SECRECY CAPACITY IN AN ALTERNATE RELAYING WIRELESS NETWORK WITH SUPERPOSITION CODING AND SUCCESSIVE DECODING

by

Chengyi Wang

Submitted in partial fulfillment of the requirements
for the degree of Master of Applied Science

at

Dalhousie University
Halifax, Nova Scotia
December 2023

To My Parents

Table of Contents

List of Figures

Abstract

The broadcasting characteristics of radio channels pose security vulnerabilities in wireless communication networks, but they can also be exploited to aid against eavesdropping. Traditionally, addressing confidentiality concerns in communication systems has focused on higher layers of the protocol stack, usually through pseudo-random bit manipulations. This thesis explores the implementation of physical layer security (PLS) within cooperative relaying systems by considering the physical properties of the communication channel and signal decoding strategies. In the analyzed network with successive relaying and superposition coding, from the perspective of the desired destination, the capacity of wireless channels is improved through i) simultaneous spectrum utilization by a source and two half-duplex relays and ii) optimization of transmitted signal parameters targeting the destination. From the perspective of the eavesdropper, its location and detection strategies may adversely affect the ability to decode the transmitted information. Specifically, the signals transmitted by relays, designed to help the destination, will actually interfere with the decoding by the eavesdropper and are considered a form of artificial noise (AN).

This thesis examines the impact of the eavesdropper position with respect to the destination location on secrecy capacity, which captures the fundamental information-theoretic limit of secure communications at the destination. Two-layer capacities are analyzed in terms of distances in the network. First, the eavesdropper follows the same decoding strategy as the destination, trying to take advantage of being close to the relays. Both the destination and eavesdropper decode the transmitted enhancement signal from relays and then, with successive interference cancellation, they recover the base layer using the signal transmitted directly from the source. Second, while the destination follows its optimum decoding for its original position, the eavesdropper attempts to take advantage of its proximity to the source of multi-layered transmission and perform decoding using the source signal only while treating relay signals as AN. Using simulations in different propagation environments, it is demonstrated in both cases that the destination can receive information securely with varying levels of bandwidth efficiency, except for very limited regions of the eavesdropper's positions, being either very close to the source or close to the destination.

List of Abbreviations Used

The following abbreviations and acronyms are used in this thesis.

2D	Two-dimensional
3D	Three-dimensional
AF	Amplify-and-Forward
AN	Artificial Noise
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
CJ	Cooperative Jamming
CSI	Channel State Information
dB	decibel (relative unit of measurement)
DF	Decode-and-Forward
DoS	Denial-of-Service
FD	Full-Duplex
HD	Half-Duplex
i.i.d	independent and identically distributed
IRI	Inter-Relay Interference
LOS	Line-of-Sight
MATLAB®	Mathematical Laboratory (Software)
MIMO	Multiple-Input Multiple-Output
PLS	Physical Layer Security
PSK	Phase Shift Keying
QAM	Quadrature Amplitude Modulation
QoS	Quality-of-Service
QPSK	Quadrature Phase Shift Keying
RV	Random Variable
SC	Superposition Coding
SIC	Successive Interference Cancellation

SISO	Single-Input Single-Output
SINR	Signal-to-Interference-plus-Noise Ratio
SNR	Signal-to-Noise Ratio
TDD	Time-Division Duplexing
TS	Time Slot

Acknowledgements

This thesis would not be possible without the help and guidance of many people.

First, I would like to express my sincere gratitude and appreciation to my supervisor, Dr. Jacek Ilow. It was his constant support, patient guidance, and enthusiastic teaching that helped me go through my two years of graduate study. I would like to thank Dr. Ilow for his valuable advice and assistance in both academic studies and personal life.

Second, I would like to extend my thanks to my defence committee members, Dr. Jose Gonzalez-Cueto and Dr. Alireza Nafarieh, for providing insightful comments on my research work.

Finally, I am very grateful to my family and friends for their support and understanding, and especially to my parents for their encouragement, which has made everything possible.

Chapter 1

Introduction

In today's world, individuals heavily depend on wireless networks for transmitting critical and private information, including credit card details, energy pricing, e-health data, command and control messages to name a few [1]. However, due to the broadcasting characteristics of radio propagation, messages transmitted through wireless channels are easier to be intercepted by unauthorized users than in wireline networks. During the network design, there are multiple security aspects that need to be considered, including, but not limited to, confidentiality, integrity, authentication and access control [2]. Data confidentiality refers to the protection of data from unauthorized access and disclosure, including means for protecting transmitted information against threats such as eavesdropping due to the public character of networks or broadcast characteristics of channels. Integrity means the message received by the recipient remains consistent with the one sent from the source, which means there is no information tampering during the transmission. Authentication refers to sender validation, i.e., confirmation of the user identity. Access control is a key goal because it stipulates who is allowed to access what content at what times.

The protection (confidentiality) of data as it moves across the shared medium is traditionally delivered through the use of encryption algorithms used to encode information in a manner that can only be decoded and read by the parties for which it is intended [3]. Encryption algorithms perform bit manipulation or scrambling to secure the data before transmission and are utilized above physical link layers in the network protocol stack. However, today's computational-based cryptography has some drawbacks in terms of security. If the eavesdropper is equipped with powerful computational capabilities, the security of these approaches could be compromised [4]. In contrast to computational-based confidentiality approaches at the bit level, physical layer security (PLS) pursued in this thesis depends on communication (modulated) signal processing and considers how actual communications take place in the physical

radio environment [1]. Specifically, in this thesis, to maximize security potential in the studied communication system, we investigate the approach in PLS based on "hiding" information bearing signals from eavesdroppers either through different forms of artificial noise or interference. An important issue for the study of wireless PLS is the measure of the secrecy performance, and, in this thesis, we pursue the evaluation of the investigated systems through secrecy capacity. The secrecy capacity provides the limit under a classical information-theoretic secrecy constraint for systems (zero probability of the message being decoded by the eavesdropper). Secrecy capacity is the counterpart to the usual point-to-point channel capacity given by Shannon's capacity formula when communications are subject to reliability constraints [5]. Both specify the limit of how fast (in bits per sec – bps) the communication can take place (in the unit bandwidth – Hz). However, similarly to Shannon's theory, secrecy capacity does not specify the channel coding (combination of modulation and forward error control) as well as security algorithms on how to reach the predicted limits in a given communication system environment. Since its inception, Shannon's capacity limit has provided the research agenda on how to reach maximum bandwidth efficiency with reliability constraints in different systems. This is what has driven research in this thesis but in the context of bandwidth efficiency for secure (and reliable) communications in the specific network topology (with two relays) and superposition coding.

This thesis characterizes PLS in wireless cooperative networks, where the source communicates with the legitimate destination with the aid of two half-duplex relays. Originally, the two relays were deployed to enable full-duplex operation of the topology considered. In this thesis, by exploiting the two path optimized transmissions to deliver the data reliably (with a high Signal-to-Noise Ratio - SNR) to the destination, we expect that this model will put the eavesdropper at a disadvantage when demodulating the signals (with the low SNRs). With two relays, the original system was doubling the connection capacity, and we investigate the impact of two-relays on secrecy capacity. The two-path transmissions via two-relays overcome the loss in spectral efficiency, which is represented by $\frac{1}{2}$ in the capacity calculation in half-duplex systems [6]. When transmission occurs between the source and the destination via a single half-duplex relay, the loss in spectral efficiency is attributed to transmitting

in two time slots (TSs) rather than one TS [7]. In the investigated communication system, the source is sending the information organized in two layers, base and enhancement. These layers, actually transmitted as one signal, are represented on two modulated signals (sent simultaneously in the same frequency band) but separated in their powers. In this superposition coding (SC) of layers, on the point-to-point links, the recovery of signals of interest depends on the detection of the stronger signal (usually representing the base layer) first, and then, after removing its effect through successive interference cancellation (SIC), the detection of the weaker signal (usually the enhancement layer) is performed second. Thanks to the assistance of two half-duplex decode-and-forward (DF) relays, each receiving node not only reuses time slots of information transmission but also uses SIC to remove the interference effects. In our system, the signal-to-interference ratio (SINR) will be decreased at the destination while we will observe higher noise levels at the eavesdropper so that the secrecy capacity will be improved.

The remainder of this chapter includes (in Sections 1.1 through 1.4) a review of fundamental principles that are exploited in this thesis, while Sections 1.5 and 1.6 provide thesis objectives and thesis organization, respectively.

1.1 Multi-layer signaling and decoding

Multi-layer signaling represents a type of non-orthogonal multiplexing of different data streams, which was initially proposed in [8] for multimedia digital radio broadcast. In these systems, we encounter receivers positioned at varying distances from the broadcast node. Depending on the distance from the transmitter, these receivers will decode different signals representing different data streams, e.g., video approximation and details layers. Distinct receiver nodes will have varying Signal-to-Noise Ratios (SNRs) depending on the path loss as a function of distance. In other words, receivers, whether they are situated nearby or far away, will have different end-to-end channel capacities at their disposal when using conventional single-resolution modulation methods like 16-ary QAM. Receivers in close proximity to the transmitter will enjoy higher SNRs, enabling them to decode symbols with fewer errors. A receiver further away from the transmitter receives the identical waveform, but distinguishing

them becomes more challenging due to increased attenuation [9]. In multi-layer transmissions, called also superposition coding (SC), receivers close to the transmitter with higher SNR will decode both layers (or signals representing two data streams), while receivers farther away receiving the same multi-layer signal will decode only one layer of information [10]- [11]. The decoding of multiple layers usually involves successive detection (or equivalently SIC) and is discussed along the SC in more details in the following subsections.

1.1.1 Superposition Coding

In the SC approach, the fundamental quality (approximation) data (e.g. video frame) is modulated using a modulation scheme that offers robust protection with larger symbol distances (resulting in lower bit error rates - BER). Simultaneously, the enhancement quality (detail) data is modulated using a separate modulation scheme superimposed on the base scheme but protected with smaller symbol distances (resulting in higher BER). In this scenario, receivers with good Channel State Information (CSI) located close to the transmitter can decode both the approximation and detail information, while receivers with poor channel conditions situated farther from the transmitter will only decode the approximation data to reconstruct the transmitted image.

The foundation for this approach relies on the deterministic attenuation of the radio signal over distance. In this model, receivers in close proximity receive the RF broadcast signal with a sufficient Signal-to-Noise Ratio (SNR) to decode both the approximation and detail data, while receivers situated far from the transmitter receive signals with an SNR adequate only for decoding the approximation data. Although both far and near receivers receive the same full constellation, their analog signal decoding depends on the received SNR levels. The far receiver can decode the signal as 4-PSK (corresponding to two high-priority/approximation bits) while the near receivers decode 16-ary QAM modulation (comprising four bits of information with two high-priority/approximation bits and two low-priority/detail bits). In the case of limited transmit power, conventional equispaced 16-ary QAM modulation suffers from significant attenuation due to poor SNR for far receivers, making the signal too

weak for faithful decoding. However, by utilizing 16-ary multi-layer signaling, the far receiver can still decode the signal as Q-PSK with a potentially acceptable BER, thus recovering an acceptable image quality (refer to Fig. 1.1). As a result of the scalability provided by the multi-layer signaling scheme, the overall performance of the broadcast system improves.

Enabling the transmission of two independent information bit streams with varying priorities on a single channel in SC is also known in the literature as hierarchical modulation. In SC as visualized in Fig. 1.1, the source node assigns a higher transmitted power for s_1 and a lower power for s_2 where s_1 represents the base layer (red bits) and s_2 represents the enhancement layer (blue bits). Different power levels are associated with simultaneously transmitted signals as $P_1 = \alpha_1^2 \cdot P$ and $P_2 = \alpha_2^2 \cdot P$, and the combined signal s(t) is as follows:

$$s(t) = \sqrt{P} \cdot \big(\alpha_1 s_1(t) + \alpha_2 s_2(t)\big) \tag{1.1}$$

where $\alpha_{1,2}^2$ represent the power fraction parameters for each layer, stipulated that (i) $(0 < \alpha_i^2 \leq 1,\ i \in \{1, 2\})$, (ii) $\alpha_1^2 + \alpha_2^2 = 1$. The P is the transmission power at the source. Figure 1.1 demonstrates an example of a superimposed signal of two QPSK constellations constituting a symmetrical 16-QAM hierarchical constellation where the base layer has higher noise protection than the enhancement layer. In practical implementation, certain bits are safeguarded with a larger distance (depicted in red), while the blue bits benefit from a shorter protection distance as shown in the diagram. This thesis explores the overarching concept of employing two data streams represented by two signals transmitted actually as one signal (all at the same time and the same frequency band). Additionally, the thesis delves into the diverse power allocations for these signals, offering control over varying levels of security capacity attainable for different data streams within the layered signaling scheme.

1.1.2 Successive Interference Cancellation

The fundamental concept of Successive Interference Cancellation (SIC) involves decoding the receiver's signals sequentially, commencing with the one having the highest received power and concluding with the one allocated the least power. In this

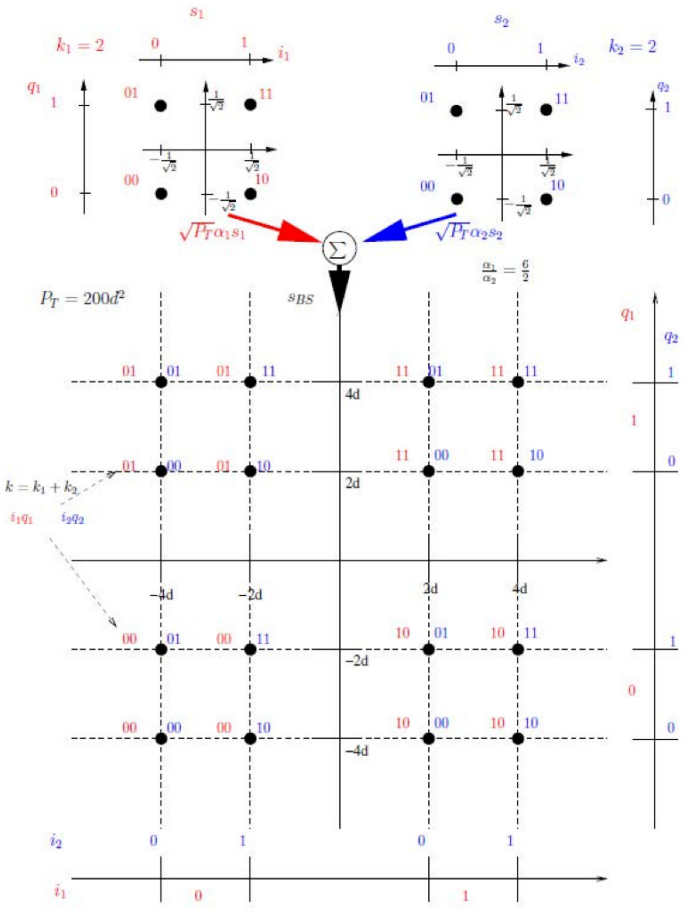

Figure 1.1: Layered coding with a 16-QAM constellation as a superposition of two QPSK constellations

context, we assume that both s_1 and s_2 are intended for the receiver. The precise procedure for decoding the superimposed message can be articulated as follows:

- The destination decodes the message s_1 by treating s_2 as noise/interference in the received signal $r(t) = \sqrt{P_t} \cdot h_{SD} \cdot s_1(t) + n(t)$, where $n(t)$ is the noise at the destination, h_{SD} is the channel gain between the source and the destination and P_t is transmit power.

- After successfully recovering s_1, the destination then subtracts its effect from $r(t)$ leading to a new modified received signal $\hat{s(t)} = r(t) - \sqrt{P_t} \cdot h_{SD} \cdot \alpha_1 \cdot s_1(t)$.

- The destination then decodes s_2 from $\hat{s(t)}$ which is traditionally only impacted by AWGN $\big($scaled version of $n(t)$ $\big)$.

Therefore, through SIC, the two superimposed signals attain distinct data rates, which in the presence of AWGN are calculated using Shannon's capacity formula (discussed later) and considering $P_T = P_1 + P_2$ as [12]:

$$R_1 = \log_2 \left(1 + \frac{P_1 \cdot |h_{SD}|^2}{P_2 |h_{SD}|^2 + \sigma_n^2}\right) \tag{1.2}$$

$$R_2 = \log_2 \left(1 + \frac{P_2 \cdot |h_{SD}|^2}{\sigma_n^2}\right) \tag{1.3}$$

where σ_n^2 represents the noise level. Capacities in (1.2) and (1.3) demonstrate the concept of the rate-splitting with different layers having different maximum bit rates (in 1Hz) depending on power allocation P_1 and P_2 out of the total power P.

1.2 Alternate Relaying with Superposition Coding

While relays offer advantages in terms of reliability and extended coverage, they also introduce challenges, including a reduction in capacity. Conventional relay-based communication with relays operating in half-duplex mode typically takes around twice the time compared to direct communication between the source and destination. In this setup, the source uses one time slot to transmit signals to the relay, and the relay utilizes another time slot to forward these signals to the destination. This reduction in the capacity of the link between the source and destination is commonly known in the literature as the pre-log factor [13].

