge of an adaptive eavesdropper's location.

(ii) To investigate if the friendly jammers can enhance security against adaptive eavesdroppers in a random wireless network where the entities are located randomly following an HPPP model.

(iii) To analyse the impact of friendly jammers in a random wireless network with a small or no secrecy protected zone.

(iv) To study the impact of friendly jammers against the active (FD) eavesdroppers instead of adaptive (HD) ones.

(v) To analyse secrecy parameters like secrecy capacity or secrecy outage probability (SOP) whereas necessary to support our intuitions for the above investigations. The analysis includes mathematical derivations of the parameters and corresponding computer simulations for numerical results.

1.4 Contributions

The thesis has the following contributions:

(i) We choose a relay-aided radio network in presence of an adaptive eavesdropper to investigate the advantages of using deceptive friendly jammers. We derive the secrecy capacity and secrecy outage probability in the absence and presence of friendly jammer to observe if the friendly jammer provides a more secure network. This work is described in Chapter 3. Here, the system model is also considered for three types of scenarios:

   (a) A half-duplex MIMO radio network, where the source chooses the best relay among a group of relays to communicate with a group of destinations. A friendly jammer is also chosen as selected to interfere with a group of adaptive eavesdroppers by emitting artificial noise (AN). The model assumes that similar entities are closely located to each other, the source knows the eavesdroppers' locations and the friendly jammer is successful in forcing the eavesdroppers to be passive listeners. We investigate the secrecy capacity for this model. We name this model **SM0** and our work has been published in [43].

   (b) The model **SM0** is enhanced to be more practical. We use a deceptive friendly jammer against an adaptive eavesdropper and this time we use a SISO network. The antenna configuration is changed to work with the assumption that the adaptive eavesdropper fails to be an active eavesdropper because of it's single antenna. Also, the model depicts the usefulness of the friendly jammer in a wireless network with devices equipped with single antenna. We derive the

secrecy capacity and secrecy outage probability of this model. The numerical results show that the friendly jammer can increase the secrecy capacity and decrease the secrecy outage probability compared the scenario without the friendly jammer. The model is named **SM1** and our work has been published in [44].

(c) The SISO model is revisited to incorporate relay with multiple antennas and we call this variation of the model **SM2**. We derive the secrecy capacity and the secrecy outage probability for this model. The numerical results again show that a friendly jammer is advantageous in enhancing the secrecy capacity and decreasing the secrecy outage probability.

(ii) We choose a practically deployable random wireless network, where a source communicates with multiple destinations randomly placed within a coverage area. Multiple eavesdroppers exist surrounding the source. We initially choose adaptive (HD) eavesdroppers and then studied the same scenario with active (FD) eavesdroppers. A group of deceptive friendly jammers are employed to tackle the eavesdropping and hostile jamming. All the destinations, eavesdroppers and friendly jammers follow the HPPP model for their locations. The source also employ a secrecy protected zone (SPZ) as an extra security measure. As SPZ is capable of deactivating any eavesdropper inside the zone, the presence of SPZ is in favour of system secrecy. We investigate secrecy capacity for various parameters of the friendly jammers and secrecy protected zone to estimate the impact of friendly jammers in enhancing the secrecy of the system models. The random wireless network in presence of HD eavesdroppers is named as **SM3** and the one with FD eavesdroppers is named as **SM4**. The works with **SM3** and **SM4** are discussed in chapters 4 and 5, respectively. The work with **SM3** has been published in [45].

In a nutshell, the overall aim of the thesis is to investigate and quantify the benefits of friendly jammers in various types of networks in presence of different types of eavesdroppers. The thesis investigates the secrecy capacity and secrecy outage probability as secrecy metrics, and also observes their variations with respect to different parameters, namely, number of antennas for the relay, node intensities of both legitimate and adversarial entities, jamming power of friendly jammers and so on.

1.5 Organisation of the Thesis

This section deals with the outline of the rest of the thesis. The primary contributions of this thesis are categorised into three content chapters: Chapters 3, 4 and 5. Chapter

3 describes the investigations of friendly jammer in a simple relay-aided network and the latter two chapters cover the investigations of the friendly jammers in a random wireless network against adaptive and active eavesdroppers, respectively. The outline and summary of the upcoming chapters are as follow:

- Chapter 2: **Literature Review.** The chapter discusses the related previous works and the research gap to motivate our works.
- Chapter 3: **Friendly Jammers against Adaptive Eavesdroppers in a Relay-aided Network.** This chapter investigates the advantages of using friendly jammers in a relay-aided wireless network in presence of an adaptive eavesdroppers. It is assumed that the location of the eavesdropper is known to the source and the friendly jammer is successful in deceiving the eavesdropper to be in reception mode with a source-like jamming signal. The investigation is done for considering various scenarios like an initial MIMO system with AN emitting friendly jammers and a SISO network with deceptive friendly jammers. For the latter scenario the relay is chosen to be equipped with either single or multiple antennas.
- Chapter 4: **Friendly Jammers in Random Wireless Network against Adaptive Eavesdroppers.** This chapter includes the impact and advantages of using deceptive friendly jammers in a random wireless network in presence of adaptive eavesdroppers. In this practically deployable system model all the entities surrounding the source are randomly placed following an HPPP model. The friendly jammers are found to be advantageous by converting most of the hostile jammers to be passive eavesdropping nodes. The impacts of varying different parameters for the friendly jammers are investigated. Also, the investigation shows that the friendly jammers can restore the secrecy of an unsafe random wireless network with small or no secrecy protected zone.
- Chapter 5: **Friendly Jammers in Random Wireless Network against FD Eavesdroppers.** This chapter deals with the problem of failing to force the active (FD) eavesdroppers to remain passive and how the friendly jammers are still beneficial for the system secrecy. The results show that the friendly jammers with sufficient jamming power can enhance the secrecy of the network.
- Chapter 6: **Concluding Remarks and Future Directions.** This chapter summarises the research contributions made in this thesis, and discusses the scope for further works in future.

Chapter 2

Literature Review

Due to the broadcasting nature, the wireless medium is very much susceptible to eavesdropping and jamming. Eavesdropping is when the adversary tries to listen to the transmission while jamming is when the interference by a malicious node is directed to legitimate entities.

The jamming attacks are also known as the active attacks. Sometimes these jammers can also be eavesdroppers. If the eavesdroppers can afford the risk of being detected, they can choose to be active attackers. The jamming signal consists of noise or can also be a signal exploiting all the available information on the codes and signals used by the victim network [46]. The jamming by adversaries causes degraded and unreliable transmission. This situation creates a hostile environment for the transmission, and throughout this thesis the jamming is denoted as the hostile jamming. This interception of the wireless transmission or degradation of the channel due to hostile jamming provide significant challenges to the physical layer security. As discussed in Chapter 1, cryptographic methods work in upper layers, and therefore, they are not suitable for tackling eavesdropping and jamming [13].

2.1 Overview: Physical Layer Security

Secure transmission in wireless communications using cryptographic approaches was initiated by Shannon [32] in 1949. However, providing secure communication over wireless networks using a cryptographic approach with the help of encryption keys presents significant challenges since the wireless medium is of open nature and thus allows eavesdroppers and attackers to intercept information transmission or to degrade the quality of transmission. In the 1970s, Wyner [31], and Csiszàr and Körner [12] opened a promising

new direction for solving the network security problem of transmitting message securely over a vulnerable wireless channel. They demonstrated that confidential messages can be transmitted securely without using an encryption key. According to Wyner's wiretap model, an information-theoretic security approach was studied to ensure reliable communication through wireless channels with maximum possible transmission rates. Wyner attempted to build his encoder and decoder in such a way that maximizes the transmission rate and also the equivocation of data seen by the eavesdropper. As the equivocation tends to equal the entropy of data source, perfect secrecy is obtained. Wyner's model is limited to the case where eavesdropper's observation is strictly worse than that of the legitimate receiver. These works are considered as the basis of information-theoretic security and one of the main performance parameters is the secrecy capacity. The expression of secrecy capacity was derived certainly from Shannon's capacity theorem [32] which expresses a channel capacity, $C = B\log_2(1 + SNR) \quad bits/sec.$ Here, C is the channel capacity and B is the bandwidth. By using the theorem, both the capacities of legitimate (main) and eavesdropping channels can be obtained and the secrecy capacity as discussed in (1.4) in Chapter 1, is the subtraction of the eavesdropping channel capacity from the main channel capacity.

In 2006, Barros and Rodrigues characterized secrecy capacity in terms of outage probability in [35] for a quasi-static Rayleigh fading single-input single-output (SISO) channel. For a transmitter having no knowledge about the eavesdropper channel, they defined the probability of transmitting at a target secrecy rate R_s greater than the secrecy capacity C_s as the probability that the information-theoretic security is compromised, in other words, this is the outage probability. They also showed that the probability of positive secrecy capacity can actually be achieved even when the eavesdropper has a better average SNR than the legitimate receivers. In their extended work [47], they considered the cases when the transmitter has either imperfect or perfect knowledge of the eavesdropper's channel. The perfect channel state information (CSI) at the transmitter depicts that the sender knows all the channel characteristics, i.e., fading distribution, average channel gain, line-of-sight component, and spatial correlation. The term imperfect CSI denotes lack of any of these information. This problem occurs when there is a channel estimation error, limited feedback or feedback delay form the receiver. If the receiver is a passive eavesdropper who is a silent entity, it is quite impossible to sense its existence or in other words, to have perfect CSI at the transmitter.

For multiple access channels, information-theoretic security was discussed by Liang et. al. [48]. Later research about multiple-input-multiple-output (MIMO) system became a matter of interest and Oggier et. al. [29] proved that perfect secrecy capacity is the difference between main channel capacity and eavesdropper's channel capacity for a MIMO broadcast channel. Again, multipath fading has to be taken under consideration

since wireless medium has to deal with fading. As a result, secrecy of fading channels became part of the literature [13, 15, 16, 49, 50]. The motivation for the research about fading channels was to observe how the high data rates with reliability can be achieved in spite of the harsh nature of wireless channel due to the multipath fading, and the effect of channel diversity on the secrecy capacity and the secure outage performance of fading channels.

Sheikholeslami et al. [51–53], introduced and exploited the idea of using an ephemeral encryption key and also an energy-efficient routing algorithm so that everlasting security can be achieved. According to them the hardware limitations of the eavesdroppers' Analog-to-Digital (A/D) converter can be exploited in a way that when the source transmits the message along with the cryptographically secured jamming signal, the destination knowing the key will deduct the jamming signal before its A/D but the eavesdroppers have to store the signal. After the transmission, the secret key will be revealed to eavesdroppers. The eavesdroppers will try to cancel the jamming signal from the recorded one at the output of their A/Ds. This will cause an overflow at the A/Ds and the eavesdroppers will not be able to retrieve the message. This method though attractive has to deal with key management. The method also relies on the current trend on the limitations of A/Ds that whether the eavesdropper want to have a wide-band A/D with low resolution and thus be susceptible to jamming or a narrow-band A/D with high resolution and lose information outside that bandwidth. With the current trend of progress in large scale electronics, eavesdroppers can use A/Ds with large capacities. In that case there is no guarantee that the eavesdropper will not be able to decrypt the jamming signal in a reasonable amount of time. Since the large-scale industrial IoT deals with wireless sensors which are low-power devices and cannot handle high computational complexity, many of the wireless networks cannot utilise this method. Therefore, using dedicated nodes as friendly jammers can be a better option to maintain the system secrecy.

This thesis investigates advantages of friendly jammers in two different types of networks. First one is a relay-aided radio or cellular network based on classical Wyner's model [31], and the second one is a random wireless network with scattered nodes. The overview of physical layer security in these models and friendly jamming are discussed below.

2.1.1 Security in Relay-aided Network

Relays help to retransmit data from transmitters to receivers, thus preventing data loss due to fading or attenuation. Many networks need the help of relays for quality transmission and hence various functions of the relay nodes have also become a matter

of interest. Proper relay precodings even help to mitigate interference and relays can be used as jammers too. Therefore, researchers investigated various relay functions such as beamforming, relay precoding, cooperative relaying, and co-operative jamming, to gain diversity and array gain [54, 55], to tackle interference [30, 56–58], to communicate using multiple relays in cooperation [59, 60], and even to jam adversaries [28, 61–63], respectively.

The idea of beamforming comes from the signal processing technique for directional signal transmission and reception. Since the beamforming includes use of antenna arrays the technique is highly useful only if the entities have multiple antennas [64, 65]. The beamforming uses an array of antennas to create constructive interference at the legitimate destinations while destructive interference at the adversaries. As a result, the destinations do not suffer from the signal attenuations. If the network users are each equipped with a single antenna, the option of beamforming depends solely on the directivity of the antenna [1]. Also, a perfect beamforming may not be achievable due to circuit complexity or the randomness of destination nodes in large-scale networks. An eavesdropper always tries to be near the legitimate entities which makes the beamforming insufficient for physical layer security.

In many practical scenarios, the relay performs a combination of these jobs. For example, Liu et al. [58], studied a scenario in cognitive radio where two sources, namely the primary and the secondary base stations, communicate with their corresponding destinations via a relay in the presence of multiple eavesdroppers. The relay performs a combined task of beamforming and cooperative jamming by using zero-forcing (ZF) precoding to cancel out the interference from the secondary base station at the primary base station's destination. The other destination and eavesdroppers suffer from the interference as they do not get this benefit from the relay. This study has similarities with the study of [30], where the authors used ZF precoding by relay for a coexisting MIMO radio network. Another recent similar work can be found in [65], where a cognitive transmitter (CT) acts as a relay. The CT uses beamforming matrices for maintaining legitimate communication and jamming the eavesdropper with artificial noise (AN) while using ZF precoding so that the legitimate destinations are not affected by the AN. In these works, the relay has a backhaul connection with the interference sources to nullify the interference at any legitimate destination. A backhaul connection is a high-speed connection with the core network (in this case, the sources). This approach is not suitable to tackle hostile jamming as the hostile jammers are illegitimate entities, and the relay fails to nullify their jamming due to no backhaul connections.

[1] Antenna directivity is the ratio of the radiation intensity in a given direction from the antenna to the radiation intensity averaged over all directions [66].

2.1.2 Security in Random Wireless Network

Since in large scale networks the nodes are located randomly, stochastic geometry became popular to predict the statistical properties of the nodes. The main sub-field of the stochastic geometry is the point-process theory where each node is considered to be a point existing inside an area set. Especially the Poisson point process has been applied largely in the fields of biology, astronomy, material sciences, and recently in image analysis and communication networks [67, 68]. The point-process theory is very much applicable to wireless ad-hoc and sensor networks, or cellular networks with extended coverage. A more precise application of random wireless network can also be found in the vehicle-to-vehicle communication involving road traffic or health-care transports [69]. The classical physical layer security model is inspired by Wyner's wiretap channel [31], which consists of only three nodes: the source, the destination and the eavesdropper. As a result, the classical methods do not deal with the randomness of locations of the nodes thus fail to incorporate the path dependency of the signals in random wireless networks [70]. For these networks, the performance metric is the signal-to-interference-plus-noise ratio (SINR) instead of signal-to-noise ratio (SNR), and the dependency of SINR on the network geometry makes the classical methods of communication theory insufficient to analyse a random wireless network. E. N. Gilbert, in 1961 [71], considered a random network with connected points of a Poisson point process (PPP) that are sufficiently close to each other. The randomness of the wireless channels can be then generalised by Gilbert's model where each pair of nodes in the random network are connected probabilistically depending on their distances [72]. In this case, several nodes sharing the same channel are affected by interference, thus replacing the SNR threshold with SINR threshold. According to ElSawy et al. [73], the aggregated interference at location y is a stochastic process and can be expressed as,

$$I_{agg} = \sum_{x \in \mathcal{I}} P_t(x) A h_{xy} \|x - y\|^{-\alpha}, \tag{2.1}$$

where, the aggregated interference depends on the locations of the interferers captured by the point process $\mathcal{I} = x_i$ and the random channel gains h_{xy}. The spatial locations of the interfere and the receiver are denoted by x and y, respectively. The notations $P_t(x)$, A and α denote the transmit power of interferer at location x, the propagation constant and the path-loss constant, respectively. In large-scale network, there is no expression for the PDF of I_{agg} so it is usually characterised by using the Laplace transform (LT) of the PDF of individual interferences [39, 73, 74]. Thus the Laplace transform of the aggregated interference is given by,

$$\mathcal{L}_{I_{agg}}(s) = \mathbb{E}[e^{-sI_{agg}}], \tag{2.2}$$

where, $\mathbb{E}(\cdot)$ is the expectation operator used here to measure the weighted sum of the aggregated interference. Using this method, we investigate the ergodic capacity of destinations and eavesdroppers, in presence of hostile and friendly jammers, for our chosen random wireless network. Our investigated work is described in Chapters 4 and 5.

Large scale network also comes with large numbers of eavesdroppers. In this framework, researchers started to investigate secrecy zones surrounding transmitters or receivers. One well known secrecy zone is called the secrecy guard zone (SGZ) and has been seen in the literature to protect the transmitter [75] or the users of a cellular network [74]. Generally, the transmitter within a secrecy guard zone ceases transmission if there exists any eavesdropper inside the zone resulting in transmission delay which degrades performance [76]. Thus many researchers adopted secrecy protected zone (SPZ) to deactivate eavesdroppers if there are any inside this zone. Liu et al., [39] published a notable work about a random wireless network where a secrecy protected zone was employed around the transmitter while the destination nodes employ an interference protected zone (IPZ) around them. The IPZs were used to create an interference-free zone where the interference was coming from other cooperative nodes. The interference protected zone was an extra measure to scan out any interferer inside the zone. For our random wireless network model, we only choose the SPZ as an extra security measure while we investigate if the friendly jammers are capable of enhancing the secrecy capacity by removing the hostile jamming form the received signals at the destinations.

2.1.3 Jamming against Eavesdroppers

Many researchers proposed jamming the adversaries with the help of source, destination and relays or by totally hiring other helper nodes. These types of jamming do not affect the legitimate entities and interfere with the adversaries only. Some researchers coined the term friendly jamming [77] or ally friendly jamming [78] for this type of jamming which does not affect the legitimate entities. Proper precoding techniques [26, 27] can be employed so that the legitimate entities can avoid this jamming or they are given the option of decoding the jamming signals from the received signals. The friendly jamming becomes very useful when a trade-off occurs between the security and reliability. When the destination fails to recover the source signal due to channel conditions or background interference, the source needs to increase the transmit power. But an increase in transmit power results in higher eavesdropping capacity thus degrading the security of the system [20]. If friendly jamming is used against the eavesdropper, the trade-off issue can be avoided.

For our system models, we choose hired helper nodes for friendly jamming. These nodes are called the friendly jammers or sometimes, the private jammers. The jamming against the eavesdroppers by the legitimate entities which include the source, relay, destination and friendly jammer is discussed below.

2.1.3.1 Transmitter, Relay and Destination based jamming

Relays can be employed to jam eavesdroppers by using cooperative jamming (CJ) protocols [28, 61–63]. CJ is the approach of user cooperation where a relay transmit a jamming signal to the eavesdropper at the same time the source transmits the message signal. This method works best if the eavesdropper is at the nearest region of the relay while the secrecy rate drops as the eavesdropper moves closer to the source and far from the relay. This in turn takes a toll on the power allocation since more power from the power budget is allocated to the relay to achieve higher secrecy rate by higher jamming power. As a result, less power is available for the source to transmit the message signal.

The jamming against eavesdroppers can be done using the source or the destination, too. However, the transmitter, receiver or relay-based jamming schemes decrease the efficiency of the system due to channel conditions and also because of strong self-interference (SI) [25], and problem can arise if the relay itself is untrusted [79, 80], i.e., acts as an eavesdropper. If the eavesdropper moves from the previous location or a new eavesdropper is introduced at a different location, jamming from one legitimate entity may not be sufficient. Not all the entities can afford multiple tasks of jamming and maintaining their regular roles especially if they are on a tight power budget. Therefore, a more effective option to deal with eavesdroppers is to employ friendly jammers (also known as private jammers) who send artificial noise (AN) to the eavesdroppers to decrease their SINR. A friendly jammer can also send deceptive source-like signal instead of emitting random bits thus deceiving the eavesdroppers. The eavesdroppers believe that the signal is coming from the source and continue their reception until the friendly jammers stop their transmission. This also creates difficulties for the eavesdroppers to detect the friendly jammers [81].

2.1.3.2 Friendly jammers

The use of AN as jamming signal was stated beneficial to secrecy by increasing the secrecy transmission rate in [38, 82, 83], prompting implementation of friendly jammers [78, 84, 85]. These jammers may or may not be chosen from the available relay nodes and they agree to jam and charge price or harvest energy from the source for the AN [24, 86]. Also they can be either proactive or reactive in nature. Proactive jammers are those

who send signals whether there is any transmission in the channel or not whereas the reactive ones only send AN after sensing a transmission in the channel. These are known as friendly jammers for the fact that if the legitimate entities receive the jamming signal they can decode it and retrieve the original message which the eavesdroppers are not capable of. As a result, friendly jammers started to be introduced in various applications such as military, health care and so on [78]. For example, Shen et. al. in [78] have proposed an ally jamming friendly scheme in a military operation where a legitimate vehicle a.k.a. ally friendly jammer sends jamming signals to unauthorised devices while all the authorised devices remain unaffected by this jamming signal. Sometimes these friendly jammers are put into test if they are trustworthy or not by using a reward or penalty method to check their reputation of trust [87]. Then the trustworthy jammers are chosen for the operation.

2.2 Motivation

Most of the previous works employing friendly jammers did not consider the case of adaptive eavesdropping. Those works included adversaries like passive eavesdroppers (who just listen) [74,78,88] or untrusted relays [79]. Motivated by this gap, we have [43] implemented friendly jammers against adaptive eavesdropping. Our motivations can be summarised as below:

i) For our investigation of using friendly jammers against adaptive eavesdroppers, we choose to work with a random wireless network. The random wireless network involves challenging mathematical derivations. This prompted us to work with two different types of networks to investigate the secrecy parameters in gradually complex scenarios for the derivations. We choose to work with a relay-aided radio network and a random wireless network. On our process of investigation, we work with three variations of the first network and two variations for the second one.

ii) We consider a relay-aided single-input-single-output (SISO) model motivated by [21, 43] in the presence of an adaptive eavesdropper. In this framework, a friendly jammer is a dedicated node only for jamming the adversary. Our initial idea was to use reactive friendly jammers that emit artificial noise (AN) to interfere with the eavesdroppers as can be seen in [43]. Later on we moved to deceptive friendly jammers which are proactive in nature. Since the adaptive eavesdroppers start to jam the legitimate entities if they sense their source to eavesdropper channels are weaken by noise, it is more practical to choose deceptive friendly jammers rather than AN emitting jammers.

iii) The analysis of the secrecy capacity and the secrecy outage probability (SOP) for our SISO model is missing from the literature. Such an analysis should be extended for multiple antennas as well. Therefore, we revisit the idea of investigating those parameters for a model where the relay has multiple antennas. Our goal is to prove that the friendly jammers improve the secrecy performance of a regular relay-aided radio network.

iv) After employing friendly jammers to a simple relay-aided network, we plan to investigate a more practical and complex network. So, we choose our next system model to be a random wireless network. The model consists of a source, with a secrecy protected zone surrounding it, communicating with multiple destinations. The network area is infiltrated with adaptive eavesdroppers except the area inside the secrecy protected zone. The eavesdroppers try to listen to the source and if failed to do that they choose to jam the destinations. We choose some deceptive friendly jammers to interfere with the eavesdroppers. All the destinations, eavesdroppers and the friendly jammers are located randomly following the homogeneous Poisson point process (HPPP). Like the relay-aided model we used before, this random wireless network also has not been studied with friendly jammers tackling the hostile jamming.

v) We choose to revisit the random wireless network with active eavesdroppers replacing the adaptive ones. The active eavesdroppers are full-duplex eavesdroppers unlike the adaptive eavesdroppers who work as half-duplex. This system model is the only one with full-duplex eavesdroppers. We present our idea of using friendly jammers in this scenario which implies that the deceptive nature of the friendly jammers will protect them from detection by the eavesdroppers. We investigate if the interference from the friendly jammers is helpful enough to maintain the system secrecy in presence of active eavesdroppers.

The research gaps and previous works related to these two models are discussed below.

2.3 Related Works

Our target is to employ friendly jammers to eliminate hostile jamming from adaptive eavesdroppers which is new in the literature. Before working with a random wireless network, we started with a relay-aided radio or cellular network. For the relay-aided network, we choose three variations of the network, namely System models **SM0**, **SM1** and **SM2**. System model **SM0** is our initial work where reactive friendly jammers emit AN against adaptive eavesdroppers to enhance the secrecy capacity [43]. System model

SM1 is a modification of the previous model. We choose a relay-aided SISO model where a deceptive friendly jammer jams an adaptive eavesdropper [44]. The third variation is system model **SM2**, where the relay has multiple antennas. The latter two models give us the results that show enhancement of system secrecy by the friendly jammer. The friendly jammer increases the secrecy capacity and decreases the secrecy outage probability. Chapter 3 discusses the relay-aided model.

Finally, we choose the random wireless network, where the derivations of secrecy parameters need the use of stochastic geometry rather than the classical methods as used for the relay-aided model. Chapter 4 includes our investigations of various parameters of friendly jammers to improve the secrecy capacity in a random wireless network with a secrecy protected zone in presence of adaptive (HD) eavesdroppers [45]. We revisit this model in chapter 5 replacing the adaptive eavesdroppers with active (FD) ones. This chapter describes the problem with removal of hostile jamming from an FD eavesdropper and the options to enhance the secrecy capacity. We name the model with HD eavesdroppers System model **SM3** and the model with FD eavesdroppers System model **SM4**.

2.3.1 Relay-aided System Model

System models **SM0-SM2** are based on regular radio or cellular communication where a source communicates with a destination via relay if a direct source to destination link is not possible due to long distance or heavy shadowing. We highlighted some of the previous works in the literature in Table 2.1 to draw some comparisons with our works. As we can see, some of these have employed friendly jammers but did not consider the case of adaptive eavesdropping. Those works included adversaries like passive eavesdroppers (who just listen) [74, 78, 88], who sometimes are the unintended users in downlink channels or untrusted relays [79, 89, 90].

TABLE 2.1: System models in some relay-aided networks in literature

Ref. No.	**Half/Full-duplex** (HD/FD)	**Friendly Jammer**	**Eavesdropper**	**Studied Secrecy Parameter**	
				Secrecy Rate/ Capacity	Secrecy Outage Probability
Yang et al. [21]	HD	×	Adaptive	✓	✓
Wang et al. [91]	HD, FD	×, Tx-jammer, AN	Passive, Active	×	✓
Ali et al. [79]	HD	✓, AN	Untrusted relay	✓	×
Yan et al. [88]	HD	✓, AN	Passive	×	✓
Shen et al. [78]†	HD	✓, AN	Passive	×	×
Tang et al. [74]††	(HD, FD users)	✓, AN	Passive	×	×
SM0 [43]	HD	✓, AN	Adaptive	✓	×
SM1 [44]	HD	✓, Deceptive	Adaptive	✓	✓
SM2	HD	✓, Deceptive	Adaptive	✓	✓

† Authors studied bit error rate (BER) and packet loss rate.
†† Connection probability and secrecy probability were investigated. The probabilities corresponds to the SINR levels in legitimate and eavesdropping channels, respectively.

Those studies are limited in the sense that sophisticated tools now-a-days allow intruders to operate in active (hostile jamming) or adaptive (active or passive depending on the channel conditions) eavesdropping modes. In 2016, Yang et. al. [21] proposed optimum relay selection scheme for secure cooperative communication in the presence of an adaptive eavesdropper. They derived closed-form expression of secure outage probability for full and statistical CSI of eavesdropping channel and approximated expression of that when the eavesdropping channel's CSI is partially known. However, they restricted their works by simply selecting the best relay from the relay nodes to achieve maximum secrecy capacity and minimum secrecy outage probability. In system model **SM0** [43], We investigated the improvement of secrecy capacity in a similar scenario with the help of a reactive friendly jammer emitting AN in a MIMO radio network. Later on we switched to a proactive deceptive friendly jammer (system models **SM1** and **SM2**).

A transmitter-based jamming is seen in [91], where the authors considered the case of full-duplex eavesdroppers capable of hostile jamming. However, a transmitter-based jamming comes with the problem of self-interference and the injection of AN was helpful against eavesdropping only while the hostile jamming from the eavesdroppers remained unaffected. Another notable work of transmitter-based friendly jamming is investigated by Wen et. al. [87] in a cooperative cognitive radio network. However, authors were interested in observing the case of an untrusted jammer rather than an adaptive or active eavesdropper.

Throughout the literature, researchers discussed several performance metrics to achieve secrecy especially four types of secrecy parameters namely the secrecy capacity, the secrecy outage probability (SOP), minimum power consumption and the secure energy efficiency (EE) [92]. While the first two parameters portray the effectiveness and reliability of a secure transmission, the latter two discuss the optimisation techniques to achieve minimum power consumption and maximum energy-efficient system, respectively for a secure but green transmission. We choose to deal with the first two parameters to find the effectiveness of the friendly jammers in enhancing the secrecy of the networks.

2.3.2 Random wireless System Model

We highlight some of the system models dealt in the literature in Table 2.2 to draw some comparisons with our work. The tabulated system models are chosen either for their PPP modelling of the node locations or for the presence of adaptive eavesdroppers and/or friendly jammers. From the table, we can see that most researchers who included friendly jammers in their system models worked with passive eavesdroppers or an untrusted relay. The untrusted relay also works as a passive eavesdropper not a hostile jammer

TABLE 2.2: System models studied in recent notable works

Ref. No.	**PPP**	**Secrecy Zones***	**Friendly Jamming†**	**Eavesdropper**
Zhou et al. [75]	✓	SGZ	Tx, Deceptive	Passive
Chae et al. [38]	✓	SPZ	Tx, AN	Passive
Liu et al. [39]	✓	SPZ, IPZ	×	Passive
Xu et al. [76]	✓	SGZ	×	Passive
Taang et al. [74]	✓	SGZ	FJ & Rx, AN	Passive
Xu et al. [93]	✓	×	Tx, AN	Passive
Wang et al. [91]	✓	×	Tx, AN	Passive & Active
Wang et al. [94]	✓	SGZ by Eve	Tx, AN	Passive & Active
Yang et al. [21]	×	×	×	Adaptive
Ali et al. [79]	×	×	FJ, AN	Untrusted relay
SM0 [43]	×	×	FJ, AN	Adaptive
SM3 [45]	✓	SPZ	FJ, Deceptive	Adaptive
SM4	✓	SPZ	FJ, Deceptive	Active

* SPZ= Secrecy Protected Zone, IPZ= Interferer Protected Zone, SGZ= Secrecy Guard Zone.
† Tx= Transmitter, Rx= Destination Receiver, FJ=Friendly Jammer, Eve=Eavesdropper.

