IMPROVING SECRECY CAPACITY IN SUCCESSIVE RELAYING WIRELESS NETWORKS WITH SINGLE AND MULTI-LAYER TRANSMISSIONS

by

Mohammed Al-Haj-Ali Abuyaghi

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

at

Dalhousie University
Halifax, Nova Scotia
April 2021

To my beloved family

Table of Contents

List of Tables

List of Figures

Abstract

Broadcasting characteristics of radio channels pose additional security risks in wireless networks. Traditionally, the confidentiality concerns in communication systems have been addressed using higher layers of protocol stack. This thesis considers using physical layer security (PLS) in cooperative relaying systems. Specifically, successive relaying is analyzed where capacity of wireless channels are enhanced through simultaneous spectrum utilization by a source and two half-duplex relays, which in turn leads to inter-relay interference (IRI). In the proposed PLS schemes, by controlling the IRI through power adjustment unique to relay-destination channel state information, IRI and fading channels are turned into a source of secrecy. In particular, the IRI is fully mitigated at the intended receiver, while at the eavesdropper, without obtaining additional system resources, the IRI increases the noise level and reduces the eavesdropper's detection capability. Furthermore, network coding is investigated to improve the secrecy capacity. Single and multi-layer signaling schemes are considered when analyzing the secrecy capacity of these systems. Numerical analysis and simulations show that with a single data stream, even though noise enhancement degrades the intended receiver's signal-to-noise ratio in zero-forcing IRI cancelation, the successive relaying system using the proposed PLS scheme achieves higher secrecy capacity in deterministic environments and ergodic secrecy capacity in fading environments compared to the conventional (single) half-duplex relaying system. Furthermore, multi-layer signaling scheme shows great promise in terms of providing different levels of secrecy rates for different data streams represented by different power allocations.

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
FIR	Finite Impulse Response
HD	Half-Duplex
i.i.d	independent and identically distributed
IoT	Internet of Things
IRI	Inter-Relay Interference
LOS	Line-of-Sight
MATLAB®	Mathematical Laboratory (Software)
MIMO	Multiple-Input Multiple-Output
NC	Network Coding
NOMA	Non-Orthogonal Multiple Access

PLS	Physical Layer Security
PSK	Phase Shift Keying
PSNG	Pseudorandom Sequence Number Generator
QAM	Quadrature Amplitude Modulation
QoS	Quality-of-Service
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
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
XOR	Exclusive Or (logical operation)
ZF	Zero-Forcing

Acknowledgements

I would like first to express my thanks and appreciation to my supervisor Dr. Jacek Ilow for his constant support, continuous guidance, valued teaching and patience. I would like also to thank him for his availability for assistance and advice all the time over the period of my studies.

Second, I would like to extend my thanks to my defense committee members: Dr. Colin O'Flynn and Dr. Muhammad H. Raza for providing insightful comments on my research work.

Third, I would like to send my special gratitude to my beloved wife Dania for the ultimate support she has provided throughout my journey.

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

Chapter 1

Introduction

Privacy and confidentiality of information transmitted over wireless medium are critical in a variety of applications. However, wireless messages are still easily vulnerable to eavesdropping and signal capture. This problem is more pronounced in radio systems than in wireline systems because of broadcasting characteristics of radio propagation. Confidentiality, Integrity, authenticity, and spectrum access control are key security factors for the design of wireless networks. Confidentiality refers to the security of sensitive information from unauthorized disclosure. Integrity ensures that the information sent are properly used and obtained by the intended recipient. The confirmation of the sender's identity by the recipient is referred to as authentication. Spectrum access management is a method for stopping denial-of-service (DoS) attacks [1]. To address confidentiality issues, cryptographic methods are typically used in the upper layers protocol stack of the network by performing computational hardness algorithms [2]. In this thesis, considering that there is never enough security, we exploit the potential of PLS based on information-theoretic security principles.

Due to the widespread use of low-cost devices, information security has become increasingly important. Network protection strategies are essential to ensure that the delivery of services across networks is secure. Millions of recently deployed low-cost wireless devices are usually equipped with minimal memory and a single antenna, resulting in very limited computing and communication capabilities. As a result, complicated cryptographic protocols and complex encryption/decryption algorithms cannot be used. Thus, several signaling processing and encoding techniques in the

physical layer have been developed to enhance and assist the protection in wireless systems. Many researchers have contributed to the search for alternative security solutions that meet the needs of today's and tomorrow's wireless networks [3].

Wireless networks are used to transmit a wide range of sensitive and confidential data, such as medical information, electronic media, financial data, and customer files. The implementation of these new advanced systems has posed a challenge to the implementation of higher-level key delivery and management. Physical Layer Security (PLS) has emerged as a viable option to defend against various malicious violations and security attacks. PLS is based on the principle of leveraging the characteristics of wireless channels for confidentiality purposes. Its aim is to prevent eavesdroppers from collecting any sensitive information from the signals they receive [4].