To address the issue of reduced spectral efficiency in half-duplex wireless relay networks, for one-way communication between the source and the destination, researchers have pursued time-division duplexing (TDD). Alternative relaying also named successive relaying as visualized in Fig. 1.2 allows the transmitter to send signals continuously, while relays take turns listening to the transmitter. The relays efficiently employ the same frequency band resources as the transmitter. A relay, upon completing a listening session, successively re-transmits the received signals to the destination. In each time slot, one relay receives new data from the transmitter, while the other relay forwards the previous data to the destination. This process is then reversed in the subsequent time slot. The relays continually alternate between listening and transmitting operations.

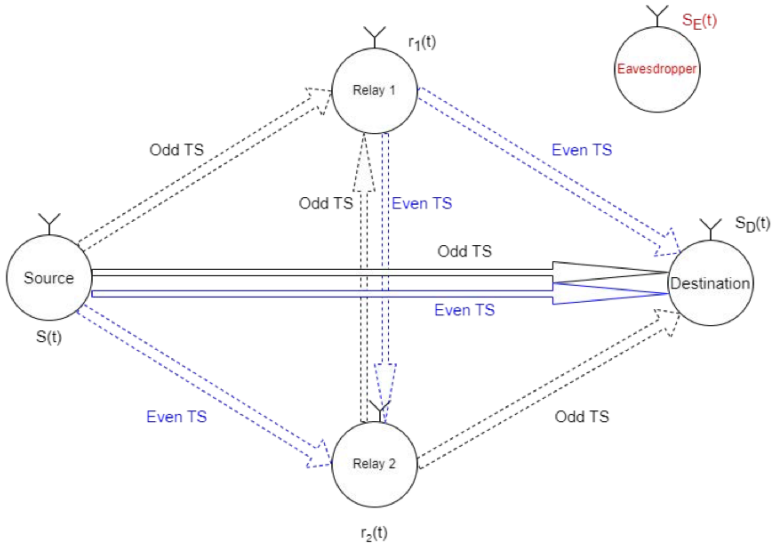

Figure 1.2: Two-path successive relaying network.

As indicated in Fig. 1.2, the individual procedures in different time slots can be explained as follows:

- In the first time slot (TS) which is an *odd* TS, the source transmits a signal $s(1)$ while R_1 is actively listening to the signal from the source and the other relay R_2 keeps silent (only in the 1st TS), the destination keeps acquiring the signal. (Indices within parenthesis indicate time.)

- In the second time slot which is a *even* time slot, the source transmits a signal $s(2)$ while R_2 is actively listening to the signal from the source, however the other relay R_1 forwards the previously received signal which is $s(1)$ to the relay R_1 and the destination rather than acting silent in the previous time slot, therefore, R_2 not only receives the signal from the source but also obtains the signal which is acting as interference from R_1. Furthermore, the destination keeps acquiring the signal $s(2)$ and $s(1)$ from the source and R_1, respectively.

- In the next *odd* TS, which is the third time slot, the source still continuously transmits the signal $s(3)$, which will be received by R_1. Meanwhile, the R_2 sends the signal $s(2)$ from the second time slot to interfere with the R_1. In addition, the destination receives $s(3)$ from the source and $s(2)$ from the relay.

- In the next *even* time slot which is the fourth time slot, the source continuously

sends the signal $s(4)$ to the relay R_2. The R_1 sends the signal from the previous time slot $s(3)$ to the R_2 which is considered as interference while the destination acquires the signal $s(4)$ from the source and the signal $s(3)$ from the R_1

Therefore, as indicated from the steps, we can generalize the process of how signal moves during the *odd* time slots, shown in the figure in blue and *even* time slots, represented by black.

- In the n^{th} *even* time slots, the source transmits the signal $s(t)$, R_2 acquires $s(t)$ from the source and interferes by the signal $s(t-1)$ from R_1, and the destination receives both the $s(t)$ and $s(t-1)$ from the source and relay respectively.

- In the $(n+1)^{th}$ *odd* time slots, the source transmits the signal $s(t+1)$, R_1 acquires $s(t+1)$ from the source and interferes by the signal $s(t)$ from R_2, and the destination receives both the $s(t+1)$ and $s(t)$ from the source and relay respectively.

- Eventually, in the last time slot $(T+1)^{th}$, the destination only receives the signal $s(T)$ from the relay R_2.

Therefore, the pre-log factor in capacity calculations is improved from $\frac{1}{2}$ to $\frac{T}{T+1}$ because the source transmits T symbols to the destination in $T+1$ time slots.

The enhancement in the pre-log factor does have its trade-offs. In the course of the listening session, apart from the initial and final time slots, the signal transmitted by one relay can potentially interfere with the signal received by the other relay concurrently, as depicted in Fig. 1.2 through the lines between relays where the color of the lines corresponds to the times when the relays transmit and listen. Therefore, if not handled with care, Inter-Relay Interference (IRI) could potentially undermine the overall system performance.

However, Inter-relay interference (IRI) cancellation poses a significant challenge in the context of successive relaying. When employing Amplify-and-Forward (AF) relaying, IRI cancellation becomes even more formidable due to the amplification and forwarding of interference and noise between relay nodes to the destination. This leads

to a diminished Signal-to-Interference-plus-Noise Ratio (SINR). Inter-Relay Interference (IRI) can be effectively mitigated in successive relaying by employing various methods, including:

- Transmitter precoding.

- Signal processing techniques implemented at the relays.

- Post-processing methods at the destination.

In this thesis, in the system under study, we follow the deployment of SIC to eliminate IRI based on removing the interfering relay strongest signal first with three layer decoding as proposed originally in [14].

1.2.1 Capacity Challenges

Channel capacity is the maximum achievable data transmission rate in a communication channel. In the context of a Single-Input Single-Output (SISO) channel with Additive White Gaussian Noise (AWGN), the capacity denoted here as C_{AWGN}, is given by Shannon's capacity limit:

$$C_{\text{AWGN}} = \Big(\log_2(1 + \tfrac{|h|^2\, P}{\sigma_n^2}) \Big) \qquad \text{[bits/s/Hz]} \tag{1.4}$$

where h is the channel gain between the source and the destination, P is transmit power, σ_n^2 is the AWGN variance (power), and $\frac{|h|^2\, P}{\sigma_n^2}$ is interpreted as received SNR. It has to be emphasized that Shannon's capacity limit in (1.4) does not imply any specific signaling to achieve the maximum theoretical limit on bandwidth efficiency (or speed of transmission in 1 Hz of bandwidth) [15], [16]. To emphasize this, we include in Fig. 1.3 (after [17]), the diagram visualizing the theoretical limit C_{AWGN} as a function of SNR and bandwidth and power efficiencies (for the reliability at the bit error rate BER=10^{-5}) for different modulation and spectral efficiencies achieved by various coded and uncoded transmission methods.

If the SNR $\gamma = \frac{|h|^2\, P}{\sigma_n^2}$ in (1.4) is a random variable (RV) as it is the case for flat fading channels, the capacity is evaluated through averaging over probability density function (pdf) $f(\gamma)$ of instantaneous γ as:

$$C_{\text{AVG}} = \mathbf{E}\Big(\log_2(1+\gamma) \Big) = \int_0^\infty \log_2(1+\gamma) \cdot f(\gamma) d\gamma \tag{1.5}$$

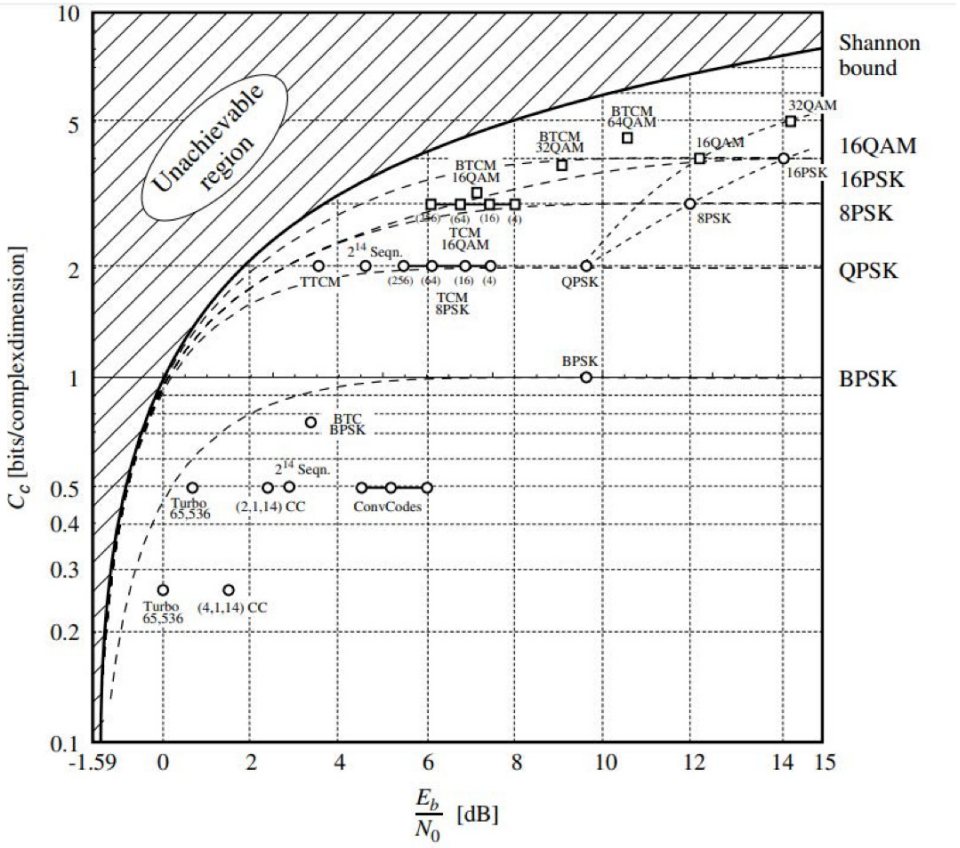

Figure 1.3: Theoretical limits on spectral and power efficiency for different signal constellations achieved by various coded and uncoded systems.

where $\mathbf{E}(\cdot)$ is the expectation operator and C_{AVG} is called ergodic capacity. In the case of Rayleigh fading channels (when $|h|$ in (1.4) is Rayleigh distributed), γ is an exponentially distributed RV with $f(\gamma) = \frac{1}{\overline{\gamma}} \exp\left(-\frac{\gamma}{\overline{\gamma}}\right)$ and the average SNR $\overline{\gamma}$. Therefore, for Rayleigh fading channels the ergodic capacity for 2D signaling as considered in this thesis is [17]:

$$C_{\text{Rayleigh}} = \frac{1}{\ln(2)} \exp\left(\frac{1}{\overline{\gamma}}\right) \mathbf{E_1}\left(\frac{1}{\overline{\gamma}}\right) \tag{1.6}$$

where $\mathbf{E_1}(x) = \int_x^\infty \frac{\exp(-t)}{t} \cdot dt$ is the exponential integral function implemented in Matlab as y=expint(x).

Because in this thesis, we work extensively with different forms of capacity limits given in (1.4), (1.5) or (1.6), our contributions as presented are more in the information-theoretic areas as what is achievable rather as how do we realized or implement the system to accomplish this limit.

1.2.2 Relaying Strategies

The signals received at the relays and at the destination undergo attenuation and modifications influenced by the wireless system environment. Consequently, relays are tasked with processing these received signals before retransmitting them to the next node. Relaying strategies are typically categorized based on how signals are handled at the relays. Among the prevailing relaying strategies, the most common and dominant relaying strategies are amplify-and-forward (AF) and decode-and-forward (DF) [18]. These two strategies have unique features in terms of their performance, complexity, flexibility, and how they handle signals.

The AF approach primarily involves processing analog signals. Relays simply amplify the received signal and forward them to the next hop nodes without decoding [18] and [19]. This strategy is favoured in systems where complex bit-level processing is required or when relays lack the capability to decode signals. Moreover, like any receiver, the signals received by the relays are subjected to additive white Gaussian noise (AWGN). The amplification of signals in the AF strategy also amplifies noise.

The DF approach pursued in this thesis deals with digital signals. In this strategy, relays decode the received signals first by eliminating all the effects from the receiving end, and later forward the new signals that have been encoded to the next nodes. While noise removal is a benefit of the DF scheme, it necessitates comprehensive data processing and decoding [20].

There are two modes that relays can operate with which are half-duplex (HD) or full-duplex (FD) mode. In HD, the relay can only perform either transmission or reception whereas in FD, the relay can simultaneously transmit and receive during a specific time slot. HD relay is easier to implement and is often the preferred choice thanks to its simpler design. In this work, we adopted DF strategy and HD mode for relays.

While the capacities presented in (1.4), (1.5) or (1.6) are applicable to point-to-point links, in this thesis, we consider the path with different layers capacities between the source and the destination where the path is composed of multiple hops and signals. In our analytical results developed, we will consider not only the bottleneck capacities of the slowest links but also have to examine the "interfering" signals

even though they carry useful information. Our goal is to motivate here the use of information bearing signals as a form of artificial noise affecting the detection capability by the eavesdropper in multi-node network topology.

1.3 Channel Modeling

Wireless systems' operation is significantly influenced by radio propagation conditions, and these conditions play a pivotal role in defining system performance. The signal attenuation with distance becomes a critical factor, especially when working with limited transmit power, as it directly impacts the received signal-to-noise ratio (SNR). Two distinct types of wireless propagation environments are examined: deterministic attenuation concerning distance and stochastic variations resulting from multi-path fading. Channel models are of paramount importance during the conceptual phase of communication system design. They serve as a means to simulate the diverse mediums that closely emulate real-world environments. Since we cannot implement in practice every conceptually proposed wireless communication system, the simulations aid in the prediction and assessment of wireless system performance when they are subjected to genuine and challenging propagation conditions. The calculation of the received signal power (or SNR) in telecommunication systems is called link budget analysis.

In this section, we review the specific propagation and fading conditions used in our field of research.

1.3.1 Deterministic Signal Attenuation with Distance

In the field of signal transmission, there is a fundamental concept that refers to an expected decrease in signal strength as a signal travels over a distance, which is named deterministic signal attenuation. There are various reasons for causing the attenuation such as power absorption by the transmission medium or bigger surface with distance the same power passes through for the same antenna size (aperture). Many investigations in literature have shown that the attenuation in different environments by utilizing numerous mathematical models [21]. In our work, we utilize a comprehensive formula that establishes a connection between power attenuation and

the distance traveled, which is expressed as follows:

$$P_r(d) = \frac{P_t}{d^\beta} \tag{1.7}$$

where P_r is the power of the received signal and P_t is the normalized power of the transmitted signal. Moreover, β is the attenuation exponent characterizing specific propagation conditions. The β is typically 2 in free-space propagation and 4 in ground wave propagation environments. Furthermore, the power attenuation exponent β is two times higher than the attenuation exponent for deterministic signal amplitude decay with the distance.

1.3.2 Additive White Gaussian Noise

Additive White Gaussian Noise (AWGN) is a type of noise that is encountered in all wireless communication systems because of thermal noise in RF front ends. It is superimposed on top of the original signal, which is important for determining the SNR in a communication channel. AWGN is defined by statistical properties of the Gaussian RV where, after matched filtering at the baseband, from the central limit theorem, the Gaussian distribution a with zero mean ($\mu = 0$) and a specific noise variance (σ_n^2) results from the superposition of small random effects (disturbances/RVs) [22]. The Gaussian RV with mean μ and variance σ_n^2 (measuring the amount of power in 1 Hz of signal bandwidth) is characterized by the probability density function:

$$pdf(n) = \frac{1}{\sqrt{2\pi\sigma_n^2}} exp^{\frac{-(n-\mu)^2}{2\sigma_n^2}} \tag{1.8}$$

Hence, the received signal in this work with the deterministic propagation conditions is be expressed as:

$$y(t) = \sqrt{P_r}s(t) + n(t) \tag{1.9}$$

where P_r is the received signal power and $n(t)$ indicates the noise added on top of the signal. In here, the SNR is determined as $\frac{P_r}{\sigma_n^2}$.

1.3.3 Rayleigh Fading

In wireless communications, slow Rayleigh fading is a result of micro-scale multipath signal propagation without dominant line-of-sight (LoS) transmission [23]. The

latter is the situation for the AWGN channel, and this is why the AWGN channel model represents the best-case scenario, and the Rayleigh channel model represents the worst-case scenario for wireless signal propagation. Rayleigh fading is modeled mathematically by multiplying the received signal with complex Gaussian RV $h = X + jY$ where $h \sim \mathcal{CN}(0,1)$ and X and Y are identical, independent distributed (i.i.d) real valued Gaussian RVs $X, Y \sim \mathcal{N}(0, \frac{1}{2})$. This multiplicative effect represents a random fading channel and is on top of the multiplicative effect associated with the deterministic signal attenuation related to the distance which controls the average SNR.

Working with the phasor interpretation of complex numbers, Rayleigh fading involves random variations in both the amplitude and phase of a radio wave during its journey from transmitter to receiver. This phenomenon arises from refraction, reflection, and scattering as the signal traverses multiple paths with distinct lengths and time delays. Consequently, the receiver captures various signal combinations (in-phase and out-of-phase additions), each experiencing individual attenuation and arriving at different times.