[79]. In some cases, they rely on only relay selection while being affected by adaptive eavesdroppers [21].

Even when the active eavesdroppers are present in the scenario, [91] used transmitter based jamming to reduce intercepting capability of the passive eavesdroppers and the hostile jammers remain untouched. Some authors have chosen just the secrecy guard zone (SGZ) to reduce the eavesdropping along with jamming from source, destination or a friendly jammer. For example, Xu et al. [76], chose a secrecy guard zone in a cognitive network in presence of an HPPP modelled eavesdropping nodes. The secrecy guard zone helps to reduce the eavesdropping and authors did not use any kind of friendly jamming. Tang et al. [74], chose to use secrecy guard zones around the receivers (full-duplex users in a cellular network) to reduce the eavesdropping, while the friendly jammers attempt to lower the capacity of passive eavesdroppers' channels only if the destination based jamming is not suitable. The authors, however, did not discuss the case of uplink communication when the users have to communicate with the base stations while having a secrecy guard zone around them. If the zone is not free from eavesdroppers, then the uplink communication can be ceased because of the function of the zone. From this point of view, employing a secrecy protected zone (SPZ) is a better idea since it can scan and deactivate any eavesdropper inside the zone. Use of SPZ can be seen in [39] along with interference protected zone (IPZ) around the destinations but the adversaries in the model were passive eavesdroppers, and the IPZs were used to reduce the interference coming from other sources. We get some inspirations from this model for our derivations of secrecy capacity in random wireless network (**SM3** and **SM4**). We leave out the IPZ from our model to simulate the situation that all the destinations are affected by hostile jamming and they cannot afford to employ an IPZ around them. However, we keep

the SPZ around the source as an extra security measure to investigate if the friendly jammers can enhance the security of the network.

Our system model **SM3** is the first to incorporate deceptive friendly jammers against adaptive eavesdroppers in a random wireless network which has an SPZ. Another variation of the model we choose as **SM4**, where the adaptive eavesdroppers are replaced by the active eavesdroppers. The current literature does not have deceptive friendly jammer as the means for friendly jamming in a random wireless network which also has an SPZ.

2.4 Conclusion

For our system models, we have chosen hiring friendly jamming nodes over source-based or destination-based jamming. The reason behind this is that the latter methods can cause strong self-interference (SI) and many user nodes may not have the required facilities, e.g., having multiple antennas or full-duplex transmission capability. In our system model **SM0** [43], friendly jammers used AN against adaptive eavesdroppers, and we assume that AN is sufficient enough to convert all hostile jammers into passive eavesdroppers. This is a rather optimistic assumption. On next step, we choose system models **SM1** and **SM2** with more realistic assumptions in a relay-aided network by considering deceptive friendly jammers who emit source-like signal to deceive the adaptive eavesdroppers. Finally, we choose system models **SM3** and **SM4** which are more practically deployable. The last two models are random wireless networks where the nodes are scattered throughout the coverage area, and the source also employs a secrecy protected zone. The reason behind the choice of the models is to employ friendly jammers in gradually complex networks where the mathematical derivations for the secrecy parameters become difficult with system geometry. The numerical results support our derivations by showing improvement in system secrecy with the help of friendly jammers against different types of eavesdroppers for various kinds of networks.

Chapter 3

Friendly Jammers against Adaptive Eavesdroppers in a Relay-aided Network

3.1 Overview

To achieve the goal of finding the efficacy of the friendly jammers against adaptive or active eavesdroppers in various types of networks, we work with two different types of wireless networks. We start with a relay-aided network found in radio or cellular communications, and our final goal is to work with a random wireless network. The former network involves more straightforward mathematical techniques to derive the secrecy parameters as it does not include random locations for nodes and works with limited numbers of nodes. After derivation of the secrecy capacity and secrecy outage probability for the relay-aided network, we move to a random wireless network which involves more difficult mathematical derivations. This chapter deals with the investigation of employing friendly jammers in the relay-aided network.

We initially work with a multiple-input-multiple-output (MIMO) radio network and derive the secrecy capacity for the model showing that the friendly jammer can increase the secrecy capacity in presence of adaptive eavesdroppers. This work has been published to the proceedings of the *IEEE GLOBECOM 2017 Workshops: 5th IEEE GLOBECOM Workshop on Trusted Communications with Physical Layer Security, Singapore* [43]. This work shows that friendly jammers are helpful to enhance the secrecy capacity by interfering with the eavesdroppers from a close location. Next, we simplify the model to work with more practical assumptions.

We consider a relay-aided single-input-single-output (SISO) model motivated by [21] and our initial model in the presence of an adaptive eavesdropper. In this framework, a friendly jammer is a dedicated node only for jamming the adversary. We implement friendly jammers emitting AN to adaptive eavesdropper in our MIMO model. A question may arise as to whether an adaptive eavesdropper which is half-duplex in nature will choose to be a hostile jammer once the eavesdropper's channel becomes noisy due to the penetration of the AN. Therefore, addressing that topic, we replace the friendly jammers as deceptive friendly jammers in all our later models discussed in the current and following chapters. The main contributions of this chapter are as follows:

1. We are the first to show the advantages of a friendly jammer against an adaptive eavesdropper. We chose AN emitting reactive friendly jammers and later switched on to deceptive ones. The deceptive friendly jammer is proactive and continuously emits a source-like signal to confuse the eavesdropper as in the case of [81]. The friendly jammer thus deceives the eavesdropper not to turn into a hostile jammer. This system model has marked advantages.

2. We derive two important performance parameters of the proposed system, namely secrecy capacity and secrecy outage probability. Simulation results show significant improvement in both metrics due to the presence of friendly jammer, validating its use in enhancing physical layer security.

3.1.1 System Models and Problem Formulation

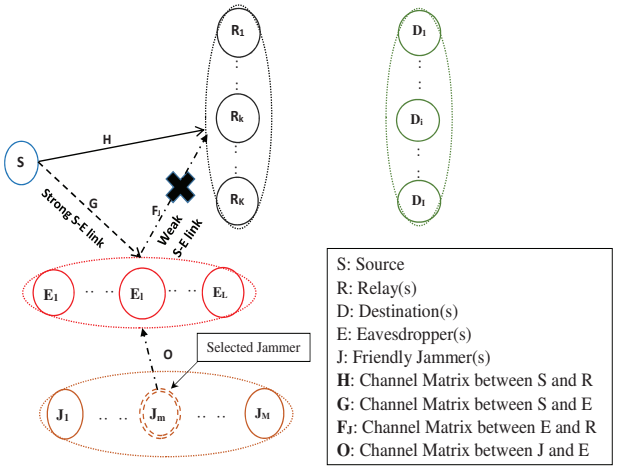
To investigate the security of a relay-aided network, we choose a simple SISO network where every entity is equipped with a single antenna which is a modified version of our initial MIMO network. We first investigate the secrecy capacity (SC) and secrecy outage probability (SOP) of this model. This work has been published in the proceedings of the *The 16th International Wireless Communications & Mobile Computing (IWCMC) Conference*, Limassol, Cyprus, 15-19 June, 2020 [44].

We also revisit the idea of investigating both secrecy parameters of a similar model in which the relay is equipped with multiple antennas. For further descriptions as follows, let us denote the initial MIMO network as System Model **SM0**, the SISO network as System Model **SM1** and the multi-antenna relay model as System Model **SM2**.

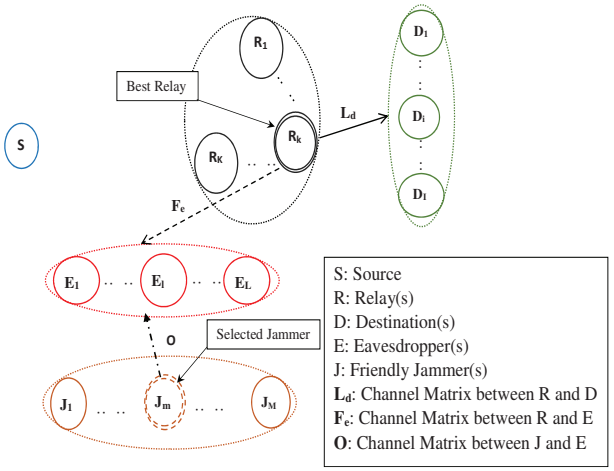
3.1.1.1 System Model SM0

The system model **SM0** is a MIMO multicast network where a source S communicates with a group of N numbered destinations via a decode-and-forward relay R_k. The relay

is chosen from a group of K numbered relays based on the criteria if the secrecy capacity at the relay R_k is the maximum compared to the other relays in the first or broadcasting phase of communication. This type of relay selection technique is found in traditional max-min relay selection (TMRS) scheme. A group of adaptive eavesdroppers try to intercept the communication and time to time try to jam the relays based on the channel condition. The source hires a friendly jammer to tackle the eavesdroppers. When an additional security measure is ensured by a friendly jammer in a relay-aided network, this is sometimes referred to as a joint relay and jammer selection (JRJS) scheme. JRJS schemes against passive eavesdroppers are found to be better than TMRS and other relay selection schemes without a friendly jammer in the existing literature [95]. The system model is shown below:



(a) With strong S-E link.



(b) With weak S-E link.

FIGURE 3.1: Multicast network. [S- source, R- relay, D- destination, E- eavesdropper and J- friendly jammer.]

This type of network where the source sends confidential message to a group of destinations is also known as a multicast network. There is no direct link between S and D due to heavy shadowing. The group of L adaptive eavesdroppers (E) located near the source and the relays but far from the destinations. Situations can be the same as that is in [21]. In this case, in phase I or broadcasting phase the eavesdroppers either listens to the source or jams the relays depending on having a strong or weak link between the source and the eavesdroppers, respectively (Fig. 3.1(a)). For simplicity, it is assumed that all the eavesdroppers act simultaneously and in the same matter that all of them are either passive (just listen) or active (jam) at a time. Also every entity in this model follow half-duplex communication. For phase II or relaying phase when the best relay retransmits the source signal to the destinations, the eavesdroppers listen to the relay (Fig. 3.1(b)). However, being far from them, eavesdroppers are unable to listen to or jam any of the destinations.

Yang et. al. [21] chose a similar SISO network and derived the corresponding secrecy capacity in this situation which as obvious depicts that eavesdroppers are lowering down the achievable secrecy rates. To improve the case and simultaneously to release the relay from the pressure of dealing with E, we introduce a group of M jammers (J) in close proximity of E. After the negotiation among the source and the jammers about the interference price demanded by them, a jammer with an optimal price is selected to jam the eavesdroppers. There are techniques proposed in literature, any of which (e.g., [24]) or the lowest bidding price can be used to select the optimal one; however, choice of such selection strategy remains out of the scope of this work. The jammer is reactive in nature *i.e.*, starts jamming after sensing a transmission through the channel. Since the eavesdroppers are considered to be not just passive, an assumption is made that their location is known. With proper beamforming the selected jammer is able to send jamming signal to the eavesdroppers only [24], and no other entities suffer from interference by the jammer. The entities from a particular group are assumed to be residing nearby each other. The wireless channel is assumed to be characterized by slow Rayleigh fading. Also, the source (S), each relay (R), each destination (D), each eavesdropper (E), and each friendly jammer (J) are equipped with n_S, n_R, n_D, n_E and n_J number of antennas, respectively. The complex channel matrices between pairs of entities are given in the Table 3.1.

TABLE 3.1: List of Notations.

Channel Matrix	**Link**	**Channel Matrix**	**Link**
$\mathbf{H}$	S-R	$\mathbf{G}$	S-E
$\mathbf{L}_d$	R-D	$\mathbf{F}_j$	E-R
$\mathbf{F}_e$	R-E	$\mathbf{O}$	J-E

The system model **SM0** is built on several optimistic assumptions such as

(i) The whole system is half-duplex though the entities are equipped with multiple antennas.

(ii) The entities from a group are closely located.

(iii) The source knows the channel state information (CSI) and locations of the eavesdroppers.

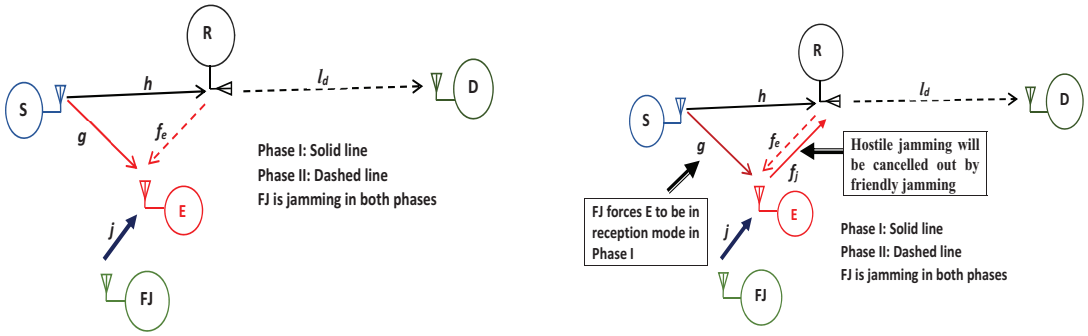
(iv) Due to their proximity, all the eavesdroppers are under the coverage of the selected friendly jammer.

(v) Artificial noise (AN) emitted by the friendly jammer is enough to convert all the eavesdroppers to be in passive mode.

Later on, we modify the system model to work with more realistic assumptions. We work with deceptive friendly jammer instead of an AN emitting one and gradually choose several models based on their practical deployment. For a radio or cellular communication point of view, we choose our system model **SM1** and **SM2** as described below. Then we choose a random wireless network. The random wireless network represents the large-scale wireless networks with scattered network nodes, and our corresponding work is described into two parts in Chapter 4 and 5.

3.1.1.2 System Model SM1

We consider a half-duplex SISO radio network in which a source S transmits signals to its corresponding destination D via a decode-and-forward (DF) relay R. There is no direct link between S and D due to heavy shadowing or long S-D distance [10,15]. The adaptive eavesdropper E is located near S and R but far from D. The CSI of the eavesdropper is assumed to be known by the source since it is not always passive in nature. In case S-E link is found strong by the eavesdropper, E listens to S (Fig. 3.2(a)). In case of a weak S-E link, eavesdropping is not so effective and E instead tries to jam R (Fig. 3.2(b)). All these happen in the first (broadcasting) phase of transmission between S and D. In second (relaying) phase of transmission, the eavesdropper tries to listen to the relay. We place a friendly jammer (FJ) near E which continuously sends deceptive jamming signal to E. Since FJ forces E to be in reception mode, at the first phase, eavesdropper's ability to eavesdrop sender's message reduces (case (a)) and the ability to jam the relay diminishes (case (b)). The friendly jamming continues up to the second phase and E faces interference due to it. Being far from the destination, E cannot jam D. The wireless channel is assumed to be characterized by slow Rayleigh fading [15]. All



(a) With strong S-E link.

(b) With weak S-E link.

FIGURE 3.2: Half-duplex SISO network. [S- source, R- relay, D- destination, E- eavesdropper and FJ- friendly jammer.]

the instantaneous SNRs are considered to be exponentially distributed and listed with other notations in Table 4.1.

TABLE 3.2: List of Notations.

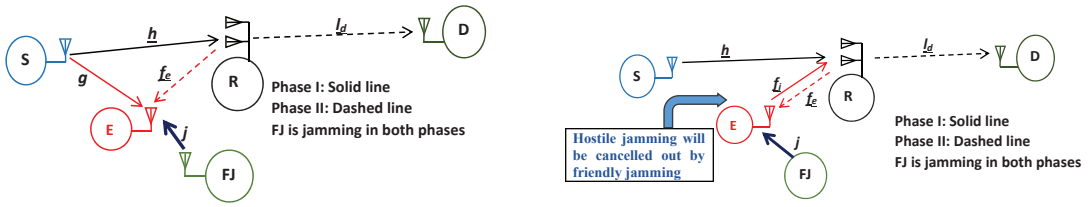
Notation	Description
h, g	Channel coeff. of S-R and S-E links, respectively.
l_d, f_e	Channel coeff. of R-D and R-E links, respectively.
f_j, j	Channel coeff. of E-R and FJ-E links, respectively.
P_X	The transmit power of X.
N_{0Y}	The noise variance of Y.
γ_{XY}	$=\frac{\lvert\omega\rvert^2 P_X}{N_{0Y}}$, instantaneous SNR of X-Y link with channel coefficient equals to ω.
$\overline{\gamma}_{XY}$	$=\frac{P_X \Lambda_{XY}}{N_{0Y}}$, average SNR of X-Y link with mean Λ_{XY}.
η	Threshold of channel gain of S-E link suitable for eavesdropping.
C_s	Secrecy capacity.
P_{out}	Secrecy outage probability.
R_s	Target secrecy rate.
α_s	2^{2R_s}.
$\lvert\cdot\rvert$, $\lVert\cdot\rVert$ and $Pr(\cdot)$	Absolute value, Euclidean norm and probability, respectively.
$[\cdot]^+$	$max(\cdot, 0)$

In order to keep the study manageable, we consider the following assumptions: *Assumption 1.* The adaptive eavesdropper performs eavesdropping when the source to eavesdropper link is sufficiently strong, otherwise it performs jamming. *Assumption 2.* Since the eavesdropper is not always passive, we assume that its location and channel

state information (CSI) can be known. This assumption is very common in existing literature [21, 47, 96, 97]. *Assumption 3.* Following [24], the friendly jammer can be placed at a location that only the eavesdropper is affected by the friendly jamming. The friendly jammer is far away from the destination and the relay can decode the friendly jamming signal if it receives the interference by any chance.

We derive secrecy capacity and secrecy outage probability of the following cases: (a) when source-eavesdropper (S-E) link is strong, and (b) when S-E link is weak. We compare both the performance of the secrecy capacity and the total secrecy outage probability in presence and absence of the friendly jammer. In the derivation that follows, the superscripts 's' and 'w' will denote the cases of strong and weak S-E links, respectively and the subscripts 'NJ' and 'FJ' will denote the cases of without and with friendly jammer, respectively. In a similar manner a superscript 's,w' will denote the case of both strong and weak S-E links.

3.1.1.3 System Model SM2



(a) With strong S-E link.

(b) With weak S-E link.

FIGURE 3.3: Relay with multiple antennas.

The system model **SM1** is modified to have a relay with 2 antennas (Fig. 3.3(a) and 3.3(b)). However, the expressions derived for the SOP can be extended for n_R antennas where, $n_R > 2$ is an integer. The system model is now a combination of single-input-single-output (SISO), single-input-multiple-output (SIMO) and multiple-input-single-output (MISO) subsystems where, the links S-E and S-FJ are SISO, links S-R and E-R are SIMO while links R-D and R-E falls under MISO categories.

TABLE 3.3: Channel Details

Channel Coefficients	**Link**	**Channel Coefficients**	**Link**
$\mathbf{h} \in \mathbb{C}^{n_R \times 1}$	S-R	$g \in \mathbb{C}^{1\times 1}$	S-E
$\boldsymbol{l}_d \in \mathbb{C}^{1\times n_R}$	R-D	$\mathbf{f}_j \in \mathbb{C}^{n_R\times 1}$	E-R
$\mathbf{f}_e \in \mathbb{C}^{1\times n_R}$	R-E	$j \in \mathbb{C}^{1\times 1}$	FJ-E

3.2 Secrecy Capacity (SC)

The secrecy capacity plays a central role in physical layer security. It is the maximum rate of communication for which an eavesdropper cannot learn any information and achieved by subtracting the eavesdropper's capacity from that of the main (legitimate) channel [21, 46], i.e.,

$$C_s = [C_{main} - C_{eavesdropper}]^+.$$

where, C_s is the secrecy capacity and C_x is the capacity of x channel. In case of a multicast network, where the destinations are multiple in number, the secrecy capacity is known as the secrecy multicast capacity. In this case, the main channel capacity is the minimum of the capacities obtained at the destinations. On the other hand, the eavesdropping channel capacity is the maximum of the capacities obtained at the eavesdroppers (if they are also multiple in number).

3.2.1 For System Model SM0

We derive secrecy capacity for multiple transmission for two explicit cases: (a) when source-eavesdropper (S-E) link is strong and (b) when S-E link is weak. The study of these two cases are motivated by the fact that in the former case the eavesdropper can extract information from the source while in the latter, the eavesdropper is more likely to disrupt transmission to destination by jamming the relays. In the derivation that follows, the superscript s and w will denote the cases of strong and weak S-E links, respectively.

3.2.2 With Strong S-E Link

Received signal at k^{th} relay, and at l^{th} eavesdropper while being jammed by m^{th} jammer in first phase can be expressed as respectively,

$$\mathbf{r}_k^s = \mathbf{H}_k\mathbf{x} + \mathbf{z}_{R_k} \tag{3.1}$$

$$\mathbf{y}_{E_l}^{s,1} = \mathbf{G}_l\mathbf{x} + \mathbf{O}_m\mathbf{u} + \mathbf{z}_{E_l'} \tag{3.2}$$

where, $\mathbf{x}$ is the source signal, $\mathbf{u}$ is the jamming signal from J to E and, $\mathbf{z}_{R_k}$ and $\mathbf{z}_{E_l'}$ denote the noise vectors of R and E, respectively. $\mathbf{O}_m\mathbf{u}$ is the interference caused by the friendly jammer resulting in a degradation in eavesdroppers' channel capacity. The

capacities of S-R_k and S-E link are derived as,

$$C^s_{S-R}(k) = \left[\log_2\left(\det\left(\mathbf{I}_{n_R} + \frac{P_S}{n_S N_{0R}}\mathbf{H}_k\mathbf{H}_k^\dagger\right)\right)\right] \tag{3.3}$$

$$C^s_{S-E} = \left[\log_2\left(\det\left(\frac{\mathbf{I}_{n_E} + \max\limits_{1\le l\le L}\frac{\underline{\Psi}_{lk}\mathbf{Q}_\Psi\underline{\Psi}_{lk}^\dagger}{N_{0E'}}}{\mathbf{I}_{n_E} + \frac{P_J}{n_J N_{0E'}}\mathbf{O}_m\mathbf{O}_m^\dagger}\right)\right)\right] \tag{3.4}$$

where $\underline{\Psi} = [\mathbf{G} \quad \mathbf{O}_m]$ is the combined channel matrix and $\mathbf{Q}_\Psi = \mathbf{Q}_S \oplus \mathbf{Q}_J = \begin{bmatrix} \mathbf{Q}_S & 0 \\ 0 & \mathbf{Q}_J \end{bmatrix} = \frac{P_S}{n_S}\mathbf{I}_{n_S} \oplus \frac{P_J}{n_J}\mathbf{I}_{n_J}$ [1]. Here, P_S is the total power distributed uniformly over n_S antennas of the source S and N_{0R} is the corresponding noise variance at the relay R_k. Generally, the best relay is chosen that maximises the secrecy capacity (i.e., capacity of main channel in both phases minus the capacity at eavesdroppers' channel in both phases) [21, 98]. Since all the relays and destinations are in close proximity to each other, the best relay can be chosen by obtaining the maximum capacity in the S-R links found in the first phase, i.e., k^{th} relay is the best relay as given by

$$k = \arg\left(\max_{1\le k\le K} C_{S-R}(k)\right). \tag{3.5}$$

In the relaying phase, received signal at i^{th} destination (D_i) from best relay R_k and capacity of R_k-D link can be expressed as respectively,

$$\begin{aligned}\mathbf{y}_{D_i} &= \mathbf{L}_{d_i}\mathbf{r}_k + \mathbf{z}_{D_i'} \\ &= \mathbf{L}_{d_i}\mathbf{H}_k\mathbf{x} + \mathbf{L}_{d_i}\mathbf{z}_{R_k} + \mathbf{z}_{D_i'} = \mathbf{A}_{ik}\mathbf{x} + \mathbf{z}_{D_i}\end{aligned} \tag{3.6}$$

$$C^s_{R-D} = \left[\log_2\left(\det\left(\mathbf{I}_{n_D} + \min_{1\le i\le I}\frac{P_S}{\mathbf{N}_{0D}n_S}\mathbf{A}_{ik}\mathbf{A}_{ik}^\dagger\right)\right)\right] \tag{3.7}$$

where, $\mathbf{N}_{0D} = N_{0D'}\mathbf{I}_{n_D} + N_{0R}\mathbf{L}_{d_i}\mathbf{L}_{d_i}^\dagger$ is the noise variance vector at D's receiver which corresponds to the combination of the receiver's own noise ($\mathbf{z}_{D_i'}$) and the noise part of relay signal ($\mathbf{L}_{d_i}\mathbf{z}_{R_k}$), i.e. $\mathbf{z}_{D_i} = \mathbf{L}_{d_i}\mathbf{z}_{R_k} + \mathbf{z}_{D_i'}$, and $\mathbf{A}_{ik} = \mathbf{L}_{d_i}\mathbf{H}_k$. Received signal at l^{th} eavesdropper (E_l) in second phase is

$$\begin{aligned}\mathbf{y}^{s,2}_{E_l} &= \mathbf{F}_{e_l}\mathbf{r}_k + \mathbf{O}_m\mathbf{u} + \mathbf{z}_{E_l'} \\ &= \mathbf{F}_{e_l}\mathbf{H}_k\mathbf{x} + \mathbf{O}_m\mathbf{u} + \mathbf{F}_{e_l}\mathbf{z}_{R_k} + \mathbf{z}_{E_l'} \\ &= \mathbf{A}_{E_{lk}}\mathbf{x} + \mathbf{O}_m\mathbf{u} + \mathbf{z}_{E_l}\end{aligned} \tag{3.8}$$

[1] $\mathbf{Q}_x = \mathbb{E}\{\mathbf{x}\mathbf{x}^\dagger\} = \frac{P_x}{n_x}\mathbf{I}_{n_x}$ is called the covariance of signal $\mathbf{x}$ with $\mathbf{x}^\dagger$ being the Hermitian transpose of $\mathbf{x}$. $\mathbf{Q}_\Psi$ represents the combination of source and friendly jamming signals at the eavesdropper's reception.

where, $\mathbf{z}_{E_l} = \mathbf{F}_{e_l}\mathbf{z}_{R_k} + \mathbf{z}_{E_l'}$ and $\mathbf{A}_{E_{lk}} = \mathbf{F}_{e_l}\mathbf{H}_k$. The capacity of R_k-E link is thereby given as

$$C_{R-E}^{s} = \left[\log_2\left(\det\left(\frac{\mathbf{I}_{n_E} + \max\limits_{1\le l\le L}\frac{\underline{\Psi}_{T_{lk}}\mathbf{Q}_{\Psi}\underline{\Psi}_{T_{lk}}^{\dagger}}{\mathbf{N}_{0E}}}{\mathbf{I}_{n_E} + \frac{P_J}{n_J\mathbf{N}_{0E}}\mathbf{O}_m\mathbf{O}_m^{\dagger}}\right)\right)\right] \tag{3.9}$$

where, $\mathbf{N}_{0E} = N_{0E'}\mathbf{I}_{n_E} + N_{0R}\mathbf{F}_{e_l}\mathbf{F}_{e_l}^{\dagger}$ is the noise variance vector at the eavesdropper which corresponds to the combination of the receiver's own noise ($\mathbf{z}_{E_l'}$) and the noise part of relay signal ($\mathbf{F}_{e_l}\mathbf{z}_{R_k}$), i.e. $\mathbf{z}_{E_l} = \mathbf{F}_{e_l}\mathbf{z}_{R_k} + \mathbf{z}_{E_l'}$, and $\underline{\Psi}_{T_{lk}} = [\mathbf{A}_E \quad \mathbf{O}_m]$.

Therefore, the secrecy multicast capacity can be expressed as,

$$\begin{aligned} C_s^s &= C_{S-R}^s(k) + C_{R-D}^s - C_{S-E}^s - C_{R-E}^s \\ &= \left[\log_2\left(\frac{\det\left(\mathbf{I}_{n_R} + \frac{P_S}{n_S N_{0R}}\mathbf{H}_k\mathbf{H}_k^{\dagger}\right)\det\left(\mathbf{I}_{n_D} + \min\limits_{1\le i\le I}\frac{P_S}{\mathbf{N}_{0D}n_S}\mathbf{A}_{ik}\mathbf{A}_{ik}^{\dagger}\right)}{\det\left(\frac{\mathbf{I}_{n_E}+\max\limits_{1\le l\le L}\frac{\underline{\Psi}_{lk}\mathbf{Q}_{\Psi}\underline{\Psi}_{lk}^{\dagger}}{N_{0E'}}}{\mathbf{I}_{n_E}+\frac{P_J}{n_J N_{0E'}}\mathbf{O}_m\mathbf{O}_m^{\dagger}}\right)\det\left(\frac{\mathbf{I}_{n_E}+\max\limits_{1\le l\le L}\frac{\underline{\Psi}_{T_{lk}}\mathbf{Q}_{\Psi}\underline{\Psi}_{T_{lk}}^{\dagger}}{\mathbf{N}_{0E}}}{\mathbf{I}_{n_E}+\frac{P_J}{n_J\mathbf{N}_{0E}}\mathbf{O}_m\mathbf{O}_m^{\dagger}}\right)}\right)\right] \end{aligned} \tag{3.10}$$

3.2.3 With Weak S-E Link

Let us first consider that the friendly jammer is not present. The received signal at k^{th} relay while being jammed by l^{th} eavesdropper is

$$\tilde{\mathbf{r}}_k^w(l) = \mathbf{H}_k\mathbf{x} + \mathbf{F}_{j_l}\mathbf{v} + \mathbf{z}_{R_k} \tag{3.11}$$

where, $\mathbf{v}$ is the interference received by the relays when eavesdroppers are active, i.e., they act as a hostile jammer. Thus the capacity at k^{th} relay in absence of friendly jammer is given by

$$\tilde{C}_{S-R}^w(k) = \left[\log_2\left(\det\left(\frac{\mathbf{I}_{n_R} + \frac{\underline{\Delta}_{lk}\mathbf{Q}_T\underline{\Delta}_{lk}^{\dagger}}{N_{0R}}}{\mathbf{I}_{n_R} + \max\limits_{1\le l\le L}\frac{P_E}{n_E N_{0R}}\mathbf{F}_{j_l}\mathbf{F}_{j_l}^{\dagger}}\right)\right)\right]$$

where $\underline{\Delta} = [\mathbf{H} \quad \mathbf{F}_j]$ and $\mathbf{Q}_T = \mathbf{Q}_S \oplus \mathbf{Q}_E = \frac{P_S}{n_S}\mathbf{I}_{n_S} \oplus \frac{P_E}{n_E}\mathbf{I}_{n_E}$.