This thesis explores and suggests methods to improve PLS in wireless cooperative networks. The two-path transmission analyzed in this thesis is a special case of cooperative communications that has recently attracted a lot of attention in terms of overcoming the loss in spectral efficiency (the pre-log factor $\frac{1}{2}$ in capacity calculations) [5]. With two half-duplex amplify-and-forward (AF) relay terminals assisting in the communication between source and destination terminals (say Alice and Bob), the system considered in this work reuses source transmission time slots for the relay transmissions, which causes inter-relay interference (IRI) [6]. The full cancellation of IRI in this system has already been investigated at Bob in both single-input single-output (SISO) and multiple-input multiple-output (MIMO) configurations [7] [8]. In addition, power control is used to eliminate the effect of relays-destination channels. These techniques increase the noise level at the eavesdropper (say Eve) and consequently decreases its signal-to-interference-plus-noise (SINR) ratio and improves the secrecy capacity of Alice-Bob transmission. Secrecy capacity in SISO decode-and-forward (DF) successive relaying was investigated in [9]. This thesis investigates the

applicability of the SISO AF setup to protect legitimate user's data from being reliably decoded by Eve even if the channels between the relays and Bob are worse than the channels between the relays and Eve.

In addition to IRI impacting the signal detection capability at the eavesdropper, in this work, the signal design to have multiple quality layers via superposition coding is considered to support different secrecy rates for different data streams. This is with the objective of providing flexible security-level configurations and Quality-of-Service (QoS) via power allocation to different sub-streams (layers).

The remainder of this chapter includes a review of the literature as well as an overview of the basic concepts used in this thesis. Section 1.5 presents the thesis objectives while Section 1.6 explains how the thesis is organized.

1.1 Cooperative Networks

Wireless communication is limited by the sender's transmitting power which leads to a limited coverage area. Relays offer the ability to extend network coverage and improve the QoS. Researchers have extensively investigated various aspects of relay networks and found that a significant improvement to wireless networks can be achieved using cooperative relays. These research activities have opened up several avenues for improving wireless system performance by investigating different types of relays and relaying strategies and evaluating their impact on reliability (diversity gain), throughput (transmission rate), and confidentiality (secrecy capacity) [10].

Conventionally, a relay is a dedicated wireless network node (i.e., physical device) that is separate from senders/receivers terminals. In cooperative networks, idle terminals can act as cooperative relay nodes and assist in the exchange of information. However, untrusted relays could have a negative impact on confidentiality (i.e., acting as an eavesdropper). In the case of reliable relays, the eavesdropper and the relays are

two separate network entities. Cooperating nodes are investing power in the relaying process to extend the reachability [10].

Existing cooperative networks from PLS perspective shows that the traditional PLS approach based on single antenna system faces major constraint such as the channel conditions. If the channel between the sender and the legitimate receiver is worse than the channel between the sender and the eavesdropper, then the secrecy rate is typically zero. To overcome such constraint, it was proposed to take advantage of multiple antenna systems [11]. However, due to cost and size limitations in a lot of wireless terminals such as Internet of Things (IoT) devices, multiple antennas may not be available at network nodes. In such case, cooperative nodes aid single-antenna nodes to enjoy the secrecy-related benefits of multiple-antenna systems [12].

Relaying Strategies

Signals arriving at the relays are attenuated and modified due to the nature of the relay environment. Relays must therefore process the received signals before they are retransmitted to the next node. Methods used by relays to deal with signals include amplify-and-forward (AF) and decode-and-forward (DF) approaches that dominate relaying strategies. These two strategies differ in terms of performance, complexity, flexibility, and signal handling.

AF strategy deals with analogue signals. Relays receive signals and amplify them to the desired threshold before forwarding them to the next nodes. This strategy is preferable for systems where bit-level processing requires complex manipulation or where relays lack the ability to decode signals. However, as is the case with any receiver, the signals received by the relays are accompanied by additive white gaussian noise (AWGN). The amplification of signals also results in noise amplification in the AF strategy.

DF strategy handles digital signals. Relays decode the signals by removing all

the effects from the receiving side, and then encode the signals to forward them to the next nodes. Although noise removal is an advantage of the DF scheme, this requires full data processing and decoding. In many scenarios, relays do not have the capability to decode signals, such as an insufficient number of antennas [13].

Relays can work in either full-duplex (FD) or half-duplex (HD) mode. In FD, the relay can transmit and receive at the same time, whereas in HD, the relay can only transmit or receive during a specific time slot. Because of its simpler design, HD relay is easier to implement and preferable to work with.

Successive Relaying

Research to overcome the drawbacks of half-duplex wireless relay networks has taken two paths. One approach uses two-way communication, where the data flow is in two directions and the receiver is also a transmitter. This approach applies network coding technique to reduce transmission time and is not appropriate for networks where data is to be transmitted in a single direction or where different bands are used for uplink and downlink transmission.