The Rayleigh complex RV represented as h has its name from the distribution of the magnitude (amplitude) of the multiplicative effect, which is denoted as $|h| = \sqrt{\Re(h)^2 + \Im(h)^2}$ is the Rayleigh RV, where the $\Re(h) = X$ and $\Im(h) = Y$ represent the real and the imaginary values of fading $\mathcal{CN}(0,1)$ coefficient h. Since $|h|$ follows a Rayleigh distribution, its probability density function can be expressed as:

$$pdf(|h|) = \frac{2|h|}{2\sigma_h^2} exp^{\frac{|h|^2}{2\sigma_h^2}} \tag{1.10}$$

where, in our case, $\sigma_h^2 = 1$ does not affect the average SNR determined by the attenuation of the signal with the distance.

The signal that passes through a Rayleigh fading channel at the receiver side in this work is expressed:

$$y(t) = \sqrt{P_r} \cdot h \cdot s(t) + n(t) \tag{1.11}$$

in which the instantaneous SNR is $\gamma = \frac{P_r |h|^2}{\sigma_n^2}$ and the average SNR $\overline{\gamma} = \frac{P_r}{\sigma_n^2}$ is controlled by the distance (deterministic signal attenuation).

1.4 Physical Layer Security

Recent research has shown substantial interest in physical layer security (PLS), which aims to protect data confidentiality using information-theoretic methods [1]. PLS has gained attention as both an alternative and a supplementary method to conventional cryptographic techniques [20]. In contrast to conventional cryptographic methods, physical layer security leverages the inherent weaknesses of wireless channels, including noise, fading, attenuation, and interference, to enhance signal reception for the intended recipient while degrading the quality of received signals for potential eavesdroppers. By incorporating this approach, we can utilize simpler cryptographic methods in higher protocol layers, combined with a physical layer approach. This is with the objective of hopefully achieving "nearly perfect secrecy". Essentially we try to ensure that the intended receiver can reliably access the source information, while eavesdroppers remain unable to decipher the transmitted message.

A generic model of wireless communication from a security perspective is demonstrated in Fig. 1.4. There are three nodes in this model, commonly called in the security literature as: Alice, Bob, and Eve. Alice is acting as a source for transmitting the signal to the legitimate receiver, which is Bob, while Eve is the eavesdropper (passive attacker) who only intercepts the transmission [4]. There are two channels, as indicated in the diagram, which are the main channel and the wiretap channel. The main channel is the link between Alice and Bob and the wiretap channel is from the source to the eavesdropper. Therefore, the secrecy capacity can be improved by two simple approaches either increasing the capacity of the main channel or reducing the capacity of the wiretap channel. In this work, Alice will be represented by two half-duplex relays and the original source. In our model, the achievable secrecy capacity will be analyzed by considering the achievable secrecy rate as the minimum of both the secrecy rate of the Source-to-Relay (S-R) link and the Relay-to-Destination (R-D) link [4].

The eavesdropper could take an active or passive role. Active Eve might attack the wireless system by sending a jamming signal that causes Denial-of-Service (DoS), whereas passive Eve is capable of intercepting the transmitted message. It's important to note that Eve is not necessarily a malicious terminal; it could be a legitimate

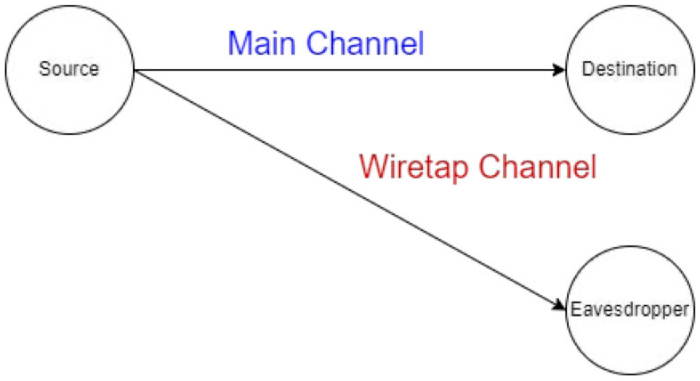

Figure 1.4: Generic model of physical layer security

terminal that should not receive content intended for other terminals. In this thesis, the emphasis is on passive eavesdropping.

1.4.1 Secrecy Capacity

To characterize the PLS performance, we utilize the achievable secrecy rates (usually 1Hz which scales linearly to a given bandwidth) at which the information could be transmitted between the source and the destination reliably with "close" to zero probability of being decoded by the eavesdropper. The maximum achievable secrecy rate is defined as the secrecy capacity. Essentially, the secrecy capacity is similar to the traditional capacity with the additional constraint of maintaining confidentiality. This can be expressed as the disparity between the capacities of the primary channel and the wiretap channel. In the context of fading channels, ergodic secrecy capacity is considered, representing the average performance over multiple independent channel realizations for a specific location of the eavesdropper and the intended receiver. It is important to note that the actual achievable secrecy rate may vary in practical implementations but should not surpass the secrecy capacity. Therefore, the secrecy capacity of the main channel is calculated as:

$$C_S = [C_B - C_E]^+ \tag{1.12}$$

where $[x]^+$ represents $max(x, 0)$, which means the secrecy capacity is never less than zero. When signals are transmitted directly from the source to the destination over channels with a deterministic attenuation (with distance) and are only affected by

the AWGN in the wiretap model, the secrecy capacity is evaluated by:

$$C_{\text{S,AWGN}} = \big[\log_2(1+\frac{P_{r,D}}{\sigma_{nD}^2}) - \log_2(1+\frac{P_{r,E}}{\sigma_{nE}^2})\big]^+ \tag{1.13}$$

where the subscripts in the received signal and noise powers indicate the nodes (and their corresponding capacities).
When signals are transmitted over Rayleigh fading channels, the secrecy capacity is expressed by:

$$C_{\text{S,Rayleigh}} = \mathbf{E}\Big[\log_2(1+\frac{|h_{SD}|^2 P_{r,D}}{\sigma_{nD}^2}) - \log_2(1+\frac{|h_{SE}|^2 P_{r,E}}{\sigma_{nE}^2})\Big]^+ \tag{1.14}$$

where $\mathbf{E}(\cdot)$ is the expectation operator, which in our simulations is replaced by time averaging over different realizations of multiplicative RV factors like $|h_{SD}|$ and $|h_{SE}|$. Also, when developing secrecy capacities formulas in Chapter 2 and 3, we will not include explicitly $\mathbf{E}(\cdot)$ operators and the ergodic averaging is implied by the fading channel as opposed to the deterministic propagation channels with AWGN. Generic P_r in (1.13) and (1.14) represents the power of the received signal due to the deterministic attenuation of the signal. Also, σ_{nD}^2 and σ_{nE}^2 describe the AWGN at the destination and the eavesdropper respectively. The channel coefficient $|h_{SD}|$ between the source and the destination and $|h_{SE}|$ between the source and the eavesdropper are instantaneous RVs not affecting the average SNRs. Our objective is to maintain confidentiality, ensuring that the secrecy capacity (SC) remains strictly positive. Typically, the capacity of additive white Gaussian noise (AWGN) channels exceeds that of Rayleigh fading channels, and similar expectations could be made for secrecy capacity, although there are no guarantees.

When working with relay transmissions operating in Decode-and-Forward mode which are utilized later in this work, the secrecy capacities are calculated using more complex formulas than those in (1.13) and (1.14) [4]

1.4.2 Artificial Noise

The primary concept behind introducing artificial noise (AN) is to safeguard the legitimate receiver from any adverse impact, while simultaneously raising the noise level in the eavesdropper's signal, making it unreliable for data detection. In this

thesis, we employ the enhancement layer as a naturally occurring substitute for AN within our system model. Consequently, the eavesdropper becomes "confused" and finds it challenging to decode the information-bearing signals intended only for the legitimate destination. The AN strategy is deployed in our SISO system setup with the aid of cooperative relays. While AN could be deployed in MIMO systems, it does require more complex resource allocation and is not pursued in this thesis [24], [25].

1.5 Thesis Objectives

The general objective of this work is to characterize the secrecy capacity of two-path successive relaying wireless networks with the legitimate receiver and the eavesdropper adopting the same or different decoding strategies depending on the eavesdropper's position with respect to the source. The focus is on networks where the signal decoding at the destination does not only depend on the relay signals, but the destination benefits in its decoding from source transmissions, i.e., the direct line of sight (LoS) between the source and the legitimate destination. The primary drawback of the conventional relaying system with single layer transmissions and retransmissions is that when the eavesdropper is situated closer to the relay than the intended recipient, the secrecy capacity is typically reduced to zero. This is because the eavesdropper has a higher SNR than the destination. However, with multi-layered transmissions, the secrecy capacity could be enhanced in the same situation because the capacities from two relays at the eavesdropper experience disparities because of different distances. Also, when the eavesdropper adopts the conventional detection of the signal from the source only, the relay signals act as the source of AN.

The focus of the analytical aspects of this thesis is to derive the formulas for the capacities at the destination and the eavesdropper as a function of different distances in the wireless network under study. These derivations assume perfect noise/signal cancellation through SIC and the availability of CSI in the form of channel gains between relays/source and the destination/eavesdropper. The practical implementations for the distribution of CSI and perfect SIC is beyond the scope of this thesis. When calculating secrecy capacities, we initially develop the formulas for AWGN channels, and then considering that fading channels are essentially AWGN channels

requiring time averaging over the realization of random gain coefficients, we handle the ergodic capacity in Rayleigh fading channels through simulations. The impact of different (βs) deterministic propagation conditions is also analyzed.

It is not feasible to assess the performance of decoding algorithms only through analytical methods in this thesis because of the complexity of the algorithms. Therefore, simulations are crucial in the analytical context of this thesis. As such, all proposed schemes and strategies are evaluated using semi-numerical methods and Monte-Carlo simulations and the results are visually presented and compared using MATLAB. This is an admissible approach for this type of research and analysis in networks with high complexities.

1.6 Thesis Organization

The remainder of this thesis is organized as follows:

In Chapter 2, we focus on a two-path relaying network with received signals representing a single data stream (from one of the relays) which is superimposed on two data streams from the source (with different power levels). In this system, the legitimate recipient and the eavesdropper are using the same decoding strategy. We present decoding at the relays and the legitimate destination (which is the same as at the relay) and we explain the source of "confusion" at the eavesdropper coming from the delayed enhancement layer acting as the artificial noise or just the distance disparity between two relays and the eavesdropper. The allocated and received power for each layer is analyzed and SNRs (with their corresponding capacities) are derived for different layers. With these, the secrecy capacities are calculated. The impact on received signal powers of each terminal position is also discussed. In the end, we evaluate the secrecy performance of each layer in terms of secrecy capacity as a function of Eve's position in both AWGN and Rayleigh fading environments.

In Chapter 3, we consider the same communication system and the same superimposed data streams as in Chapter 2 except a different decoding strategy is used by the eavesdropper. The intended receiver follows the same decoding strategy as in Chapter 2 optimized for the destination position. In this setup, the eavesdropper is

attempting i) to take advantage of being closer to the source and ii) to benefit only from LoS transmission from the source. However, it is demonstrated through secrecy capacity calculations that in this scenario, the retransmitted signal from the relays indeed adversely affects the eavesdropper and relays act as the source of artificial noise. Finally, the secrecy capacity of each layer is determined through analytical derivations and through simulations as a function of the eavesdropper's position in both AWGN and Rayleigh fading channels.

Chapter 4 provides conclusions and potential future investigations.

Chapters 2 and 3 are presenting contributions that are unique to this thesis.

Chapter 2

Secrecy Analysis with Destination and Eavesdropper Following the Same Decoding Strategy

The primary objective of this chapter is to analyze the secrecy capacity within the studied system when both the destination and eavesdropper employ the same decoding strategy. In the system with alternate relaying and two-layer transmission, signal transmission power is optimized for the destination's specific location. As anticipated and validated through simulations, the eavesdropper's position detrimentally influences its ability to recover signals of interest from both layers. More precisely, the detection capacity for the enhancement layer $s_2(t)$ is impacted by the increased distance from one of the relays, resulting in a difference in capacities between the destination and eavesdropper.

The decoding strategies in the alternate relaying system with the two-layer transmission have been previously explored in [14] and [26], and for the sake of completeness, they are reviewed in Section 2.1. However, the main emphasis of this thesis is to enhance our comprehension of the secrecy capacity at the legitimate destination. Therefore, in this chapter, we undertake a comprehensive secrecy analysis and evaluate the performance for both AWGN and Rayleigh fading environments.

This chapter is structured as follows: Section 2.1 introduces layered transmission (referred to as superposition coding) in the alternate relaying network. Specifically, this section presents the signal decoding at the relays and the legitimate destination with the corresponding SNRs for decoding two layers. Section 2.2 presents analytical derivations for secrecy capacity for each layer when the receiver and eavesdropper adopt the same decoding strategy. Section 2.3 demonstrates the simulation results, assessing the system's performance in terms of secrecy capacity for both AWGN and Rayleigh fading environments. Section 2.4 concludes a summary of this chapter.

2.1 Alternate Relaying Using Superposition Coding

We employ a two-path alternate relaying system comprising four components: a source, two half-duplex relay nodes (R_1, R_2), and a destination, as illustrated in Fig. 2.1. In this system, the source consistently transmits information, aided by the relays, which alternate between receiving and forwarding signals to the destination.

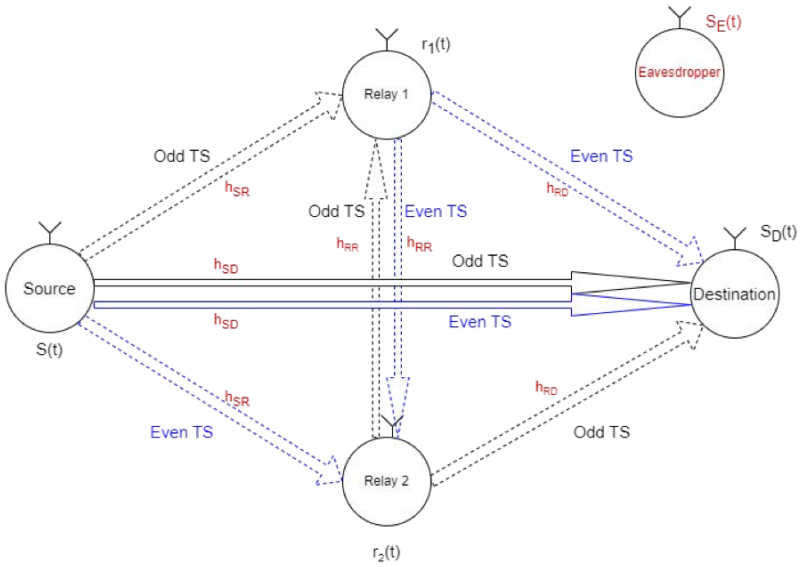

Figure 2.1: The system model: Two-path successive relaying network.

The links in the system are affected by AWGN, and in addition, they experience Rayleigh fading, which we will evaluate in two scenarios. In this network, the channel gain coefficients between the source and relays are denoted as h_{SR}, the channel gain coefficient between the source and the destination is given as h_{SD}, the channel gain coefficients between the relays are expressed as h_{RR} (assumed to be reciprocal), and h_{RD} represents the channel gain coefficients between the relays and the destination. Furthermore, the power levels of the AWGN at both relays and the destination are initially normalized to one.

Furthermore, our work is based on the half-duplex mode of operation for relays. Cooperation is accomplished within a span of two turns between the source and the destination. Moreover, the re-transmissions from relays cause inter-relay interference (IRI), which is removed by using the successive interference cancellation approach. This method also impacts the reception at the destination. In our research, we assume

that the reception times at both the relays and the destination for various signals from the source and relays occur simultaneously, implying a synchronized state within the node or network. However, being synchronized during data transmission might not always be adequate, as the actual requirement is synchronous reception.

The implementation of SC by the source is achieved by splitting a source message (k bits) into two layers: the base layer and the enhancement layer, with k_1 and k_2 bits in each layer, where $k_1 + k_2 = k$. These layers correspond to QAM symbols from the M_1-QAM and M_2-QAM constellations, where $M_1 = 2^{k_1}$ and $M_2 = 2^{k_2}$. If we were using M_1-QAM and M_2-QAM for $s_1(t)$ and $s_2(t)$, we would have the capacity $C_1 = k_1$ [bps/Hz] and $C_2 = k_2$ [bps/Hz]. However, in our information-theoretic analysis within this thesis, we refrain from explicitly detailing the value of k_1 and k_2, as well as the specific modulations and forward error control codes necessary for achieving these capacities. The emphasis is on pursuing the maximum possible capacities while considering various SNR environments.

Assume that SC is deployed by the source to send the message to the destination. The source signal $s(t)$ is superimposed by the two data streams, denoting the base and enhancement layers. This superimposed signal is described by the following equation:

$$s(t) = \sqrt{P_T} \cdot \Big(\alpha_1 s_1(t) + \alpha_2 s_2(t)\Big) \tag{2.1}$$

where $s_1(t)$ represents the base layer and the enhancement layer is denoted by $s_2(t)$. This notation indicates that the two modulated signals, s_1 and s_2, have the same unit energy, i.e., $\mathbf{E}|s_1|^2 = \mathbf{E}|s_2|^2 = 1$, where $\mathbf{E}(\cdot)$ is the expectation operator. Furthermore, each layer is associated with a different power level represented by the power fraction $\alpha_{1,2}^2$, given that (i) $0 < \alpha_i^2 \leq 1$, $i \in 1, 2$, (ii) $\alpha_1^2 + \alpha_2^2 = 1$, and P_T is the total transmit power at the source. Therefore, the assigned power for the base layer is $P_1 = \alpha_1^2 \cdot P_T$, and the power of the enhancement layer is $P_2 = \alpha_2^2 \cdot P_T$. These powers are combined as the total transmit power at the source, where $P_1 + P_2 = P_T$.