In presence of friendly jammer J, it will send AN to the eavesdroppers thus engaging them in reception mode with J only, there is no interference ($\mathbf{F}_{j_l}\mathbf{v}$) received by the relays. Then the capacity of $S - R_k$ link becomes

$$C_{S-R}^w(k) = \left[\log_2\left(\det\left(\mathbf{I}_{n_R} + \frac{P_S}{n_S N_{0R}}\mathbf{H}_k\mathbf{H}_k^{\dagger}\right)\right)\right] \tag{3.12}$$

The best relay will be chosen as per the previous strategy (see (3.5)) and capacities of the R_k-D and R_k-E links will be same as before (see (3.7) and (3.9), respectively). Therefore the secrecy multicast capacity can be expressed as,

$$\begin{aligned} C_s^w &= C_{S-R}^w(k) + C_{R-D}^w - C_{R-E}^w \\ &= \left[\log_2 \left(\frac{\det\left(\mathbf{I}_{n_R} + \frac{P_S}{n_S N_{0R}} \mathbf{H}_k \mathbf{H}_k^\dagger\right) \det\left(\mathbf{I}_{n_D} + \min\limits_{1\le i\le I} \frac{P_S}{\mathbf{N}_{0D} n_S} \mathbf{A}_{ik} \mathbf{A}_{ik}^\dagger\right)}{\det\left(\frac{\mathbf{I}_{n_E} + \max\limits_{1\le l\le L} \frac{\Psi_{T_{lk}} \mathbf{Q}_\Psi \Psi_{T_{lk}}^\dagger}{\mathbf{N}_{0E}}}{\mathbf{I}_{n_E} + \frac{P_J}{n_J \mathbf{N}_{0E}} \mathbf{O}_m \mathbf{O}_m^\dagger} \right)} \right) \right] \end{aligned} \tag{3.13}$$

With the help of Monte-Carlo simulation the secrecy performance of the above system model for various scenarios are presented in the numerical results section.

3.2.4 For System Model SM1

We first derive the capacities for various links in absence and presence of the friendly jammer. Also, we derive the corresponding capacities for strong and weak S-E link in absence of the friendly jammer. In case of friendly jammer being present the strength of S-E link becomes irrelevant since the eavesdropper becomes passive all the way throughout the communication. Then we derive the corresponding secrecy capacities.

3.2.4.1 Without Friendly Jammer

1. **Strong S-E Link:**

In case of strong S-E link, the capacities for the source to relay and source to eavesdropper links are given as, respectively,

$$\begin{aligned} C_{S-R}^{(s)} &= \log_2\left(1 + \frac{|h|^2 P_S}{N_{0R}}\right) = \log_2(1+\gamma_{SR}), \\ C_{S-E}^{(s)} &= \log_2\left(1 + \frac{|g|^2 P_S}{N_{0E}}\right) = \log_2(1+\gamma_{SE}), \end{aligned}$$

where, $\gamma_{xy} = \frac{|w|^2 P_S}{N_{0y}}$ denotes the instantaneous signal-to-noise ratio (SNR) of the X-Y link with channel coefficient of w. The superscript 's' is used to indicate the strong S-E link when the link has channel gain above the threshold η. P_S is the transmit power of the source and the relay is assumed to be capable of correctly decoding the source signal before transmitting it, hence in this case, the transmit power of relay is $P_R = P_S$. Similarly, for relay to destination and eavesdropper links we have, respectively,

$$C_{R-D}^{(s)} = \log_2\left(1 + \frac{|l_d|^2 P_S}{N_{0D}}\right) = \log_2(1+\gamma_{RD}),$$

$$C_{R-E}^{(s)} = \log_2\left(1 + \frac{|f_e|^2 P_S}{N_{0E}}\right) = \log_2(1 + \gamma_{RE}).$$

The achievable secrecy capacity following [21] can be derived as,

$$C_{s,NJ}^{(s)} = \log_2\left[\frac{1 + \min(\gamma_{SR}, \gamma_{RD})}{1 + \gamma_{SE} + \gamma_{RE}}\right]. \tag{3.14}$$

2. **Weak S-E Link:**

For weak S-E link, the eavesdropper stops listening to the source and hence the capacity of S-E link equals zero. However, the eavesdropper starts to jam the relay thus the capacity for the source to relay link is given as,

$$C_{S-R}^{(w)} = \log_2\left(1 + \frac{|h|^2 P_S}{N_{0R} + |f_j|^2 P_E}\right) = \log_2\left(1 + \frac{\gamma_{SR}}{1 + \gamma_{ER}}\right).$$

Similarly, for relay to destination and eavesdropper links we have, respectively,

$$C_{R-D}^{(w)} = \log_2\left(1 + \frac{|l_d|^2 P_S}{N_{0D}}\right) = \log_2(1 + \gamma_{RD}).$$
$$C_{R-E}^{(w)} = \log_2\left(1 + \frac{|f_e|^2 P_S}{N_{0E}}\right) = \log_2(1 + \gamma_{RE}).$$

The achievable secrecy capacity then can be derived as,

$$C_{s,NJ}^{(w)} = \log_2\left[\frac{1 + \min(\frac{\gamma_{SR}}{1+\gamma_{ER}}, \gamma_{RD})}{1 + \gamma_{RE}}\right]. \tag{3.15}$$

3.2.4.2 With Friendly Jammer

The friendly jammer transmits a deceptive jamming signal which has the similar pattern of the source signal, and being closer (in distance) to the eavesdropper, the friendly jammer can occupy its receiving channel. Therefore, regardless of the strength of the S-E link, the eavesdropper always listen to the friendly jammer. The capacities for the source to relay and source to eavesdropper links are given as, respectively,

$$C_{S-R}^{(s,w)} = \log_2\left(1 + \frac{|h|^2 P_S}{N_{0R}}\right) = \log_2(1 + \gamma_{SR}),$$
$$C_{S-E}^{(s,w)} = \log_2\left(1 + \frac{|g|^2 P_S}{N_{0E} + |j|^2 P_J}\right) = \log_2\left(1 + \frac{\gamma_{SE}}{1 + \gamma_{JE}}\right).$$

Similarly, for relay to destination and eavesdropper links we have, respectively,

$$C_{R-D}^{(s,w)} = \log_2\left(1 + \frac{|l_d|^2 P_S}{N_{0D}}\right) = \log_2(1 + \gamma_{RD}),$$
$$C_{R-E}^{(s,w)} = \log_2\left(1 + \frac{|f_e|^2 P_S}{N_{0E} + |j|^2 P_J}\right) = \log_2\left(1 + \frac{\gamma_{RE}}{1 + \gamma_{JE}}\right).$$

Therefore, the achievable secrecy capacity can be derived as,

$$C_{s,FJ}^{(s,w)} = \log_2 \left[\frac{1 + \min(\gamma_{SR}, \gamma_{RD})}{1 + \frac{\gamma_{SE} + \gamma_{RE}}{1 + \gamma_{JE}}} \right]. \tag{3.16}$$

In case of the first phase of communication, equation (3.19) shows that regardless of the strength of S-E link, the eavesdropper tends to listen to the source thus the chance of hostile jamming is eliminated and the eavesdropper's capacity is affected by the friendly jamming in both phases of transmission. As a result, the secrecy capacity increases in the presence of the friendly jammer.

3.2.5 For System Model SM2

3.2.5.1 Without Friendly Jammer

1. **Strong S-E Link:**

The capacities for the Source (S) to Relay (R) and Eavesdropper (E) links are given as, respectively,

$$C_{S-R}^{(s)} = \log_2 \left(1 + \frac{\|\mathbf{h}\|^2 P_S}{N_{0R}} \right) = \log_2(1 + \gamma_{SR}),$$
$$C_{S-E}^{(s)} = \log_2 \left(1 + \frac{|g|^2 P_S}{N_{0E}} \right) = \log_2(1 + \gamma_{SE}).$$

Similarly, for Relay (R) to Destination (D) and Eavesdropper (E) links we have, respectively,

$$C_{R-D}^{(s)} = \log_2 \left(1 + \frac{\|\boldsymbol{l}_d\|^2 P_S}{n_R N_{0D}} \right) = \log_2(1 + \gamma_{RD}),$$
$$C_{R-E}^{(s)} = \log_2 \left(1 + \frac{\|\mathbf{f}_e\|^2 P_S}{n_R N_{0E}} \right) = \log_2(1 + \gamma_{RE}).$$

The achievable secrecy capacity can be observed as follows,

$$C_{s,NJ}^{(s)} = \log_2 \left[\frac{1 + \min(\gamma_{SR}, \gamma_{RD})}{1 + \gamma_{SE} + \gamma_{RE}} \right]. \tag{3.17}$$

2. **Weak S-E Link:**

For weak S-E link, the capacity of S-R link suffers from hostile jamming as shown below,

$$C_{S-R}^{(w)} = \log_2 \left(1 + \frac{\|\mathbf{h}\|^2 P_S}{N_{0R} + \|\mathbf{f}_j\|^2 P_E} \right) = \log_2 \left(1 + \frac{\gamma_{SR}}{1 + \gamma_{ER}} \right).$$

Similarly, for relay to destination and eavesdropper links we have, respectively,

$$C_{R-D}^{(s)} = \log_2\left(1 + \frac{\|\boldsymbol{l}_d\|^2 P_S}{n_R N_{0D}}\right) = \log_2(1+\gamma_{RD}),$$
$$C_{R-E}^{(s)} = \log_2\left(1 + \frac{\|\mathbf{f}_e\|^2 P_S}{n_R N_{0E}}\right) = \log_2(1+\gamma_{RE}).$$

The achievable secrecy capacity then can be derived as,

$$C_{s,NJ}^{(w)} = \log_2\left[\frac{1+\min(\frac{\gamma_{SR}}{1+\gamma_{ER}}, \gamma_{RD})}{1+\gamma_{RE}}\right]. \tag{3.18}$$

3.2.5.2 With Friendly Jammer

Similar to the SISO model, we assume that the friendly jammer is deceiving the eavesdropper throughout the transmission. Therefore, regardless of the S-E link strength, the capacities for the S-R and S-E links are given as, respectively,

$$C_{S-R}^{(s,w)} = \log_2\left(1 + \frac{\|\mathbf{h}\|^2 P_S}{N_{0R}}\right) = \log_2(1+\gamma_{SR}),$$
$$C_{S-E}^{(s,w)} = \log_2\left(1 + \frac{|g|^2 P_S}{N_{0E}+|j|^2 P_J}\right) = \log_2\left(1 + \frac{\gamma_{SE}}{1+\gamma_{JE}}\right).$$

Similarly, for relay to destination and eavesdropper links we have, respectively,

$$C_{R-D}^{(s,w)} = \log_2\left(1 + \frac{\|\mathbf{l}_d\|^2 P_S}{n_R N_{0D}}\right) = \log_2(1+\gamma_{RD}),$$
$$C_{R-E}^{(s,w)} = \log_2\left(1 + \frac{\|\mathbf{f}_e\|^2 P_S}{n_R N_{0E}+|j|^2 P_J}\right) = \log_2\left(1 + \frac{\gamma_{RE}}{1+\gamma_{JE}}\right).$$

Therefore, the achievable secrecy capacity can be derived as,

$$C_{s,FJ}^{(s,w)} = \log_2\left[\frac{1+\min(\gamma_{SR}, \gamma_{RD})}{1+\frac{\gamma_{SE}+\gamma_{RE}}{1+\gamma_{JE}}}\right]. \tag{3.19}$$

3.3 Secrecy Outage Probability (SOP)

It is the probability that the secrecy is lower than the target secrecy rate. Mathematically speaking, SOP can be defined as

$$P_{out} = Pr(C_s < R_s),$$

where, $R_s > 0$ is the target secrecy rate.

3.3.1 For System Model SM1

3.3.1.1 Without Friendly Jammer

1. **Strong S-E Link:** The corresponding SOP can be expressed by Proposition 3.1.

Proposition 3.1. *The secrecy outage probability (SOP) with strong S-E link in the absence of the friendly jammer, $P_{out,NJ}^{(s)}$, is given in (3.20).*

Proof. In sequence of equalities concluding (3.20), the first equality is given by the definition of SOP, the second equality is from (3.14), and the last equality is achieved by simple integration. For the purpose of derivation of SOP, we define a parameter $\alpha_s = 2^{R_s}$, and let $\overline{\gamma}_{XY} = \frac{P_X \Lambda_{XY}}{N_{0Y}}$ denote the average SNR of the link X-Y which is the mean for the exponentially distributed γ_{XY}. The quantity Λ_{XY} is the mean value of average channel gains of that link. Here, two integration operations were performed with respect to x and y replacing $|g|^2$ and γ_{RE}, respectively.

$$
\begin{aligned}
P_{out,NJ}^{(s)} &= Pr(C_{s,NJ}^{(s)} < R_s | g \geq \eta) = Pr\left(\log_2\left[\frac{1+\min(\gamma_{SR},\gamma_{RD})}{1+\gamma_{SE}+\gamma_{RE}}\right] < R_s | g \geq \eta\right) \\
&= Pr\left(\min(\gamma_{SR},\gamma_{RD}) < \alpha_s - 1 + \alpha_s\gamma_{SE} + \alpha_s\gamma_{RE} | g \geq \eta\right) \\
&= \int_{\eta}^{\infty} p_g(x) \int_{0}^{\infty} Pr\left(\min(\gamma_{SR},\gamma_{RD}) < \alpha_s - 1 + \alpha_s\frac{P_S x}{N_{0E}} + \alpha_s y\right) p_{\gamma_{RE}}(y) dy dx \\
&= \int_{\eta}^{\infty}\int_{0}^{\infty}\left[1 - Pr\left(\gamma_{SR} > \alpha_s - 1 + \alpha_s\frac{P_S x}{N_{0E}} + \alpha_s y\right) Pr\left(\gamma_{RD} > \alpha_s - 1 + \alpha_s\frac{P_S x}{N_{0E}} + \alpha_s y\right)\right] \\
&\quad \times p_g(x) p_{\gamma_{RE}}(y) dy dx \\
&= \int_{\eta}^{\infty} \frac{e^{-\left(\frac{x}{\Lambda_{SE}}\right)}}{\Lambda_{SE}} \int_{0}^{\infty}\left[1 - \exp\left(-\left(\frac{1}{\overline{\gamma}_{SR}} + \frac{1}{\overline{\gamma}_{RD}}\right)\left(\alpha_s - 1 + \alpha_s\frac{P_S x}{N_{0E}} + \alpha_s y\right)\right)\right] \frac{e^{-\left(\frac{y}{\overline{\gamma}_{RE}}\right)}}{\overline{\gamma}_{RE}} dy dx \\
&= \int_{\eta}^{\infty} \frac{e^{-\left(\frac{x}{\Lambda_{SE}}\right)}}{\Lambda_{SE}} dx - \int_{\eta}^{\infty}\left[\frac{\frac{1}{\Lambda_{SE}\overline{\gamma}_{RE}} \exp\left(-\left(\frac{1}{\overline{\gamma}_{SR}} + \frac{1}{\overline{\gamma}_{RD}}\right)\left(\alpha_s - 1 + \alpha_s\frac{P_S x}{N_{0E}}\right) - \frac{x}{\Lambda_{SE}}\right)}{\frac{1}{\overline{\gamma}_{RE}} + \frac{\alpha_s}{\overline{\gamma}_{SR}} + \frac{\alpha_s}{\overline{\gamma}_{RD}}}\right] dx \\
&= e^{-\left(\frac{\eta}{\Lambda_{SE}}\right)} - \frac{\exp\left[-\left(\frac{1}{\overline{\gamma}_{SR}} + \frac{1}{\overline{\gamma}_{RD}}\right)(\alpha_s - 1) - \frac{\eta}{\Lambda_{SE}}\left(1 + \frac{\alpha_s\overline{\gamma}_{SE}}{\overline{\gamma}_{SR}} + \frac{\alpha_s\overline{\gamma}_{SE}}{\overline{\gamma}_{RD}}\right)\right]}{\left[1 + \frac{\alpha_s\overline{\gamma}_{SE}}{\overline{\gamma}_{SR}} + \frac{\alpha_s\overline{\gamma}_{SE}}{\overline{\gamma}_{RD}}\right]\left[1 + \frac{\alpha_s\overline{\gamma}_{RE}}{\overline{\gamma}_{SR}} + \frac{\alpha_s\overline{\gamma}_{RE}}{\overline{\gamma}_{RD}}\right]}.
\end{aligned}
\tag{3.20}
$$

□

2. **Weak S-E Link:** With weak S-E link, the eavesdropper becomes a hostile jammer and starts to jam the relay. In this scenario, the SOP can be described by Proposition 3.2.

Proposition 3.2. *SOP for weak S-E link, $P_{out,NJ}^{(w)}$, is derived similarly as above and given in (3.21) as follows.*

Proof. The second equality comes from (3.15) and the last equality uses [99, Eq. 3.322.2] in which $erf(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt$ is known to be the error function.

$$
\begin{aligned}
P_{out,NJ}^{(w)} &= Pr(C_{s,NJ}^{(w)} < R_s | g < \eta) = Pr\left(\log_2 \left[\frac{1 + \min\left(\frac{\gamma_{SR}}{1+\gamma_{ER}}, \gamma_{RD} \right)}{1 + \gamma_{RE}} \right] < R_s | g < \eta \right) \\
&= Pr(g < \eta) \int_0^\infty Pr\left(\min\left(\frac{\gamma_{SR}}{1 + \frac{P_E x}{N_{0R}}}, \gamma_{RD} \right) < \alpha_s - 1 + \alpha_s \frac{P_R x}{N_{0E}} \right) \times p_{f_e}(x) dx \\
&= \left[1 - e^{-\left(\frac{\eta}{\Lambda_{SE}}\right)} \right] \int_0^\infty \left[1 - \exp\left[- \left(\frac{\frac{P_E x}{N_{0R}} + 1}{\overline{\gamma}_{SR}} + \frac{1}{\overline{\gamma}_{RD}} \right) \right] \left(\alpha_s - 1 + \alpha_s \frac{P_R x}{N_{0E}} \right) \right] \\
&\quad \times \frac{1}{\Lambda_{RE}} \exp\left(- \frac{x}{\Lambda_{RE}} \right) dx \\
&= \left[1 - e^{-\left(\frac{\eta}{\Lambda_{SE}}\right)} \right] - \left[1 - e^{-\left(\frac{\eta}{\Lambda_{SE}}\right)} \right] \exp\left(- \left(\frac{\alpha_s - 1}{\overline{\gamma}_{SR}} + \frac{\alpha_s - 1}{\overline{\gamma}_{RD}} \right) \right) \frac{1}{\Lambda_{RE}} \\
&\quad \times \int_0^\infty \exp\left(- \left(\frac{(\alpha_s - 1) P_E x}{N_{0R} \overline{\gamma}_{SR}} + \frac{\alpha_s P_R x}{N_{0E} \overline{\gamma}_{SR}} + \frac{\alpha_s P_R x}{N_{0E} \overline{\gamma}_{RD}} + \frac{\alpha_s P_R P_E x^2}{N_{0R} N_{0E} \overline{\gamma}_{SR}} + \frac{x}{\Lambda_{RE}} \right) \right) dx \\
&= \left[1 - e^{-\left(\frac{\eta}{\Lambda_{SE}}\right)} \right] \left[1 + \exp(-d_0) \frac{1}{\Lambda_{RE}} \sqrt{\frac{\pi}{4a}} \exp\left(\frac{b^2}{4a} \right) \left(erf\left(\frac{b}{2\sqrt{a}} \right) - 1 \right) \right], \qquad (3.21)
\end{aligned}
$$

where, $d_0 = \left(\frac{1}{\overline{\gamma}_{SR}} + \frac{1}{\overline{\gamma}_{RD}} \right)(\alpha_s - 1)$, $a = \frac{\alpha_s P_E P_R}{N_{0E} N_{0R} \overline{\gamma}_{SR}}$, $erf(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt$ and $b = \frac{1}{\Lambda_{RE}} \left[1 + \frac{(\alpha_s - 1)\overline{\gamma}_{ER}}{\overline{\gamma}_{SR}} + \frac{\alpha_s \overline{\gamma}_{RE}}{\overline{\gamma}_{SR}} + \frac{\alpha_s \overline{\gamma}_{RE}}{\overline{\gamma}_{RD}} \right]$.

□

3.3.1.2 With Friendly Jammer

The friendly jammer forces the eavesdropper to remain as a passive listener all the way through the transmission and so the SOP is given as follows.

Proposition 3.3. *The secrecy outage probability for the given model in the presence of a friendly jammer, $P_{out,FJ}^{(s,w)}$, is derived in (3.24) (see next page).*

Proof. In deriving (3.24), the second equality follows from (3.19). We perform three integral operations with respect to variables x, y and z replacing $|g|^2$, γ_{RE} and γ_{JE}, respectively. The outcomes of integration with respect to y and x, respectively are portrayed in (3.22) and (3.23), respectively. Then with the help of the defined I_1 and I_2 we derived (3.24).

$$I_1 = \int_0^{\infty} \left[1 - \exp\left(-\left(\frac{1}{\overline{\gamma}_{SR}} + \frac{1}{\overline{\gamma}_{RD}}\right)\left(\alpha_s - 1 + \alpha_s \frac{P_S x}{N_{0E}(1+z)} + \frac{\alpha_s y}{1+z}\right)\right)\right] \frac{e^{-\left(\frac{y}{\overline{\gamma}_{RE}}\right)}}{\overline{\gamma}_{RE}} dy$$
$$= 1 - \frac{\exp\left[-\left(\frac{1}{\overline{\gamma}_{SR}} + \frac{1}{\overline{\gamma}_{RD}}\right)\left(\alpha_s - 1 + \alpha_s \frac{P_S x}{N_{0E}(1+z)}\right)\right]}{1 + \frac{1}{1+z}\left(\frac{\alpha_s \overline{\gamma}_{RE}}{\overline{\gamma}_{SR}} + \frac{\alpha_s \overline{\gamma}_{RE}}{\overline{\gamma}_{RD}}\right)}. \tag{3.22}$$

$$I_2 = \int_0^{\infty} \frac{e^{-\left(\frac{x}{\Lambda_{SE}}\right)}}{\Lambda_{SE}} I_1 dx = \int_0^{\infty} \frac{e^{-\left(\frac{x}{\Lambda_{SE}}\right)}}{\Lambda_{SE}} \left[1 - \frac{\exp\left[-\left(\frac{1}{\overline{\gamma}_{SR}} + \frac{1}{\overline{\gamma}_{RD}}\right)\left(\alpha_s - 1 + \alpha_s \frac{P_S x}{N_{0E}(1+z)}\right)\right]}{1 + \frac{1}{1+z}\left(\frac{\alpha_s \overline{\gamma}_{RE}}{\overline{\gamma}_{SR}} + \frac{\alpha_s \overline{\gamma}_{RE}}{\overline{\gamma}_{RD}}\right)}\right] dx$$
$$= 1 - \frac{1}{\Lambda_{SE}} \times \frac{\exp\left[-\left(\frac{1}{\overline{\gamma}_{SR}} + \frac{1}{\overline{\gamma}_{RD}}\right)(\alpha_s - 1)\right]}{1 + \frac{1}{1+z}\left(\frac{\alpha_s \overline{\gamma}_{RE}}{\overline{\gamma}_{SR}} + \frac{\alpha_s \overline{\gamma}_{RE}}{\overline{\gamma}_{RD}}\right)}$$
$$\times \int_0^{\infty} \exp\left[-\left(\frac{x}{\Lambda_{SE}}\right)\left(1 + \frac{1}{1+z}\left(\frac{\alpha_s \overline{\gamma}_{SE}}{\overline{\gamma}_{SR}} + \frac{\alpha_s \overline{\gamma}_{SE}}{\overline{\gamma}_{RD}}\right)\right)\right] dx$$
$$= 1 - \frac{\exp\left[-\left(\frac{1}{\overline{\gamma}_{SR}} + \frac{1}{\overline{\gamma}_{RD}}\right)(\alpha_s - 1)\right]}{\left(1 + \frac{1}{1+z}\left(\frac{\alpha_s \overline{\gamma}_{SE}}{\overline{\gamma}_{SR}} + \frac{\alpha_s \overline{\gamma}_{SE}}{\overline{\gamma}_{RD}}\right)\right)\left(1 + \frac{1}{1+z}\left(\frac{\alpha_s \overline{\gamma}_{RE}}{\overline{\gamma}_{SR}} + \frac{\alpha_s \overline{\gamma}_{RE}}{\overline{\gamma}_{RD}}\right)\right)}. \tag{3.23}$$

$$P_{out,FJ}^{(s,w)} = Pr\left(C_{s,FJ}^{(s,w)} < R_s\right) = Pr\left(\log_2\left[\frac{1 + \min(\gamma_{SR}, \gamma_{RD})}{1 + \frac{\gamma_{SE} + \gamma_{RE}}{1 + \gamma_{JE}}}\right] < R_s\right)$$
$$= \int_0^{\infty} \frac{e^{-\left(\frac{x}{\Lambda_{SE}}\right)}}{\Lambda_{SE}} \int_0^{\infty}\int_0^{\infty} \left[1 - \exp\left\{-\left(\frac{1}{\overline{\gamma}_{SR}} + \frac{1}{\overline{\gamma}_{RD}}\right)\left(\alpha_s - 1 + \alpha_s \frac{P_S x}{N_{0E}(1+z)} + \frac{\alpha_s y}{1+z}\right)\right\}\right]$$
$$\times \left[\frac{\exp\left\{-\left(\frac{z}{\overline{\gamma}_{JE}} + \frac{y}{\overline{\gamma}_{RE}}\right)\right\}}{\overline{\gamma}_{JE}\overline{\gamma}_{RE}}\right] dz dy dx = 1 - \int_0^{\infty} \left[\frac{\exp(-d_0)}{\left(1 + \frac{d_1}{1+z}\right)\left(1 + \frac{d_2}{1+z}\right)}\right] \frac{e^{-\left(\frac{z}{\overline{\gamma}_{JE}}\right)}}{\overline{\gamma}_{JE}} dz. \tag{3.24}$$

where, $d_0 = \left(\frac{1}{\overline{\gamma}_{SR}} + \frac{1}{\overline{\gamma}_{RD}}\right)(\alpha_s - 1)$, $d_1 = \frac{\alpha_s \overline{\gamma}_{SE}}{\overline{\gamma}_{SR}} + \frac{\alpha_s \overline{\gamma}_{SE}}{\overline{\gamma}_{RD}}$ and $d_2 = \frac{\alpha_s \overline{\gamma}_{RE}}{\overline{\gamma}_{SR}} + \frac{\alpha_s \overline{\gamma}_{RE}}{\overline{\gamma}_{RD}}$. □

The secrecy outage probabilities for the cases of strong and weak S-E links relate to two independent events. By the definition of total probability theorem, the total secrecy outage probability in absence of friendly jammer is a summation of strong and weak S-E link probabilities [100], i.e.,

$$P_{out,NJ} = P_{out,NJ}^{(s)} + P_{out,NJ}^{(w)}. \tag{3.25}$$

However, due to friendly jamming the eavesdropper turns on the reception mode regardless of the strength of the S-E link, so the total secrecy outage probability in presence of the friendly jammer will be simply (3.24).

3.3.2 For System Model SM2

To derive the expressions of the secrecy outage probabilities we follow the mathematical manipulations for the previous model.

3.3.2.1 Without Friendly Jammer

1. **Strong S-E Link:**

In case of strong S-E link, the eavesdropper listens to the source in first phase and listens to the relay in second phase. No hostile jamming happens in this situation. The corresponding SOP can be derived as follows,

$$
\begin{aligned}
&P_{out,NJ}^{(s)} = Pr(C_{s,NJ}^{(s)} < R_s | g \geq \eta) \\
&= Pr\left(\log_2\left[\frac{1+\min(\gamma_{SR},\gamma_{RD})}{1+\gamma_{SE}+\gamma_{RE}}\right] < R_s | g \geq \eta\right) \\
&= \int_{\eta}^{\infty} p_g(x) \int_{0}^{\infty} Pr\left(\min(\gamma_{SR},\gamma_{RD}) < \alpha_s - 1 + \alpha_s \frac{P_S x}{N_{0E}} + \alpha_s y\right) p_{\gamma_{RE}}(y) dy dx \\
&= \int_{\eta}^{\infty} \frac{e^{-\left(\frac{x}{\Lambda_{SE}}\right)}}{\Lambda_{SE}} \int_{0}^{\infty} \left[1 - \exp\left(-\left(\frac{1}{\overline{\gamma}_{SR}} + \frac{1}{\overline{\gamma}_{RD}}\right)\left(\alpha_s - 1 + \alpha_s \frac{P_S x}{N_{0E}} + \alpha_s y\right)\right)\right] \\
&\quad \times \frac{y^{n_R-1} e^{-\left(\frac{y}{\overline{\gamma}_{RE}}\right)}}{(\overline{\gamma}_{RE})^{n_R}(n_R-1)!} dy dx \\
&= \int_{\eta}^{\infty} \frac{e^{-\left(\frac{x}{\Lambda_{SE}}\right)}}{\Lambda_{SE}} \left[1 - \frac{\exp\left(-\left(\frac{1}{\overline{\gamma}_{SR}} + \frac{1}{\overline{\gamma}_{RD}}\right)\left(\alpha_s - 1 + \alpha_s \frac{P_S x}{N_{0E}}\right)\right)}{(\overline{\gamma}_{RE})^{n_R}(n_R-1)!}\right. \\
&\quad \left. \times \int_{0}^{\infty} \exp\left[-\frac{y}{\overline{\gamma}_{RE}}(1+d_2)\right] y^{n_R-1} dy\right] dx \\
&= \int_{\eta}^{\infty} \frac{e^{-\left(\frac{x}{\Lambda_{SE}}\right)}}{\Lambda_{SE}} \left[1 - \frac{\exp\left(-\left(\frac{1}{\overline{\gamma}_{SR}} + \frac{1}{\overline{\gamma}_{RD}}\right)\left(\alpha_s - 1 + \alpha_s \frac{P_S x}{N_{0E}}\right)\right)}{(1+d_2)^{n_R}}\right] dx \\
&= e^{-\left(\frac{\eta}{\Lambda_{SE}}\right)} - \frac{\exp(-d_0)\exp\left[-\frac{\eta}{\Lambda_{SE}}(1+d_1)\right]}{[1+d_1][1+d_2]^{n_R}},
\end{aligned}
\tag{3.26}
$$

where, $d_0 = \left(\frac{1}{\overline{\gamma}_{SR}} + \frac{1}{\overline{\gamma}_{RD}}\right)(\alpha_s - 1)$, $d_1 = \frac{\alpha_s \overline{\gamma}_{SE}}{\overline{\gamma}_{SR}} + \frac{\alpha_s \overline{\gamma}_{SE}}{\overline{\gamma}_{RD}}$ and $d_2 = \frac{\alpha_s \overline{\gamma}_{RE}}{\overline{\gamma}_{SR}} + \frac{\alpha_s \overline{\gamma}_{RE}}{\overline{\gamma}_{RD}}$.