The second approach uses time-division duplexing (TDD) in one-way communication. Successive relaying allows the transmitter to transmit continuously, while relays take turns listening to the transmitter as visualized in Fig. 1.1. Using the same band utilized by the transmitter, the relay that completed the listening session transmits signals previously received to the next hop receivers. In the figure, R_1 and R_2 take turns listening to A in *even* (black) and *odd* (blue) TSs, respectively. Listening and transmitting are carried out successively and continuously by the relays. This improves the pre-log factor in capacity calculations from $\frac{1}{2}$ to $\frac{T}{T+1}$, where T is the number of time slots used by the transmitter without interruption, before one or more relays take over and retransmit data while the original transmitter withholds its transmissions [14]. The pre-log factor $\frac{1}{2}$ in capacity calculations is due to nodes

listening half of the time and transmitting only half of the time.

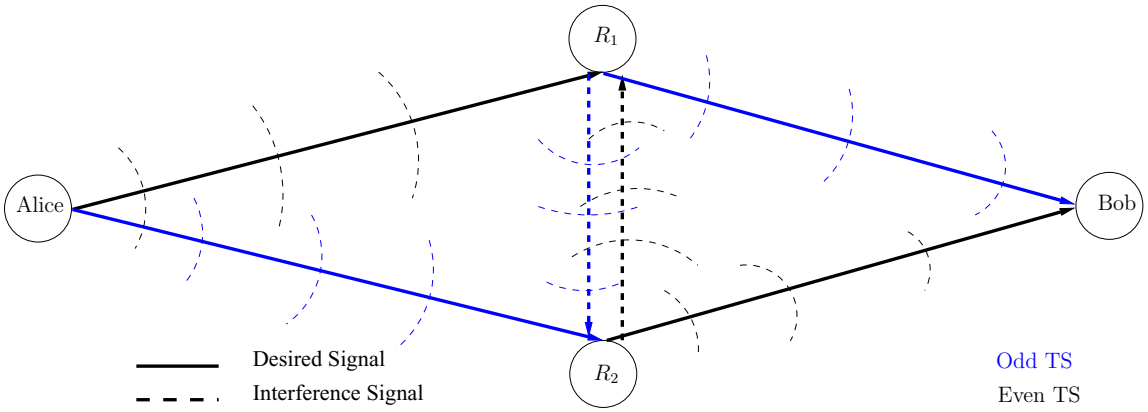


Figure 1.1: Two-path successive relaying network

Although the pre-log factor is significantly improved, successive relaying is costly. During the listening session, the signals transmitted by Alice to the listening relay are accompanied by interference from the transmitting relay (shown by the dashed path in Fig. 1.1). If this IRI is not mitigated by the relays themselves [15], by Alice through precoding [16], or by Bob through Finite Impulse Response (FIR) [8] or other processing technique, it degrades the quality of the received signals at the final destination(s).

Propagation Characteristics

Radio propagation conditions have a critical role to play in the operation of wireless systems. They determine the performance of these systems, because with limited transmit power, the signal attenuation with distance affects the received signal-to-noise ratio (SNR). Specifically, two types of wireless propagation environments are considered: deterministic attenuation with distance and stochastic variability due to multi-path fading. In this subsection, we focus on the conditions of propagation encountered by signals passing through the wireless link, in which understanding them can help in achieving our goal (i.e., improving the confidentiality).

Deterministic Signal Attenuation

As with any transmission medium, wireless signal power decays from a distance as signals travel through a channel. This loss of signal power is known as deterministic signal attenuation. Various mathematical models for different environments are presented in the literature to capture this phenomenon [17].

This work adopts a generalized formula linking attenuation to distance travelled as follows:

$$P_r(d) = \frac{P_t}{d^\beta} \tag{1.1}$$

where P_r and P_t represent the power of the received and transmitted signals, respectively. The β parameter corresponds to the propagation condition; this value is usually 2 in free-space conditions and 4 in ground wave propagation.

Additive White Gaussian Noise

The existence of wideband noise is a natural phenomenon in the radio frequency (RF) front end of wireless receivers. This noise is universally present at the front end of the RF, e.g. as thermal noise resulting from a large number of random small interference effects. As stated in the central limit theorem, the large number of random variables (RVs) forms a Gaussian distribution, which has a probability density function with a zero mean ($\mu = 0$) and a noise variance σ_n^2 [18].

In this context, the received signal in deterministic channel can be represented as

$$y(t) = \sqrt{P_r}\, s(t) + n(t)\ , \tag{1.2}$$

and the signal-to-noise ratio is determined by P_r/σ_n^2.

Rayleigh Fading

When travelling to receivers, signals are subject to refraction, reflection and dispersion as they pass through different types of objects. Thus, the receiver obtains a

combination of multiple copies of the same set of signals, yet each copy has its own attenuation and time of arrival. Delays are assumed to be less than the duration of the symbol, so that time-dispersive (frequency selective) channels do not have to be addressed. This phenomenon is known as fading, where the combined effects of all copies of signals received from different multi-paths are represented as a multiplicative factor affecting the received signals.

The most common and detrimental situation in wireless communications is the lack of a line of sight between two communicators. When the pass-band signals arrive along two independent components, i.e. in-phase and quadrature, the fading is represented in each case as an independent, identically distributed (i.i.d) Gaussian RV. The resulting complex variable representation of this effect is conventionally denoted as h. This fading coefficient h is a complex normal RV: $(\mathcal{CN}(0, \sigma_h^2))$. This applies only if there is no line-of-sight (LOS) path [19].