2.1.1 Processing and Capacities at the Relays

From the relay's perspective, the primary feature of the SC is the implementation of Successive Interference Cancellation (SIC) to remove the IRI and access the

superimposed layers. At the source, these layers have been prearranged based on the allocated fraction of the total power, as indicated in (2.1). As depicted in Fig. 2.1, R_1 receives a composite signal formed by contributions from both the source and the other relay, R_2. This signal can be defined as:

$$r_1(t) = h_{SR} \cdot \left(\sqrt{P_T} \cdot \left(\alpha_1 s_1(t) + \alpha_2 s_2(t) \right) \right) + h_{RR} \sqrt{P_T} s_2(t-1) + n_{R_1}(t) \tag{2.2}$$

where $n_{R_1}(t)$ is the AWGN at the relays and the $h_{RR}\sqrt{P_T}s_2(t-1)$ represents the IRI between relays. Three signals will be decoded by the relay in the following order: $s_2(t-1)$, $s_1(t)$, and $s_2(t)$ out of (2.2). Ultimately, the relay will only be forwarding data from $s_2(t)$.

First, the relay recovers $s_2(t-1)$ from (2.2) since the relays are close to each other. In free space propagation where the path attenuation factor $\beta = 2$, the expectation value of the channel gain coefficient between relays $E(|h_{RR}|^2) = \frac{1}{d_{RR}^2}$ and the expectation value of the channel gain coefficient between the source and the relay $E(|h_{SR}|^2) = \frac{1}{d_{SR}^2}$, which gives SNR for decoding $s_2(t-1)$ which is $\frac{E(|h_{RR}|^2)}{E(|h_{SR}|^2)} = \frac{d_{SR}^2}{d_{RR}^2}$. In our simulation later on, the SNR is given by $\frac{\left(\frac{\sqrt{39}}{2}\right)^2 + \left(\frac{1}{2}\right)^2}{\left(\frac{1}{2}+\frac{1}{2}\right)^2} = 10$. In the ground wave propagation, the SNR is given by $\frac{\left(\frac{\sqrt{39}}{2}\right)^4 + \left(\frac{1}{2}\right)^4}{\left(\frac{1}{2}+\frac{1}{2}\right)^4} = 95.1$. With this SNR, the first term in (2.2) is equivalent to the signal directly from the source, which can be considered as noise. As such, $s_2(t-1)$ can be decoded reliably with this SNR = 10dB regardless of the propagation environment (β), assuming the power of $n_{R_1}(t)$ is not excessive.

Second, the relay utilizes SIC to remove the impact of $s_2(t-1)$ and recovers $s_1(t)$ from (2.3) because it is associated with the second highest power among $s_2(t-1)$, $s_1(t)$ and $s_2(t)$ represented in (2.2). Assuming that $s_2(t-1)$ is decoded correctly, the relay can remove its impact from (2.2), and with this, the relay uses it for recovering $s_1(t)$.

$$\hat{r_1}(t) = h_{SR} \cdot \left(\sqrt{P_T} \cdot \left(\alpha_1 s_1(t) + \alpha_2 s_2(t) \right) \right) + n_{R_1}(t) \tag{2.3}$$

In the end, to recover $s_2(t)$ in (2.3), the relay uses SIC again to remove the impact of $s_1(t)$ and the relay recovers $s_2(t)$ from:

$$\hat{\hat{r_1}}(t) = h_{SR} \cdot \sqrt{P_T} \cdot \alpha_2 s_2(t) + n_{R_1}(t) \tag{2.4}$$

It is the data represented by $s_2(t)$ that the relay forwards to the destination in the next time slot (TS). However, processing occurring at the relays is not critical for further developments in this thesis as long as the relay will forward $s_2(t)$.

At the relays, the attainable data rate of the base layer is denoted by $C_R^{S_1} = \log_2\left(1 + \frac{|h_{SR}|^2 P_1}{|h_{SR}|^2 P_2 + \sigma_R^2}\right)$ after mitigating the interference of $s_2(t-1)$. The achievable capacity of the enhancement layer is given by $C_R^{s_2} = \log_2\left(1 + |h_{SR}|^2 P_2\right)$, i.e., decoding the base layer is constrained by the power allocated to the enhancement layer, which causes interference. Therefore, the total data rate is limited by $C_R = \log_2\left(1 + |h_{SR}|^2 P_T\right)$.

The information transmission is beneficial through the direct link between the source and the destination. The achievable data rate at the destination is represented by R_D, which is $R_D \leq C = \log_2\left(1 + \frac{|h_{SR}|^2 P_1}{|h_{SR}|^2 P_2 + \sigma_R^2}\right)$.

In this network, the relays R_1 and R_2 operate in the Decode-and-Forward mode with channel information between the source and relays. Therefore, the relays are capable of decoding three layers, $s_2(t-1)$, $s_1(t)$, and $s_2(t)$ out of (2.2). However, while the destination can recover both the base and enhancement layers with the assistance of relays, the destination can only decode $s_1(t)$ because $s_2(t)$ is treated as noise. Consequently, the achievable data rate is enhanced by removing the impact of the enhancement layers transmitted through the direct connection between the source and the destination.

The need for the relays to transmit partial information from the source implies that the relays only forward the delayed enhancement layers to the destination. This arrangement facilitates a new data rate for decoding the base layer without interference from the enhancement layer. Moreover, the adoption of this alternate relaying approach aims to address the loss of spectral efficiency that occurs when using conventional relaying schemes.

2.1.2 Processing at the Destination

At the destination, the received signal comprises the direct link signal from the source and the delayed enhancement layers from the relay, represented as:

$$s_D(t) = h_{SD} \cdot \left(\sqrt{P_T} \cdot (\alpha_1 s_1(t) + \alpha_2 s_2(t))\right) + h_{RD}\sqrt{P_T} s_2(t-1) + n_D(t) \qquad (2.5)$$

where $n_D(t)$ is the AWGN at the destination with variance σ_D^2. In this thesis, it is assumed that the noise power, denoted by σ_D^2, is equal to the strength of the signal $h_{SD}\sqrt{P_T}\alpha_2 s_2(t)$ received at the destination, which represents the enhancement layer from the source. As introduced earlier, the h_{SD} is the channel gain coefficient between the source and the destination, and the h_{RD} is the channel gain coefficient between the relays and the destination.

Out of the composite representation of $s_1(t)$, $s_2(t)$, and $s_2(t-1)$ in (2.5), the signal $s_2(t-1)$ is decoded first at the destination first because the relay is closer to the destination than the source. Here, $s_2(t-1)$ denotes the delayed enhancement layer sent by the relays. This decoding approach builds on favorable channel conditions between the relays and the destination so that the signal transmitted by the source could be viewed as noise. The SNR influencing the detection of $s_2(t-1)$ in free space propagation is given by $\frac{E(|h_{RD}|^2)}{E(|h_{SD}|^2)} = \frac{d_{SD}^2}{d_{RD}^2} = \frac{\left(\frac{\sqrt{39}}{2}+1\right)^2}{\left(\frac{\sqrt{1}}{2}\right)^2+(1)^2} = 13.6$ when decoding $s_2(t-1)$ first out of (2.5). With this interpretation, taking into account the specific positions of the source, the destination, and the relays as presented later in Section 2.3. We can reliably retrieve the enhancement layer at the destination with this SNR, despite the one symbol delay. Additionally, since σ_D^2 is substantially smaller than the power of $h_{SD} \cdot \left(\sqrt{P_T} \cdot (\alpha_1 s_1(t) + \alpha_2 s_2(t))\right)$, we ignored it here.

The destination then employs SIC to eliminate the impact of $s_2(t-1)$ in (2.5) after knowing $s_2(t-1)$. This leads to:

$$\hat{s_D}(t) = h_{SD} \cdot \left(\sqrt{P_T} \cdot (\alpha_1 s_1(t) + \alpha_2 s_2(t))\right) + n_D(t) \tag{2.6}$$

The destination uses (2.6) to decode the base layer $s_1(t)$ in the present of $s_2(t)$, treating the latter as noise, similar to the Additive White Gaussian Noise (AWGN) decoding, after successfully removing $s_2(t-1)$ from (2.5).

When examining the capacities at the destinations to decode $s_2(t-1)$ and $s_1(t)$, the SNRs covered in this section are employed in Section 2.2.1.

2.1.3 Processing at the Eavesdropper

The received signal at the eavesdropper is represented as follows:

$$s_E(t) = h_{SE} \cdot \left(\sqrt{P_T} \cdot (\alpha_1 s_1(t) + \alpha_2 s_2(t))\right) + h_{RE}\sqrt{P_T} s_2(t-1) + n_E(t) \tag{2.7}$$

where h_{SE} represents the channel gain coefficient between the source and the eavesdropper, h_{RE} represents the channel gain coefficients between the relays and the eavesdropper, and $n_E(t)$ is the AWGN at the eavesdropper with variance σ_E^2, which is comparable to the AWGN at the destination. The channel gain coefficients h_{RE} are determined based on the worst-case scenario between the relays and the eavesdropper.

The eavesdropper employs the same decoding order as the destination to extract information. In the initial stage of Successive Interference Cancellation (SIC), the eavesdropper decodes the delayed enhancement layer $s_2(t-1)$, which has the highest power, as described in (2.7). This is illustrated below:

$$\hat{s_E}(t) = h_{SE} \cdot \Big(\sqrt{P_T} \cdot (\alpha_1 s_1(t) + \alpha_2 s_2(t))\Big) + n_E(t) \tag{2.8}$$

After successfully decoding the signal $s_2(t-1)$ and suppressing its effect from the received signal, the eavesdropper recovers the base layer $s_1(t)$ from (2.8).

2.2 Capacity and Secrecy Capacity Calculations

In this section, we provide a detailed explanation of the capacity at the relays, the destination, and the eavesdropper.

With reference to $P_1 = \alpha_1^2 \cdot P_T$ and $P_2 = \alpha_2^2 \cdot P_T$, along with the channel gain coefficients of different links between nodes, the capacity at the relays can be expressed as:

$$C_{Relay} = \frac{1}{2}\Bigg(\log_2\Big(1 + \frac{|h_{RR}|^2 P_T}{|h_{SR}|^2 P_2 + |h_{SR}|^2 P_1 + N_o}\Big) + \log_2\Big(1 + \frac{|h_{SR}|^2 P_2}{|h_{SR}|^2 P_1 + N_o}\Big)\Bigg) \tag{2.9}$$

where the first term in (2.9) is the data rate of $s_2(t-1)$, and the last term represents the data rate of $s_1(t)$.

The capacity in (2.9) is fixed when h_{ij} are deterministic numbers depend on distances between nodes i and j, i.e., (i=S and j=R) or (i=R and j=D) which can be represented as $h_{ij} = \frac{1}{d_{ij}^{\frac{\beta}{2}}}$. When the h_{ij} is representing Rayleigh fading channel, h_{ij} is denoted by $\frac{1}{d_{ij}^{\frac{\beta}{2}}}\big(X + jY\big)$, where X and Y denote the real and imaginary values of h, therefore, the capacity in (2.9) is a random variable. In the later situation, we need to evaluate the ergodic capacity of (2.9) by averaging in time over the number

of possible realization of h_{ij}, i.e., $C_{Relay}^{Avg} = \mathbf{E}(C_{Relay})$. To simplify the expressions, we only present formulas for capacities in a deterministic environment (without fading), but we will work in a fading environment later with average capacities are RV which is representing h_{ij}.

2.2.1 Capacity at Destination Using Relayed Signal First

Because the delayed enhancement layer signal is decoded first, the capacity of the delayed enhancement layer at the destination based on (1.4) is given by:

$$\begin{aligned} C_D^{s_2} &= \log_2\left(1 + \frac{|h_{RD}|^2}{|h_{SD}|^2(\alpha_1^2 + \alpha_2^2) + \sigma_D^2}\right) \\ &\approx \log_2\left(1 + \frac{|h_{RD}|^2}{|h_{SD}|^2(1 + \alpha_2^2)}\right) \end{aligned} \tag{2.10}$$

After successfully recovering the delayed enhancement layer signal from the received signal, the destination achieves a data rate for the base layer given by:

$$C_D^{s_1} = \log_2\left(1 + \frac{|h_{SD}|^2\alpha_1^2 P_T}{|h_{SD}|^2\alpha_2^2 P_T + N_o}\right) \tag{2.11}$$

where $N_o = |h_{SD}|^2\alpha_2^2 P_T$. which also can be written as:

$$C_D^{s_1} = \log_2\left(1 + \frac{\alpha_1^2}{2 \cdot \alpha_2^2}\right) \tag{2.12}$$

2.2.2 Capacity at Eavesdropper Using Relayed Signal First

In this chapter, we consider that the eavesdropper follows the same decoding as the desired destination. Therefore, the capacity for decoding $s_1(t)$ and $s_2(t)$ at the eavesdropper will have the same generic expression as at the destination, except that we have to account for different channel gain coefficients between the senders (source and relays) and the eavesdropper. Therefore, the capacity at the eavesdropper of $s_2(t-1)$ can be expressed as:

$$C_E^{s_2} = \log_2\left(1 + \frac{|h_{RE}|^2}{|h_{SE}|^2 + |h_{SD}|^2\alpha_2^2}\right) \tag{2.13}$$

and the capacity of the base layer is calculated as:

$$C_E^{s_1} = \log_2\left(1 + \frac{|h_{SE}|^2\alpha_1^2}{(|h_{SE}|^2 + |h_{SD}|^2)\alpha_2^2}\right) \tag{2.14}$$

When working with the channel gain coefficient h_{RE}, there are two coefficients, which are from R_1 to the eavesdropper and R_2 to the eavesdropper. However, we work with the worst-case scenario of two distances because we assumed that the network coding is used on data represented as $s_2(t)$ received from R_1 and R_2. Due to networking, we need to recover data from both R_1 and R_2 to get the data represented on $s_2(t-1)$. As a result, we can only retrieve data encoded on $s_2(t-1)$ to the extent that the two links have the lowest speed (capacity): between (i) R_1 and the eavesdropper and (ii) R_2 and the eavesdropper.

2.2.3 Secrecy Capacity Calculations

Secrecy capacity represents the theoretical upper limit of the maximum achievable secrecy rate. The secrecy capacity of the delayed enhancement layers is given by:

$$C_S^{s_2} = \left[C_D^{s_2} - C_E^{s_2}\right]^+ . \tag{2.15}$$

where $C_D^{s_2}$ is calculated as in (2.10) and $C_E^{s_2}$ is calculated as in (2.13).

Furthermore, the secrecy capacity of the base layers is given by:

$$C_S^{s_1} = \left[C_D^{s_1} - C_E^{s_1}\right]^+ . \tag{2.16}$$

where $C_D^{s_1}$ is calculated as in (2.12) and $C_E^{s_1}$ is calculated as in (2.14).

2.3 Performance Evaluation

In our simulation, the source, R_1, R_2, and the destination are fixed at specific locations as visualized in Fig. 2.2. The source is located at coordinates $(-\frac{\sqrt{39}}{2}, 0)$, and the destination is situated on the horizontal axis at coordinates $(1, 0)$. We do not specify the precise units for distances in this thesis because the actual distances rely on the transmit power P_t in (1.7), which is selected to be 1 in our simulation without stating the real-world value power unit (i.e., kilowatts or watts). The reason behind this choice is rooted in the modification of power and distance parameters to achieve reliable decoding at the destination. Specifically, adjustments were made to the power and distance settings with the aim of achieving SNRs for $s1(t)$ and $s2(t-1)$ at approximately 10dB. Relay R_1 is positioned on the vertical axis at coordinates $(0, \frac{1}{2})$,

R_2 is on the vertical axis at coordinates $(0, -\frac{1}{2})$. In this chapter, the position of the eavesdropper varies in the right-half plane initially within the square, which has a side length of 8, as illustrated in Fig. 2.2. The distances between each node characterize deterministic channel gain coefficients. We use $\beta = 2$ for free space propagation and $\beta = 4$ for ground wave propagation to account for the impact of various propagation environments. We assess the secrecy capacity performance of the network in both deterministic channels in Section 2.3.1 and channels with Rayleigh fading in Section 2.3.2. The initial average received SNR at the destination is approximately 10 dB for both layers, resulting in a BER of 10^{-5} achievable in real-world applications. Performance in Rayleigh fading channels in Section 2.3.2 is evaluated using Monte-Carlo simulations, averaging SNRs and link capacities over 10^6 independent channel realizations for a given position of the destination and the fixed position of the eavesdropper.