2. **Weak S-E Link:**

For weak S-E link the mean channel gain falls under the threshold η so the eavesdropper starts to jam the relay in first phase. The corresponding SOP can be derived as follows,

$$
\begin{aligned}
P_{out,NJ}^{(w)} &= Pr(C_{s,NJ}^{(w)} < R_s | g < \eta) = Pr\left(\log_2\left[\frac{1+\min\left(\frac{\gamma_{SR}}{1+\gamma_{ER}}, \gamma_{RD}\right)}{1+\gamma_{RE}}\right] < R_s | g < \eta\right) \\
&= Pr\left(\min\left(\frac{\gamma_{SR}}{1+\gamma_{ER}}, \gamma_{RD}\right) < \alpha_s - 1 + \alpha_s \gamma_{RE} | g < \eta\right) \\
&= Pr(g < \eta) \int_0^\infty Pr\left(\min\left(\frac{\gamma_{SR}}{1+\frac{P_E x}{N_{0R}}}, \gamma_{RD}\right) < \alpha_s - 1 + \alpha_s \frac{P_R x}{N_{0E}}\right) \times p_{f_e}(x) dx \\
&= \left[1 - e^{-\left(\frac{\eta}{\Lambda_{SE}}\right)}\right] \int_0^\infty \left[1 - \exp\left[-\left(\frac{\frac{P_E x}{N_{0R}}+1}{\overline{\gamma}_{SR}} + \frac{1}{\overline{\gamma}_{RD}}\right)\right]\left(\alpha_s - 1 + \alpha_s \frac{P_R x}{N_{0E}}\right)\right] \\
&\times \frac{x^{n_R-1} \exp\left(-\frac{x}{\Lambda_{RE}}\right)}{\Lambda_{RE}^{n_R}(n_R-1)!} dx \\
&= \left[1 - e^{-\left(\frac{\eta}{\Lambda_{SE}}\right)}\right] - \left[1 - e^{-\left(\frac{\eta}{\Lambda_{SE}}\right)}\right] \exp\left(-\left(\frac{\alpha_s - 1}{\overline{\gamma}_{SR}} + \frac{\alpha_s - 1}{\overline{\gamma}_{RD}}\right)\right) \times \frac{1}{\Lambda_{RE}^{n_R}(n_R-1)!} \\
&\times \int_0^\infty \exp\left(-\left(\frac{(\alpha_s-1)P_E x}{\overline{\gamma}_{SR}} + \frac{\alpha_s P_R x}{N_{0E}\overline{\gamma}_{SR}} + \frac{\alpha_s P_R x}{N_{0E}\overline{\gamma}_{RD}} + \frac{\alpha_s P_R P_E x^2}{N_{0R}N_{0E}\overline{\gamma}_{SR}} + \frac{x}{\Lambda_{RE}}\right)\right) x^{n_R-1} dx \\
&= \left[1 - e^{-\left(\frac{\eta}{\Lambda_{SE}}\right)}\right]\left[1 - \frac{\exp(-d_0)}{\Lambda_{RE}^{n_R}(n_R-1)!} \int_0^\infty x^{n_R-1} \exp(-bx - ax^2)\right], \qquad (3.27)
\end{aligned}
$$

where, $a = \frac{\alpha_s P_E P_R}{N_{0E}N_{0R}\overline{\gamma}_{SR}}$ and $b = \frac{1}{\Lambda_{RE}}\left[1 + \frac{(\alpha_s-1)\overline{\gamma}_{ER}}{\overline{\gamma}_{SR}} + \frac{\alpha_s\overline{\gamma}_{RE}}{\overline{\gamma}_{SR}} + \frac{\alpha_s\overline{\gamma}_{RE}}{\overline{\gamma}_{RD}}\right]$.

Following the case of the SISO model the total secrecy outage probability in absence of friendly jammer can be obtained using (3.25).

3.3.2.2 With Friendly Jammer

Since the friendly jammer is jamming the eavesdropper by deceiving it with a source-like signal, the corresponding SOP can be given by (3.29). The mathematical manipulation is shown below,

We have,

$$P_{out,FJ}^{(s,w)} = Pr\left(C_{s,FJ}^{(s)} < R_s | g \geq \eta\right) = Pr\left(\log_2\left[\frac{1+\min(\gamma_{SR},\gamma_{RD})}{1+\frac{\gamma_{SE}+\gamma_{RE}}{1+\gamma_{JE}}}\right] < R_s | g \geq \eta\right)$$
$$= \int_0^\infty \frac{e^{-\left(\frac{x}{\Lambda_{SE}}\right)}}{\Lambda_{SE}} \int_0^\infty \int_0^\infty \left[1-\exp\left(-\left(\frac{1}{\overline{\gamma}_{SR}}+\frac{1}{\overline{\gamma}_{RD}}\right)\left(\alpha_s - 1 + \alpha_s \frac{P_S x}{N_{0E}(1+z)} + \frac{\alpha_s y}{1+z}\right)\right)\right]$$
$$\times \frac{e^{-\left(\frac{z}{\overline{\gamma}_{JE}}\right)}}{\overline{\gamma}_{JE}} \times \frac{y^{n_R-1}e^{-\left(\frac{y}{\overline{\gamma}_{RE}}\right)}}{(\overline{\gamma}_{RE})^{n_R}(n_R-1)!} dz dy dx$$
$$= \int_0^\infty \frac{e^{-\left(\frac{x}{\Lambda_{SE}}\right)}}{\Lambda_{SE}} \left(\int_0^\infty \frac{e^{-\left(\frac{x}{\Lambda_{SE}}\right)}}{\Lambda_{SE}} I_1 dx\right) \frac{e^{-\left(\frac{z}{\overline{\gamma}_{JE}}\right)}}{\overline{\gamma}_{JE}} dz. \tag{3.28}$$

Let,

$$I_1 = \int_0^\infty \left[1-\exp\left(-\left(\frac{1}{\overline{\gamma}_{SR}}+\frac{1}{\overline{\gamma}_{RD}}\right)\left(\alpha_s - 1 + \alpha_s \frac{P_S x}{N_{0E}(1+z)} + \frac{\alpha_s y}{1+z}\right)\right)\right] \frac{y^{n_R-1}e^{-\left(\frac{y}{\overline{\gamma}_{RE}}\right)}}{(\overline{\gamma}_{RE})^{n_R}(n_R-1)!} dy$$
$$= 1 - \frac{\exp\left[-\left(\frac{1}{\overline{\gamma}_{SR}}+\frac{1}{\overline{\gamma}_{RD}}\right)\left(\alpha_s - 1 + \alpha_s \frac{P_S x}{N_{0E}(1+z)}\right)\right]}{\left[1+\frac{1}{1+z}\left(\frac{\alpha_s\overline{\gamma}_{RE}}{\overline{\gamma}_{SR}}+\frac{\alpha_s\overline{\gamma}_{RE}}{\overline{\gamma}_{RD}}\right)\right]^{n_R}}.$$

Again let,

$$I_2 = \int_0^\infty \frac{e^{-\left(\frac{x}{\Lambda_{SE}}\right)}}{\Lambda_{SE}} I_1 dx = \int_0^\infty \frac{e^{-\left(\frac{x}{\Lambda_{SE}}\right)}}{\Lambda_{SE}} \left[1 - \frac{\exp\left[-\left(\frac{1}{\overline{\gamma}_{SR}}+\frac{1}{\overline{\gamma}_{RD}}\right)\left(\alpha_s - 1 + \alpha_s \frac{P_S x}{N_{0E}(1+z)}\right)\right]}{\left[1+\frac{1}{1+z}\left(\frac{\alpha_s\overline{\gamma}_{RE}}{\overline{\gamma}_{SR}}+\frac{\alpha_s\overline{\gamma}_{RE}}{\overline{\gamma}_{RD}}\right)\right]^{n_R}}\right] dx$$
$$= 1 - \frac{\exp\left[-\left(\frac{1}{\overline{\gamma}_{SR}}+\frac{1}{\overline{\gamma}_{RD}}\right)(\alpha_s - 1)\right]}{\Lambda_{SE}\left[1+\frac{1}{1+z}\left(\frac{\alpha_s\overline{\gamma}_{RE}}{\overline{\gamma}_{SR}}+\frac{\alpha_s\overline{\gamma}_{RE}}{\overline{\gamma}_{RD}}\right)\right]^{n_R}} \int_0^\infty \exp\left[-\left(\frac{1}{\overline{\gamma}_{SR}}+\frac{1}{\overline{\gamma}_{RD}}\right)\left(\frac{\alpha_s P_S x}{N_{0E}(1+z)}\right) - \frac{x}{\Lambda_{SE}}\right] dx$$
$$= 1 - \frac{\exp\left[-\left(\frac{1}{\overline{\gamma}_{SR}}+\frac{1}{\overline{\gamma}_{RD}}\right)(\alpha_s - 1)\right]}{\Lambda_{SE}\left[1+\frac{1}{1+z}\left(\frac{\alpha_s\overline{\gamma}_{RE}}{\overline{\gamma}_{SR}}+\frac{\alpha_s\overline{\gamma}_{RE}}{\overline{\gamma}_{RD}}\right)\right]^{n_R}} \int_0^\infty \exp\left[-\frac{x}{\Lambda_{SE}}\left(1+\frac{1}{1+z}\left(\frac{\alpha_s\overline{\gamma}_{SE}}{\overline{\gamma}_{SR}}+\frac{\alpha_s\overline{\gamma}_{SE}}{\overline{\gamma}_{RD}}\right)\right)\right] dx$$
$$= 1 - \frac{\exp\left[-\left(\frac{1}{\overline{\gamma}_{SR}}+\frac{1}{\overline{\gamma}_{RD}}\right)(\alpha_s - 1)\right]}{\left[1+\frac{1}{1+z}\left(\frac{\alpha_s\overline{\gamma}_{RE}}{\overline{\gamma}_{SR}}+\frac{\alpha_s\overline{\gamma}_{RE}}{\overline{\gamma}_{RD}}\right)\right]^{n_R}} \times \frac{1}{1+\frac{1}{1+z}\left(\frac{\alpha_s\overline{\gamma}_{SE}}{\overline{\gamma}_{SR}}+\frac{\alpha_s\overline{\gamma}_{SE}}{\overline{\gamma}_{RD}}\right)}$$
$$= \left[1 - \frac{\exp(-d_0)}{\left(1+\frac{d_1}{1+z}\right)\left(1+\frac{d_2}{1+z}\right)^{n_R}}\right].$$

Hence, using the expressions for I_1 and I_2 in (3.28) we have,

$$P_{out,FJ}^{(s,w)} = 1 - \frac{\exp(-d_0)}{\overline{\gamma}_{JE}} \int_0^\infty \left[\frac{\exp-\left(\frac{z}{\overline{\gamma}_{JE}}\right)}{\left(1+\frac{d_1}{1+z}\right)\left(1+\frac{d_2}{1+z}\right)^{n_R}}\right] dz, \tag{3.29}$$

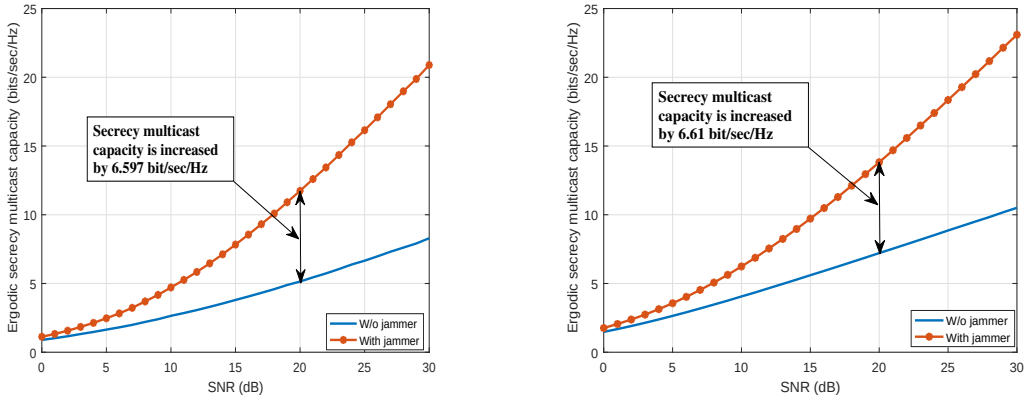
where, $d_0 = \left(\frac{1}{\overline{\gamma}_{SR}}+\frac{1}{\overline{\gamma}_{RD}}\right)(\alpha_s - 1)$, $d_1 = \frac{\alpha_s\overline{\gamma}_{SE}}{\overline{\gamma}_{SR}}+\frac{\alpha_s\overline{\gamma}_{SE}}{\overline{\gamma}_{RD}}$ and $d_2 = \frac{\alpha_s\overline{\gamma}_{RE}}{\overline{\gamma}_{SR}}+\frac{\alpha_s\overline{\gamma}_{RE}}{\overline{\gamma}_{RD}}$.

3.4 Numerical Results

We discuss the numerical results in two subsections. Since the system model **SM2** is a revisit of the system model **SM1**, the corresponding secrecy performances are discussed together whereas, the results of system model **SM0** is discussed separately.

3.4.1 System Model SM0

The benefit of deploying friendly jammer in terms of achievable multicast secrecy capacity is shown for both cases of strong (Fig. 3.4(a)) and weak (Fig. 3.4(b)) S-E links. In Fig. 3.4(a), the eavesdroppers' capacity is being subtracted from the main channel capacity in both phases while in Fig. 3.4(b) the main channel suffers from interference and eavesdropping in the first and second phases, respectively. In each subfigure, the performance is found better with the use of friendly jammer than without it.



(a) With strong S-E link.

(b) With weak S-E link.

FIGURE 3.4: Performance comparison between the cases of without and with jammer.

Fig. 3.5 depict the effect of hostile and friendly jamming powers (P_E and P_J, respectively) on secrecy multicast capacity. It shows that P_E degrades the secrecy multicast capacity and increase in P_E causes more degradation of the secrecy capacity. However, when the friendly jammer is appointed it eliminates the hostile jamming in the first phase and lowers the eavesdroppers' capacity in the second phase. Thus if we increase the value of P_J the secrecy multicast capacity will be enhanced. Fig. 3.6-3.8 follow this concept.

Fig. 3.6 shows the effect of varying friendly jamming power on the secrecy capacity with respect to channel SNR for strong and weak S-E links, respectively. With the jamming power the secrecy capacity increases, however, the rate of increase is not uniform. For

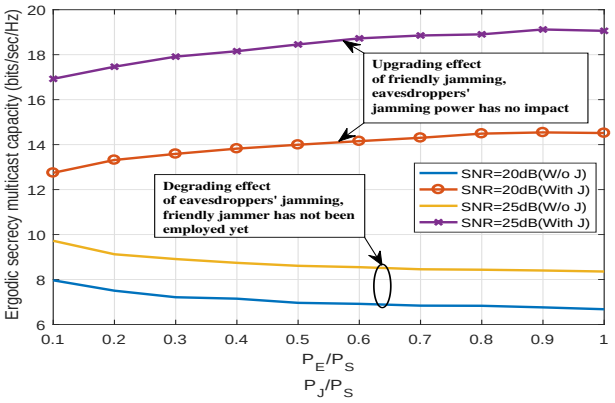
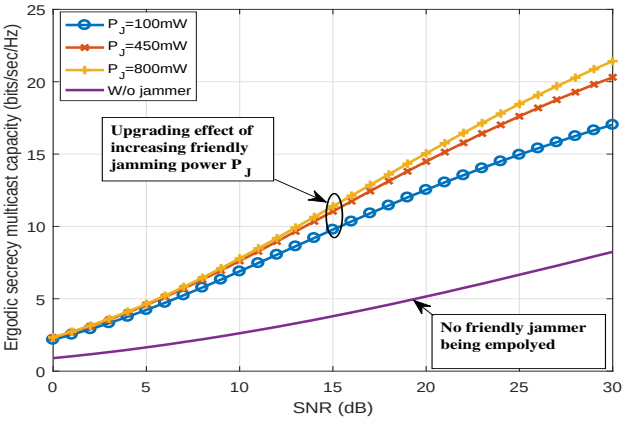


FIGURE 3.5: Impact of hostile (P_E) and friendly (P_J) jamming on secrecy multicast capacity .

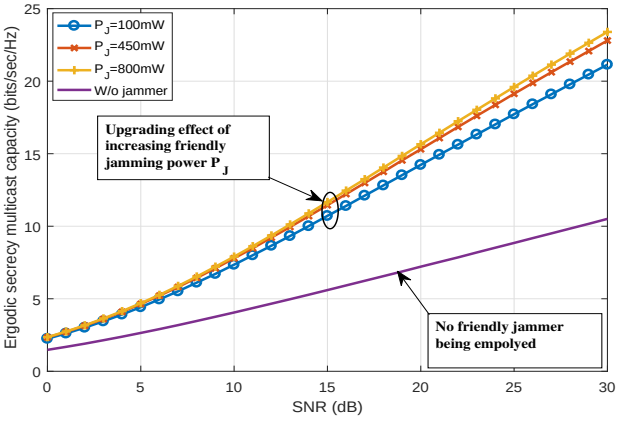
example, according to Fig. 3.6(a) for P_J being increased from 100mW to 450mW, the capacity increases around $0.36 - 0.56\%$, but for P_J being increased from 450mW to 800mW, the rate is around $0.1 - 0.16\%$. Fig. 3.6(b) also shows similar characteristics.

Fig. 3.7 shows the effects of varying P_J with respect to increasing P_S. We observe that, although larger P_J causes increase in secrecy multicast capacity, it does not mean that more jamming power by J will result in similar increase of secrecy multicast capacity. Fig. 3.7(a) shows that for P_S=400mW, when P_J was increased to 450mW from 100mW the value of secrecy multicast capacity was increased by 2.8bit/sec/Hz but as P_J became 800mW from 450mW, the capacity increased only 0.89bit/sec/Hz. Similarly for weak S-E link in Fig. 3.7(b) the increase in secrecy multicast capacity is not uniform with respect to the increase in the value of P_J. This is why a bargain or an auction strategy is needed at the beginning to optimize the interference price charged by the friendly jammer for its power allocation.

Fig. 3.8 on the other hand, shows the degrading effect of eavesdroppers' jamming power on the secrecy multicast capacity when there is no friendly jammer. For an increase of 350mW in the hostile jamming power, the capacity degrades by $0.04 - 0.11\%$ (Fig. 3.8(a)). However, with increasing SNR or source power performances, with high jamming (P_E being 450-800mW) almost coincide and since friendly jammer eradicates the effect of eavesdroppers' jamming; therefore all the curves depicting secrecy multicast capacity with jammer coincide. Moreover, all the plots show that, with the help of friendly jammer, higher secrecy multicast capacity can be achieved compared to the scenario where the friendly jammer is absent.



(a) With strong S-E link.

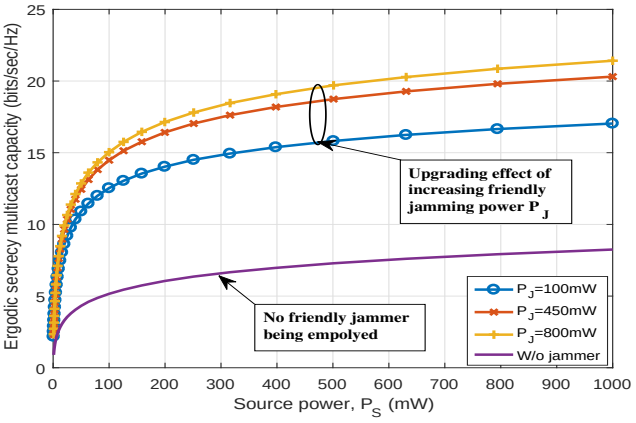


(b) With weak S-E link.

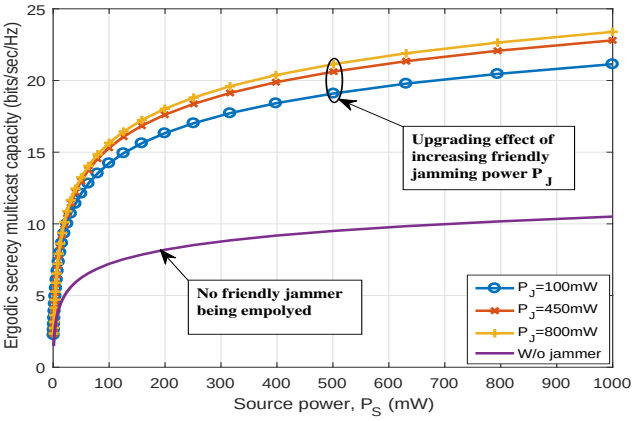
FIGURE 3.6: Performance comparison between the cases of with and without friendly jammer. P_E was considered as a fraction of P_S and P_J was considered to be 100mW, 450mW or 800mW.

3.4.2 System Models SM1 and SM2

We conduct simulations to investigate the improvement in the secrecy capacity and SOP performances due to the presence of friendly jamming. We consider $P_S = P_R$, $N_{0R} = N_{0D} = N_{0E} = 1.0$, $R_s = 3.0$ bits/s/Hz. The ratio of average main channel gain to average eavesdropper channel gain is denoted by MER$= \frac{\Lambda_M}{\Lambda_E}$ where, $\Lambda_{SR} = \Lambda_{RD} = \Lambda_M = 1$ and $\Lambda_{SE} = \Lambda_{RE} = \Lambda_E = \text{MER}^{-1}$. This criteria is set to simulate the variations in SNR strengths in the eavesdropping links. Therefore, the average SNRs are $\overline{\gamma}_{SR} = \frac{P_S\Lambda_M}{N_{0R}}$, $\overline{\gamma}_{RD} = \frac{P_S\Lambda_M}{N_{0D}}$, $\overline{\gamma}_{SE} = \frac{P_S\Lambda_E}{N_{0E}}$ and $\overline{\gamma}_{RE} = \frac{P_S\Lambda_E}{N_{0E}}$. For reciprocity, $f_j = f_e$ thus $\overline{\gamma}_{ER} = \frac{P_E\Lambda_E}{N_{0R}}$ and assuming proper beamforming by the friendly jammer caused $\overline{\gamma}_{JE} = \frac{P_J\Lambda_{JE}}{N_{0E}}$ with $\Lambda_{JE} = 1$.



(a) With strong S-E link.



(b) With weak S-E link.

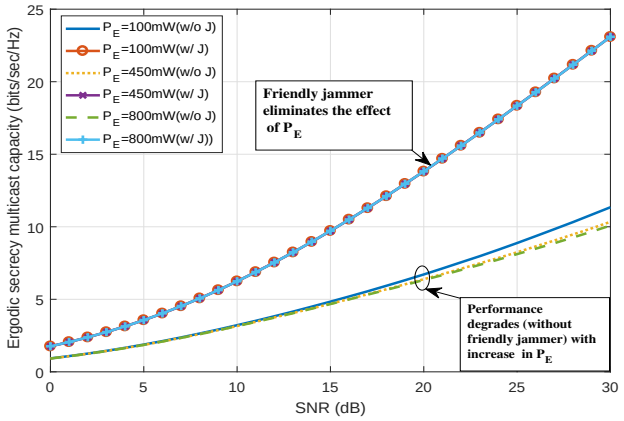
FIGURE 3.7: Secrecy multicast capacity vs P_S with varying friendly jamming power P_J; P_E considered as a fraction of P_S while the value of P_J was taken as 100mW, 450mW or 800mW.

3.4.3 Secrecy Capacity (SC)

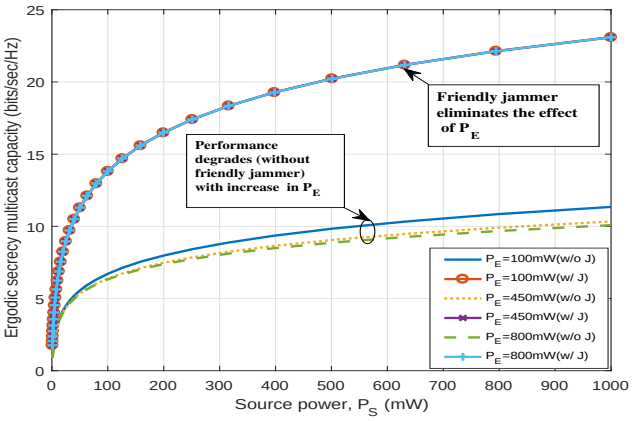
We show the secrecy capacity of the SISO model against SNR (Fig. 3.9) and MER (Fig. 3.10). For Fig. 3.9 the MER is chosen to be 25dB. The figure shows that friendly jammer increases the secrecy capacity regardless of the strength of S-E link. On the other hand, Fig. 3.11 shows the impact of higher number of relay antennas on secrecy capacity vs MER characteristics.

We also observe that a low power friendly jamming was enough to enhance the secrecy capacity. Then with the low jamming power of 10dB, secrecy capacity at 30dB of SNR for different MERs are shown in Table 3.4 with the help of Fig. 3.10 and 3.11 .

Table 3.4 shows that the value of secrecy capacity increases with the increasing value of MER as expected. For each value of MER, the friendly jammer enhances the secrecy



(a) Secrecy Multicast capacity vs. SNR .



(b) Secrecy Multicast capacity vs. source power P_S.

FIGURE 3.8: Comparison of performance between the case of with (w/ J) and without friendly jammer (w/o J) with varying eavesdroppers' jamming power P_E. P_J was considered as a fraction of P_S and P_E was considered to be 100mW, 450mW or 800mW.

TABLE 3.4: Secrecy Capacity, C_s Analysis.

MER (dB)	$C_s(n_R = 1)$ (bits/s/Hz)			$C_s(n_R = 4)$ (bits/s/Hz)		
	Without FJ		With FJ	Without FJ		With FJ
	Strong S-E link	Weak S-E link		Strong S-E link	Weak S-E link	
5	0.4828	0.2216	2.09	0.8566	0	3.567
15	2.683	1.615	5.106	3.959	0.7376	6.625
25	5.554	5.302	7.228	7.03	6.147	8.782

capacity from the original value found in absence of friendly jammer. Because high value of MER depicts inferior eavesdropping channel, at higher MER for higher SNRs as spotted in Fig. 3.9-Fig. 3.10, hostile jamming has low impact on secrecy capacity thus the strong S-E link gives more secrecy capacity than that with a weak S-E link when no friendly jammer was employed. However, a higher MER will always give a better result, it is the low MER scenarios where FJ becomes a greater help.

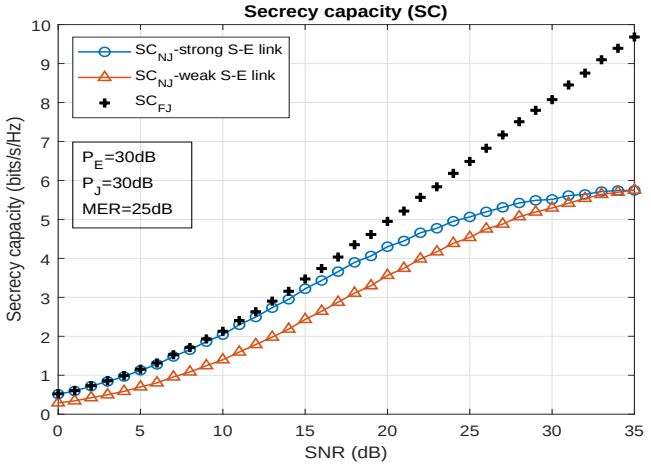


FIGURE 3.9: Enhancement of secrecy capacity in presence of FJ.

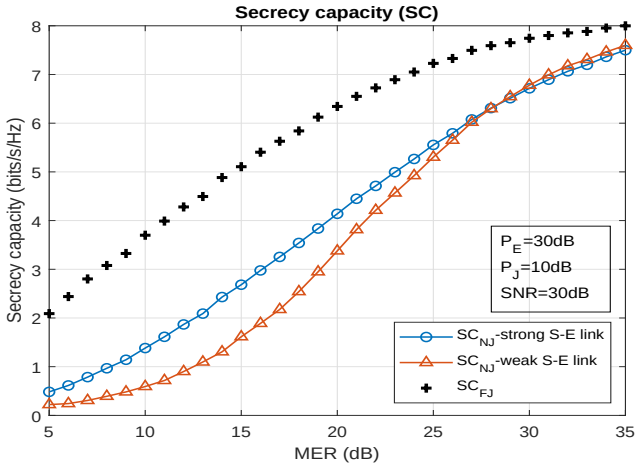


FIGURE 3.10: Impact of MER on secrecy capacity.

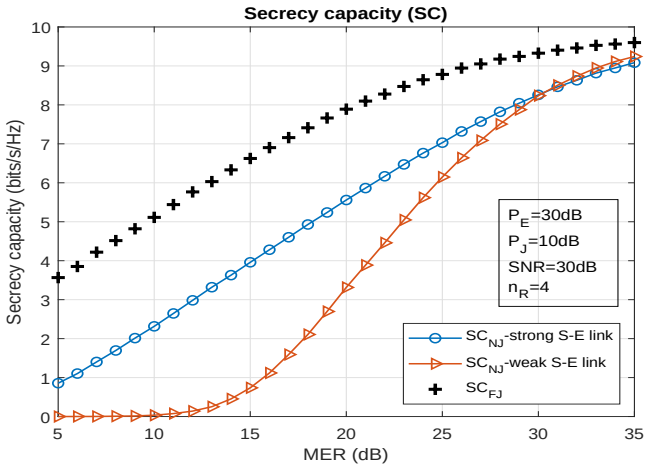


FIGURE 3.11: Impact of MER on secrecy capacity with $n_R = 4$.