In this context, the received signal in the Rayleigh fading channel can be represented as

$$y(t) = \sqrt{P_r}\, h\, s(t) + n(t)\ , \tag{1.3}$$

and the signal-to-noise ratio is determined by $P_r\, |h|^2/\sigma_n^2$.

Capacity Challenge

Although relays can provide promising solutions in terms of reliability and range expansion, challenges such as capacity reduction are also emerging. Communicating via conventional relays takes approximately twice as much time as direct communication between the source and the destination. In conventional relay networks, a time slot is used by the source to send signals to the relay, and another time slot is used by the relays to forward signals to the destination. In the literature, this decrease in the capacity of the link between the source and the destination is referred to as the pre-log factor [20].

The channel capacity is the maximum data rate that can be achieved when data is transmitted over a communication channel. In the case of direct SISO Rayleigh channel, the average capacity C can be expressed as

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

where h is the channel between the source and the destination, P is the signal transmitting power, σ_n^2 is the AWGN variance, and $\mathbf{E}(\cdot)$ is the expectation operator. When the signal passes through the relay, the capacity is scaled to $\frac{1}{2}$ due to the additional time slot used in the process. This is the pre-log factor of conventional relaying system capacity. Note that the exact expression of the average relay capacity depends on the type of network and the relay strategies adopted by the network.

To overcome capacity deficiency, studies have provided solutions for some types of networks. However, this remains an unresolved issue for other networks. In two-way communications, the pre-log factor has been improved to $\frac{2}{3}$ in DF strategy. This improvement is achieved using network coding by reducing relay transmissions for two independent signals from two time slots to one time slot. The relay waits for two terminals to send their signals in succession. It then encodes the signals so that each terminal can delete its own data and decode the desired data.

The physical layer (analog) network coding scheme using AF further eliminated the pre-log factor by allowing two terminals to be sent at the same time. The relays then transmit the received signals to both terminals. The terminals are familiar with their signals and have the channel information required to remove their own signals and decode the desired signals [21].

These solutions do not work for one-way flow when the signals are moving in one direction. Therefore, successive relaying is one of the solutions to normalize the pre-log factor and thus enhance the channel capacity [22].

1.2 Physical Layer Security

Unlike the traditional cryptographic approaches, physical layer security takes advantage of the imperfections of wireless channels, such as noise, fading, attenuation, and interference to boost the signal reception at the intended receiver and degrade the received signal quality at the eavesdropper [23]. By employing this, we can use simpler cryptographic approaches on the upper layers in combination with a physical layer approach to have almost perfect secrecy [10], which simply means to enable the intended receiver to successfully obtain source information, while the eavesdroppers are not able to interpret the transmitted message.

As shown in Fig. 1.2, a generic wireless network communication model consisting of three nodes is considered, namely the transmitter (Alice), the intended receiver (Bob), and the eavesdropper (Eve). The link between Alice and Bob is called the main channel, while the link between Alice and Eve is called the wiretap channel. In this thesis, the transmissions from Alice eventually are going to be replaced by transmissions from two relays. The vital concept of secrecy capacity is based on the objective of maximizing main channel capacity or minimizing wiretap channel capacity, which can be achieved by utilizing the dynamic nature of wireless channels. When the capacity of the wiretap channel is greater than the capacity at the main channel, the secrecy capacity is zero. [24].

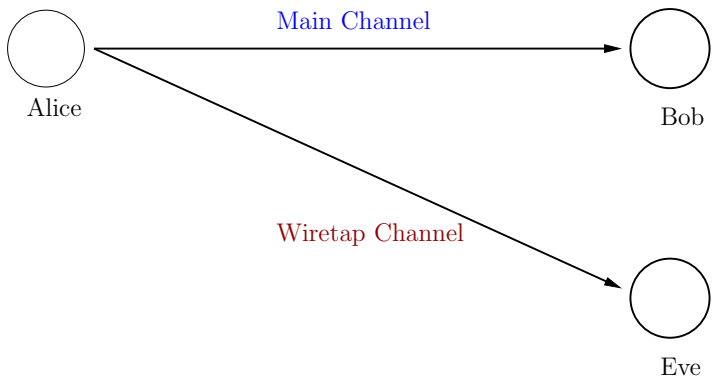


Figure 1.2: PLS basic model

The eavesdropper could be either active or passive. Active Eve could attack the wireless system by sending a jamming signal that causes Denial-of-Service (DoS), while passive would be able to intercept the transmitted message. In fact, Eve is not necessarily a malicious terminal, it could be a legitimate terminal that doesn't suppose to receive some content that are intended to other terminals. In this thesis, the focus is on passive eavesdropping.

Secrecy Capacity

Physical layer security is commonly characterized by achievable secrecy rates. The secrecy capacity is defined as the maximum achievable rate at which information can be transmitted secretly from the sender to its intended receiver. In other words, secrecy capacity can be seen as equivalent to the traditional capacity with a confidentiality constraint. This can be represented as the difference between the capacities of the main channel and the wiretap channel. In case of fading channels, ergodic secrecy capacity is considered, which is the average link over multiple independent channel realizations for a given position of the eavesdropper and the intended receiver. It is worth mentioning that the achievable secrecy rate may vary in practical implementation. It cannot, however, exceeds the secrecy capacity [25].