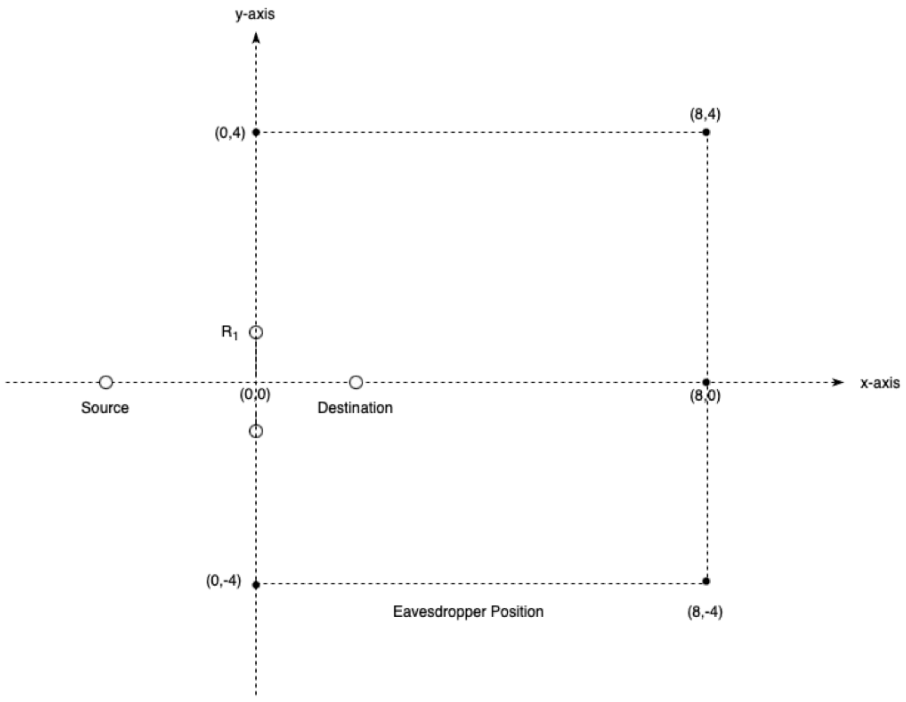

Figure 2.2: X-Y plane for the eavesdropper position.

When assessing the performance of the layered transmission, the power fraction parameter α_1^2 for the base layer $s_1(t)$ and α_2^2 for the enhancement layer $s_2(t)$ are chosen as 0.95 and 0.05, respectively. This choice results in an approximate 10^{-12}

BER for $s_1(t)$ and 10^{-5} BER for $s_2(t)$ in practical applications.

2.3.1 Simulations for AWGN

At the destination, in the AWGN environment when $\beta = 2$ for free space propagation, the theoretical capacity ($C_D^{s_2}$ and $C_D^{s_1}$) are calculated using (2.10) and (2.12) for the enhancement layer $s_2(t-1)$ and the base layer $s_1(t)$, respectively with $|h_{SD}|^2 = \frac{1}{d_{SD}^2}$ and $|h_{RD}|^2 = \frac{1}{d_{RD}^2}$. With the distances in our topology, this is $C_D^{s_2} = 3.8$ [bps/Hz] and $C_D^{s_2} = 3.4$ [bps/Hz]. Similarly, in the AWGN environment when $\beta = 4$ for ground wave propagation, the theoretical capacities $C_D^{s_2}$ and $C_D^{s_1}$ are obtained from (2.10) and (2.12), however this time with $|h_{SD}|^2 = \frac{1}{d_{SD}^4}$. Therefore, $C_D^{s_2} = 7.5$ [bps/Hz] and $C_D^{s_1} = 3.4$ [bps/Hz].

Considering (2.15) and (2.16), we observe that the secrecy capacity is the difference between the capacity at the desired destination and the eavesdropper. It should be noted that secrecy capacity has a limit, which is the capacity at the destination when the eavesdropper is extremely far away and its decoding capacity drops to zero. It should be observed that the destination's capacity in a given propagation environment remains constant since the destination location is maintained.

Figure. 2.3 presents a 2D slice plot for secrecy capacity. In this figure, the eavesdropper is moving down the line from the origin to the destination and eventually passes it. This corresponds in Fig. 2.2 to the x-axis when y = 0, indicating the distance of the eavesdropper from the origin along the x-axis. The secrecy capacity of the enhancement layer and the base layer when the eavesdropper is located at coordinates $(8, 0)$ which is the edge of the square as shown in Fig. 2.2 is 2.59 and 1.67 [bps/Hz], respectively.

Similar to Fig. 2.3, Fig. 2.4 depicts the secrecy capacity, but we let the eavesdropper move up to 100 from the origin along the x-axis. From Fig. 2.4, we can observe that when the eavesdropper is far away from the source, its capacity approaches zero. Consequently, the secrecy capacity approaches the capacity at the destination, which is 3.8 [bps/Hz] for the enhancement layer. Moreover, a similar observation can be made for the base layer.

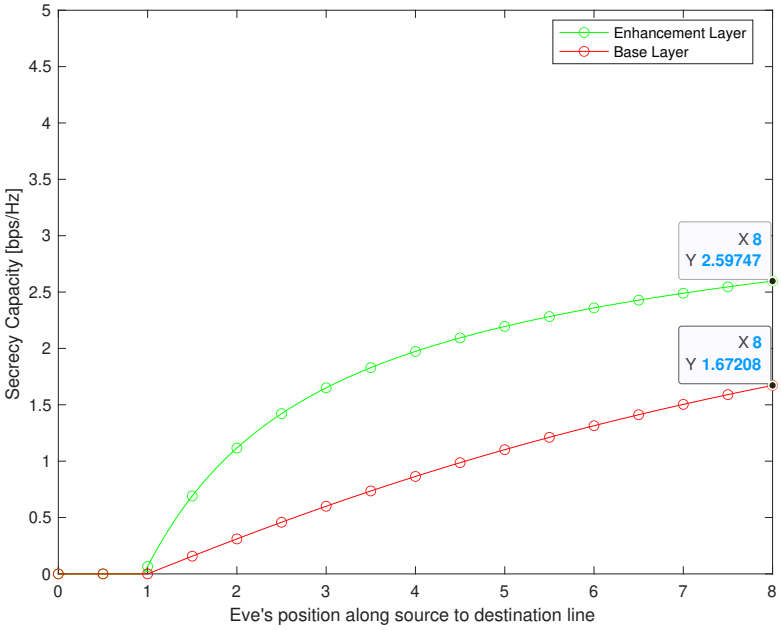

Figure 2.3: Secrecy performance when the eavesdropper is located along the x-axis (for $\beta = 2$ and in AWGN).

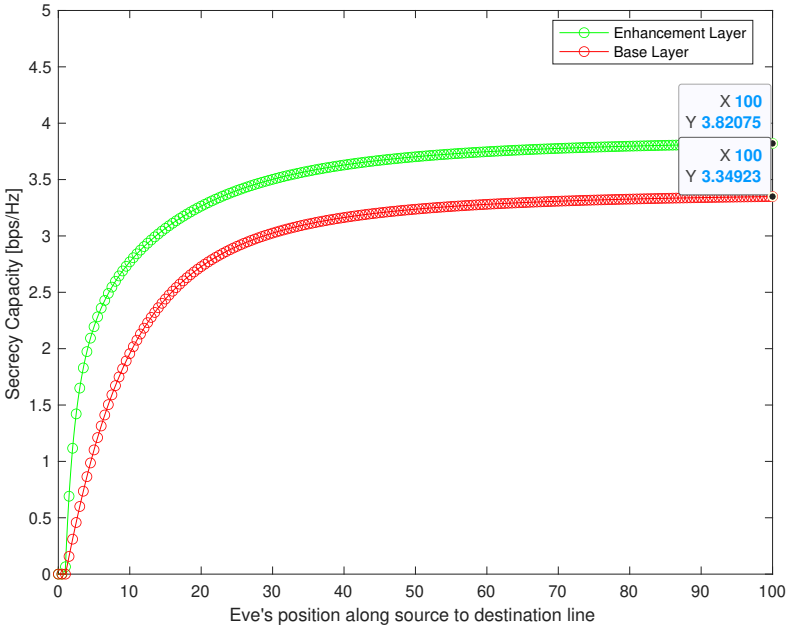

Figure 2.4: Secrecy performance when the eavesdropper is located along the x-axis and far away from the source (for $\beta = 2$ and in AWGN).

To provide a more comprehensive view of the system's performance, Fig. 2.5 displays a three-dimensional (3D) plot of the secrecy capacity along the z-axis and the x-y plane represents the eavesdropper's location inside the region depicted in Fig. 2.2. The results demonstrated in this 3D plot are for the AWGN propagation environment with $\beta = 2$ (free space propagation). The plots in Figs. 2.4 and 2.5 suggest that the secrecy capacity is rather poor if the eavesdropper is aware of the decoding strategy and it can position itself in the vicinity of the relays and the destination.

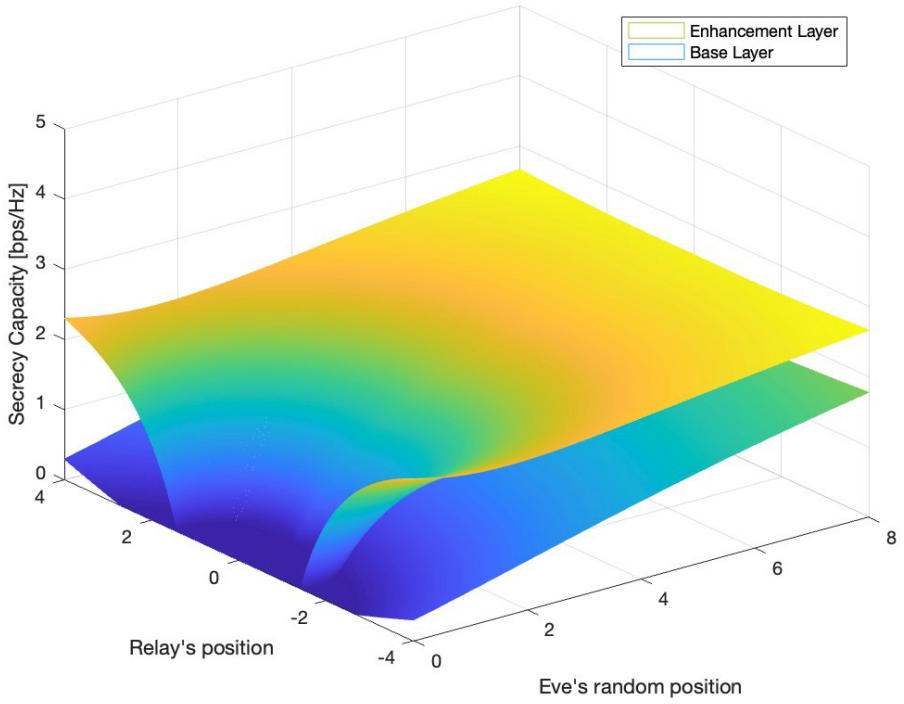

Figure 2.5: Secrecy performance along z-axis when eavesdropper is located in x-y plane (for $\beta = 2$ and in AWGN).

Furthermore, we study the influence of ground wave attenuation with $\beta = 4$ on the system's performance. In Fig. 2.6, the secrecy capacity of the enhancement layer and the base layer when $\beta = 4$ is represented by the green and red lines, respectively, and the purple line represents the secrecy capacity of the enhancement layer when $\beta = 2$, while the blue line represents the secrecy capacity of the base layer under the same condition. In this figure, similar to Fig. 2.4, the eavesdropper's position is along the x-axis, as in Fig. 2.2. Since the distance from the origin may be great, secrecy at

the edge position (when x = 100) is determined by the destination capacity. From Fig. 2.6, we can observe that secrecy capacity reaches its maximum faster with a bigger β than if $\beta = 2$. The reason is that a higher β contributes to enhanced security, as the capacity at the destination is maximized at a smaller rate, and the eavesdropper's SNR improves more rapidly with distance. The propagation environment with $\beta = 4$ makes the system more robust against eavesdropping. When the eavesdropper is far away, the secrecy capacity of the enhancement layer is equivalent to the capacity of $s_2(t)$ at the destination, which is 7.5 [bps/Hz] and there is a 3.7 [bps/Hz] improvement in secrecy capacity with the aid of a higher value of β.

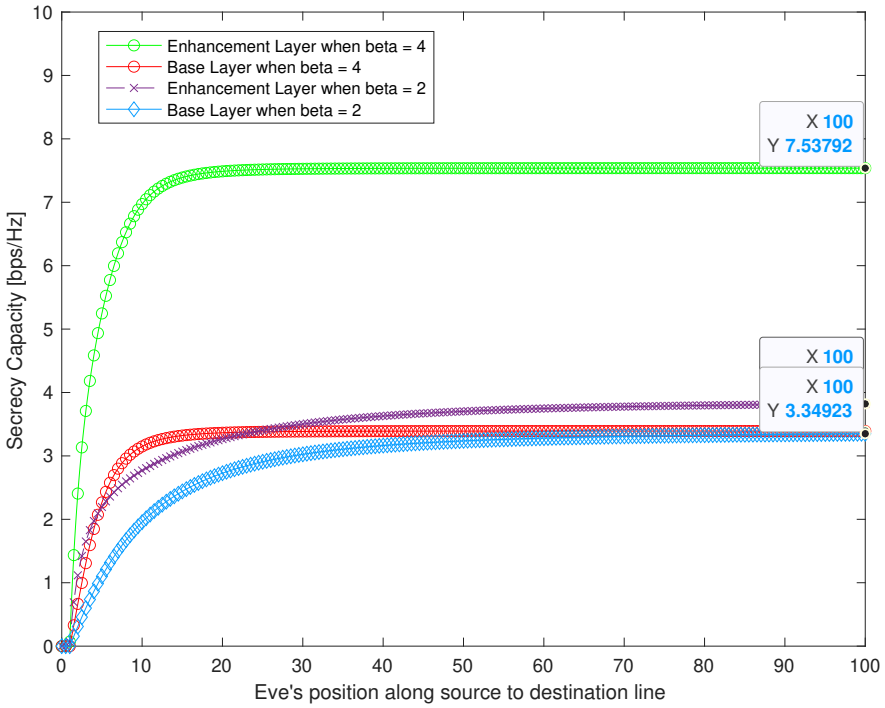

Figure 2.6: Secrecy performance when eavesdropper is located along the x-axis and far away from the source (for $\beta = 2$ and $\beta = 4$ comparison and in AWGN).

2.3.2 Simulations for Rayleigh Fading

In a Rayleigh fading environment, as indicated in Chapter 1, the secrecy capacity is the average of the secrecy capacity over several realizations of the multiplicative factors related to the Rayleigh fading in time. In Rayleigh fading environments,

when $\beta = 2$ with average SNRs of approximately 10dB, the theoretical capacity of the enhancement layer achieves 3.26 bps/Hz, and the base layer attains 2.85 bps/Hz. When $\beta = 4$ with the same average SNR, the capacity of $s_2(t)$ and $s_1(t)$ is 6.74 [bps/Hz] and 2.84 [bps/Hz] respectively.

Figure 2.7 provides a 2D slice plot illustrating the performance of the secrecy capacity in Rayleigh fading environments for both the base layer and the enhancement layer which corresponds to the simulation set up in AWGN and the result shown in Fig. 2.3. In both figures, the eavesdropper changes its position along the x-axis from the origin to the destination, as in Fig. 2.2. From Fig. 2.7, when the eavesdropper is located at coordinates $(8, 0)$, the secrecy capacity is 2.51 [bps/Hz] for $s_2(t)$ and 1.48 [bps/Hz] for $s_1(t)$ in Rayleigh fading, which is lower than the secrecy capacity in AWGN when the eavesdropper is located at the same position.

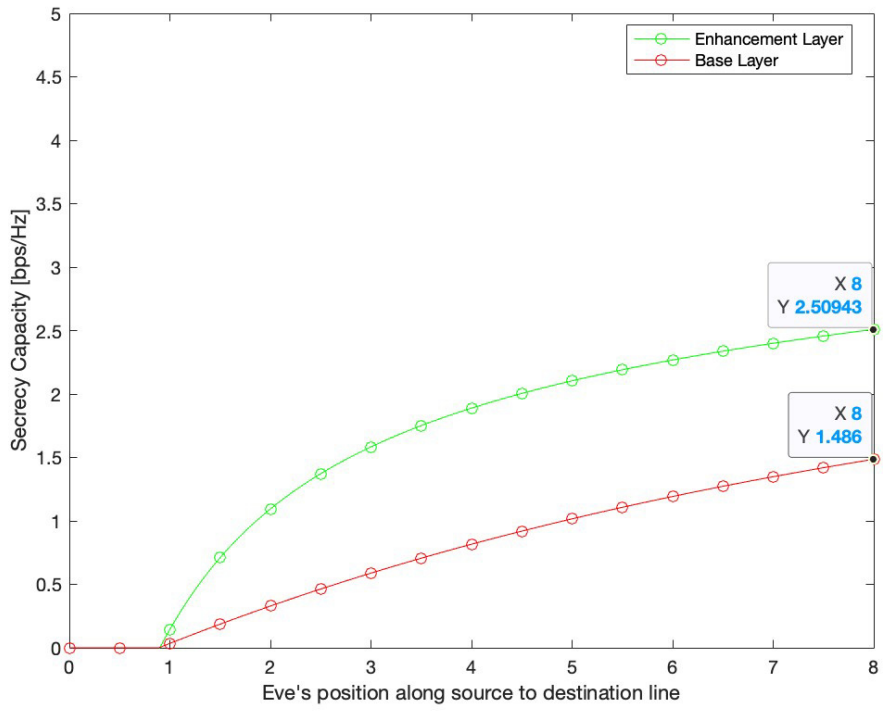

Figure 2.7: Secrecy performance when eavesdropper is located along the x-axis (for $\beta = 2$ and in Rayleigh fading).