The results also show that an increase in antenna number is not beneficial for secrecy if the S-E link is weak. The reason behind this is the hostile jamming link or E-R link being SIMO instead of SISO. The SIMO link comparatively gives more capacity than a

corresponding SISO or MISO link [101]. Therefore, the relay suffers from more hostile jamming if n_R increases. However, with the help of friendly jammer this problem can be mitigated by stopping the hostile jamming as discussed above.

3.4.4 Secrecy Outage Probability (SOP)

The SOP with friendly jammer for the SISO model is found lower than that in absence of the friendly jammer as shown by Fig. 3.12. At 30dB of SNR, for 25dB MER, the SOP becomes $\frac{1}{10}^{th}$ due to the use of friendly jamming. Here, both P_E and P_J are chosen to be 30dB. The SOP performance is then observed with low friendly jamming power of

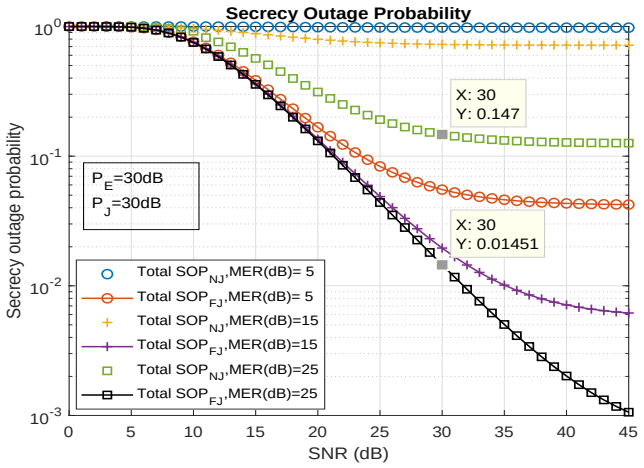


FIGURE 3.12: Friendly jamming reduces SOP at various MERs.

TABLE 3.5: SOP Analysis.

$\mathbf{P}_J$ **(dB)**	**MER (dB)**	**SOP**		**Δ SOP**
		NJ	**FJ**	
30	5	0.9836	0.08337	0.90023
	15	0.7479	0.04879	0.69911
	25	0.1913	0.0439	0.1474
10	5	0.9836	0.6307	0.3529
	15	0.7479	0.1884	0.5595
	25	0.1913	0.06096	0.13034

10dB. The performance with different P_J and MERs at 25dB of SNR, given in Table 3.5 shows that with increase in MER, the SOP decreases as expected. The SOP for friendly jammer case is found to be lower than the corresponding one with no friendly jammer case irrespective of friendly jamming power or channel gain ratio MER, indicating the advantage that friendly jammer offers to enhance the security.

This shows that, at quite low MER of 5dB, SOP is almost 1.0 without friendly jammer, but it improves significantly to a very low value (0.08337) once FJ is used with 30dB power. We also observe for large values of Λ_{ER} ($2 \times \Lambda_{RE}$, 1.00) and the outcomes were similar. Therefore, friendly jammer is proved to be capable of decreasing the secrecy outage of this model .

With multiple relay antennas, we can see from Fig. 3.13 that the friendly jammer gives lower SOP compared to the scenario with no friendly jammer. The system model is now a combination of SISO, SIMO and MISO subsystems where, the links S-E and S-FJ are SISO, links S-R and E-R are SIMO while links R-D and R-E falls under MISO categories. Looking at the increase in SOP difference between corresponding NJ and FJ cases (Δ SOP) in the following tables, we can see that the friendly jammer is improving the SOP performance.

TABLE 3.6: SOP vs n_R Analysis (Fig. 3.14). P_J = 30dB, P_E = 30dB, SNR=25dB.

n_R	**MER**=15dB			**MER**=25dB		
	SOP-NJ	**SOP-FJ**	**ΔSOP**	**SOP-NJ**	**SOP-FJ**	**ΔSOP**
1	0.7479	0.04879	0.69911	0.1913	0.0439	0.1474
2	0.8644	0.053	0.8114	0.2959	0.04435	0.25155
4	0.8908	0.06015	0.83065	0.4846	0.04515	0.43946
8	0.8923	0.07192	0.82038	0.6574	0.04646	0.61094
10	0.8925	0.07706	0.81544	0.6792	0.04704	0.63216

TABLE 3.7: SOP vs P_J Analysis (Fig. 3.15). $n_R = 4$, P_E = 30dB, SNR=25dB.

P_J (dB)	**MER**=15dB			**MER**=25dB		
	SOP-NJ	**SOP-FJ**	**ΔSOP**	**SOP-NJ**	**SOP-FJ**	**ΔSOP**
10	0.8908	0.04879	0.69911	0.4846	0.0439	0.1474
20		0.053	0.8114		0.04435	0.25155
30		0.06015	0.83065		0.04515	0.43946
40		0.07192	0.82038		0.04646	0.61094
50		0.07706	0.81544		0.04704	0.63216

Both Tables 3.6 and 3.7 show that the deceptive friendly jammer decreases SOP compared to the corresponding no friendly jammer cases. An increase in P_J causes more interference to the eavesdropper who already in reception mode deceived by FJ thus lowering the value of SOP.

3.5 Conclusion

This chapter describes the study of the effect of friendly jamming on wireless physical layer security for a relay-aided transmission. The transmission is intercepted by the

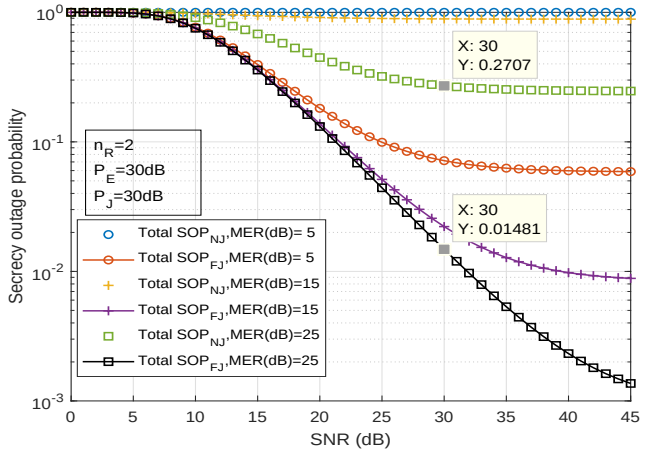


FIGURE 3.13: Friendly jamming decreasing SOP.

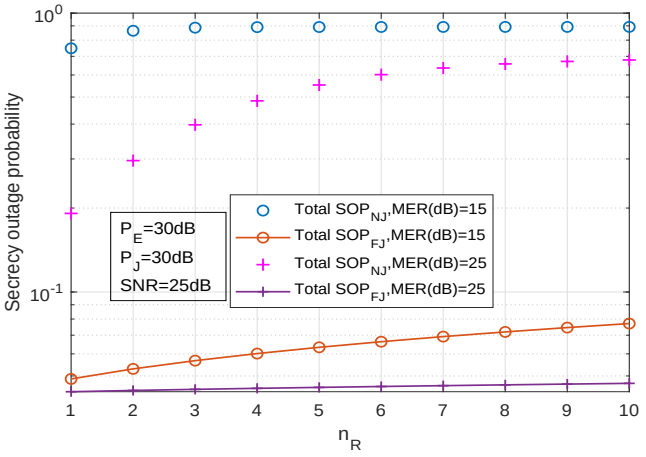


FIGURE 3.14: SOP vs relay antenna number (n_R) characteristics.

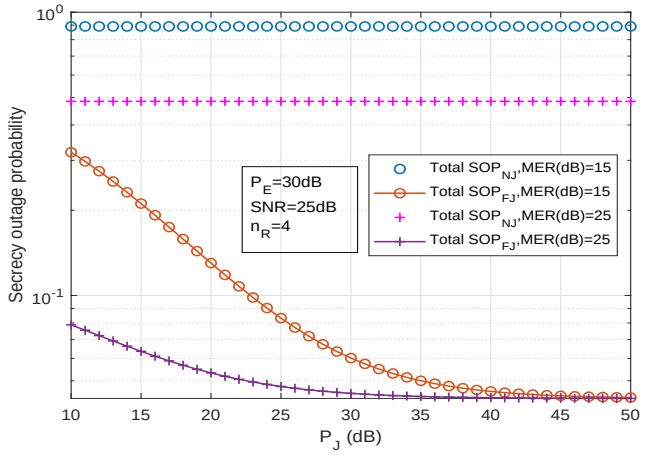


FIGURE 3.15: SOP vs friendly jamming power (P_J)characteristics.

eavesdropper in the both broadcasting and relaying phases of the transmission. The eavesdropper also jams the relay if the source to eavesdropper link is not strong enough. We placed a friendly jammer near the eavesdropper who transmits source-like signal to

deceive the eavesdropper thus lowering down the capacity of the eavesdropping channel. Moreover, the deceptive jamming signal forces the eavesdropper to be in reception mode and not become a hostile jammer. We derived the secrecy capacity and secrecy outage probability in presence and absence of a friendly jammer. The numerical results show that the friendly jammer ensures more secrecy capacity, and the secrecy outage probability decreases compared to the system model that does not incorporate the friendly jammer. The investigation includes two models; one with a relay equipped with a single antenna and the second model has a relay with multiple antennas to study the effect of antenna diversity on the secrecy parameters. Both models were benefited from friendly jamming as shown by the numerical results.

Chapter 4

Friendly Jammers in Random Wireless Network against Adaptive Eavesdroppers

4.1 Overview

Studies about large-scale wireless networks are being carried out gradually, especially with the extending demand around wireless sensor networks (WSNs) and IoT devices. Since in large scale networks the nodes are located randomly, stochastic geometry has become popular to predict the statistical properties of the nodes. The main sub-field of the stochastic geometry is the point-process theory where each node is considered to be a point existing inside an area set [70, 72]. For large scale wireless network use of homogeneous Poisson point process (HPPP) is very popular as it is useful to portray a random wireless network [102]. This model is also suitable to characterise the signal-to-interference-plus-noise ratio (SINR) whereas the classical physical layer security approaches work with mainly SNRs [70]. For our first system model we chose a conventional radio network with the assumption that the source and the friendly jammer knows the locations of the eavesdropper. For our second system model we choose a more practical setup of a random wireless network where multiple destinations, eavesdroppers and friendly jammers are placed following HPPP. We are the first to study an HPPP model where the friendly jammers attempt to convert the hostile jammers into passive eavesdroppers by exploiting the half-duplex nature of the adaptive eavesdroppers with the help of source-like jamming signals. Deceiving adaptive eavesdroppers to be passive by friendly jammers is a new concept and we are investigating our intuition about it throughout this thesis for two different types of system models.

Our contributions are as follows,

i. We are the first to consider deceptive friendly jamming in a homogeneous Poisson point process (HPPP) network with the aid of friendly jammers. The friendly jammers will send source-like signals to the adaptive eavesdroppers who are half-duplex in nature. As a result, eavesdroppers that are sending hostile jamming signals to the destinations will start to listen to the friendly jamming signals. We mathematically analyse the impact of friendly jamming to show that friendly jammers can reduce both the hostile jamming and the passive eavesdropping. As a result, the secrecy capacity is enhanced. We also utilise a secrecy protected zone around the source to keep the zone free from any eavesdropper. Our analysis reveals how much friendly jammers are helpful against adaptive eavesdroppers if the secrecy protected zone is very small, given the limitation of constructing large protection zone.

ii. We derive secrecy capacity of our channel model. We also investigate the secrecy performance of a wide range of network parameters. Our observations include the secrecy performance for different intensities of the nodes acting as destinations, passive eavesdroppers, hostile jammers and friendly jammers. Also, other parameters like friendly jamming power, radius of secrecy protected zones etc. are also varied to further analyse the secrecy performance. The numerical results section shows that our model provides good secrecy capacity with a moderately high node intensity or power of friendly jammers, and that the friendly jammers are very effective for secrecy enhancement if the secrecy protected zone is very small or the node intensity of destinations are not large enough.

The ergodic capacity is derived for the following scenarios.

(i) At destinations in the absence of hostile jammers;

(ii) At destinations in the presence of hostile jammers;

(iii) At the worst-case eavesdropper in the absence of friendly jammers, and

(iv) At the worst-case eavesdropper in the presence of friendly jammers.

We assume that the eavesdroppers are cooperating with each other thus the hostile jamming does not affect the eavesdropping links. Similarly, the friendly jammers are also working in cooperation with each other and with the legitimate entities. The destinations are unaffected by the friendly jamming. This work has been published in *Journal of Network and Computer Applications*, Elsevier [45].

4.1.1 System Model and Problem Formulation

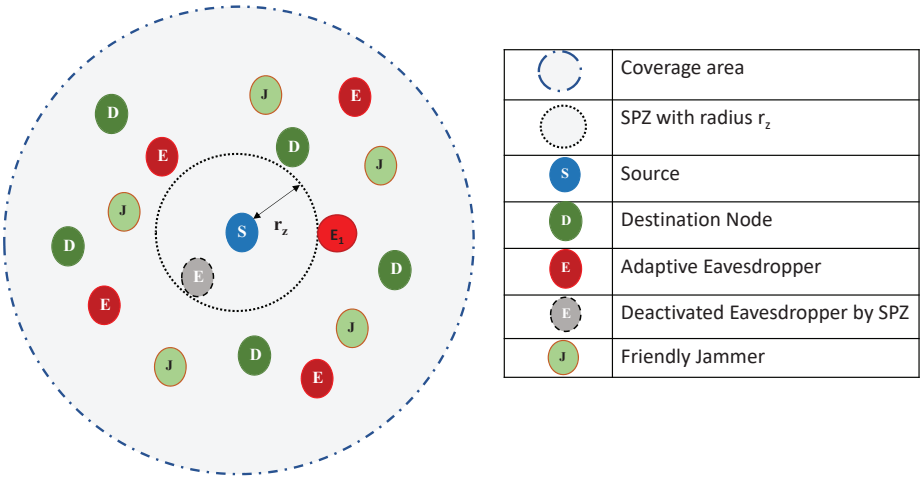


FIGURE 4.1: Random wireless network with secrecy protected zone. The legends used are as follows: S- source, D- destination, E- eavesdropper and J- friendly jammer.

The system model in Fig. 4.1 consists of a source transmitting information to multiple destination nodes. A secrecy protected zone with a radius of r_z encircles the source S. Any eavesdropper residing inside this zone are deactivated by the source and the worst-case eavesdropper is assumed to be the one which is located at the nearest point from the zone. A group of friendly jammers are located surrounding the zone to tackle the eavesdropping. We have considered the eavesdroppers to be adaptive and half-duplex, i.e., they either listen to the source or jam the destination. The friendly jammers are deceptive jammers and try to force the eavesdroppers to be in reception mode, and utilise zero-forcing (ZF) precoding so that the destination can avoid the friendly jamming. In this random network, the locations of the destinations, the eavesdroppers and the friendly jammers follow the homogeneous PPP. All the entities are equipped with a single antenna and are stationary nodes. This model is named as System model **SM3**.

The notations for various parameters are listed in Table 4.1. For the simplicity of analysis, we let the noise variances for all members from the same set to be the same and all the jammers from the same set emit signals at the same level. Wireless signal impairment is considered to follow Rayleigh fading.

In the HPPP model, the location of the nodes are random and corresponding path-losses are inevitable while deriving the expressions of the secrecy parameters. In this framework, the secrecy parameters are obtained with the help of the probability density function (PDF) of the distance of the node from central node (in this model the source S). According to M. Haenggi [41], without the protected zone when the m^{th} node is

TABLE 4.1: List of Notations.

Notation	Description
x_X, y_Y, n_Y	Emitted signal from X, received signal at Y and noise at receiver Y, respectively.
Φ_D, Φ_E, Φ_H, Φ_J	Set of destinations, passive eavesdroppers, hostile jammers (active eavesdroppers) and friendly jammers, respectively.
D_n, E_k and J_ℓ	The n^{th} destination, k^{th} eavesdropper (passive or hostile) and ℓ^{th} friendly jammer, respectively. $D_n \in \Phi_D$, $E_k \in \Phi_E$ (for passive E), $E_k \in \Phi_H$ (for hostile E) and $J_\ell \in \Phi_J$.
h_n, g_k	Channel coeff. of $S - D_n$ and $S - E_k$ links, respectively experiencing independent Rayleigh fading.
$f_{k,n}$, j_{lk}	Channel coeff. of $E_k - D_n$ and $J_\ell - E_k$ links, respectively experiencing independent Rayleigh fading.
P_X	The transmit power of X.
N_{0Y}	The noise variance of Y, assumed to be same for all Y.
$n_Y \sim \mathcal{N}(0, N_{0Y})$	AWGN noise of receiver Y.
γ_{XY}	$=\frac{\lvert\omega\rvert^2 P_X}{N_{0Y}}$, instantaneous SNR of $X - Y$ link with channel coefficient equals to ω.
$\overline{\gamma}_{XY}$	$=\frac{P_X \Lambda_{XY}}{N_{0Y}}$, average SNR of $X - Y$ link.
Λ_{XY}	Mean of the channel coefficient of $X - Y$ link. It is assumed to be same for all the pair of entities from the same link.
η	Threshold of channel gain of $S - E$ link suitable for eavesdropping.
r_z	Radius of secrecy protected zone.
$\lambda_X = \frac{\#\Phi_X}{Area}$	Intensity of X nodes in the coverage area.
λ_{Eve}	Total intensity of the eavesdroppers' nodes ($\lambda_{Eve} = \lambda_E + \lambda_H$).
R_{XY}	Ergodic capacity at Y for transmission from X to Y.
C_s	Secrecy capacity.
α	Path-loss constant.
δ	$\frac{2}{\alpha}$.

situated at a distance of r_m from the source, the PDF of the distance is given as

$$f_{x_m}(x) = \frac{(\pi\lambda)^m \delta}{\Gamma(m)} x^{(m\delta-1)} \exp(-\pi\lambda x^\delta), \tag{4.1}$$

where, $x = r_m^\alpha$, $\delta = \frac{2}{\alpha}$ while α being the path-loss coefficient and λ being the intensity of the nodes. Again, $\Gamma(x)$ denotes the Gamma function. For a circular space, the distance between the source and the n^{th} destination node will have the following PDF,

$$f_{r_{d,n}}(x) = 2\pi\lambda_D x \exp(-\pi\lambda_D x^2) \frac{(\pi\lambda_D x^2)^{n-1}}{(n-1)!}. \tag{4.2}$$

Our analysis needs the PDF of distances when a secrecy zone is enforced. With the source employing a secrecy protected zone of radius ρ, Liu et. al. [39] have discussed the scenario of randomly located eavesdroppers following HPPP. The PDF of the distance from the origin, in this case the source, to the k^{th} nearest eavesdropper, is given as

$$f_{r_{e,k}}(r) = 2\pi\lambda r \exp\left[-\pi\lambda(r^2 - \rho^2)\right] \frac{\left[-\pi\lambda(r^2 - \rho^2)\right]^{k-1}}{(k-1)!}, \tag{4.3}$$

which gives the following PDF of the distance of the nearest node from the source,

$$f_{r_{e,1}}(r) = 2\pi\lambda r \exp\left[-\pi\lambda(r^2 - \rho^2)\right]. \tag{4.4}$$

4.2 Secrecy Capacity

The secrecy capacity can be obtained by subtracting the maximum eavesdropper's capacity from the minimum main channel capacity. Mathematically speaking,

$$C_s = [R_{SD_{min}} - R_{SE_{max}}]^+, \tag{4.5}$$

where, $R_{SD_{min}}$ is the minimum ergodic capacity obtained from a group of destination nodes, and $R_{SE_{max}}$ is the maximum ergodic capacity obtained from a group of eavesdropping nodes or in other words the ergodic capacity of the worst-case eavesdropper. Again, $[X]^+ = max(0, x)$.

In the following derivations, the suffices 'noHJ' and 'HJ' denote the absence and presence of the hostile jammers, respectively and in a similar manner the absence and presence of the friendly jammers are represented by the suffices 'noFJ' and 'FJ', respectively.

4.2.1 Ergodic Capacity of Destination in Absence of Hostile Jamming

In the absence of hostile jammers, the received signal at the n^{th} destination is given by,

$$y_{D_n} = h_n x_S + n_D. \tag{4.6}$$

The notations have usual meaning defined in Table 2 and Section 4.2. We assume that all the destination nodes have same noise variance. Following [39], the ergodic capacity for the n^{th} destination without hostile jammers can be derived as,

$$\begin{aligned}
R_{SD_{n,NoHJ}} &= \mathbb{E}_{h_n, r_{d_n}} \left\{ \log_2 \left(1 + \frac{P_S |h_n|^2}{r_{d_n}^{\alpha} N_{0D}} \right) \right\} \\
&= \mathbb{E}_{r_{d_n}} \left\{ \int_0^{\infty} \log_2 \left(1 + \frac{P_S x}{r_{e1}^{\alpha} N_{0D}} \right) \frac{e^{-\frac{x}{\Lambda_{SD}}}}{\Lambda_{SD}} dx \right\} \\
&= \int_0^{\infty} \int_0^{\infty} \log_2 \left(1 + \frac{P_S x}{y^{\alpha} N_{0D}} \right) \frac{e^{-\frac{x}{\Lambda_{SD}}}}{\Lambda_{SD}} \times 2\pi\lambda_D y \exp(-\pi\lambda_D y^2) \frac{(\pi\lambda_D y^2)^{n-1}}{(n-1)!} dx dy \\
&= \frac{2(\pi\lambda_D)^n}{\ln 2 (n-1)!} \int_0^{\infty} \exp \left\{ \frac{y^{\alpha} N_{0D}}{\Lambda_{SD} P_S} - \pi\lambda_D y^2 \right\} y^{(2n-1)} \times \mathcal{E}_1 \left(\frac{y^{\alpha} N_{0D}}{\Lambda_{SD} P_S} \right) dy.
\end{aligned} \tag{4.7}$$

The first equality of (4.7) comes from the definition of secrecy capacity. The second and third equalities follow the probability density functions (PDFs) of Rayleigh fading in $S - D_n$ link and the destination between S and D_n, respectively. The outcome of

integration with respect to x is found by [99, Eq. 4.337] where, $\mathcal{E}_1(x) = \int_x^\infty \frac{e^{-t}}{t} dt$ is the exponential integral function.

4.2.2 Impact of Hostile Jamming on the Capacity of the Destination

For some eavesdroppers, the link between the source and an eavesdropper is not strong enough for eavesdropping. In such case, they will rather switch to jamming the destination due to their adaptive nature. This hostile jamming will affect the achievable capacity at the destination. According to [103] and [39], the lower order statistics of the interference, such as expectation and variance, have more impact on SINR than the higher order ones. This helps us to model the interference from the hostile jammers by PPP. Keeping that in mind we derive the expression for ergodic capacity at the n^{th} destination as shown below.

The received signal at the n^{th} destination while being jammed by k^{th} eavesdropper is given as,

$$y_{D_n} = h_n x_S + f_{k,n} x_E + n_D. \tag{4.8}$$

The ergodic capacity is then derived as,

$$R_{SD_{n,HJ}} = \mathbb{E}_{h_n, r_{d_n,k}, f_{k,n}} \left\{ \log_2 \left(1 + \frac{P_S |h_n|^2 r_{d_n}^{-\alpha}}{N_{0D} + \sum\limits_{E_k \in \Phi_H} P_E |f_{k,n}|^2 r_{d_n,k}^{-\alpha}} \right) \right\} \tag{4.9}$$

The SINR at the n^{th} destination can be written as,

$$\gamma_{SD_n} = \frac{P_S |h_n|^2 r_{d_n}^{-\alpha}}{N_{0D} + \sum\limits_{E_k \in \Phi_H} P_E |f_{k,n}|^2 r_{d_n,k}^{-\alpha}} = \frac{S_{SD_n}}{N_{0D} + I_{ED_n}}. \tag{4.10}$$

Assuming noise is dominated by the interference, the success probability of transmission from source to destination D_n can be given by,

$$\begin{aligned} Pr(\gamma_{SD_n} > \tau) &= Pr(S_{SD_n} > \tau I_{ED_n}) \\ &= Pr\left(|h_n|^2 > \tau I_{ED_n} P_S^{-1} r_{d_n}^{\alpha} \right) \\ &\overset{(a)}{=} \mathbb{E}_{I_{ED_n}} \left(\exp\left(-\frac{\tau I_{ED_n} P_S^{-1} r_{d_n}^{\alpha}}{\Lambda_{SD}} \right) \right) \\ &\overset{(b)}{=} \mathcal{L}_{I_{ED_n}} \left(\frac{\tau}{\Lambda_{SD} P_S r_{d_n}^{-\alpha}} \right). \end{aligned} \tag{4.11}$$

Since the S-D link is assumed to have Rayleigh fading, (a) follows from the exponential distribution for $|h_n|^2$, and (b) follows the definition of the Laplace transformation. The cumulative distribution function (CDF) of the SINR will be,

$$\begin{aligned} F_{\gamma_{SD_n}} = Pr(\gamma_{SD_n} \leq \tau) &= 1 - Pr(\gamma_{SD_n} > \tau) \\ &= 1 - \mathcal{L}_{I_{ED_n}}\left(\frac{\tau}{\Lambda_{SD} P_S r_{d_n}^{-\alpha}}\right). \end{aligned}$$

Let, $s = \frac{\tau}{\Lambda_{SD} P_S r_{d_n}^{-\alpha}}$. Then,

$$\begin{aligned} &\mathcal{L}_{I_{ED_n}}(s) = \mathbb{E}_{I_{ED_n}}\left(\exp\left(-sI_{ED_n}\right)\right) \\ &= \mathbb{E}_{I_{ED_n}}\left(\exp\left(-s\sum_{E_k \in \Phi_H} P_E |f_{k,n}|^2 r_{d_n,k}^{-\alpha}\right)\right) \\ &= \mathbb{E}_{\Phi_H}\left(\prod_{E_k \in \Phi_H} \mathbb{E}_{f_{k,n}}\left(\exp\left(-sP_E |f_{k,n}|^2 r_{d_n,k}^{-\alpha}\right)\right)\right) \\ &\overset{(c)}{=} \exp\left(-2\pi\lambda_H \int_0^\infty \left[1 - \mathbb{E}_{f_{k,n}}\left(\exp\left(-sP_E |f_{k,n}|^2 z^{-\alpha}\right)\right)\right] z dz\right) \\ &= \exp\left(-2\pi\lambda_H \int_0^\infty \left[1 - \frac{1}{1 + s\Lambda_{ED} P_E z^{-\alpha}}\right] z dz\right), \end{aligned} \tag{4.12}$$

where, (c) follows the probability generating functional of the PPP [39, 91], and (4.12) is due to the Rayleigh fading assumption of the interference channel.

Let, $t = (s\Lambda_{ED} P_E)^{-\frac{2}{\alpha}} z^2$ and $M_D = \pi\lambda_H \left(\frac{\Lambda_{ED} P_E}{\Lambda_{SD} P_S}\right)^\delta \Gamma(1+\delta)\Gamma(1-\delta)$. From (4.12), we get

$$\begin{aligned} \mathcal{L}_{I_{ED_n}}(s) &= \exp\left(-2\pi\lambda_H \int_0^\infty \left[1 - \frac{1}{1 + t^{-\frac{\alpha}{2}}}\right] \frac{1}{2} (s\Lambda_{ED} P_E)^{\frac{2}{\alpha}} dt\right) \\ &= \exp\left(-\pi\lambda_H (s\Lambda_{ED} P_E)^{\frac{2}{\alpha}} \int_0^\infty \left[\frac{1}{1 + t^{\frac{\alpha}{2}}}\right] dt\right) \\ &\overset{(e)}{=} \exp\left(-\pi\lambda_H (s\Lambda_{ED} P_E)^{\delta} \Gamma(1+\delta)\Gamma(1-\delta)\right) \\ &= \exp(-M_D r_{d_n}^2 \tau^\delta), \end{aligned} \tag{4.13}$$

where (e) is obtained from the mathematical manipulation given at the top of page 64, the last two equalities of which come from [99, Eq. 8.384] and [99, Eq. 8.331.1], respectively.

$$
\begin{aligned}
\text{Let,}\quad I &= \int_0^{\infty}\left[\frac{1}{1+t^{\frac{\alpha}{2}}}\right]dt \\
&= \int_1^{0} x\left[-\frac{1}{x^2}\times\frac{1}{nt^{n-1}}\right]dx \quad \left[\text{where, } x=\frac{1}{t^n+1} \text{ and } n=\frac{1}{\delta}\right] \\
&= \frac{1}{n}\int_0^{1}\frac{1}{x}\times\frac{t}{t^n}dx = \frac{1}{n}\int_0^{1}(1-x)^{\frac{1}{n}-1}x^{(1-\frac{1}{n})-1}dx \\
&= \frac{1}{n}B\left[\frac{1}{n},1-\frac{1}{n}\right] \qquad \text{[From definition of Beta function]} \\
&= \delta B\left[\delta,1-\delta\right] \\
&= \delta\Gamma(\delta)\Gamma(1-\delta) = \Gamma(1+\delta)\Gamma(1-\delta).
\end{aligned}
$$

Substituting (4.13) into (4.9) we get (4.14), where the second equality comes from the CDF of the SINR and the fifth equality is because we let $\tau = s\Lambda_{SD}P_S r_{d_n}^{-\alpha}$.

$$
\begin{aligned}
R_{SD_{n,HJ}} &= \int_0^{\infty}\int_0^{\infty}\log_2(1+\tau)f_{\gamma_{SD_n}}(\tau)f_{r_{d_n}}(x)d\tau dx \\
&= \frac{1}{\ln 2}\int_0^{\infty}\int_0^{\infty}\ln(1+\tau)d\left[1-\mathcal{L}_{I_{ED_n}}\left(\frac{\tau}{\Lambda_{SD}P_S r_{d_n}^{-\alpha}}\right)\right]f_{r_{d_n}}(x)dx \\
&= \int_0^{\infty}\Bigg[-\frac{1}{\ln 2}\ln(1+\tau)\mathcal{L}_{I_{ED_n}}\left(\frac{\tau}{\Lambda_{SD}P_S r_{d_n}^{-\alpha}}\right)\Bigg|_0^{\infty} \\
&\quad +\frac{1}{\ln 2}\int_0^{\infty}\mathcal{L}_{I_{ED_n}}\left(\frac{\tau}{\Lambda_{SD}P_S r_{d_n}^{-\alpha}}\right)\frac{1}{1+\tau}d\tau\Bigg]f_{r_{d_n}}(x)dx \\
&= \int_0^{\infty}\left[\frac{1}{\ln 2}\int_0^{\infty}\mathcal{L}_{I_{ED_n}}\left(\frac{\tau}{\Lambda_{SD}P_S r_{d_n}^{-\alpha}}\right)\frac{1}{1+\tau}d\tau\right]f_{r_{d_n}}(x)dx \\
&= \int_0^{\infty}\left[\frac{1}{\ln 2}\int_0^{\infty}\exp\left(-M_D r_{d_n}^2\tau^{\delta}\right)\frac{1}{1+\tau}d\tau\right]f_{r_{d_n}}(x)dx \\
&= \frac{2\pi\lambda_D}{\ln 2}\int_0^{\infty}\left[\int_0^{\infty}\frac{(\pi\lambda_D x^2)^{n-1}}{(n-1)!}\exp\left\{-x^2(M_D\tau^{\delta}+\pi\lambda_D)\right\}\frac{x}{1+\tau}dx\right]d\tau \\
&= \frac{2(\pi\lambda_D)^n}{\ln 2(n-1)!}\int_0^{\infty}\left[\int_0^{\infty}\exp\left\{-x^2(M_D\tau^{\delta}+\pi\lambda_D)\right\}\frac{x^{2n-1}}{1+\tau}dx\right]d\tau \\
&= \frac{(\pi\lambda_D)^n}{\ln 2}\int_0^{\infty}\frac{1}{(1+\tau)(M_D\tau^{\delta}+\pi\lambda_D)^n}d\tau. \qquad (4.14)
\end{aligned}
$$

The first equality of (4.14) comes from the expected values of the success probability variable τ and the distance between S and D_n. The second equality is from the CDF of the SINR. The following steps are derived from the rules of integration and substitution of $\mathcal{L}_{I_{ED_n}}(s)$ from (4.13) with $s = \frac{\tau}{\Lambda_{SD} P_S r_{d_n}^{-\alpha}}$ as discussed above. The sixth equality follows the expression of the PDF of distance between S and D_n. The ergodic capacity in (4.14) can be calculated using numerical integration.