Based on the definition, the secrecy capacity of the main channel is determined by:

$$C_S = [C_B - C_E]^+ . \tag{1.5}$$

where $^+$ represents the maximum between the calculated value and zero. Then, the secrecy capacity over deterministic channel $C_{S,AWGN}$ and Rayleigh fading channel $C_{S,fading}$ are respectively given by

$$C_{S,AWGN} = \left[\Big(\log_2(1 + \frac{P_r}{\sigma^2_{n_B}}) \Big) - \Big(\log_2(1 + \frac{P_r}{\sigma^2_{n_E}}) \Big) \right]^+ \tag{1.6}$$

$$C_{S,fading} = \left[\Big(\log_2(1 + \frac{|h_{AB}|^2 P_r}{\sigma^2_{n_B}}) \Big) - \Big(\log_2(1 + \frac{|h_{AE}|^2 P_r}{\sigma^2_{n_E}}) \Big) \right]^+ \tag{1.7}$$

where P_r represents the received power, $\sigma^2_{n_B}$ and $\sigma^2_{n_E}$ are the noise power of Bob and Eve, respectively. In addition, h_{AB} and h_{AE} are the instantaneous channel coefficients for the main channel and wiretap channel, respectively. To have confidentiality, our goal is to keep the secrecy capacity C_S strictly positive. Usually, the secrecy capacity of AWGN channels is higher than the secrecy capacity of Rayleigh fading channels. This observation leads us to the following conclusion, if we can cancel the effect of the fading channel, we can enhance the secrecy capacity.

In addition to the use of fading characteristics of the wireless channel, a number of other techniques can be used to improve the secrecy performance of wireless communication systems, such as coding schemes (channel coding and network coding), power allocation and signal design (cooperative jamming via artificial noise, and power control) [26]. Applicable techniques are used in this work to enhance physical layer security.

PLS Techniques

This subsection presents the principles behind PLS exploited in thesis.

Artificial Noise

The main idea behind injecting artificial noise (AN) is to ensure that the intended receiver is not adversely affected, but that the eavesdropper's signal has an increased noise level that prevents it from reliably detecting data. In the case of this thesis, we use IRI, which occurs naturally in our system model, as a replacement. As a result, eavesdropper would be confused and unable to decode the information-carrying signals sent to it.

The use of AN is common in MIMO systems, and it requires resource allocation [27]. When cooperative relays are involved, however, AN can be used in SISO systems.

Power Control

The basic idea behind power control is that eavesdroppers are unaware of the main channel's state information (CSI). Power control can be accomplished by weighting the transmitted signal with a weighting coefficient in order to normalize the propagation effect on the main channel while keeping the eavesdropper with a higher noise level. As a result, only the intended receiver can reliably decode the data. The transmitted signal can be written as:

$$x = g\ s \tag{1.8}$$

where s is the transmitted signal and g is the weighting coefficient. With a constraint that $|h_{AB}| \cdot g = 1$, where h_{AB} is the main channel's fading coefficient. As a result of this, the received signal at Bob becomes:

$$\begin{aligned} y_B &= h_{AB}\ g\ s + n_B \\ &= s + n_B \end{aligned} \tag{1.9}$$

where n_B is the AWGN at the intended receiver. As a result, the receiver will be able to decode its received signal directly without the need for a channel coefficient h_{AB}, while the eavesdropper's signal becomes:

$$y_E = h_{AE}\ g\ s + n_E \tag{1.10}$$

where n_E is the AWGN at the eavesdropper.

According to the literature, the AN scheme achieves higher secrecy rate when the transmitter has more antennas than the eavesdropper. To put it another way, by adding artificial noise through a helpful interferer, a technique known as cooperative jamming (CJ) can be used to confuse an eavesdropper. A relay node sends a jamming signal to the eavesdropper in cooperative wireless networks, while the source sends its message to the destination. This method is most used in MIMO systems [4]. In SISO two-path relay networks, on the other hand, IRI can play the role of CJ without

consuming additional resources. As a result, a multi-component PLS scheme can be developed to outperform the conventional scheme in terms of secrecy capacity.

1.3 Signaling Schemes

An important characteristic of cooperative networks is its capability to improve the performance of communication systems with multi-layer transmissions and network coding. In this section, we introduce these two signaling schemes which we build on in our research.

Superposition Coding

In a digital broadcast transmission system concerned with multimedia transmission, we deal with receivers situated at different distances from the broadcast node. This implies that different receiver nodes would experience different SNR depending on the path loss with distance. In other words, different receivers, close and distant, would have different end-to-end channel capacities available to them using conventional single-resolution modulation such as 16-ary QAM. The receivers located close to the transmitter recover signaling waveforms with higher SNR, allowing symbols to be decoded with fewer errors. Far receivers from the transmitter receive the same waveforms, but they are more difficult to discern due to higher attenuation [28].