The secrecy capacity is depicted in Fig. 2.8, which is similar to Fig. 2.7, except the eavesdropper is allowed to move up to 100 from the origin along the x-axis under the

Rayleigh fading propagation. As the eavesdropper moves farther away, its capacity approaches zero, and the secrecy capacity is equivalent to the capacity of the desired destination. With an average SNR of 13.59, the enhancement layer achieves a secrecy capacity of 3.51 [bps/Hz], closely aligning the calculated theoretic capacity of the enhancement layer at the destination (3.26 [bps/Hz]). Despite the calculated theoretical result being lower than the simulation result, we still consider it comparable as we did not account for the impact of the third layer $s_2(t)$.

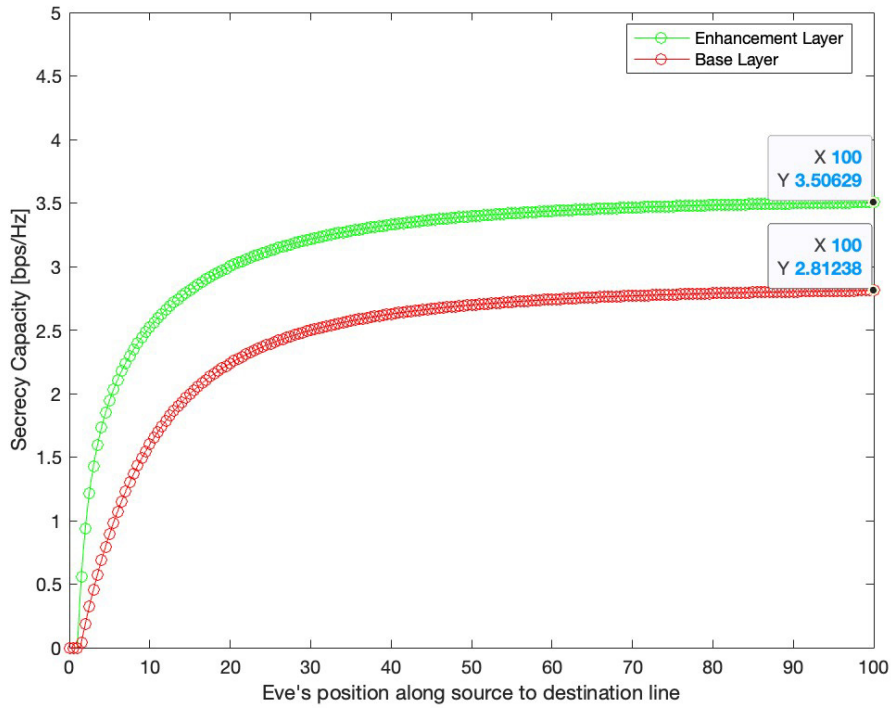

Figure 2.8: Secrecy performance when eavesdropper is located along the x-axis and far away from the source (for $\beta = 2$ and in Rayleigh fading).

Subsequently, we elaborate on the secrecy capacity results through the utilization of a 3D diagram as shown in Fig. 2.9. This 3D plot represents a propagation environment with Rayleigh fading and $\beta = 2$. Figure 2.9 provides the secrecy capacity along the z-axis when the eavesdropper moves around in a square (x-y plane) as shown in Fig. 2.2. Similarly to AWGN channels, Figs. 2.8 and 2.9 indicate that the secrecy capacity is relatively low if the eavesdropper knows the decoding approach and can adjust its location close to the relays and the destination.

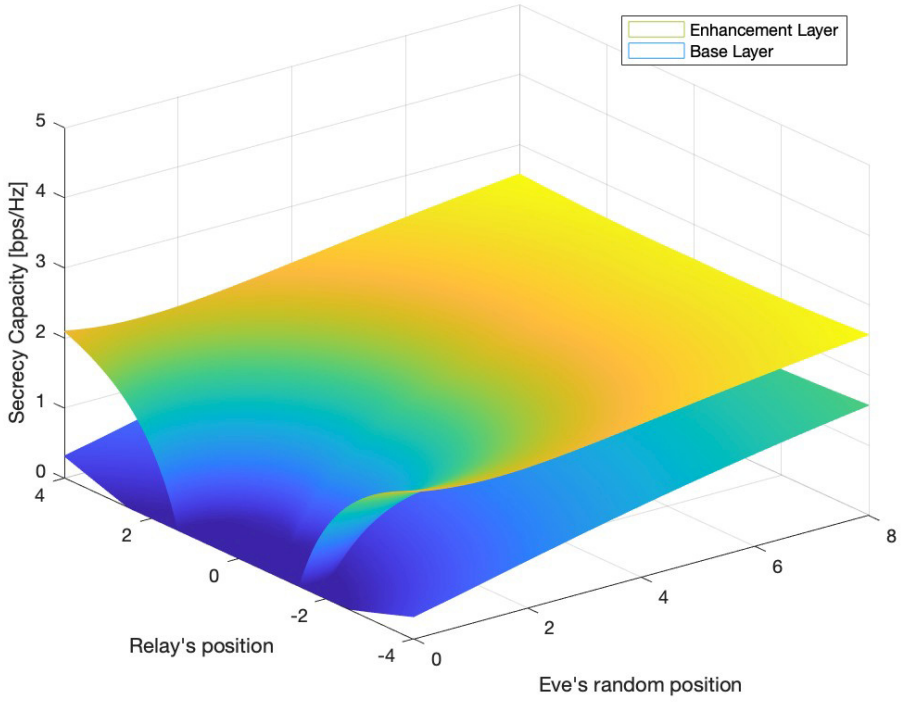

Figure 2.9: Secrecy performance along z-axis when eavesdropper is located in x-y plane (for $\beta = 2$ and in Rayleigh fading).

Figure 2.10 shows similar conclusions to those discussed in Fig. 2.6. However, this time, it pertains to the Rayleigh fading environment with the eavesdropper placed along the x-axis (on the line between the origin and the destination, but moving farther away than in Fig. 2.7 when $\beta = 2$). We present the secrecy capacities for two layers in the circumstances when $\beta = 2$ and $\beta = 4$. When $\beta = 4$, in the Rayleigh fading environment, using (1.6), $C_D^{s_2} = 7.1$ [bps/Hz] and $C_D^{s_1} = 3.6$ [bps/Hz], which are the same as the secrecy capacities when the eavesdropper is far away and its capacity is near to zero, confirming the correctness of our simulations to some extent.

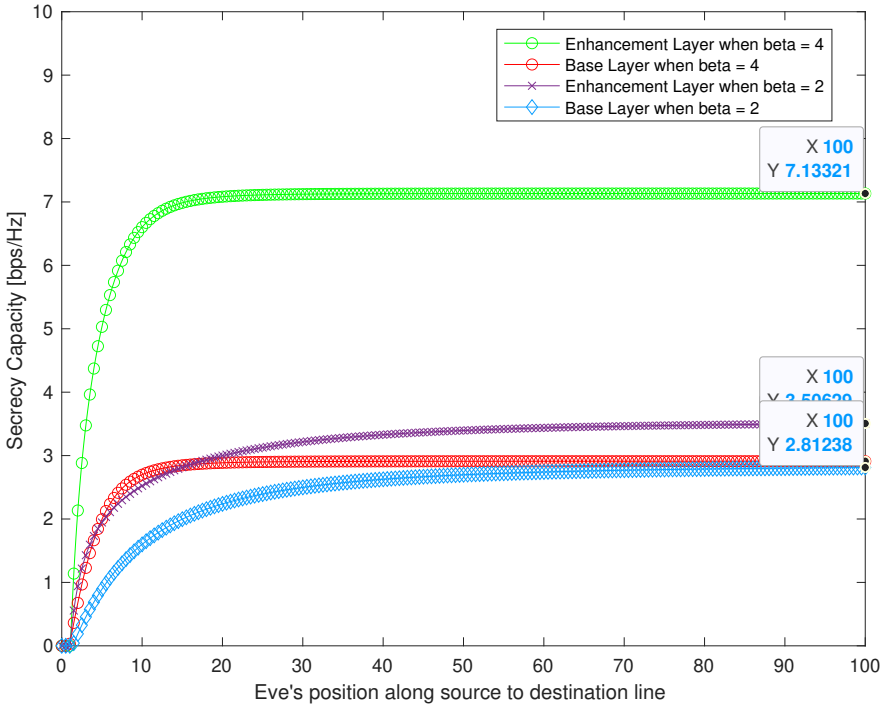

Figure 2.10: Secrecy performance when eavesdropper is located along the x-axis and far away from the source (for $\beta = 2$ and $\beta = 4$ comparison and in Rayleigh fading).

2.4 Summary

Our study focuses on a wireless network that uses successive relaying and layered transmission within a Single-Input Single-Output (SISO) configuration. The system includes two half-duplex relays that operate using the decode-and-forward (DF) strategy. However, if the eavesdropper is positioned close to the relays and the destination, and the destination and the eavesdropper use the same decoding strategy, the secrecy capacity is quite low. From the simulation results, we can observe that as the distance between the eavesdropper and the source increases, the secrecy capacity becomes comparable to the capacity of the destination. This is because the eavesdropper loses its detection capability, regardless of the propagation environment. Furthermore, the capacity for secrecy is improved when comparing $\beta = 4$ to $\beta = 2$, as higher beta results in greater signal strength reduction with distance.

Chapter 3

Secrecy Analysis for Destination and Eavesdropper Using Different Decoding Strategies

In this chapter, we continue to utilize the same two-path successive relaying system introduced in Chapter 2. In this system, the source transmits a superimposed signal to the destination with the aid of relays and utilizes the direct link between them. The relays operate based on the Decode-and-Forward strategy, implementing SIC in half-duplex mode. As a result, the relays alternate between receiving and decoding the information in each time slot.

This chapter explores a scenario where the eavesdropper is close to the source, trying to take advantage of this by switching the decoding strategy to relay exclusively on line-of-sight (LOS) from the source. In this situation, signals transmitted from the relays act as artificial noise to confuse the eavesdropper. The core idea here is that from the perspective of the eavesdropper, the signals transmitted by relays will be perceived by the eavesdropper as a jamming signal. This degrades the SINR, limiting the eavesdropper capacity. Consequently, it improves the secrecy capacity because the destination, at a fixed position, is using its optimum decoding strategy.

This chapter is organized as follows: Section 3.1 explores how the signal is processed by the eavesdropper and how the relayed signal acts as artificial noise to interfere with the eavesdropper. In Section 3.2, we delve into the calculation of the capacity of each layer at the eavesdropper. The capacities at the destination are the same as in the previous chapter. The simulation results, evaluating the performance of the system in both AWGN and Rayleigh fading environments, are presented in Section 3.3. Finally, Section 3.4 provides a conclusion to the chapter.

3.1 Interference from Relays Affecting Eavesdropper

In this chapter, the signal from the relays plays a critical role in information transmission because it serves as a form of artificial noise (AN) to interfere with the eavesdropper who does not follow the same decoding strategy as the destination. There are two potential reasons for the eavesdropper not to follow the same decoding strategy as the destination uses only the signal received straight from the source and treats relay signals as interference. The first reason for the eavesdropper not to adopt the same tactic as the destination is the lack of knowledge about the destination's decoding algorithm. (This is against the cryptography principle of Kerckhoffs, which says that a cryptosystem should be secure even if all of its components, except the key, is public knowledge.) In PLS, the location of the destination and the matching channel conditions are the source of randomness, which serves as the key. The second reason is that the eavesdropper is trying to take advantage of the stronger path between the source and the eavesdropper. Typically, the initial obstacle preventing an eavesdropper from being aware of the decoding strategy is not regarded as a robust security mechanism because, ultimately, the decoding strategy becomes public. In both scenarios, the eavesdropper only utilizes the signal directly from the source and treats relay signals as interference. This interference introduces an additional layer of security, making it challenging for the eavesdropper to detect signals accurately. In contrast to Chapter 2, where the eavesdropper could receive the signal well from the relays and follow the same decoding strategy as the destination. In this chapter, the eavesdropper's capacity is reduced to recover information from the source only in the presence of interference from the relays. The following is Section 3.1.1, which revisits the detection at the destination, while Section 3.1.2 presents the eavesdropper's detection process, relying on the line-of-sight (LOS) from the source.

3.1.1 Detection at Destination

In this chapter, the destination adheres to the decoding strategy outlined in Chapter 2. As a review of the procedure, the destination initiates the decoding process with the data in $s_2(t-1)$ due to the destination being in the vicinity of the relays rather than the source. Subsequently, the signal of $s_1(t)$ is recovered from the received

signal, with the impact of the signal of $s_2(t-1)$ removed through SIC. The destination only needs to decode the data in $s_2(t-1)$ and $s_1(t)$ because the information in $s_2(t)$ is identical to that in $s_2(t-1)$.

3.1.2 Detection at Eavesdropper Relying on LOS

In this chapter, we presume that the eavesdropper is in close proximity to the source, potentially obviating the need for a complicated SIC decoding process as employed by the destination (what the eavesdropper was doing in Chapter 2). The signal received by the eavesdropper is described as the summation of signals originating from both the source and the relays. It can be expressed as:

$$s_E(t) = h_{RE}\sqrt{P_T}s_2(t-1) + h_{SE}\sqrt{P_T}\cdot\big(\alpha_1 s_1(t) + \alpha_2 s_2(t)\big) + n_E(t) \tag{3.1}$$

where the $n_E(t)$ is the total AWGN noise at the eavesdropper with the variance σ_E^2. This thesis assumes that the noise power (σ_E^2) is equal to the power level of the signal $h_{SD}\sqrt{P_T}\alpha_2 s_2(t)$ at the destination, which represents the enhancement layer from the source.

Due to the stronger channel gain coefficient h_{SE} between the source and the eavesdropper compared to h_{RE} which represents the channel gain coefficients between the relays and the eavesdropper, the eavesdropper prioritizes decoding the signal $(\alpha_1 s_1(t) + \alpha_2 s_2(t))$ and disregarding $s_2(t-1)$. In this approach, the eavesdropper first recovers data encoded in $s_1(t)$. Subsequently, using SIC after mitigating the impact of $s_1(t)$ in (3.1), the eavesdropper then recovers data represented in $s_2(t)$. The signals from the relays, represented by the first term in (3.1) are treated as noise in this decoding process. In this scenario, we assert that the signal from the relays acts as artificial noise. In this thesis, we consider two relays (R_1 and R_2), however, in our expressions for SNR, we only use a generic R because we aim to maximize the power of noise to counteract the artificial noise from relays by using NC on data represented a signal from R_1 and R_2. Consequently, the signal after removing the impact of the baser layer signal can be expressed as:

$$\hat{s_E}(t) = h_{SE}\sqrt{P_T}\alpha_2 s_2(t) + h_{RE}\sqrt{P_T}s_2(t-1) + n_E(t) \tag{3.2}$$

In this scenario, the last two terms in (3.2) represent the noise corresponding to the detection of $s_2(t)$ from the source, with $h_{RE}\sqrt{P_T}s_2(t-1)$ representing artificial noise

from the relay and AWGN ($n_E(t)$) to impair the eavesdropper's ability to acquire information.

3.2 Capacity and Secrecy Capacity Calculations

We examine the capacity expression and the secrecy capacity formulas in this section for the delayed enhancement layers that are re-transmitted by relays at the destination and the eavesdropper, as well as the base layers that are derived from the signal transmitted from the source. The eavesdropper processes the signals it receives from the source and relays in a different way than the destination, which uses the same decoding mechanism for signal processing.

3.2.1 Capacity at Destination Using Relayed Signal First

In this chapter, we assume that the destination utilizes the same decoding strategy as discussed in Chapter 2. Consequently, the capacities of $s_2(t-1)$ and $s_1(t)$ at the destination remain identical to those presented in (2.10) and (2.12).

3.2.2 Capacity at Eavesdropper Using Source Signal First

When considering the capacity of the base and the enhancement layers at the eavesdropper, unlike decoding the delayed enhancement layer signal first, the eavesdropper initially recovers the base layer $s_1(t)$ from (3.1) as it has the highest power, while the enhancement layer $s_2(t)$ is treated as interference during reception. Therefore, the capacity of the base layer signal at the eavesdropper is calculated as:

$$\begin{aligned} C_{_E}^{s_1} &= \log_2(1 + \frac{|h_{_{SE}}|^2\alpha_1^2 P_T}{|h_{_{SE}}|^2\alpha_2^2 P_T + |h_{_{RE}}|^2 P_T + N_o}) \\ &= \log_2(1 + \frac{|h_{_{SE}}|^2}{|h_{_{SE}}|^2\alpha_2^2 + |h_{_{RE}}|^2 + |h_{_{SD}}|^2\alpha_2^2}) \end{aligned} \tag{3.3}$$

In this expression, $N_o = |h_{_{SD}}|^2\alpha_2^2 P_T$ is assumed to be the same as the total AWGN noise at the destination. The achievable data rate is limited by the worst channel conditions between the relays and the eavesdropper. Therefore, the channel gain between the relays and the eavesdropper $h_{_{RE}}$ is determined by the maximum distance between R_1 and the eavesdropper and R_2 and the eavesdropper.