4.2.3 Main Channel Capacity

The main channel capacity can be derived as follows,

$$C_{main} = \min_{D_n \in \Phi_D} R_{SD_n}, \tag{4.15}$$

where R_{SD_n} is derived in (4.7) and (4.14) in specific cases.

4.2.4 Worst-case Eavesdropper's Capacity

We consider the nearest eavesdropper outside the zone, E_1 as the worst-case eavesdropper, as it is likely to be in the best position to eavesdrop effectively due to its closeness to the source. We also assume that the eavesdroppers are capable of decoding the hostile jamming from other eavesdroppers which is possible if they are collaborating with each other.

4.2.4.1 In absence of friendly jammers

In the absence of friendly jammers, the received signal at the worst-case eavesdropper will be,

$$y_{E_1} = g_1 x_S + n_E. \tag{4.16}$$

Following [39], the ergodic capacity for the worst-case eavesdropper can be derived as follows,

$$
\begin{aligned}
R_{SE_{1,NoFJ}} &= \mathbb{E}_{g_1,r_{e1}}\left\{\log_2\left(1+\frac{P_S|g_1|^2}{r_{e1}^{\alpha}N_{0E}}\right)\right\}\\
&= \mathbb{E}_{r_{e1}}\left\{\int_{\eta}^{\infty}\log_2\left(1+\frac{P_S x}{r_{e1}^{\alpha}N_{0E}}\right)f_{|g_1|^2}(x)dx\right\}\\
&= \int_{r_z}^{\infty}\int_{\eta}^{\infty}\log_2\left(1+\frac{P_S x}{y^{\alpha}N_{0E}}\right)\frac{e^{-\frac{x}{\Lambda_{SE}}}}{\Lambda_{SE}}\times 2\pi\lambda_E\exp\left[-\pi\lambda_E(y^2-r_z^2)\right]ydxdy\\
&= \int_{r_z}^{\infty}\left[\frac{1}{\ln 2}\left\{e^{-\frac{\eta}{\Lambda_{SE}}}\ln\left(\frac{P_S\eta}{y^{\alpha}N_{0E}}+1\right)+\exp\left(\frac{y^{\alpha}N_{0E}}{P_S\Lambda_{SE}}\right)E_1\left(\frac{P_S\eta+y^{\alpha}N_{0E}}{P_S\Lambda_{SE}}\right)\right\}\right]\\
&\times 2\pi\lambda_E\exp\left[-\pi\lambda_E(y^2-r_z^2)\right]ydy.\\
&= \frac{2\pi\lambda_E\exp\left(\pi\lambda_E r_z^2\right)}{\ln 2}\int_{r_z}^{\infty}\left\{e^{-\frac{\eta}{\Lambda_{SE}}}\ln\left(\frac{P_S\eta}{y^{\alpha}N_{0E}}+1\right)+\exp\left(\frac{y^{\alpha}N_{0E}}{P_S\Lambda_{SE}}\right)\right.\\
&\left.\times\mathcal{E}_1\left(\frac{P_S\eta+y^{\alpha}N_{0E}}{P_S\Lambda_{SE}}\right)\right\}y\exp\left(-\pi\lambda_E y^2\right)dy. \qquad (4.17)
\end{aligned}
$$

where, r_{e1} is the distance of the eavesdropper from the source and η is the threshold to indicate that the link between the source and the eavesdropper is strong enough for eavesdropping. The third equality uses the expressions of the PDFs of the Rayleigh fading of the channel between S and E_1, and the distance between them to obtain the expected values. The PDF of the distance between S and E_1 follows (4.4). Again, in the last equality $\mathcal{E}_1(x)=\int_x^{\infty}\frac{e^{-t}}{t}dt$ is the exponential integral function.

4.2.4.2 In presence of friendly jammers

The received signal and SINR at the worst-case eavesdropper while being jammed by ℓ^{th} friendly jammer can be written respectively as,

$$y_{E_1} = g_1 x_S + j_{\ell 1}x_J + n_E, \qquad (4.18)$$

and

$$\gamma_{SE} = \frac{P_S|g_1|^2 r_{e1}^{-\alpha}}{N_{0E}+\sum\limits_{J_\ell\in\Phi_J}P_J|j_{\ell 1}|^2 r_{\ell,e1}^{-\alpha}} = \frac{S_{SE}}{N_{0E}+I_{JE}}. \qquad (4.19)$$

Assuming noise is dominated by the interference, the success probability of transmission from source to E_1 (or eavesdropping by E_1) can be given by following the manipulation

in (4.11),

$$\begin{aligned} Pr(\gamma_{SE} > \tau) &= Pr\left(|g_1|^2 > \tau I_{JE} P_S^{-1} r_{e1}^{\alpha}\right) \\ &= \mathbb{E}_{I_{JE}}\left(\exp\left(-\frac{\tau I_{JE} P_S^{-1} r_{e1}^{\alpha}}{\Lambda_{SE}}\right)\right) \\ &= \mathcal{L}_{I_{JE}}\left(\frac{\tau}{\Lambda_{SE} P_S r_{e1}^{-\alpha}}\right). \end{aligned} \tag{4.20}$$

Following (4.13) we have,

$$\begin{aligned} \mathcal{L}_{I_{JE}}(s) &= \exp\left(-\pi\lambda_J (s\Lambda_{JE} P_J)^{\delta}\Gamma(1+\delta)\Gamma(1-\delta)\right) \\ \Rightarrow \mathcal{L}_{I_{JE}}\left(\frac{\tau}{\Lambda_{SE} P_S r_{e1}^{-\alpha}}\right) &= \exp\left(-\pi\lambda_J \left(\frac{\Lambda_{JE} P_J}{\Lambda_{SE} P_S}\right)^{\delta}\right. \\ &\quad \left.\times\Gamma(1+\delta)\Gamma(1-\delta)\tau^{\delta} r_{e1}^2\right) \\ &= \exp\left(-M_E r_{e1}^2 \tau^{\delta}\right), \end{aligned}$$

where, $M_E = \pi\lambda_J \left(\frac{\Lambda_{JE} P_J}{\Lambda_{SE} P_S}\right)^{\delta} \Gamma(1+\delta)\Gamma(1-\delta)$. Therefore, following (4.14), the ergodic capacity at the worst-case eavesdropper, regardless of the strength of S-E link can be written as (4.21) as follows,

$$\begin{aligned} R_{SE_{1,FJ}} &= \int_{r_z}^{\infty}\int_{0}^{\infty} \log_2(1+\tau) f_{\gamma_{SE}}(\tau) f_{re1}(x) d\tau dx \\ &= \frac{1}{\ln 2}\int_{r_z}^{\infty}\int_{0}^{\infty} \ln(1+\tau) d\left[1 - \mathcal{L}_{I_{JE}}\left(\frac{\tau}{\Lambda_{SE} P_S r_{e1}^{-\alpha}}\right)\right] f_{re1}(x) dx \\ &= \int_{r_z}^{\infty}\left[\frac{1}{\ln 2}\int_{0}^{\infty} \mathcal{L}_{I_{JE}}\left(\frac{\tau}{\Lambda_{SE} P_S r_{e1}^{-\alpha}}\right)\frac{1}{1+\tau} d\tau\right] f_{re1}(x) dx \\ &= \int_{r_z}^{\infty}\left[\frac{1}{\ln 2}\int_{0}^{\infty} \exp\left(-M_E r_{e1}^2 \tau^{\delta}\right)\frac{1}{1+\tau} d\tau\right] f_{re1}(x) dx \\ &= \frac{2\pi\lambda_E \exp(\pi\lambda_E r_z^2)}{\ln 2}\int_{0}^{\infty}\left[\int_{r_z}^{\infty} \exp\left\{-x^2(M_E\tau^{\delta} + \pi\lambda_E)\right\}\frac{x}{1+\tau} dx\right] d\tau \\ &= \frac{2\pi\lambda_E \exp(\pi\lambda_E r_z^2)}{\ln 2}\int_{0}^{\infty}\left[\frac{\exp\{\left(-M_E\tau^{\delta} - \pi\lambda_E\right) r_z^2\}}{2(1+\tau)\left(M_E\tau^{\delta} + \pi\lambda_E\right)}\right] d\tau \\ &= \frac{\pi\lambda_E}{\ln 2}\int_{0}^{\infty}\left[\frac{\exp\{-M_E\tau^{\delta} r_z^2\}}{(1+\tau)\left(M_E\tau^{\delta} + \pi\lambda_E\right)}\right] d\tau. \end{aligned} \tag{4.21}$$

The mathematical manipulations to achieve the ergodic capacity at the worst-case eavesdropper in presence of friendly jammers (in (4.21)) follow the similar steps of deriving the ergodic capacity at D_n in presence of hostile jammers (in (4.14)). In both cases, we derive the ergodic capacity at a particular node affected by aggregated interference from the jammers of opposing party. The derivations deal with corresponding PDFs for channel links and distances among the randomly placed nodes following HPPP.

4.2.5 Secrecy Capacity

The secrecy capacity now can be derived as,

$$C_s = C_{main} - R_{SE_1}, \tag{4.22}$$

where, C_{main} will be obtained by taking the minimum ergodic capacity at destinations using (4.14) or (4.7) in presence or absence of hostile jammers, respectively. On the other hand, R_{SE_1} can be obtained from (4.21) or (4.17) in presence or absence of friendly jammers, respectively.

4.3 Numerical Results

In this section, we illustrate numerical results to depict how the secrecy capacity varies in various scenarios with the absence or presence of friendly jammer and under different channel characteristics. The parameters and channel characteristics we used to obtain simulation results are as follows. We considered $N_{0R} = N_{0D} = N_{0E} = 1$. The ratio of average main channel gain to average eavesdropper channel gain is denoted by MER= $\frac{\Lambda_{SD}}{\Lambda_{SE}}$, where $\Lambda_{SD} = 1$ and $\Lambda_{SE} = \text{MER}^{-1}$. This criteria is set to simulate the variations in SNR strengths in the eavesdropping links [21]. The mean of SNR threshold is chosen as $\eta = MER^{-1}$. We also considered $\Lambda_{ED} = 1$ which represents one worst-case scenario that the link between the hostile jammers and the destinations are strong. On the other hand, to simulate proper beamforming by the friendly jammers we considered $\Lambda_{JE} = 1$. The intensity of total eavesdropping nodes, λ_{Eve}, is considered throughout the simulation to be $0.01/km^2$.

4.3.1 In the absence of both hostile and friendly jammers

Fig. 4.2 shows the impact of growing passive eavesdroppers' intensity on the secrecy capacity. As the intensity of passive eavesdroppers increases the secrecy capacity decreases. Also, Table 4.2 shows that if the intensity of destinations decreases to a lower

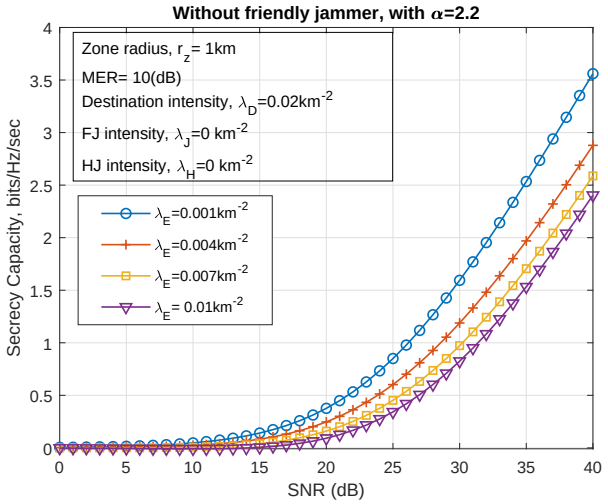


FIGURE 4.2: Impact of different node intensities of passive eavesdroppers on secrecy capacity.

value the secrecy may be compromised. This figure echoes with [39] that if the destination nodes have lower intensity than that of the eavesdroppers then secrecy will be compromised unless we employ a secrecy protected zone and/or the eavesdroppers have weaker channel. In our model we have included both a secrecy protected zone and MER to mitigate this problem. However, for a small zone and small MER, we cannot achieve higher secrecy capacity as shown by Fig. 4.2 and Table 4.2. In this scenario employing friendly jammers will be helpful as discussed in the following subsections.

TABLE 4.2: Impact of varying λ_D on secrecy capacity with $\lambda_E = 0.001km^{-2}$.

SNR (dB)	Secrecy Capacity (bits/Hz/Sec)	
	$\lambda_D = 0.02km^{-2}$	$\lambda_D = 0.006km^{-2}$
15	0.1411	0.01913
25	0.8501	0.2217
35	2.534	1.13

4.3.2 Impact of hostile jammers on main channel capacity

Passive eavesdropping degrades the secrecy capacity but does not affect the main channel capacity. However, the hostile jamming inserts interference in the destinations' channel thus lowering it down. Fig. 4.3 shows the degradation in main channel capacity due increase in hostile jammers' intensity.

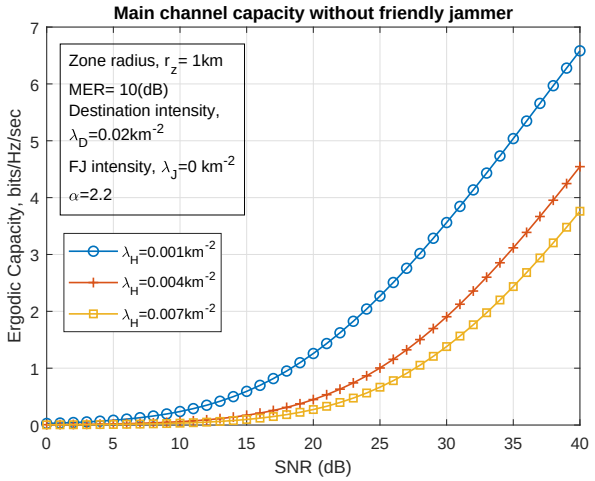


FIGURE 4.3: Impact of hostile jamming on main channel capacity.

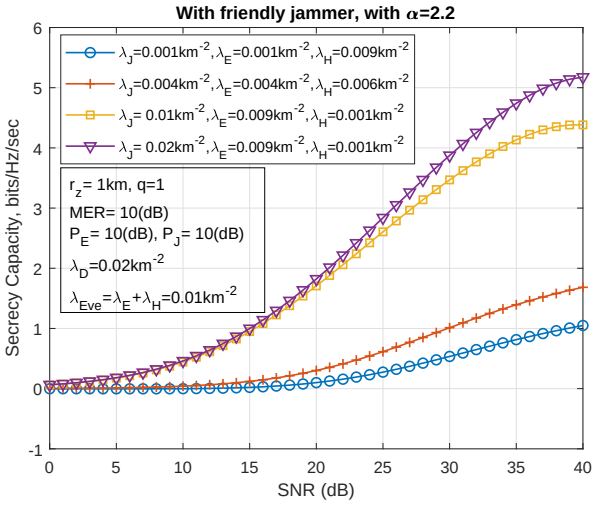


FIGURE 4.4: Impact of friendly jammers on secrecy capacity.

4.3.3 Impact of friendly jammers on secrecy capacity

Fig. 4.4 and Table 4.3 show the impact of friendly jammers on the secrecy capacity. We can see that as the intensity of friendly jammers increases more hostile jammers become passive eavesdroppers. However, forcing all the hostile jammers into the reception mode may not be practical so we assigned the lowest possible hostile jamming intensity to $0.001/km^2$. In this framework, we employ the following factors. At the beginning the estimated intensity of the friendly jammers is $0.001/km^2$. As the intensity of the friendly jammers starts to increase more hostile jammers become passive eavesdroppers until it hits the lowest value as discussed above. We model the change in eavesdropping node

intensities according to the following relations,

$$\lambda_E^{old} + \lambda_H^{old} = \lambda_E^{new} + \lambda_H^{new} = \lambda_{Eve} \tag{4.23a}$$

$$\lambda_H^{new} = \lambda_H^{old} - q \times \lambda_J. \tag{4.23b}$$

$$\text{If} \quad \lambda_H^{new} \leq \lambda_H^{old} - q \times \lambda_J$$

$$\lambda_H^{new} = 0.001, \tag{4.23c}$$

where q is a positive real number introduced to control the relationship between λ_H and λ_J. With every new value of λ_J, a new set of λ_E and λ_H are calculated using (4.23). Throughout this chapter we consider $q = 1$ unless stated otherwise.

TABLE 4.3: Impact of varying λ_D on secrecy capacity for $\lambda_J = 0.01km^{-2}$ and $\lambda_J = 0.004km^{-2}$ with corresponding parameter sets from Fig. 4.4.

SNR (dB)	Secrecy Capacity (bits/Hz/Sec)			
	$\lambda_J = 0.01km^{-2}$		$\lambda_J = 0.004km^{-2}$	
	$\lambda_D = 0.02km^{-2}$	$\lambda_D = 0.006km^{-2}$	$\lambda_D = 0.02km^{-2}$	$\lambda_D = 0.006km^{-2}$
15	0.9492	0.319	0.1202	0
25	2.606	1.231	0.6901	0
35	4.132	2.378	1.394	0

Both Fig. 4.4 and Table 4.3 show that at the beginning when the friendly jammers had a very low intensity they could not enhance the secrecy very much. Every time, the hostile jammers jam the destinations, the eavesdropper's capacity is deducted from the main channel capacity. Therefore, the intensity of the friendly jammers needs a rise from the early value. The deceptive friendly jammers are forcing some of the hostile jammers to be passive eavesdroppers. At the same time, the friendly jamming causes interference at the eavesdroppers. As a result, the secrecy capacity is enhanced. We can also draw a comparison between Table 4.3 and Table 4.2 which shows that friendly jammers can provide more secrecy capacity than that of the scenario where friendly jammers are absent.

Now, we observe the degree of improvement in secrecy capacity due to high intensity of FJ nodes for different intensity of destinations. This can be expressed as,

$$\Delta_{v,w} = \frac{|C_{s,v} - C_{s,w}|}{SNR(dB)}, \tag{4.24}$$

where, $C_{s,x}$ represents the secrecy capacity for $\lambda_D = xkm^{-2}$. The following table enlist the degree of improvement for corresponding intensity of friendly jammers. From Table 4.4, we see the degree of improvement with a high λ_J is higher than that with a low λ_J since a higher FJ node intensity is providing higher secrecy capacity. The table also shows that with a higher destination node intensity a low λ_J is still capable to ensure

TABLE 4.4: Observation of the degree of improvement in secrecy capacity due to the FJ intensity with corresponding parameter sets from Table 4.3.

SNR (dB)	$\Delta_{0.02,0.006}$	
	$\lambda_J = 0.01km^{-2}$	$\lambda_J = 0.004km^{-2}$
15	0.042	0.008
25	0.055	0.028
35	0.05	0.0398

a non-zero secrecy capacity. The secrecy capacity rises with an increase in SNR but the rise becomes slower at the higher region of the SNR producing a flatter curve as shown by Fig. 4.4. That is why the degree of improvement achieves a higher value with the increase in SNR ranging between 15 to 25 dB, but becomes almost fixed in the higher ranges of 25 to 35 dB of SNR. We can say that for this setup, for higher ranges of SNR, the degree of improvement per dB of SNR is around 0.05 bits/Hz/sec for $\lambda_J = 0.01km^{-2}$, and around $0.03 - 0.04$ bits/Hz/sec for $\lambda_J = 0.004km^{-2}$.

Therefore, both Tables 4.3 and 4.4 conclude that if the intensity of destinations is higher than that of the eavesdroppers then a non-zero secrecy capacity is possible to achieve even with a low λ_J, and when the intensity of destinations is lower than the total eavesdroppers the secrecy is compromised unless there are sufficient numbers of FJ nodes to tackle the adversaries.

4.3.3.1 With $q < 1$

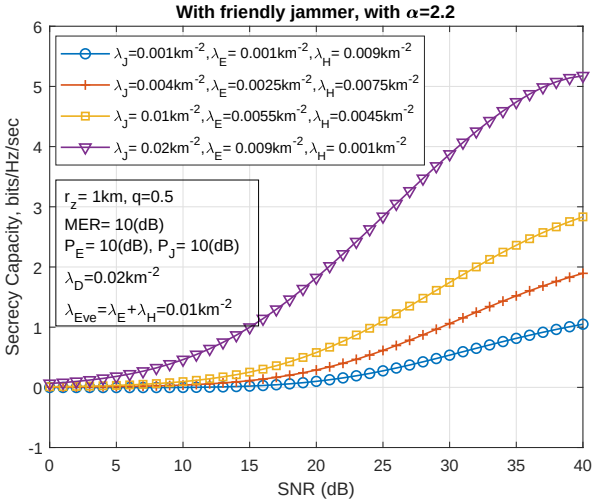


FIGURE 4.5: Impact of lower value of q. Here, $q = 0.5$.

In (4.23), by changing the value of q one can control the success of the friendly jammers in converting the hostile jammers into the passive eavesdroppers. Fig. 4.5 and the

results show that for $q < 1$, obviously we need a larger intensity for friendly jamming nodes to force most of the hostile jammers in their reception mode.

Table 4.5 shows the impact of different values of q on the simulation of secrecy capacity. The table collects data from Fig. 4.4 and 4.5, and also shows the degradation of performance if the value of q is lowered to 0.25. However, we observe that at high node intensities for FJ and destinations, positive secrecy capacity can be guaranteed in case of a moderate value of q.

TABLE 4.5: Impact of varying q on secrecy capacity compared to Fig. 4.4 (case of $q = 1$) with $\lambda_J = 0.01km^{-2}$ and $\lambda_D = 0.02km^{-2}$ at 25 dB SNR.

q	Node Intensities, km^{-2}		Secrecy Capacity (bits/Hz/Sec)
	λ_E	λ_H	
1	0.009	0.001	2.606
0.5	0.0055	0.0045	1.10
0.25	0.00325	0.00675	0.8883

4.3.3.2 With weaker J-E link

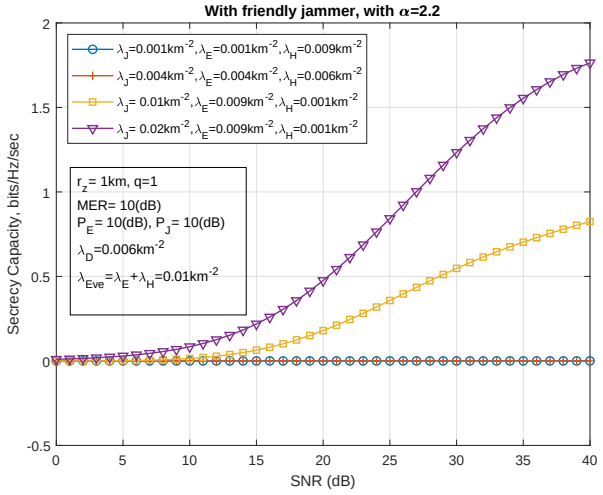
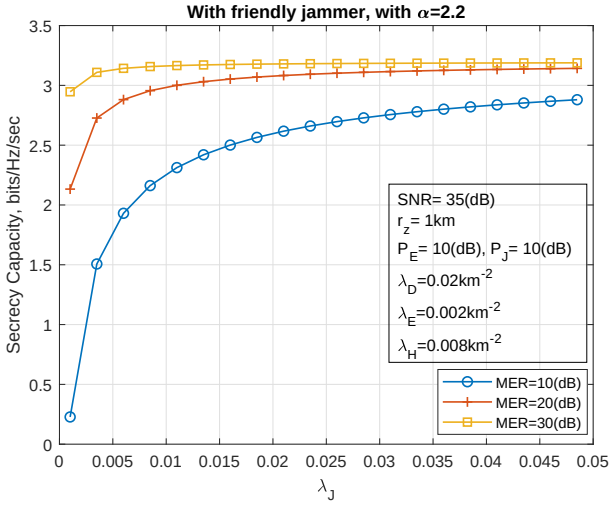


FIGURE 4.6: Impact of weak J-E link. Here, $\lambda_{JE} = 2(MER)^{-1}$.

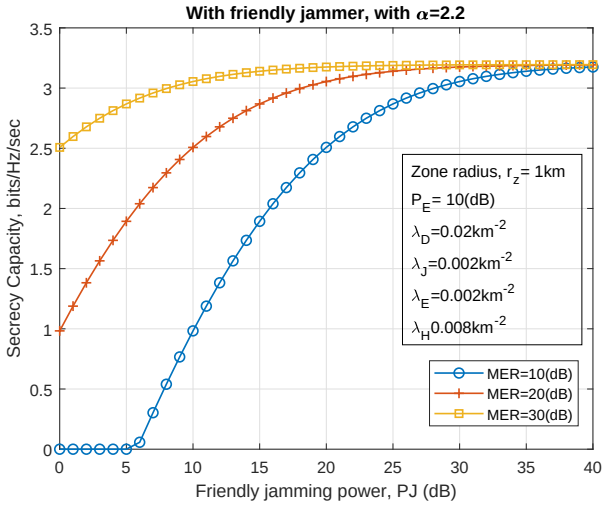
Fig. 4.6 shows that when the destination intensity is lower than that of the eavesdropper, and the channel between friendly jammers and eavesdroppers are not sufficiently strong; the secrecy can be highly compromised. However, with the increase of friendly jammer intensity, this problem can be mitigated.

4.3.3.3 Impact of node intensity and power of friendly jamming

Fig. 4.7(a) and 4.7(b) show that with the increase of intensity of friendly jammer (FJ) nodes or FJ power the secrecy capacity increases as expected. In both scenarios variation in intensity of FJ nodes or the friendly jamming power has no impact on the main channel capacity which stays the same as 3.195 bits/Hz/sec. The worst eavesdroppers capacity



(a) Impact of increasing node intensity of FJ.



(b) Impact of increasing power of FJ.

FIGURE 4.7: Secrecy enhancement with varying FJ parameters.

however tends to decrease because of the increase in λ_J or P_J in corresponding cases thus increasing the secrecy capacity. The figures also show that for a given intensity of adversary nodes, increasing the node intensity or the power of FJ nodes up to a much higher value, causes a stable value for secrecy capacity. In particular, Fig. 4.7(a) shows that as soon as the FJ node intensity becomes equal or more than that of the total

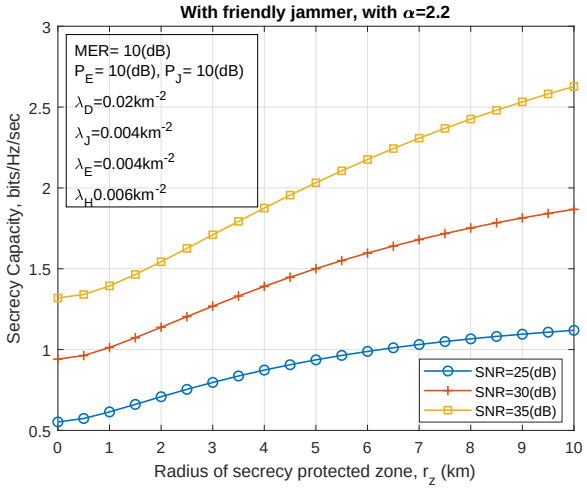
eavesdroppers the secrecy capacity tends to have a more stable value especially for low MERs.

Fig. 4.7(b) shows that increase in P_J increases the secrecy capacity and as obvious with higher MER, the corresponding secrecy capacity is higher. However, around $P_J = 25dB$, all the curves representing different MER scenarios tend to overlap each other giving a stable secrecy capacity. A high MER is definitely beneficial to secrecy performance of the system and our observation states that if the MER is low then the friendly jammers are useful to enhance the system secrecy. From both figures, we can say that a moderate node intensity and jamming power for friendly jammers are sufficient to enhance the secrecy performance of the system.