The traditional single-layer signaling system designed to cater commonly to all receivers in the desired coverage area will transmit at a rate (determined by the level of modulation) equal to that of the minimum capacity receiver, which is the far receiver, to achieve a desired minimum acceptable image quality. This causes the 'close' receivers with larger channel capacity, capable of operating with higher modulation levels, to operate in a deprecated mode. Thus, the single-layer signaling system has low overall efficiency due to lack of scalability.

To overcome this lack of efficiency, the idea of superimposing high-rate information on low-rate information has been proposed [29]. In this scheme, the base quality (approximation) data of each video frame is modulated by modulation scheme protected with larger symbol distance (lower bit error rate - BER), and the enhancement quality (details) data is modulated using another modulation scheme superimposed on top of the base scheme and protected with smaller distance (higher BER). In this approach, receivers with good CSI (close to the transmitter) will decode both the approximation and details information, while the receivers with poor channel conditions (far from the transmitter) will decode only the approximation data to reconstruct the transmitted image.

The premise for this approach is based on deterministic attenuation of the radio signal over distance. In this model, the near receivers receive the RF broadcast signal with SNR sufficient to decode both the approximation and details, while far receivers receive signal with SNR sufficient to decode only 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 only decode 4-PSK (two high priority / approximation bits) while the near receivers decode 16-ary QAM modulation (four bits of information with two high priority / approximation and two low priority / detail bits). For a limited transmit power, the conventional equi-spaced 16-ary QAM modulation suffers from high attenuation due to poor SNR for far receivers, rendering the signal too weak to be decoded faithfully. However, by using 16-ary multi-layer signaling, the far receiver can still decode the signal as Q-PSK with potentially acceptable BER and thus recover an acceptable image quality. As a result of this scalability with multi-layer signaling scheme, the overall performance of the broadcast system improves. Enabling transmission of two independent information bit streams with unequal priority on a single channel is also known in the literature as hierarchical modulation or superposition coding (SC) [30] [31]. Fig 1.3 shows a block

diagram for superimposing two bit streams at the transmitter, each using a QPSK constellation. From the figure, the source node assigned higher transmitted power for

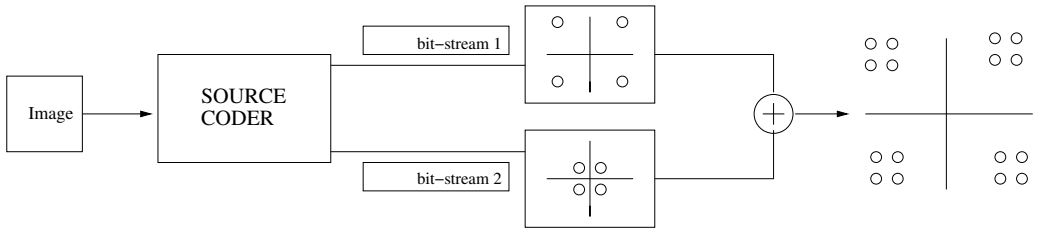


Figure 1.3: Superposition coding block diagram at the transmitter

s_1 and lower power for s_2. These simultaneously transmitted signals with different power levels $P_1 = \alpha_1^2 \cdot P$ and $P_2 = \alpha_2^2 \cdot P$ are combined into $s(t)$ as follows:

$$s(t) = \sqrt{P} \cdot \Big(\alpha_1 s_1(t) + \alpha_2 s_2(t)\Big) \tag{1.11}$$

where $\alpha_{1,2}^2$ are the fractions of power assigned to each layer, provided that (i) ($0 < \alpha_i^2 \leq 1$, $i \in \{1, 2\}$), (ii) $\alpha_1^2 + \alpha_2^2 = 1$, and P is the transmitted power at the sender. Figure 1.4 illustrates a superimposed signal of two QPSK constellations forming a symmetrical 16-QAM hierarchical constellation with higher noise protection in the base layer than in the enhancement layer. In practical implementation, as shown in the figure, some bits are protected with a greater distance (red bits in the figure), while blue bits are protected with a smaller distance. In this thesis, the general concept of having two data streams represented by two signals is discussed, as well as the different power allocations for these signals in order to control the different levels of security that can be achieved for the different data streams that in layered signaling scheme.

In Chapter 3, layered signaling is used at the transmitter side to superimpose the data streams in layers and transmit them to the relays, where the secrecy capacity for each layer is investigated.