After the eavesdropper adopts the approach of SIC to remove the impact of the base layer $s_1(t)$ based on (3.2), the achievable capacity of the enhancement layer at the eavesdropper is expressed as:

$$\begin{aligned} C_{E}^{s_2} &= \log_2(1 + \frac{|h_{SE}|^2 \alpha_2^2 P_T}{|h_{RE}|^2 P_T + N_o}) \\ &= \log_2(1 + \frac{|h_{SE}|^2 \alpha_2^2}{(|h_{RE}|^2 + |h_{SD}|^2)\alpha_2^2}) \end{aligned} \tag{3.4}$$

3.2.3 Secrecy Capacity Calculations

Within the domain of wireless communication and information security, security capacity signifies the upper limit for effectively transmitting confidential data through a communication channel, safeguarding against interception and decryption attempts by unauthorized entities, commonly referred to as eavesdroppers [27]. As elaborated earlier, the secrecy capacity associated with the delayed enhancement layers is expressed as:

$$C_{S}^{s_2} = \left[C_{D}^{s_2} - C_{E}^{s_2}\right]^{+} . \tag{3.5}$$

where $C_{D}^{s_2}$ is calculated as in (2.10) and $C_{E}^{s_2}$ is calculated as in (3.4).

Furthermore, the secrecy capacity of the base layers is given by:

$$C_{S}^{s_1} = \left[C_{D}^{s_1} - C_{E}^{s_1}\right]^{+} . \tag{3.6}$$

where $C_{D}^{s_1}$ is calculated as in (2.12) and $C_{E}^{s_1}$ is calculated as in (3.3).

3.3 Performance Evaluation

In this section, we analyze the secrecy capacity of different decoding strategies at the eavesdropper and the destination in deterministic and Rayleigh fading channels. Throughout our simulations, the source, two relays (R_1 and R_2), and destination are positioned at fixed locations as illustrated in Fig. 3.1 which is the same layout as in Chapter 2 simulations. The source is positioned on the horizontal axis at $(-\frac{\sqrt{39}}{2}, 0)$. The destination is located on the horizontal axis at coordinates (1,0). Two relays (R_1 and R_2) are located at coordinates $(0,\frac{1}{2})$ and $(0,-\frac{1}{2})$, respectively. In this chapter, we considered a scenario where the eavesdropper is positioned within a square with a side of 8 centered at the origin. The inter-node distances characterize

the deterministic channel gain coefficients as in $h_{_{ij}} = \frac{1}{d^{(\frac{\beta}{2})}{}_{ij}}$ where (i, j stands for nodes such as $i = S$ and $j = D$). We assume that the power path loss factor is $\beta = 2$ and $\beta = 4$ in order to capture the impacts of free space propagation and ground wave propagation, respectively. To assess the performance of Rayleigh fading channels, we employ Monte-Carlo simulations based on averaging SNR and link capacities over 10^6 independent channel realizations for a specific position of the destination and the eavesdropper.

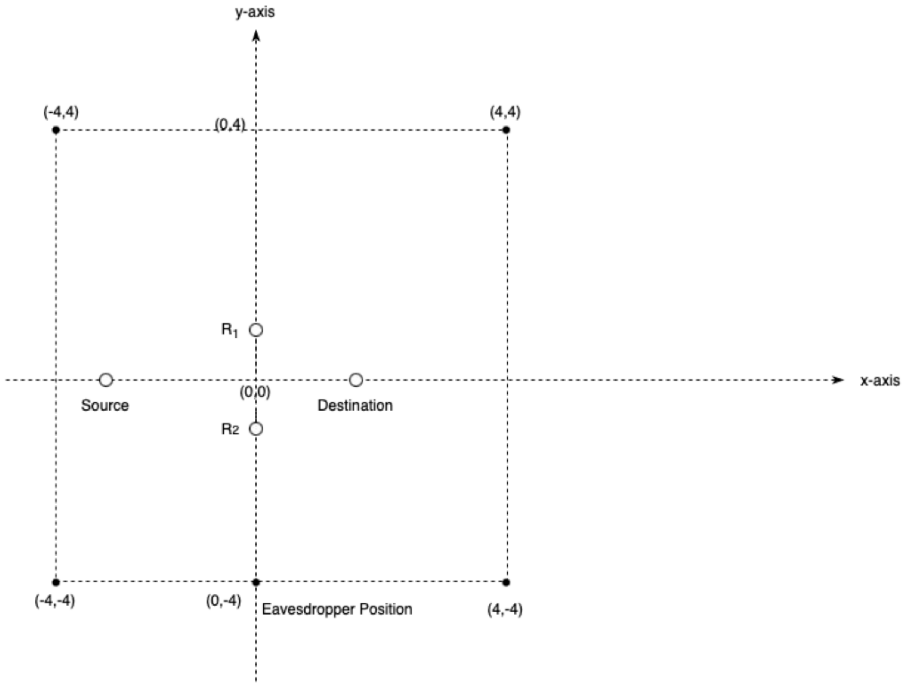

Figure 3.1: X-Y plane for the eavesdropper position.

As previously discussed in Chapter 2, the power allocation in this chapter assigns 95% of the transmit power to the base layer s_1 and 5% to the enhancement layer s_2. This distribution of power is chosen to achieve a practical implementation with a BER close to 10^{-12} for the base layer s_1 and 10^{-5} for the enhancement layer s_2.

Considering (3.3) and (3.4), it should be noted that the relayed signal functions as artificial noise, which considerably improves the secrecy capacity. Furthermore, it should be noted that the secrecy capacity reaches its limit, which is the capacity at the destination when the eavesdropper is really far away and its decoding ability decreases to zero. Also, it should be anticipated that the destination's capacity in

a particular propagation environment remains unchanged as long as the destination location remains intact.

3.3.1 Simulation for AWGN

As there are no changes for the destination as discussed in Section 2.2.1, the theoretical capacities for $s_2(t)$ and $s_1(t)$ can be obtained from (2.10) and (2.12). When $\beta = 2$ with $|h_{RD}|^2 = \frac{1}{d_{RD}^2}$ and $|h_{SD}|^2 = \frac{1}{d_{SD}^2}$, the calculated capacities are 3.8 [bps/Hz] and 3.4 [bps/Hz] respectively. When $\beta = 4$ with $|h_{SD}|^2 = \frac{1}{{d_{RD}}^4}$ and $|h_{SE}|^2 = \frac{1}{{d_{SE}}^4}$, the capacity for s_2 and s_1 is 7.5 [bps/Hz] and 3.4 [bps/Hz] respectively.

Figure 3.2 presents a 2D slice plot for secrecy capacity in which the eavesdropper is changing its position from the coordinates $(-4, 0)$ along the x-axis to the point $(4, 0)$ (as referred to Fig. 3.1, with position $(1, 0)$ corresponding to the destination. In this figure, with $\beta = 2$, when the eavesdropper is located at coordinates $(4, 0)$, the secrecy capacity of the enhancement layer is 3.78 [bps/Hz], and for the base layer, it is 3.03 [bps/Hz], respectively.

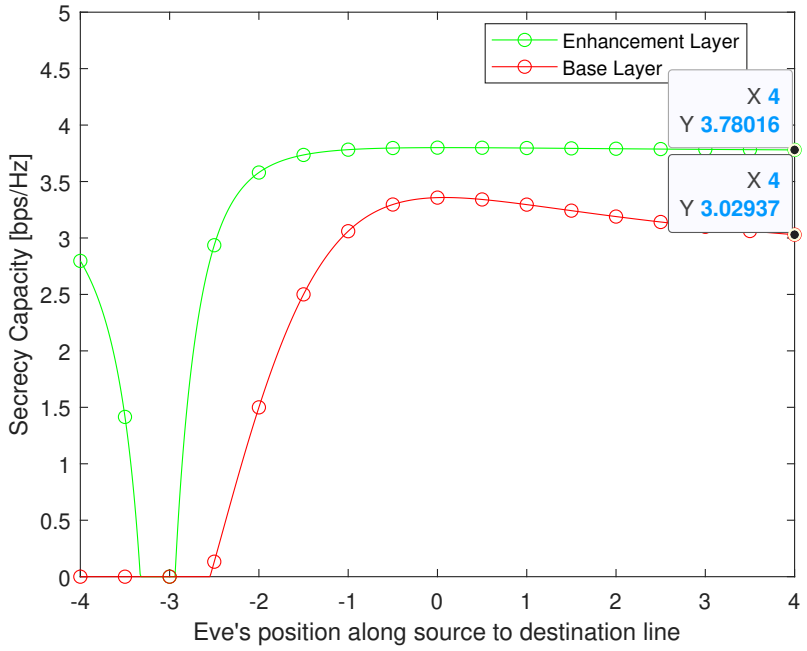

Figure 3.2: Secrecy performance when eavesdropper is located along the x-axis (for $\beta = 2$ and in AWGN).

Upon comparing Fig. 3.2 to Fig. 2.3, noticeable improvements in the secrecy capacity of both the enhancement layer and the base layer are observed when the eavesdropper is situated within the square (as referred to Fig. 3.1). This improvement is attributed to the relayed signal, which serves as artificial noise, significantly impacting the eavesdropper's capacity. As demonstrated in Fig. 3.2, the secrecy capacity of the enhancement layer approaches its theoretical maximum when the eavesdropper is located in close proximity to the relay.

Figure 3.3 highlights the secrecy capacity in a similar situation as Fig. 3.2 except we extend the eavesdropper's location from the coordinates $(-4, 0)$ along the x-axis to the coordinates $(100, 0)$. In this figure, as the eavesdropper moves farther away from the source, its capacity tends to zero. As a result, the secrecy capacity approaches the capacity at the destination, which is 3.8 [bps/Hz] for the enhancement layer and 3.35 [bps/Hz] for the base layer.

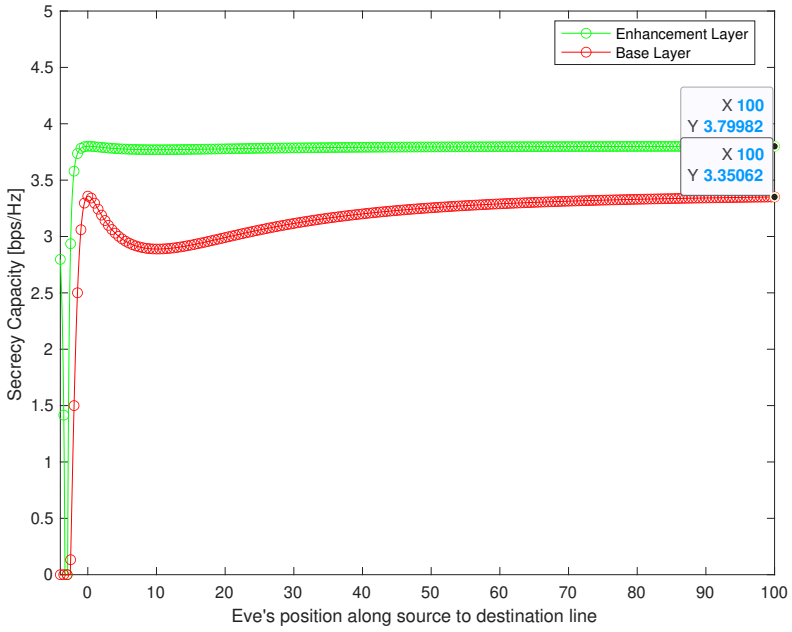

Figure 3.3: Secrecy performance when eavesdropper is located along the x-axis and far away from the source (for $\beta = 2$ and in AWGN).

A more comprehensive perspective on the system's performance is provided through a 3D plot, depicted in Fig. 3.4. This 3D plot indicates the secrecy capacity along the z-axis, and the x-y plane shows the eavesdropper's location in the region shown in

Fig. 3.1. This figure corresponds to the AWGN propagation environment when $\beta = 2$. From both Figs. 3.3 and 3.4, we may conclude that if the eavesdropper does not know the decoding algorithm and is positioned itself near the relays or far away from the source, the secrecy capacity is rather high.

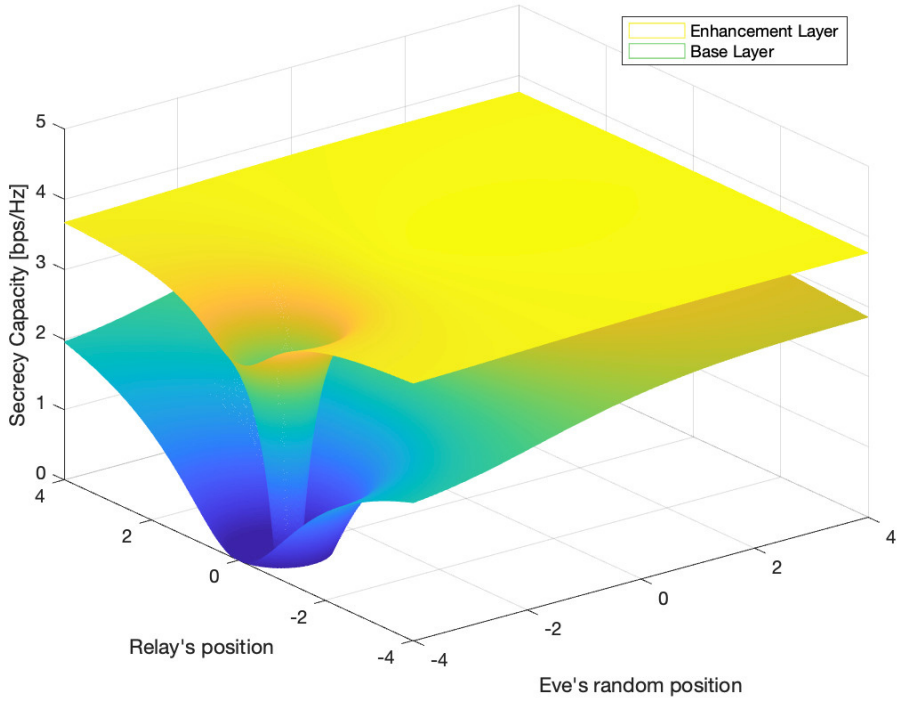

Figure 3.4: Secrecy performance along z-axis when eavesdropper is located in x-y plane (for $\beta = 2$ and in AWGN).

Furthermore, we explore the impact of ground wave attenuation on secrecy capacity with $\beta = 4$, comparing it with free space propagation $\beta = 2$, as shown in Fig. 3.5. In this figure, the secrecy capacity of the enhancement and base layers is represented by the green and red curves for $\beta = 4$, while the curves in purple and blue represent $\beta = 2$. Similar to Fig. 3.3, the eavesdropper's location varies along the x-axis from the coordinates $(-4, 0)$ to the coordinates $(100, 0)$ except in ground wave attenuation with $\beta = 4$. When the eavesdropper is positioned far away from the source or near the relays, the secrecy capacity becomes equivalent to the destination capacity.

Figure 3.5 illustrates how higher β contributes to improved security, particularly when the eavesdropper's SNR decreases with distance and the destination capacity

fills up at a slower rate. In scenarios where the eavesdropper is far away, a situation analogous to $\beta = 2$ occurs, with the capacity of the enhancement layer matching the capacity of $s_2(t)$ at the destination, obtained at 7.5 [bps/Hz]. Notably, there is a 3.7 [bps/Hz] improvement in secrecy capacity attributed to the higher β value.

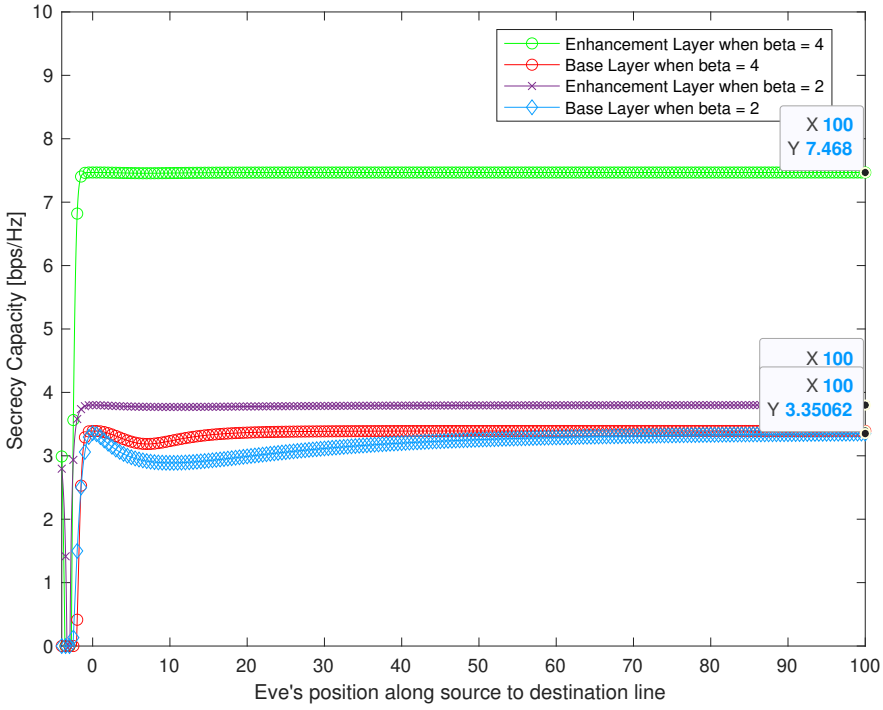

Figure 3.5: Secrecy performance when eavesdropper is located along the x-axis and far away from the source (for $\beta = 2$ and $\beta = 4$ comparison and in AWGN).