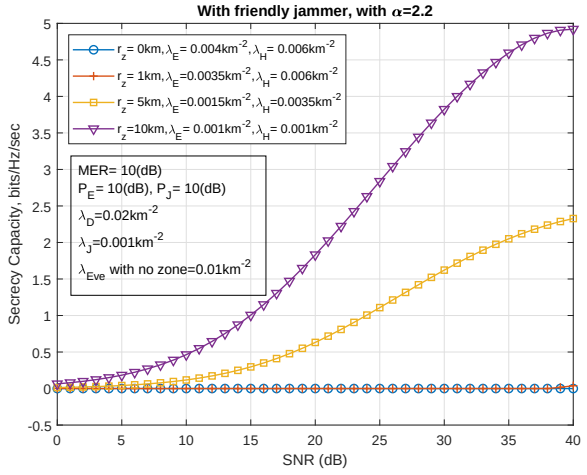
Depending on the situation, a source will hire either more friendly jammers or hire more jamming power from the existing friendly jammers. If the destinations and the eavesdroppers are scattered in a large area, hiring more friendly jammers will be effective to tackle the adaptive eavesdropping. The task of beamforming towards the eavesdroppers will be then shared among the friendly jammers. On the other hand, for a small coverage area, few friendly jammers with high power will be enough. For our model, we have considered that the friendly jammers charge the source for their interference price in currency. Another alternative option is to hire friendly jammers in exchange of energy. The source will decide which type of jammers to hire depending on the available resources. Generally, for small business companies may hire energy harvesting nodes as friendly jammers, on the other hands, military organisations may afford FJ nodes in exchange of money.

4.3.4 Impact of secrecy protected zone

Fig. 4.8(a) shows the impact of a secrecy protected zone. A bigger zone will eliminate more eavesdropping threats resulting in a higher secrecy capacity. However, friendly jammers are still necessary to achieve high secrecy capacity, because having a large secrecy protected zone is not so practical. Also here, we kept the total eavesdroppers' intensity fixed. In practice for immobile nodes, the intensity should decrease because of the expanding secrecy protected zone (Fig. 4.8(b)). That will give more secrecy on the cost of expanding infrastructure and scanning devices. As we can see from Fig. 4.8(b), if the friendly jammers' intensity is negligible a larger secrecy zone can attempt to decrease the eavesdroppers' intensity enough to achieve a desired secrecy capacity.



(a) Considering a fixed eavesdroppers' intensity outside the zone.



(b) Impact of r_z on secrecy capacity following (4.25).

FIGURE 4.8: Impact of secrecy protected zone on secrecy capacity.

For this figure, we consider the following approach,

$$\lambda_E^{old} + \lambda_H^{old} = \lambda_{Eve} \tag{4.25a}$$

$$\lambda_E^{new} = \lambda_E^{old} - 0.0005 \times r_z \tag{4.25b}$$

$$\text{If} \quad r_z \geq 3\,\text{km}$$

$$\lambda_H^{new} = \lambda_H^{old} - 0.0005 \times r_z \tag{4.25c}$$

As secrecy protected zone grows larger and larger, more and more eavesdroppers are being deactivated (reduced by 0.05% of r_z). Since the hostile jammers are located far from the source we assumed that after the zone radius r_z reaches an arbitrary threshold of 3 km, the hostile jammers found to be active. For a zone radius larger than the

threshold, most of the hostile jammers become deactivated by the secrecy protected zone. The threshold of the zone radius can be changed to any value for simulation purposes. The minimum value of the intensity of the hostile jammers or passive eavesdroppers are chosen to be $0.001/km^2$ each considering that zone may not deactivate all the adversaries.

From Fig. 4.8(b) we can conclude that a larger secrecy zone can enhance the secrecy capacity, but if a larger zone is not achievable then hiring friendly jammers is a good alternative as seen by Fig. 4.7.

4.4 Conclusion

In this chapter, we investigated the advantages of using friendly jammers against adaptive eavesdroppers in a random wireless network. Due to the nature of randomness of the HPPP allocations of the eavesdropping nodes and the hostile jammers, the source will suffer lots of overhead for beamforming and jamming. Therefore, hiring deceptive friendly jammers is a good alternative since these nodes are also randomly located following an HPPP, and deceives eavesdroppers into thinking that they are listening to the source. The friendly jammers convert some of the hostile jammers into passive listeners while simultaneously interfering the passive eavesdropping nodes. We derive the expressions of secrecy capacity corresponding to scenarios whether the system has employed friendly jammers or not. Our numerical results show that employment of friendly jammers improves the secrecy of the system. We investigated the secrecy capacity by varying the node intensity of eavesdroppers and other parameters, and every time friendly jammers became advantageous to achieve a non-zero secrecy capacity. The friendly jammers also give better secrecy capacity if the source cannot afford a large secrecy protected zone. Therefore, an optimum choice among secrecy zone radius, intensity of friendly jammer nodes and amount of friendly jamming power can give desired secrecy capacity.

Chapter 5

Friendly Jammers in Random Wireless Network against FD Eavesdroppers

5.1 Overview

We reconsider System model **SM3** now with full-duplex (FD) eavesdroppers instead of adaptive ones. This model is named System model **SM4** in which all the eavesdroppers have double antenna, in that case each eavesdropper acts as an active eavesdropper that can simultaneously listen and jam. In this case, it will be impossible for the friendly jammers to convert the eavesdroppers into passive mode as we can see from a source-based jamming scenario in presence of FD eavesdroppers in [91]. However, the eavesdroppers will still face interference due to the friendly jamming. Our target is to deceive the eavesdroppers by the source-like jamming signals so that they do not try to remove the friendly jamming from their received signals thus suffer from interference instead. We consider that the eavesdroppers have only two antennas and are busy with simultaneous reception and jamming. We assume that the eavesdroppers do not use both the antennas for reception as a means to remove the friendly jamming. There are two reasons behind this assumption. Firstly, the deceptive nature of the friendly jammers keeps them undetected by the eavesdroppers [81]. Secondly, in real world it is not easy to remove a jamming signal perfectly due to imperfect antenna alignments, imperfect alignment of the jamming signals from the friendly jammers and uncorrelated noise received by the eavesdropping antennas [77].

5.1.1 System Model and Problem Formulation

We revisit the random wireless network in **SM3**, and this time all the eavesdroppers are active, i.e., full-duplex (FD) in nature (Fig. 5.1). Each eavesdropper is equipped with $n_E \geq 2$ antennas. The FD nature allows the eavesdroppers to be passive listeners and hostile jammers at the same time. For a worse-case scenario, we considered that the eavesdroppers are capable of cancelling their self-interference (SI) and also that every eavesdropper are unaffected by other eavesdroppers' jamming.

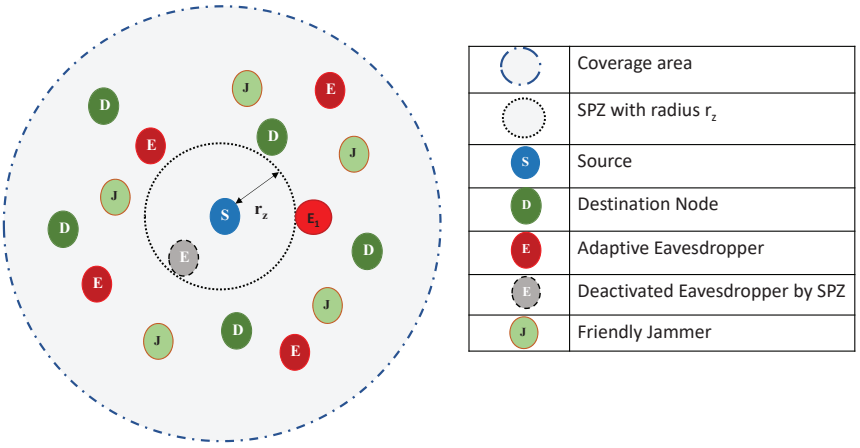


FIGURE 5.1: Random wireless network with secrecy protected zone in presence of FD eavesdroppers.

We derive the secrecy capacity for this model. The following sections deal with the derivation of the secrecy capacity and the simulation to observe the advantage of using friendly jammers in this scenario.

5.2 Secrecy Capacity

The derivations for the expressions of ergodic capacities follow the similar manipulations given in Chapter 4. While deriving the secrecy capacity we consider the presence of both hostile and friendly jammers.

5.2.1 Ergodic Capacity at Destination

We derive the ergodic capacity at n^{th} destination while being jammed by the k^{th} eavesdropper as given by,

$$R_{SD_n} = \mathbb{E}_{h_n, r_{d_n,k}, f_{k,n}} \left\{ \log_2 \left(1 + \frac{P_S |h_n|^2 r_{d_n}^{-\alpha}}{N_{0D} + \sum\limits_{E_k \in \Phi_H} P_E \frac{||\mathbf{f}_{k,n}||^2}{n_E} r_{d_n,k}^{-\alpha}} \right) \right\}, \tag{5.1}$$

where, $\mathbf{f}_{k,n}$ is the channel coefficient vector of the $E_k - D_n$. Assuming noise is dominated by the interference, the success probability of transmission from source to destination D_n can be given by,

$$Pr(\gamma_{SD_n} > \tau) = \mathcal{L}_{I_{ED_n}} \left(\frac{\tau}{\Lambda_{SD} P_S r_{d_n}^{-\alpha}} \right).$$

Let, $s = \frac{\tau}{\Lambda_{SD} P_S r_{d_n}^{-\alpha}}$. Then,

$$\begin{aligned}
&\mathcal{L}_{I_{ED_n}}(s) = \mathbb{E}_{I_{ED_n}} \left(\exp\left(-s I_{ED_n} \right) \right) \\
&= \mathbb{E}_{I_{ED_n}} \left(\exp\left(-s \sum_{E_k \in \Phi_H} P_E \frac{\|f_{k,n}\|^2}{n_E} r_{d_n,k}^{-\alpha} \right) \right) \\
&= \exp\left(-2\pi\lambda_H \int_0^\infty \left[1 - \mathbb{E}_{f_{k,n}} \left(\exp\left(-s P_E \|f_{k,n}\|^2 z^{-\alpha} \right) \right) \right] z dz \right) \\
&= \exp\left(-2\pi\lambda_H \int_0^\infty \left[1 - \frac{1}{(1 + s\Lambda_{ED} \frac{P_E}{n_E} z^{-\alpha})^{n_E}} \right] z dz \right),
\end{aligned} \tag{5.2}$$

where, the last equality follows the exponential distribution of Rayleigh fading channel and the utilisation of [99, Eq. 3.326.2[10]]. Using (5.2) into (5.1), we have,

$$R_{SD_n} = \frac{(\pi\lambda_D)^n}{\ln 2} \int_0^\infty \frac{1}{(1+\tau)(M_D \tau^\delta + \pi\lambda_D)^n} d\tau, \tag{5.3}$$

where, $M_D = \pi\lambda_H \left(\frac{\Lambda_{ED} P_E}{\Lambda_{SD} P_S n_E} \right)^\delta I_1$ with $I_1 = \int_0^\infty \left[1 - \frac{1}{(1+t^{-\frac{1}{\delta}})^{n_E}} \right] dt$ and $t = \left(s \frac{\Lambda_{ED} P_E}{n_E} \right)^\delta z^2$, where the pdf of the distance between the destination and eavesdropper, r_{d_n} is considered to be a function of z.

The main channel capacity can be derived as follows,

$$C_{main} = \min_{D_n \in \Phi_D} R_{SD_n}, \tag{5.4}$$

5.2.2 Ergodic Capacity at Worst-case Eavesdropper

Following the similar techniques as described for (5.3), ergodic capacity at the worst-case eavesdropper while being jammed by the ℓ^{th} friendly jammer is given by

$$R_{SE_1} = \mathbb{E}_{g_1, r_{e1}, j_{\ell,1}}\left\{\log_2\left(1 + \frac{P_S\|g_1\|^2 r_{e1}^{-\alpha}}{N_{0E} + \sum\limits_{J_\ell \in \Phi_J} P_J\|j_{\ell 1}\|^2 r_{\ell,e1}^{-\alpha}}\right)\right\}$$
$$= \frac{\pi\lambda_E}{\ln 2}\int_0^\infty \left[\frac{\exp\{-M_E\tau^\delta r_z^2\}}{(1+\tau)\left(M_E\tau^\delta + \pi\lambda_E\right)}\right] d\tau, \tag{5.5}$$

where, $M_E = \pi\lambda_J\left(\frac{\Lambda_{JE}P_J}{\Lambda_{SE}P_S}\right)^\delta I_2$ with $I_2 = \int_0^\infty \left[1 - \frac{1}{(1+t^{-\frac{1}{\delta}})^{n_E}}\right] dt$.

5.2.3 Secrecy Capacity

The secrecy capacity can be derived form the subtraction of (5.5) from (5.4). Therefore, the secrecy capacity is as follows,

$$C_s = \left[\min_{D_n \in \Phi_D}\left(\frac{(\pi\lambda_D)^n}{\ln 2}\int_0^\infty \frac{1}{(1+\tau)(M_D\tau^\delta + \pi\lambda_D)^n} d\tau\right) - \frac{\pi\lambda_E}{\ln 2}\int_0^\infty \frac{\exp\{-M_E\tau^\delta r_z^2\}}{(1+\tau)\left(M_E\tau^\delta + \pi\lambda_E\right)} d\tau\right]^+. \tag{5.6}$$

The secrecy capacity in (5.6) can be calculated with the help of numerical integration.

5.3 Numerical Results

The parameters and channel characteristics we used for the computational results are chosen as same in Chapter 4. We consider $N_{0D} = N_{0E} = 1$. The ratio of average main channel gain to average eavesdropper channel gain is again denoted by MER= $\frac{\Lambda_{SD}}{\Lambda_{SE}}$ where, $\Lambda_{SD} = 1$ and $\Lambda_{SE} = \text{MER}^{-1}$. There is no SNR threshold, η to be considered as the eavesdroppers do not depend on the channel conditions for jamming. $\Lambda_{ED} = 1$ is consider to represent strong hostile jamming link between any pair of E and D which is a worst-case scenario for destinations' point of view. On the other hand, to simulate proper beamforming by the friendly jammers we considered $\Lambda_{JE} = 1$. The intensity of total eavesdropping nodes, λ_{Eve}, is considered throughout the simulation to be $0.01/km^2$. For FD eavesdropping case, both λ_E and λ_H have the same value as λ_{Eve}.

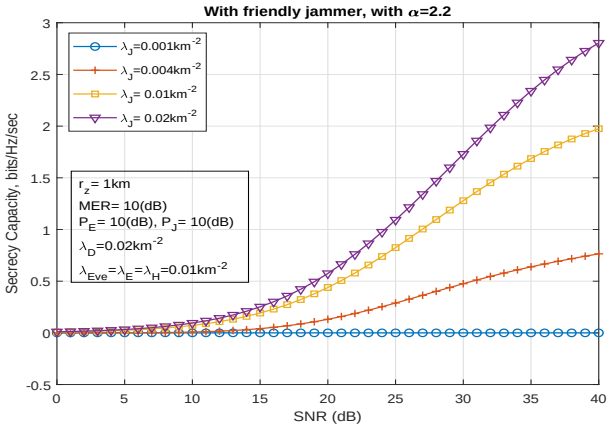


FIGURE 5.2: Impact of FD eavesdroppers on secrecy capacity.

5.3.1 Impact of Friendly Jammers

Fig. 5.2 shows that with the increasing intensity of the friendly jamming nodes the secrecy capacity is rising. Since the hostile jamming is not affected by the friendly jamming the secrecy capacity is found to be lower than that of the adaptive eavesdropper case.

A comparison is drawn between the setups for Fig. 4.4 and Fig. 5.2 representing adaptive (HD) and active (FD) eavesdroppers' impacts on the secrecy capacity, C_s, respectively in Table 5.1.

TABLE 5.1: Comparison between the setups for Fig. 4.4 and Fig. 5.2 at 25 dB SNR.

λ_J (km^{-2})	C_s (Fig. 4.4) (bits/Hz/Sec)	C_s (Fig. 5.2),(bits/Hz/Sec)			
		$P_J = 10dB$	$P_J = 20dB$	$P_J = 30dB$	$P_J = 40dB$
0.001	0.2744	0	0.722	1.347	1.477
0.004	0.6143	0.2888	1.222	1.457	1.492
0.01	2.606	0.8249	1.373	1.481	1.495
0.02	2.839	1.092	1.433	1.489	1.496

From the table we can see that the FD eavesdroppers are degrading the secrecy capacity compared to the scenario with adaptive eavesdroppers. Since the eavesdroppers cannot be deceived by friendly jamming in this case, a large density of eavesdroppers are simultaneously listening to the source and jamming the destinations. This results in a large eavesdroppers' capacity being deducted from the main channel capacity which itself is low due to hostile jamming. Hence, we need higher intensity and/or power for the friendly jamming nodes.

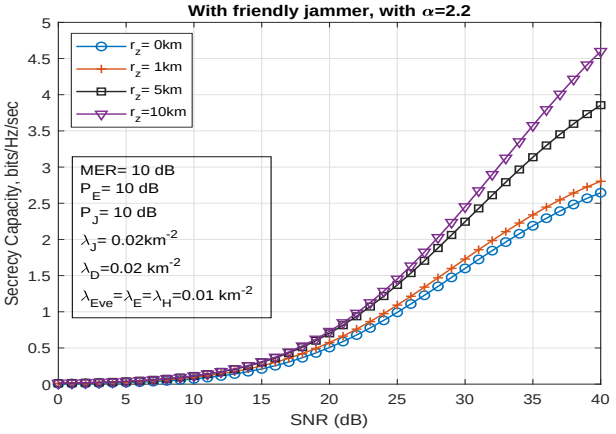


FIGURE 5.3: Impact of zone radius on secrecy capacity at higher SNRs.

5.3.2 Impact of Radius of Secrecy Protected Zone

Section 5.3.1 already showed that we need higher node intensity along with higher jamming power for friendly jammers to increase the secrecy capacity. We also analyse the impact of secrecy protected zone on the secrecy capacity in presence of FD eavesdroppers. Fig. 5.3 shows the rise of secrecy capacity with the increase in r_z. At 25 dB SNR, the values of secrecy capacity for corresponding secrecy protected zone radius are shown in Table 5.2, where, $\frac{\Delta C_s}{\Delta r_z} = \frac{C_s^{new} - C_s^{old}}{r_z^{new} - r_z^{old}}$ depicts the increase in secrecy capacity due to rise in r_z.

TABLE 5.2: Secrecy capacity (C_s) obtained from Fig. 5.3 at 25 dB SNR.

r_z (km)	C_s (bits/Hz/sec)	$\frac{\Delta C_s}{\Delta r_z}$ (bits/Hz/sec per km)
0	0.993	-
1	1.092	0.099
5	1.372	0.070
10	1.453	0.016

Table 5.2 shows that at a moderate SNR of 25 dB, even with a secrecy protected zone radius of 10 km, the secrecy capacity rises up to only 1.453 bits/Hz/sec. If we observe the data in Table 5.1, we can see with zone radius of 1 km, and the same λ_J, the secrecy capacity can rise up to 1.496 bits/Hz/sec for 40 dB of friendly jamming power.

This prompted us to plot the secrecy capacity versus zone radius characteristics as shown by Fig. 5.4.

Fig. 5.4 shows that with higher friendly jamming power, at a moderate SNR of 25 dB, the secrecy capacity reaches a saturated value regardless of the zone radius. The data obtained form the plot is tabulated in Table 5.3

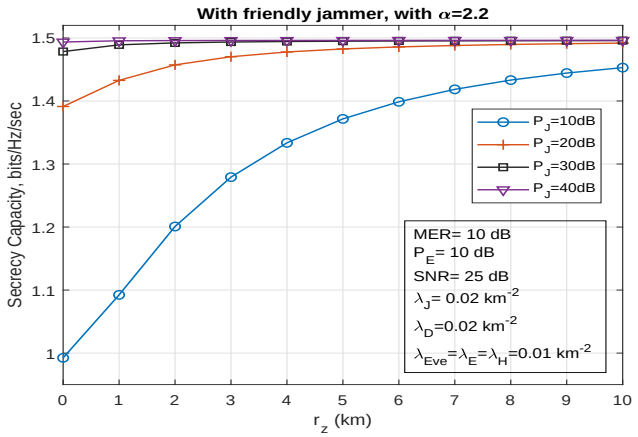


FIGURE 5.4: Secrecy capacity versus zone radius characteristics for various friendly jamming powers.

TABLE 5.3: C_s vs. r_z characteristics at 25 dB SNR.

r_z (km)	C_s (Fig. 5.4),(bits/Hz/Sec)			
	$P_J = 10dB$	$P_J = 20dB$	$P_J = 30dB$	$P_J = 40dB$
0	0.993	1.391	1.478	1.494
1	1.092	1.433	1.489	1.496
5	1.372	1.483	1.495	1.496
10	1.453	1.92	1.496	1.496

As Table 5.3 shows, for the given setup the maximum secrecy capacity at a combination of higher zone radius and friendly jamming power is 1.496 bits/Hz/sec. The table also depicts that if the source can hire higher jamming power from a sufficient friendly jamming nodes, the zone radius does not need to be high. In practice, it is unlikely that the source can afford a larger secrecy protected zone. Therefore, again the friendly jammers are a great option.

5.4 Conclusion

Chapters 3 and 4 show us that the friendly jammers can be employed against adaptive eavesdroppers effectively by deceiving them with a deceptive source-like jamming signal. The adaptive eavesdroppers stay in reception mode listening to both source and friendly jamming signals thus having a degraded eavesdropping channel, and also most of the hostile jamming is removed due to this. As a result, friendly jammers boost up the secrecy capacity. However, in case of FD eavesdroppers this is not the case. The eavesdroppers simultaneously listen and jam thus converting them to be in passive mode is not possible. The eavesdroppers will still receive the deceptive jamming signals. We

assume that the deception still works to infiltrate the eavesdropping channels with interference and the eavesdroppers are not able to discard the jamming signals since the signals are similar to source signal. As a result, although hostile jamming cannot be removed but the eavesdroppers suffer from the friendly jamming.

Due to high node intensity of the eavesdroppers the secrecy capacity is not as high as that with the case of adaptive eavesdroppers. A high node intensity and/or jamming power for the friendly jammers will cause more interference to the eavesdroppers thus lowering down their capacities. So, to achieve higher secrecy capacity the source again needs to do a trade-off between choosing more friendly jammer and more friendly jamming power or both if allowed by the resources. We can conclude that employing friendly jammers against the FD eavesdroppers is beneficial to the security of the system.

Chapter 6

Concluding Remarks and Future Directions

6.1 Concluding Remarks

The primary contributions of this thesis is to investigate the advantages of friendly jammers against different type of eavesdroppers in various types of wireless networks. The previous works do not include adaptive eavesdroppers against friendly jammers where the friendly jammers can tackle the hostile jamming by the eavesdroppers. In every scenario we investigated, the friendly jammer is found to be beneficial to system secrecy. Our main target is to study the usefulness of friendly jammers in random wireless networks. The random wireless network includes geometrically scattered nodes and the derivation for secrecy parameters become difficult for the randomness of the node locations. So, we started with simple relay-aided network before investigating the complex secrecy measures of the random wireless network.

6.1.1 In Relay-aided Network

We presented our works for the relay-aided network in Chapter 3 which involves a two-phase communication. In first phase, the source transmits signal to a decode-and-forward (DF) relay and an eavesdropper tries to listen to the source or jam the relay depending on the quality of source to eavesdropper link. In second phase, the relay retransmits the source signal to destination and the eavesdropper tries to listen to the relay. The eavesdropper chosen in this model is an adaptive or half-duplex (HD) eavesdropper. An adaptive eavesdropper can either be a passive eavesdropper who silently listens or

a hostile jammer who jams the legitimate entities. The eavesdropper chooses its role depending on the strength of the eavesdropping channel.

We worked with three types of networks and named them as system models **SM0**, **SM1** and **SM2**. System model **SM0** is a multiple-input-multiple-output (MIMO) network with multiple relays, destinations, adaptive eavesdroppers and friendly jammers. A relay and a friendly jammer were chosen for transmission relaying and jamming the eavesdroppers, respectively. It was assumed that the locations of the eavesdroppers are known to source, and that the artificial noise (AN) of the friendly jammer is enough to force the eavesdroppers to stop jamming. Comprehensive analyses and results showed that the friendly jammer was successful to enhance the secrecy capacity of the system. A conference paper was published on this work [43].

We chose **SM1** to relax the assumptions we made in **SM0**. We choose a single-input-single-output (SISO) network with deceptive friendly jammer. It helped with the assumption that the source knew the location of the only adaptive eavesdropper. Using AN as friendly jamming had a chance of turning the eavesdropper a continuous hostile jammmer. Therefore, choosing a deceptive friendly jammer was a better option. The deceptive friendly jammer continuously emitted a source-like signal which deceived the eavesdropper. The deception forced the eavesdropper to be in reception mode. As a result, the hostile jamming in first phase was eliminated and the eavesdropping channels in both phases suffered from friendly jamming. The mathematical analyses and numerical results showed that with the help of friendly jammer, the secrecy capacity was increased and the secrecy outage probability was decreased, i.e., the security of the system was enhanced. This work has been published in [44].

We revisited system model **SM1** with a multi-antenna relay thus creating system model **SM2**. This was done to incorporate the idea that the relay could be a base station with multiple antennas and this made the derivations to obtain the expressions of the secrecy outage probabilities (SOPs) more complex. Also, the simulations became complex and time consuming due to introduction of multiple antennas. Again, the numerical results showed that the friendly jammer was capable of increasing the secrecy capacity and decreasing the secrecy outage probability.

We can conclude that the friendly jammer is capable of tackling the adaptive eavesdropping in a relay-aided communication.

6.1.2 In Random Wireless Network

We chose our final system model, a random wireless network. A random wireless network represents a network where all the nodes are scattered around the coverage area. As a result, system geometry and path loss were taken into account. Our system model included a single source in a circular coverage area. The source was communicating with multiple destinations in presence of multiple eavesdroppers. The source employed a secrecy protected zone inside which any eavesdropper would become deactivated. A group of deceptive friendly jammers were placed randomly outside the zone to deceive the eavesdroppers with a source-like signal. All the destinations, eavesdroppers and friendly jammers were located randomly following a homogeneous Poisson point process (HPPP). We worked with two versions of the model, one where the eavesdroppers were adaptive (system model **SM3**) and in the other version, the eavesdroppers were active (system model **SM4**).

6.1.2.1 With Adaptive (HD) Eavesdroppers (SM3)

In Chapter 4, we presented **SM3**. We considered the randomly placed eavesdroppers were adaptive or half-duplex. Every entity in this model was equipped with single antenna. The friendly jammers tried their best to convert all the hostile jammers into passive eavesdroppers. We made a realistic choice that all the hostile jammers were not deceived by the friendly jamming, so the system model had some adaptive eavesdroppers working as passive listeners while others as hostile jammers. The secrecy capacity of the network was derived with the help of HPPP theory. The derivation involved mathematical manipulations with the nature of randomness of the node locations along with the channel fading characteristics, unlike the previous relay-aided models which only considered the channel fading.

We came up with a formula to control the rate of conversion from hostile jammer to passive eavesdropper due to friendly jamming, and simulated the derived expressions of the secrecy capacity. The friendly jammers were found to be useful in enhancing the system security by diminishing some of the hostile jamming and at the same time interfering with the passive eavesdroppers.

The mathematical analyses and numerical results showed that the source might need to choose whether to hire more friendly jammer nodes or to ask for more jamming power from the existing friendly jammers, depending on the situation. Such situation can occur when the node intensity of the destinations are lower than that of the adaptive eavesdroppers. Another situation occurs if the system model incorporates no or a small

secrecy protected zone. Considering the scattering nature of the node locations in the system, the source should hire more friendly jammers and then if the resources allow, consider asking for more jamming power from them. A journal paper is published from this work [45].

6.1.2.2 With Active (FD) Eavesdroppers (SM4)

Chapter 5 investigated **SM4**. We considered the adversaries to be active or full-duplex eavesdroppers, i.e., they could simultaneously listen to the source and jam the destinations. The eavesdroppers were the only entities in that model to have two antennas. We assumed that the eavesdroppers were deceived by the friendly jamming and did not use both the antennas to omit the friendly jamming. The assumption was made based on realistic scenario where an eavesdropper can fail to remove the friendly jamming from its received signal. However, being full-duplex, the eavesdroppers did not stop jamming the destinations. So, the friendly jammers had only one job that was to interfere with the eavesdropping channels.

Since the hostile jamming was not possible to remove, the system had to deal with a higher number of both passive eavesdropping and hostile jamming nodes compared to the earlier version of that model with adaptive eavesdroppers. We derived the secrecy capacity and the numerical results showed the lower secrecy capacity compared to that found in Chapter 4. However, the non-zero secrecy capacity was still possible to achieve if friendly jammers were employed. Obviously, the source there needed to hire more friendly jammers with higher jamming power to achieve higher secrecy capacity similar to that with the earlier version of the model with adaptive eavesdroppers. It was also seen that increasing the radius of secrecy protected zone did not have much impact as that with increase in high powered friendly jamming node intensity. As a result, the source needs more friendly jamming nodes with higher power to deal with active eavesdroppers.

The use of friendly jammers was found to be beneficial to system secrecy in both relay-aided radio network and also in random wireless network. The relay-aided system models in **SM0**, **SM1** and **SM2** dealt with small number of entities and the mathematical derivation was pretty straight forward and followed the classical physical layer model inspired by Wyner [31]. On the other hand, the random wireless networks in **SM3** and **SM4** included scattered nodes. Stochastic geometry and Poisson point process were employed to investigate the secrecy capacity in random wireless networks. The use of friendly jammers were found to be advantageous to enhance the system secrecy in the relay aided network against adaptive eavesdroppers. We gradually moved to

more practical scenarios with those models. Friendly jammers used AN in **SM0** and a source-like deceptive signal in **SM1** and **SM2**. **SM2** showed the secrecy parameters derivations with a multi-antenna relay. We used deceptive friendly jammers in **SM3** against adaptive eavesdroppers. We followed the rules of stochastic geometry and HPPP in deriving the secrecy capacity of this model. In **SM4**, we chose active eavesdroppers and our work with **SM2** helped us to derive the secrecy capacity with a multi-antenna eavesdropper. All the mathematical analyses and numerical results showed that the friendly jammers enhance the secrecy performance in each of those models.

6.2 Future Directions

The target of this thesis was to achieve higher secrecy capacity in random wireless network with friendly jammers and to investigate how the friendly jammer related parameters impact the secrecy capacity. In way to achieve that we also observed the advantages of friendly jammers in relay-aided networks. This section discusses a few of the possible future research directions from this thesis outcomes.