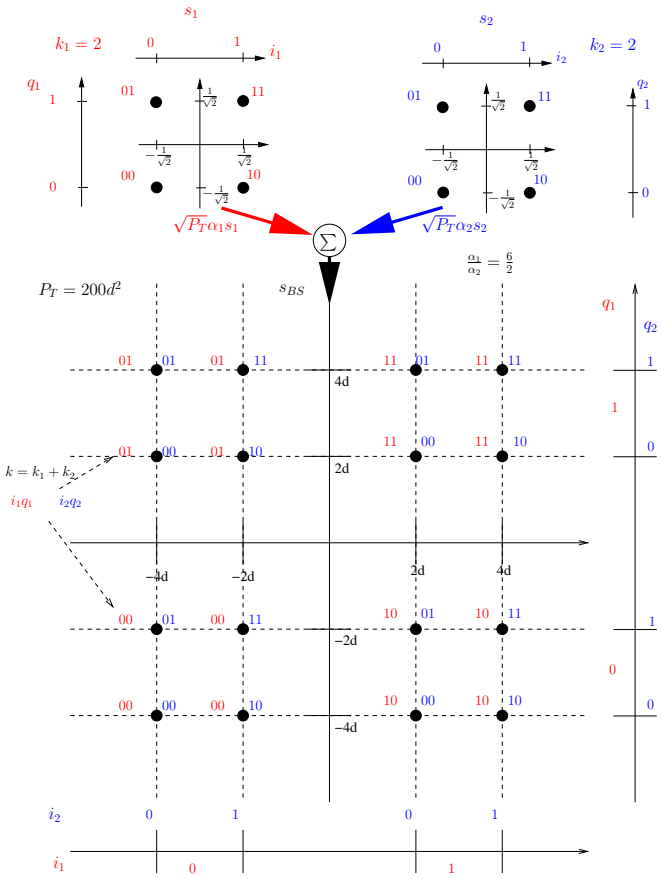


Figure 1.4: Layered coding with a 16-QAM constellation as a superposition of two QPSK constellations.

Network Coding

In one-way communication, network coding (NC) is applicable by performing XOR operation on the bit level between every two consecutive packets, after which the encoded packet is transmitted. In one form of NC deployed in this thesis, rather than transmitted original data message m_i, where i represents time index, we are sending coded (XORed) version of the message in a form of symbol c_i. The XOR operation is performed at the receiver between the coded packet and the previously decoded massage. The first packet on the transmitter is XORed with a predefined number or pseudorandom sequence number generator (PSNG) and the same is done on the receiver [32]. Table 1.1 illustrates this NC mechanism.

Table 1.1: Network coding at bit level.

At the transmitter	At the receiver
$c_1 = \text{PSNG} \oplus m_1$	$m_1 = c_1 \oplus \text{PSNG}$
$c_2 = m_1 \oplus m_2$	$m_2 = c_2 \oplus m_1$
$c_3 = m_2 \oplus m_3$	$m_3 = c_3 \oplus m_2$
$c_n = m_{n-1} \oplus m_n$	$m_n = c_n \oplus m_{n-1}$

1.4 Interference Cancellation Techniques

In this thesis, the received signal at the intended receiver as well as at the eavesdropper is a summation of a desired information bearing signal and the delayed version of the previous transmissions referred as inter-relay interference. In order to remove IRI at the intended receiver and use IRI as source of confusion at eavesdropper, good understanding of interference cancellation techniques is required. In the context of this thesis, in addition to removal of IRI, we need to decode two layers of signaling in multi-layer transmissions which deploy successive interference cancellation (SIC). In wireless networks affected by interference, SIC techniques can be used at the receiver to estimate and filter signals based on to their power levels. This method works well if the signals arriving at the receivers are of varying strength.

Successive Interference Cancellation

The basic idea of SIC is that the signals of the receiver are decoded successively, starting with the one that has the maximum received power and ending with the one that has the minimum allocated power. Here we assume that s_1 and s_2 are forwarded to the intended receiver (Bob). The specific steps to decode the superimposed message can be expressed as follows:

- Bob decodes the message s_1 by treating s_2 as interference/noise.
- Upon successfully recovery of s_1, Bob then subtract its effect from $s(t)$ leading to a new modified received signal $s'(t)$.

- Bob then decodes s_2 from $s'(t)$ which is typically affected only by AWGN.

Due to SIC process, the two superimposed signals would achieve two different data rates. Considering $P = P_1 + P_2$, the following rate pair can be achieved [33]:

$$R_1 = \log_2 \left(1 + \frac{P_1 |h_1|^2}{P_2 |h_1^2 + \sigma_n^2} \right) \tag{1.12}$$

$$R_2 = \log_2 \left(1 + \frac{P_2 |h_2|^2}{\sigma_n^2} \right) \tag{1.13}$$

The above concept is called rate-splitting, which leads to have different capacity for each layer based on the power allocation [34].

Inter-Relay Interference Cancellation

The transmitter in a successive relaying network sends signals to a listening relay, while a transmitting relay forwards previously received signals to a destination. If the transmitting relay operates in the same frequency band as the source, interference with the listening relay occurs, which is referred to as IRI. Due to comparable signal strengths and the relay nodes' inability to perform the required signal processing, SIC may not be feasible in this scenario.

In two-path AF successive relaying system, IRI is a critical issue. The data from the other relay interferes with the data received from the source by a relay. This is because, starting with $t = 2$, there is always a relay transmitting data concurrently with the source. Thus, if the intended user is able to remove the IRI while the eavesdropper is unable, the intended receiver's SNR will be greater than the eavesdropper's SINR. As a result, a positive secrecy capacity is achieved at that specific position of Eve. The effect of confusing the Eve with IRI is one of the flavors of cooperative jamming techniques, given that no additional system resources such as power or bandwidth are consumed since IRI is already part of the system's operation.