3.3.2 Simulation for Rayleigh Fading

We show ergodic temporal averaging of multiplicative factors associated with Rayleigh fading over many realizations. According to (1.6), the enhancement layer's theoretical capacity in a Rayleigh fading environment is 3.26 [bps/Hz], with an average SNR of 13.59. The base layer simultaneously attains 2.85 [bps/Hz] for $\beta = 2$ (free space propagation). Moreover, $s_2(t)$ and $s_1(t)$ have capacities of 6.74 [bps/Hz] and 2.84 [bps/Hz] for $\beta = 4$. Fig. 3.6 shows a 2D slice plot that visualizes how well the base layer and enhancement layer perform in terms of secrecy capacity. Notably, when the eavesdropper is placed at coordinates $(4, 0)$, the secrecy capacity is 3.54

[bps/Hz] for $s_2(t)$ and 2.27 [bps/Hz] for $s_1(t)$. We can see that this enhancement is in line with the observations in the AWGN from Fig. 2.7 and Fig. 3.6.

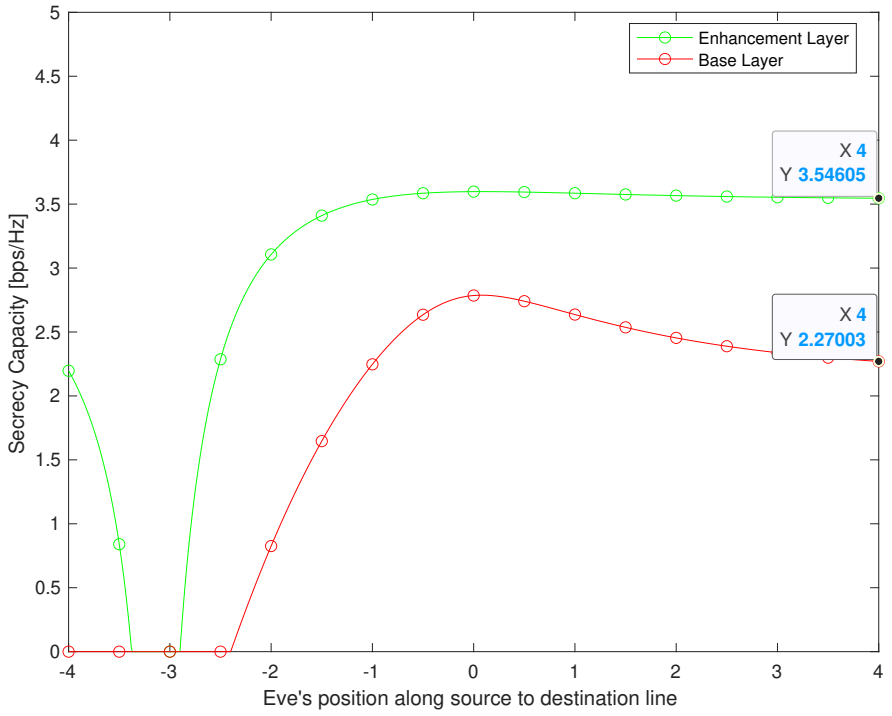

Figure 3.6: Secrecy performance when eavesdropper is located along the x-axis (for $\beta = 2$ and in Rayleigh fading).

The secrecy capacity demonstrated in Fig. 3.7 is similar to Fig. 3.6, except the eavesdropper moves farther away along the x-axis to the coordinates $(100, 0)$. The capacity of the eavesdropper approaches zero as it is positioned far away, while the capacity for secrecy matches the capacity at the intended destination. The enhancement layer reaches 3.58 [bps/Hz] with the same average SNR as the AWGN, which is quite close to the estimated theoretical capacity of the enhancement layer at the destination (3.26 [bps/Hz]).

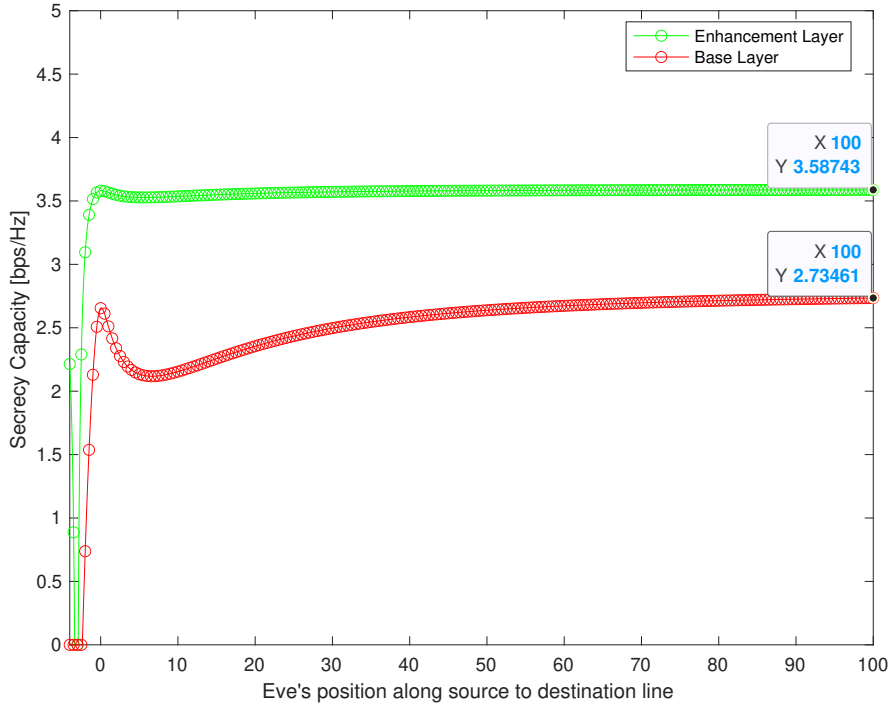

Figure 3.7: Secrecy performance when eavesdropper is located along the x-axis and far away from the source (for $\beta = 2$ and in Rayleigh fading).

Meanwhile, a deeper exploration of these results is facilitated through a three-dimensional (3D) diagram, offering a more detailed and comprehensive understanding of the system's performance. Figure 3.8 corresponds to Rayleigh fading propagation environment for free space propagation with $\beta = 2$.

Additionally, compared to scenarios where $\beta = 2$, the impact of a higher value of β on the secrecy capacity is found to be significantly improved as shown in Fig. 3.9. Higher β secrecy capacities approach maximum capacity more quickly than lower β secrecy capacities. It is regularly found that this improvement occurs and the enhancement layer's secrecy capability experiences considerable improvement with a greater β. The same holds true in the Rayleigh fading, as it does in AWGN, a greater value of β helps to improve the secrecy capacity of the enhancement layer, which is 7.1 [bps/Hz], resulting in a 3.5 [bps/Hz] improvement.

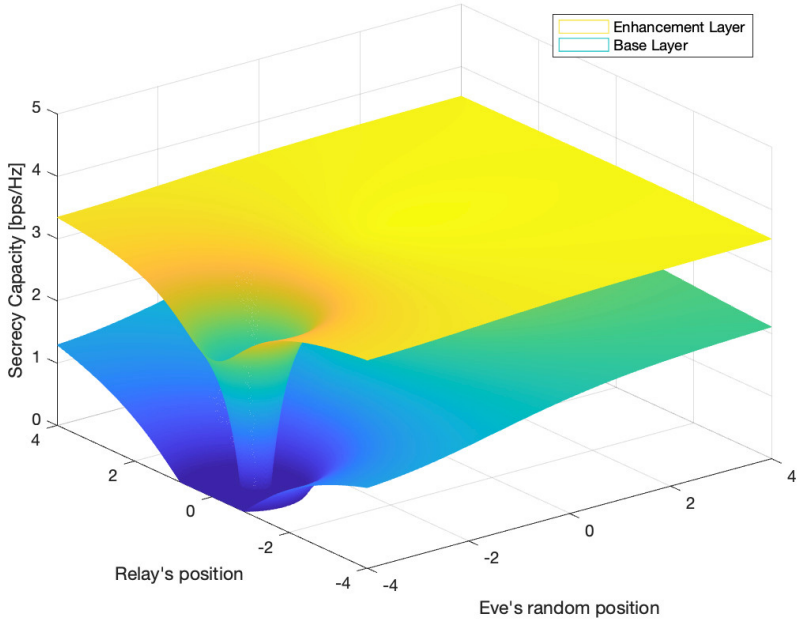

Figure 3.8: Secrecy performance along z-axis when eavesdropper is located in x-y plane (for $\beta = 2$ and in Rayleigh fading).

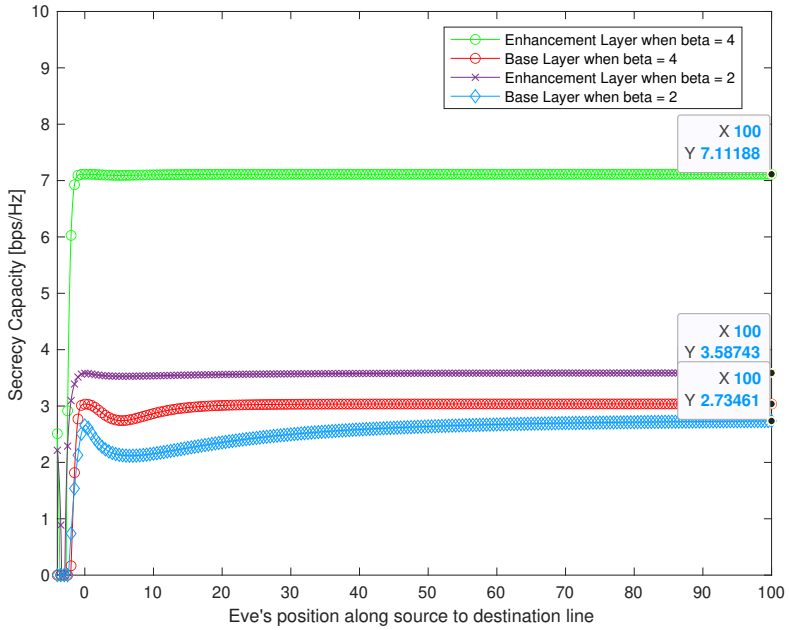

Figure 3.9: Secrecy performance when eavesdropper is located along the x-axis and far away from the source (for $\beta = 2$ and $\beta = 4$ comparison in Rayleigh fading).

3.4 Summary

In this chapter, we examined the security of a wireless network that uses alternate relaying and layered transmission with superposition coding and when the destination and eavesdropper follow different decoding strategies. This chapter examined a scenario where the eavesdropper is in close proximity to the relays and relies on Line-of-Sight (LOS) between the source and destination to obtain information. With this, the signals from relays act as artificial noise, degrading the eavesdropper's ability to decode information. This is in contrast to the previous chapter, where the eavesdropper employed the same decoding strategy as the destination. The findings of the simulation show that the relay signals are essential in reducing the eavesdropper's capacity to detect layers of interest and this increases the secrecy capacity.

Chapter 4

Conclusions

This chapter presents a summary of the contributions in this thesis and proposes potential avenues for future research in this area. Section 4.1 explains the contribution of this thesis, and Section 4.2 provides suggestions for potential future work.

4.1 Thesis Contributions

In this work, we delved into the secrecy capacity of the Single-Input Single-Output (SISO) configuration in a two-path Decode-and-Forward (DF) relaying cooperative network with half-duplex relays. The primary objective is to safeguard the transmitted signal from eavesdropping, ensuring secure information acquisition by the legitimate user from the source and the relay. Initially, we outlined the secrecy capacity of the scenario in which both the destination and the eavesdropper adopt the same decoding strategy. In this context, we hypothesize that the eavesdropper is on the same half-plane as the destination, i.e., close to the relay and the destination. We realized that the secrecy capacity approaches the theoretical capacity at the destination as the eavesdropper moves away from the source and relays. Moreover, in the environment of ground wave propagation, the secrecy capacity has shown a noticeable improvement due to the high value of β, which helps to have better security.

Subsequently, we analyze the case in which the eavesdropper adopts a different strategy than the destination, following the decoding only relying on the signal from the source. In this situation, we assume that the eavesdropper is near the source, taking advantage of the direct line-of-sight between the source and the eavesdropper to acquire information. The secrecy capacity is significantly improved because the relayed signal acts as an artificial noise to interfere with the eavesdropper. Furthermore, the same observation from the previous scenario regarding the impact of higher β applies in this situation.

4.2 Suggested Future Work

This section outlines potential areas for future research and development.

1. Transmission and Reception Synchronization

   In this thesis, the equidistant positioning of the destination from the relays is the fundamental assumption, resulting in the presumption of perfect synchronization for all transmission signals including the one from the source. While there are approaches and network protocols that facilitate synchronous operations, certain technologies, such as Orthogonal Frequency Division Multiplexing (OFDM), which operates with very low symbol rates on each sub-carrier, can offer a solution to this challenge. However, in real-life scenarios marked by varying distances between nodes, this can pose a significant challenge due to the inevitable differences in signal propagation delays.

2. Multi-Layer Transmissions Generalization

   Our thesis research was built upon the principles of superposition coding, a technique that involves merging two data streams into a unified signal to enhance confidentiality. Exploring the amalgamation of multiple data streams into a singular signal and determining the power allocation for each layer of the signal is valuable. This approach allows for the customization of security levels depending on the nature of the data stream, such as audio or video.

3. Securing Information in Close-Proximity Scenarios

   In this thesis, the simulation results have shown that the destination can securely receive information with different levels of efficiency. However, the information is insecure when the eavesdropper's position is in close proximity to the source or the destination. Therefore, there is an opportunity to investigate how to protect the information from being intercepted when the eavesdropper is located in those areas.

Bibliography

[1] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

[2] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*. Springer, 2010.

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

[4] Q. Y. Liau and C. Y. Leow, "Physical layer security in two-path successive relaying," in *2015 IEEE 20th International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD)*, 2015, pp. 180–183.

[5] T. Q. Duong, X. Zhou, and H. V. Poor, *Trusted communications with physical layer security for 5G and beyond*, ser. IET telecommunications series. Institution of Engineering and Technology, 2017.

[6] H. Yuan, Y. Feng, C. Yang, Z. Zhuang, and B. Dai, "Two-user Gaussian broadcast wiretap channel with common message and feedback: Revisit," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 178–193, 2024.

[7] K. Sundaresan and S. Rangarajan, "Cooperation versus multiplexing: Multicast scheduling algorithms for OFDMA relay networks," *IEEE/ACM Transactions on Networking*, vol. 22, no. 3, pp. 756–769, 2014.

[8] S. Vanka, S. Srinivasa, Z. Gong, P. Vizi, K. Stamatiou, and M. Haenggi, "Superposition coding strategies: Design and experimental evaluation," *IEEE Transactions on Wireless Communications*, vol. 11, no. 7, pp. 2628–2639, 2012.

[9] T. Cover, "Broadcast channels," *IEEE Transactions on Information Theory*, vol. 18, no. 1, pp. 2–14, 1972.

[10] R. Zhang and L. Hanzo, "A unified treatment of superposition coding aided communications: Theory and practice," *IEEE Communications Surveys Tutorials*, vol. 13, no. 3, pp. 503–520, 2011.

[11] M. M. Da Silva, A. Correia, R. Dinis, N. Souto, and J. Silva, *Transmission Techniques for Emergent Multicast and Broadcast Systems*. New York, USA: CRC Press, Auerbach Publications, June 2010.

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

[13] J. Laneman, D. Tse, and G. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3062–3080, 2004.

[14] R. Alsakarnah, "Enhancing the performance of multicast systems with layered transmissions," Ph.D. dissertation, Dalhousie University, 2019.

[15] W. Nam, S.-Y. Chung, and Y. H. Lee, "Capacity bounds for two-way relay channels," in *2008 IEEE International Zurich Seminar on Communications*, 2008, pp. 144–147.

[16] Y. Fan, C. Wang, J. Thompson, and H. V. Poor, "Recovering multiplexing loss through successive relaying using repetition coding," *IEEE Transactions on Wireless Communications*, vol. 6, no. 12, pp. 4484–4493, 2007.

[17] C. Schlegel and L. Pérez, *Trellis and Turbo Coding*. John Wiley & Sons, Ltd, 2015, ch. 1, pp. 1–26.

[18] B. Sunil and N. B. T, "Performance analysis and comparison of AF and DF relaying systems in Rayleigh fading channel considering poisson interference field," in *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, 2015, pp. 1–5.

[19] M. Yu, J. Li, and H. Sadjadpour, "Amplify-forward and decode-forward: the impact of location and capacity contour," in *MILCOM 2005 - 2005 IEEE Military Communications Conference*, 2005, pp. 1609–1615 Vol. 3.

[20] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Communications Surveys Tutorials*, vol. 21, no. 3, pp. 2734–2771, 2019.

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

[22] S. S. Haykin and M. Moher, *Modern Wireless Communication*. Prentice-Hall, Inc., 2004.

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

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

[25] H.-M. Wang and T.-X. Zheng, *Physical layer security in random cellular networks*. Springer, 2016.

[26] M. A.-H.-A. Abuyaghi, "Improving secrecy capacity in successive relaying wireless networks with single and multi-layer transmissions," Master's thesis, Dalhousie University, 2021.

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