6.2.1 Changing Relaying Strategies

The relays in **SM0**, **SM1** and **SM2** were all decode-and-forward (DF) relays. We can change the relaying strategies and use other types of relays to investigate the secrecy of the networks. The relays can be amplify-and-forward (AF) or compute-and-forward (CoF) in nature. The brief description about these strategies are given below,

(i) AF Relays:

The DF relays have the full processing ability to decode, re-modulate and then retransmit the source signals. On the other hand, AF relays are less complex and simply amplify and retransmit their received signals without decoding. The AF relay also amplifies the noise in its retransmitted signal. An AF relay is faster than the DF one since the latter creates a delay while decoding the received signal. A common assumption in AF protocols is that the destination must know all the fading coefficients throughout the hops from source to destination while in case of DF protocols the destination needs to know only the source-destination (if any) and relay-destination channel fading coefficients [104]. Changing the relays as AF in **SM0**, **SM1** and **SM2** will change the derivation significantly.

(ii) CoF Relays:

The compute-and-forward (CoF) protocol can maximise the network throughput in interference-limited networks [105]. Let us consider a scenario where a second source is

communicating with the destination in **SM1** and **SM2** via a second relay. The CoF protocol allows the relays to decode linear equations of the source signals using the noisy linear combinations provided by the channel. The destination can decode the desired messages by solving sufficient linear combinations sent by the relays [106, 107]. Before retransmitting the signals, the relays attempt to decode out the effective noise received by them. An adaptive eavesdropper can be considered, located between the relays and the destination, trying to listen to both the relays. If the eavesdropping link is weak, then the eavesdropper jams the destination. If the eavesdropper has an omnidirectional antenna, both relays may also receive hostile jamming. A deceptive friendly jammer can be introduced to force the eavesdropper to be in reception mode. The challenge will be to derive the secrecy capacity and secrecy outage probability in this scenario and investigate if the friendly jammer is beneficial to the system secrecy.

6.2.2 Other Secrecy Parameters for SM3 and SM4

The thesis chose secrecy capacity as a means for investigation of advantages of friendly jammers in a random wireless network. The randomness of node locations introduced complex mathematical derivations and simulations for the secrecy metrics. Some other secrecy parameters we can investigate are as follows,

(i) Secrecy Outage Probability

The secrecy outage probability (SOP) for a given target secrecy rate, R_s can be expressed as,

$$P_{out} = Pr(C_s < R_s) = Pr\left(\frac{1 + \min\limits_{D_n \in \Phi_D} \gamma_{SD_n}}{1 + \gamma_{SE_1}} < 2^{R_s}\right) \approx Pr\left(\frac{\min\limits_{D_n \in \Phi_D} \gamma_{SD_n}}{\gamma_{SE_1}} < 2^{R_s}\right), \quad (6.1)$$

where, the numerator stands for the SINR of the source (S) to n^{th} destination D_n link, and the denominator includes the SINR of the source to worst-case eavesdropper E_1 link. According to Tao et al. [108], the typical user and eavesdroppers operate in moderate to high SINR region which gives us the last equality. Ideally, the friendly jammers will decrease the SOP of the networks given in System Models **SM3** and **SM4**.

(ii) Throughput, Success Probability and Connection Outage Probability

The **throughput** at individual destinations in presence of hostile jammers can be derived as a check on reliability of legitimate transmission. The throughput at destination

D_n can be expressed as [109],

$$\mathcal{T}_n = \frac{\log_2(1+\beta_{D_n})}{r_{d_n}}(P_{SUC_{D_n}})^{r_{d_n}}, \tag{6.2}$$

where, $P_{SUC_{D_n}}$ is the **success probability** that the destination received the signal, and can be expressed by following [70, Eq. 5.14] as,

$$P_{SUC_{D_n}} = Pr(SINR > \beta_{D_n}) = \mathbb{E}_{r_{d_n}}\left[\exp\left\{-\pi\lambda_H\beta_{D_n}^{\delta}r_{d_n}^2\Gamma(1+\delta)\Gamma(1-\delta)\right\}\right], \tag{6.3}$$

where, the notations depict same meanings as in Table 4.1 with $\beta_{D_n} > 0$ is the minimum required SINR for a successful reception. In a similar way, the success probability at the worst-case eavesdropper can be derived. Ideally, with increase in λ_J, the success probability at the worst-case eavesdropper should be decreased, and also λ_H can be decreased in case of adaptive eavesdroppers. As a result, the throughput will also increase, however, a derivation for throughput will quantify the improvement.

Again, the **connection outage probability (COP)**, i.e., failure of reception, at any particular receiver can be found as,

$$P_{COP} = 1 - P_{SUC}. \tag{6.4}$$

The evaluation of the above secrecy performance measures using Monte Carlo simulation is a promising future direction.

6.2.3 Mobile Eavesdroppers

Random wireless networks in vehicular or healthcare communications may have mobile nodes. Even if the legitimate entities are stationary, eavesdroppers can be mobile devices. For mobile nodes, the node intensity of a particular entity group is hardly uniform with time and space. Since the node intensity becomes a variable, the Poisson point process applied in this network cannot be a homogeneous one [72]. For homogeneous PPP, the node intensity of eavesdroppers, λ_{Eve} is a non-zero constant considering other parameters remain unchanged in the network. In case of inhomogeneous PPP, the node intensity becomes a function, $\lambda_{Eve}(x)$, where x is a point under consideration for acceptance or rejection. For **SM3** and **SM4**, x can be a location point on the coverage area and the node intensity of the eavesdroppers becomes dependent on the location. Incorporating the variable node intensity for the eavesdroppers opens new challenges for the derivation of secrecy capacity and secrecy outage probability. A comparative analysis can be done between the performance of stationary and mobile friendly jammers to tackle the mobile eavesdroppers.

6.2.4 Hostile Jammers with Adaptive Power

The jammers that continuously transmit jamming signals are called constant jammers, and those that jam time-to-time while trying to save energy fall under the category of intermittent or random jammers [20]. Although the adaptive eavesdroppers do not go into sleep phase like the intermittent jammers, their nature causes random jamming in the legitimate channel. However, there are other kinds of jammers, and one of them is an adaptive jammer. An adaptive jammer has the intelligence to adjust its jamming power as required to disrupt the legitimate transmission. DeBruhl et al., on the other hand, considered adaptive jammers as nodes who continually adapt the attack parameters with performance information obtained from the victim system [19]. These jammers are similar to the adaptive eavesdroppers since they have two phases namely, the observing phase when they listen to the transmission and jamming phase when they jam.

Let us consider the system is attacked by adaptive eavesdroppers with adaptive hostile jamming ability. From Fig. 3.5, we see that increase in hostile jamming power results in a low secrecy capacity. The main channel capacity suffers from high power hostile jamming causing a drop in secrecy capacity. The friendly jammers are not capable of controlling the hostile jamming power. However, a sufficiently high node intensity for friendly jammers can force all of the hostile jammers to turn into passive eavesdroppers. So, the target is to achieve a high non-zero secrecy capacity for this scenario.

6.2.5 Applying Deep Learning

Channel model and channel state information (CSI) estimation is a part and parcel of physical layer security. However, in many cases the channel model may not be accurately known. In that case, the physical layer algorithms including decoding, detection and message recovery will not be computationally efficient. The Deep learning (DL) detectors can learn directly from data and eliminate the necessity for CSI and fading characteristics estimation [110,111]. A time-consuming Monte-Carlo simulation is highly used in estimating the secrecy performance of wireless networks. By using a DL based algorithm, the channel behavior could be accurately and quickly predicted resulting in an optimized system design.

In **SM3** and **SM4**, all the friendly jammers are using same level of jamming power. The eavesdroppers are scattered around the secrecy protected zone and suffer from an aggregated interference due to friendly jamming from several friendly jammers. Every friendly jammer faces different number of eavesdroppers which also means that different friendly jammers are tackling different amounts of passive eavesdropping and hostile jamming in

SM3. Therefore, we cannot allocate same amount of power to every friendly jammer for efficient jamming. Lee et al. discussed the use of deep learning in transmit power control as part of resource management in device-to-device communications [112]. A proper adjustment of transmit power is important in order to achieve a high performance as well as to maximise energy efficiency. Deep learning models can be investigated to estimate the channels between a pair of friendly jammer and eavesdropper, and to optimise the jamming power for each friendly jammer. Also, for system model incorporating mobile nodes deep learning is worth investigating to analyse node mobility patterns [113].

Bibliography

[1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 16, no. 3, pp. 1550–1573, September 2014.

[2] J. L. Massey, "An introduction to contemporary cryptology," *Proc. IEEE*, vol. 76, no. 5, pp. 533–549, May 1988.

[3] P. Gandotra and R. K. Jha, "A survey on green communication and security challenges in 5G wireless communication networks," *Journal of Network and Computer Applications*, vol. 96, pp. 39 – 61, 2017.

[4] A. H. Sodhro, S. Pirbhulal, and V. H. C. de Albuquerque, "Artificial intelligence-driven mechanism for edge computing-based industrial applications," *IEEE Trans. on Industrial Informatics*, vol. 15, no. 7, pp. 4235–4243, July 2019.

[5] A. H. Sodhro, S. Pirbhulal, and A. K. Sangaiah, "Convergence of IoT and product lifecycle management in medical health care," *Future Generation Computer Systems*, vol. 86, pp. 380 – 391, 2018.

[6] A. H. Sodhro, G. Fortino, S. Pirbhulal, M. M. Lodro, and M. A. Shah, "Energy-efficient communications in wireless body sensor networks," in *Networks of the Future: Architectures, Technologies, and Implementations, Chapman & Hall/CRC Computer and Information Science Series*, M. Elkhodr, Q. F. Hassan, and S. Shahrestani, Eds. CRC Press (Taylor & Francis Group), October 2017, ch. 16, pp. 339–354.

[7] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1878–1911, Second quarter 2019.

[8] D. Wang, B. Bai, K. Lei, W. Zhao, Y. Yang, and Z. Han, "Enhancing information security via physical layer approaches in heterogeneous iot with multiple access

mobile edge computing in smart city," *IEEE Access*, vol. 7, pp. 54 508–54 521, May 2019.

[9] C. Nykvist, M. Larsson, A. H. Sodhro, and A. Gurtov, "A lightweight portable intrusion detection communication system for auditing applications," *International Journal of Communication Systems, Wiley Online Library*, vol. 33, no. 7, pp. 1–16, January 2020.

[10] T. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. USA: Prentice Hall PTR, 2001.

[11] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

[12] I. Csiszar and J. Korner, "Broadcast channels with confidential messageges," *IEEE Trans. on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[13] Y. Liang, H. Poor, and S. S. (Shitz), "Secure communication over fading channels," *IEEE Trans. on Information Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[14] L. Lai, H. El Gamal, and H. V. Poor, "Authentication over noisy channels," *IEEE Trans. on Information Theory*, vol. 55, no. 2, pp. 906–916, February 2009.

[15] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels*, 2nd ed. New York: Wiley, 2005.

[16] M. Z. I. Sarkar and T. Ratnarajah, "On the secure outage performance for wireless multicasting through slow fading channels," in *Proceedings of the* IEEE I*nf. T*heory W*orkshop (*ITW*)*, 30 Aug.-3 Sept. 2010, pp. 1–5.

[17] T. M. Hoang, H. Q. Ngo, T. Q. Duong, H. D. Tuan, and A. Marshall, "Cell-free massive mimo networks: Optimal power control against active eavesdropping," *IEEE Trans. on Communications*, vol. 66, no. 10, pp. 4724–4737, October 2018.

[18] X. Lu, W. Yang, Y. Cai, X. Guan, and L. Wang, "Discriminatory channel estimation in mimo relay systems against active eavesdropper," in *Proc. of the 11th International Conference on Wireless Communications and Signal Processing (WCSP)*, October 2019, pp. 1–6.

[19] B. DeBruhl, Z. Weinberg, Y. S. Kim, and P. Tague, "Stir-ing the wireless medium with self-tuned, inference-based, real-time jamming," in *Proceedings of the 2012 IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS)*, ser. MASS '12, 2012, p. 326–334.

[20] J. Zhu, Y. Zhu, and B. Zheng, "Physical-layer security and reliability challenges for indutrial wireless networks," IEEE A*ccess*, vol. 5, pp. 5313–5320, April, 2017.

[21] L. Yang, J. Chen, H. Jiang, S. A. Vorobyov, and H. Zhang, "Optimal relay selection for secure cooperative communications with an adaptive eavesdropper," *IEEE Trans. on Wireless Commun.*, vol. 16, no. 1, pp. 26–42, October 2016.

[22] A. Mukherjee and A. L. Swindlehurst, "A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures," in *Proc. Asilomar Conf. Signals, Syst. Comput. (ASILOMAR), Pacific Grove, CA, USA*, November 2011, pp. 265–269.

[23] Z. Li, T. Jing, L. Ma, Y. Huo, and J. Qian, "Worst-case cooperative jamming for secure communications in CIoT networks," *Sensors (Basel)*, vol. 16, no. 3(339), pp. 1–19, March 7, 2016.

[24] K. Cumanan, Z. Ding, M. Xu, and H. Poor, "Secure multicast communications with private jammers," in *Proc. of the* IEEE *17th International Workshop on Signal Processing Advances in Wireless Commun. (*SPAWC*)*, July 3-6, 2016, pp. 1–6.

[25] K. Cumanan, H. Xing, P. Xu, G. Zheng, X. Dai, A. Nallanathan, Z. Ding, and G. K. Karagiannidis, "Physical layer security jamming: Theoretical limits and practical designs in wireless networks," IEEE *Access*, vol. 5, pp. 3603–3611, December, 2016.

[26] S. Liu, Y. Hong, and E. Viterbo, "Artificial noise revisited," *IEEE Trans. on Information Theory*, vol. 61, no. 7, pp. 3901–3911, July 2015.

[27] H. Guo, Z. Yang, L. Zhang, J. Zhu, and Y. Zou, "Power-constrained secrecy rate maximization for joint relay and jammer selection assisted wireless networks," *IEEE Trans. on Communications*, vol. 65, no. 5, pp. 2180–2193, January 2017.

[28] X. Guan, Y. Cai, Y. Wang, and W. Yang, "Increasing secrecy capacity via joint design of cooperative beamforming and jamming," in *Proc. of the 22nd Annual* IEEE *International Sym. on Personal, Indoor and Mobile Radio Commun. (*PIMRC*): Fundamentals and* PHY, September 11-14, 2011.

[29] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channels," *IEEE Trans. Intell. Transp. Syst.*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[30] J. E. Giti, M. Z. I. Sarkar, S. A. H. Chowdhury, M. M. Ali, and T. Ratnarajah, "Secure wireless multicasting through co-existing MIMO radio systems," in *Proc. of The 9th International Forum on Strategic Technology* (IFOST), October 21-23, 2014, pp. 195–198.

[31] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[32] C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 29, pp. 656–715, 1949.

[33] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT05)*, 2005, pp. 2152–2155.

[34] T. Liu, H. Poor, and S. S. (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. on Information Theory*, vol. 55, no. 6, pp. 2547–2553, June 2008.

[35] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *Proc.* IEEE I*ntl.* S*ymposium on* I*nformation* T*heory*, July 2006, pp. 356–360.

[36] 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. on Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, August 2011.

[37] A. Mukherjee and A. L. Swindlehurst, "Detecting passive eavesdroppers in the mimo wiretap channel," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2012, pp. 2809–2812.

[38] S. H. Chae, W. Choi, J. H. Lee, and T. Q. Quek, "Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone," *IEEE Trans. on. Information Forensics and Security*, vol. 9, no. 10, pp. 1617–1628, October 2014.

[39] W. Liu, Z. Ding, T. Ratnarajah, and J. Xue, "On ergodic secrecy capacity of random wireless networks with protected zones," *IEEE Trans. on Vehicular Technology*, vol. 65, no. 8, pp. 6146–6158, August 2016.

[40] F. Qamar, K. Dimyati, M. N. Hindia, K. A. Noordin, and I. S. Amiri, "A stochastically geometrical poisson point process approach for the future 5G D2D enabled cooperative cellular network," *IEEE Access*, vol. 7, pp. 60 465–60 485, May 2019.

[41] M. Haenggi, "On distance of uniformly random networks," *IEEE Trans. on Information Theory*, vol. 51, no. 10, pp. 3584–3586, 2005.

[42] ——, "A geometric interpretation of fading in wireless networks: Theory and applications," *IEEE Trans. on Information Theory*, vol. 54, no. 12, pp. 5500–5510, December 2008.

[43] J. E. Giti, B. Srinivasan, and J. Kamruzzaman, "Impact of friendly jammers on secrecy multicast capacity in presence of adaptive eavesdroppers," in *IEEE GLOBECOM Workshops (GC Wkshps)*, December 4-8, 2017, pp. 1–6.

[44] J. E. Giti, A. Sakzad, B. Srinivasan, J. Kamruzzaman, and R. Gaire, "Friendly jammer against an adaptive eavesdropper in a relay-aided network," in *2020 International Wireless Communications and Mobile Computing (IWCMC)*, June 15-19, 2020, pp. 1707–1712.

[45] J. E. Giti, A. Sakzad, B. Srinivasan, J. Kamruzzaman, and R. Gaire, "Secrecy capacity against adaptive eavesdroppers in a random wireless network using friendly jammers and protected zone," *Journal of Network and Computer Applications*, vol. 165, p. 102698, 2020.

[46] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[47] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. on Information Theory*, vol. 54, no. 6, pp. 2515–2535, June 2008.

[48] Y. Liang and H. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. on Information Theory*, vol. 54, no. 3, pp. 976–1002, March 2008.

[49] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT2007), Nice, France*, 2007, pp. 1301–1305.

[50] P. Gopala, L. Lai, and H. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. on Information Theory*, vol. 54, no. 10, pp. 4687–4698, October 2008.

[51] A. Sheikholeslami, D. Goeckel, and H. Pishro-Nik, "Jamming based on an ephemeral key to obtain everlasting security in wireless environments," *IEEE Trans. on Wireless Commun.*, vol. 14, no. 11, pp. 6072–6081, November 2015.

[52] A. Sheikholeslami, M. Ghaderi, H. Pishro-Nik, and D. Goeckel, "Energy-efficient routing in wireless networks in the presence of jamming," *IEEE Trans. on Wireless Commun.*, vol. 15, no. 10, pp. 6828–6842, October 2016.

[53] ——, "Energy-efficient secrecy in wireless networks based on random jamming," *IEEE Trans. on Communications*, vol. 65, no. 6, pp. 2522–2533, June 2017.

[54] Z. Yuan, C. Chen, L. Bai, Y. Jin, and J. Choi, "Secure relay beamforming with correlated channel models in dual-hop wireless communication networks," in *Proc. of IEEE Global Commun. Conf. (GLOBECOM)*, December 4-8, 2016, pp. 1–6.

[55] Y. Jing and H. Jafarkhani, "Beamforming in wireless relay networks," in IEEE I*nf. T*heory and A*pplications* W*orkshop*, January 27-February 1, 2008, pp. 1–9.

[56] C. Masouros and T. Ratnarajah, "Interference as a source of green signal power in cognitive relay-assisted co-existing MIMO wireless transmissions," *IEEE Trans. on Communications*, vol. 60, no. 2, pp. 525–536, June 2012.

[57] W. Liu, M. Z. I. Sarkar, and T. Ratnarajah, "Combined approach of zero forcing precoding and cooperative jamming: A secrecy tradeoff," in *Proc. of IEEE Wireless Communications and Networking Conference (WCNC)*, April 2013, pp. 1825–1829.

[58] W. Liu, M. Z. I. Sarkar, T. Ratnarajah, and H. Du, "Securing cognitive radio with a combined approach of beamforming and cooperative jamming," *IET Commun.*, vol. 11, no. 1, pp. 1–9, December 22, 2016.

[59] Q. F. Zhou, F. C. M. Lau, and S. F. Hau, "Asymptotic analysis of opportunistic relaying protocols," *IEEE Trans. on Wireless Commun.*, vol. 8, no. 8, pp. 3915–3920, August 2009.

[60] K. Elkhalil, M. E. Eltayeb, H. Shibli, H. R. Bahrami, and T. Y. Al-Naffouri, "Opportunistic relay selection in multicast relay networks using compressive sensing," in *Proc. of IEEE Global Commun. Conf. (GLOBECOM)*, December 8-12, 2014.

[61] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *Proceedings of* IEEE/SP *15th* W*orkshop on* S*tatistical* S*ignal* P*rocessing, 2009 (*SSP *'09), Cardiff, Wales, UK*, 31 Aug.-03 Sept. 2009, pp. 417–420.

[62] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," *IEEE Signal Processing Letters*, vol. 20, no. 1, pp. 39–42, January 2013.

[63] E. R. Alotaibi and K. A. Hamdi, "Optimal cooperative relaying and jamming for secure communication," *IEEE Wireless Commun. Letts.*, vol. 4, no. 6, pp. 689–692, December 2015.

[64] J. Zhang, G. Zheng, I. Krikidis, and R. Zhang, "Specific absorption rate-aware beamforming in MISO downlink SWIPT systems," *IEEE Transactions on Communications*, vol. 68, no. 2, pp. 1312–1326, February 2020.

[65] Q. Li and L. Yang, "Beamforming for cooperative secure transmission in cognitive two-way relay networks," *IEEE Trans. on. Information Forensics and Security*, vol. 15, pp. 130–143, 2020.

[66] C. A. Balanis, *Antenna theory: Analysis and Design*, 3rd ed. Wiley-Interscience, 2005.

[67] M. Bertero, P. Boccacci, G. Desiderà, and G. Vicidomini, "Image deblurring with poisson data: from cells to galaxies," *Inverse Problems*, vol. 25, no. 12, p. 123006, November 2009.

[68] C. Choi and F. Baccelli, "Poisson cox point processes for vehicular networks," *IEEE Trans. on Vehicular Technology*, vol. 67, no. 10, pp. 10 160–10 165, October 2018.

[69] A. H. Sodhro, M. S. Obaidat, Q. H. Abbasi, P. Pace, S. Pirbhulal, A. Yasar, G. Fortino, M. A. Imran, and M. Qaraqe, "Quality of service optimization in an iot-driven intelligent transportation system," *IEEE Wireless Communications*, vol. 26, no. 6, pp. 10–17, December 2019.

[70] M. Haenggi, *Stochastic Geometry for Wireless Networks [Electronic Resource].* Cambridge, UK: Cambridge University Press, 2012.

[71] E. Gilbert, "Random plane networks," *Journal of the Society for Industrial and Applied Mathematics*, vol. 9, no. 4, pp. 533–543, 1961.

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

[73] H. ElSawy, E. Hossain, and M. Haenggi, "Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 15, no. 3, pp. 996–1019, 2013.

[74] W. Tang, S. Feng, Y. Ding, and Y. Liu, "Physical layer security in heterogeneous networks with jammer selection and full-duplex users," *IEEE Trans. on Wireless Commun.*, vol. 16, no. 12, pp. 7982–7995, December 2017.

[75] 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. on Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, August 2011.

[76] X. Xu, B. He, W. Yang, X. Zhou, and Y. Cai, "Secure transmission design for cognitive radio networks with poisson distributed eavesdroppers," *IEEE Trans. on. Information Forensics and Security*, vol. 11, no. 2, pp. 373–387, February 2016.

[77] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun, "On limitations of friendly jamming for confidentiality," in *Proc. IEEE Symp. Security and Privacy*, May 19-22, 2013, pp. 160–173.

[78] W. Shen, P. Ning, X. He, and H. Dai, "Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time," in *Proc. IEEE Symp. Security and Privacy*, May 19-22, 2013, pp. 174–188.

[79] B. Ali, N. Zamir, M. F. U. Butt, and S. X. Ng, "Physical layer security: Friendly jamming in an untrusted relay scenario," in *Proc. of the 24th European Signal Processing Conf. (*EUSIPCO*)*, August 29- September 2, 2016, pp. 958–962.

[80] F. Zhou, R. Wang, and J. Bian, "Robust destination jamming aided secrecy precoding for an af mimo untrusted relay system," *Wireless Communications and Mobile Computing*, pp. 1–9, 2019.

[81] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: A survey," *Int. J. Ad Hoc and Ubiquitous Computing*, vol. 17, no. 4, pp. 197–215, 2014.

[82] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. on Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[83] J. P. Vilela, M. Bloch, J. Barros, and S. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. on. Information Forensics and Security*, vol. 6, no. 2, pp. 256–266, June 2011.

[84] K. Banawan, S. Ulukus, P. Wang, and B. Henz, "Secure rates in multiband broadcast channels with combating jammers," in *Proc. of IEEE Military Commun. Conf. (MILCOM)*, December 1-3, 2016, pp. 1–6.

[85] S. Q. Nguyen and H. Y. Kong, "Secrecy enhancement in two-hop DF relaying system under hardware impairment," *Int. J. Electronics, Taylor & Francis Group*, vol. 104, no. 3, pp. 442–461, 2017.

[86] J. Yue, B. Yang, and X. Guan, "Fairness-guaranteed pricing and power allocation with a friendly jammer against eavesdropping," in *Proc. of the International Conf. on Wireless Commun. and Signal Processing (*WCSP*)*, October 25-27, 2012, pp. 1–6.

[87] Y. Wen, Y. Huo, L. Ma, T. Jing, and Q. Gao, "A scheme for trustworthy friendly jammer selection in cooperative cognitive radio networks," *IEEE Trans. on Vehicular Technology*, vol. 68, no. 4, pp. 3500–3512, April 2019.

[88] S. Yan, Y. Shang, and M. Zhang, "Compromised secrecy region with friendly jammers in heterogeneous cellular networks," in *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Honolulu, HI*, April 15-19, 2018, pp. 848–852.

[89] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. on Vehicular Technology*, vol. 61, no. 8, pp. 3693–3704, October 2012.

[90] A. Kuhestani, A. Mohammadi, and M. Mohammadi, "Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers," *IEEE Trans. on. Information Forensics and Security*, vol. 13, no. 2, pp. 341–355, February 2018.

[91] W. Wang, K. C. Teh, S. Luo, and K. H. Li, "Secure transmission in MISOME wiretap channels with half and full-duplex active eavesdroppers," in *Proc. of IEEE Global Commun. Conf. (GLOBECOM)*, December 4-8, 2017, pp. 1–6.

[92] D. Wang, B. Bai, W. Chen, and Z. Han, "Achieving high energy efficiency and physical-layer security in AF relaying," *IEEE Trans. on Wireless Commun.*, vol. 15, no. 1, pp. 740–752, January 2016.

[93] Q. Xu, P. Ren, and D. Xu, "Combating unknown eavesdroppers by using multipath wireless receptions," in *Proc. of IEEE International Conference on Communications (ICC), Shanghai, China*, May 20-24, 2019, pp. 1–6.

[94] W. Wang, K. C. Teh, K. H. Li, and S. Luo, "On the impact of adaptive eavesdroppers in multi-antenna cellular networks," *IEEE Trans. on. Information Forensics and Security*, vol. 13, no. 2, pp. 269–279, February 2018.

[95] G. Li, X. Sheng, J. Wu, and H. Yu, "Securing transmissions by friendly jamming scheme in wireless networks," *Journal of Parallel and Distributed Computing*, vol. 144, pp. 260–267, 2020.

[96] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, March 2010.

[97] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE Journal on Selected Areas in Commun.*, vol. 30, no. 2, pp. 359–368, February 2012.

[98] B. V. Nguyen and K. Kim, "Secrecy outage probability of optimal relay selection for secure AnF cooperative networks," *IEEE Commun. Letts.*, vol. 19, no. 12, pp. 2086–2089, December 2015.

[99] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA: Academic, 2007.

[100] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*, 3rd ed. New York, NY: McGraw Hill, 1991.

[101] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication.* USA: Cambridge University Press, 2005.

[102] M. Haenggi and R. K. Ganti, "Interference in large wireless networks," *Foundations and Trends® in Networking*, vol. 3, no. 2, pp. 127–248, 2009.

[103] M. Haenggi, "Mean interference in hard-core wireless networks," *IEEE Commun. Letts.*, vol. 15, no. 8, pp. 792–794, August 2011.

[104] P. E. Elia, K. Vinodh, M. Anand, and P. V. Kumar, "D-MG tradeoff and optimal codes for a class of AF and DF cooperative communication protocols," *IEEE Trans. on Information Theory*, vol. 55, no. 7, pp. 3161–3185, July 2009.

[105] B. Nazer and M. Gastpar, "Compute-and-Forward: Harnessing interference through structured codes," *IEEE Trans. on Information Theory*, vol. 57, no. 10, pp. 6443–6486, October 2011.

[106] A. Sakzad, J. Harshan, and E. Viterbo, "Integer-forcing mimo linear receivers based on lattice reduction," *IEEE Trans. on Wireless Commun.*, vol. 12, no. 10, pp. 4905–4915, October 2013.

[107] A. Sakzad, E. Viterbo, J. Boutros, and Y. Hong, "Phase precoded compute-and-forward with partial feedback," in *Proc.* IEEE I*ntl.* S*ymposium on* I*nformation* T*heory*, 2014, pp. 2117–2121.

[108] L. Tao, W. Yang, Y. Cai, and D. Chen, "On secrecy outage probability and average secrecy rate of large-scale cellular networks," *Wireless Communications and Mobile Computing*, pp. 1–14, 2018.

[109] P. H. Nardelli, H. Alves, C. H. [de Lima], and M. Latva-aho, "Throughput maximization in multi-hop wireless networks under a secrecy constraint," *Computer Networks*, vol. 109, pp. 13 – 20, 2016, special issue on Recent Advances in Physical-Layer Security.

[110] N. Farsad, N. Shlezinger, A. J. Goldsmith, and Y. C. Eldar, "Data-driven symbol detection via model-based machine learning," 2020, arXiv:2002.07806 [eess.SP].

[111] R.-F. Liao, H. Wen, J. Wu, H. Song, F. Pan, and L. Dong, "The rayleigh fading channel prediction via deep learning," *Wireless Communications and Mobile Computing*, pp. 1–12, 2018.

[112] W. Lee, M. Kim, and D. Cho, "Deep learning based transmit power control in underlaid device-to-device communication," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2551–2554, 2019.

[113] C. Zhang, P. Patras, and H. Haddadi, "Deep learning in mobile and wireless networking: A survey," *IEEE Communications Surveys Tutorials*, vol. 21, no. 3, pp. 2224–2287, 2019.