In SISO systems, full cancellation of IRI in this system has proposed in the literature at the intended receiver in both SISO and MIMO configurations [7] [8]. The

selected approach for enhancing confidentiality when working with successive relaying is explained in Appendix A.

1.5 Thesis Objectives

The general objective of this thesis is to enhance the secrecy capacity of two-path successive relaying wireless networks. The focus is on networks in which relays play only a minor role in signal processing. The availability of CSI at each node in different propagation channels is used to improve secrecy capacity in these networks. The key disadvantage of the conventional relaying system is that if the eavesdropper is closer to the relay than the intended receiver, the eavesdropper has a higher SNR, and therefore secrecy capacity is typically zero. In the same circumstances, when the possibility of incorporating another relay occurs, the secrecy capacity improves. Due to framework and algorithm sophistication, it is not realistic to evaluate the performance of algorithms built using only analytical methods in this thesis. Thus, a combination of analytical and simulation findings is used. With a large number of computer simulations running in the MATLAB® computing environment, all proposed schemes and algorithms have been validated and compared. This is an acceptable research methodology for solving networking problems and adapting designs for this type of research.

In single data stream at the transmitter side, we can enhance the confidentiality of one-way two-path cooperative networks with dedicated half-duplex relays, where signals only arrive at their destinations via the relay channel. This is achieved by using power control and IRI as artificial noise which confuse the eavesdropper. Advanced signal processing cancels the IRI generated in these networks at the destination, while power control aims to eliminate the fading effect of relays-destination channels. As a result, Eve's SNR is deteriorating, and the secrecy capacity of the main channel is significantly improved. The use of network coding is also examined to achieve

the main objective, it has been found that based on the position of Eve, a pair of capacities define the boundary of its data rate. The capacity at Eve is a function of its distance from each relay. Thus, for coded messages, the minimum capacity at Eve is considered and, as a result, secrecy capacity is improved.

When considering layered transmission for the same successive relaying networks, a portion of the total transmitted power is allocated for each layer. Then the secrecy capacity of each layer is examined using the same PLS scheme described above and observe performance of each data stream. Decoding superimposed layered data necessarily involves the use of SIC, which results in rate splitting for each layer and, as a result, a difference in secrecy capacity for each layer.

1.6 Thesis Organization

Results of the research described in this thesis have been published in the form of a conference paper [35], and the following two chapters are reflecting the contributions that is published in this papers.

The remainder of this thesis is organized as follows:

In Chapter 2, we focus on two-path relaying networks with single data stream signaling. First, the received signals at both relays, the intended receiver and the eavesdropper are defined. Then, the PLS scheme components which are proposed to enhance the confidentiality are discussed. Specifically, we present how to exploit IRI as an artificial noise while mitigating it at the intended receiver. In addition, power control is employed to eliminate the fading effect of relays-destination channels. Network coding is also examined in terms of secrecy capacity enhancement. After that, we derived the secrecy capacity based on the proposed PLS scheme. Finally, the secrecy performance is evaluated of this relay network as a function of Eve's distance from the relays in both deterministic and fading environments.

In Chapter 3, we consider superposition coding of the transmitted signals in two-path relaying networks. the superimposed signals design and the allocated power to each data stream are introduced, the impact on the received signals at the relays, intended receiver, and the eavesdropper is also highlighted. In the next step, we apply the same PLS scheme on the new signal design, introduce the concept of rate splitting, and accordingly, the secrecy capacity formulas. At the end, we evaluate the performance of the same relaying network with layered transmission in terms of secrecy capacity as a function of Eve's distance in both deterministic and fading channels.

Chapter 4 presents the contribution of this research and the potential for future investigations.

Appendix A derives the full IRI cancellation for SISO two-path relay network, which is used in Chapter 2 and 3.

Chapter 2

Secrecy Capacity in Successive Relaying with Single Layer Transmissions

Successive relaying in wireless cooperative networks has been shown to improve channel capacity compared to single relay channel. In this chapter, we suggest a PLS scheme to improve the secrecy capacity, especially when the eavesdropper is close to the relays. This improvement is achieved in our work by (a) utilizing IRI as artificial noise, (b) adjusting the power control to cancel the fading effect between the relays and the intended receiver, and (c) applying network coding. When IRI is cancelled at the intended receiver, the eavesdropper cannot avoid this additional noise, which makes decoding the signal received difficult. Power control adds another layer of protection at the top of the existing AWGN and IRI. When applying network coding to the successive relaying system, the capacity of the eavesdropper is reduced because we take into consideration the minimum capacity between the relays and the eavesdropper, and the secrecy capacity is increased compared to the conventional single relay system.

PLS techniques are easy to design when extra resources are available at wireless network nodes (i.e., multi-antennas). Cooperative networks, however, help SISO networks to enjoy MIMO network functions. For example, cooperative jamming technique requires an extra antenna to send the artificial noise signal, while in cooperative networks, the artificial noise is built into the system and can be used to achieve the same goal without extra resources. This conclusion is beneficial and aids the security of the massive implementation of low-cost devices in the era of IoT using cooperative

communications.

This chapter is organized as follows; Section 2.1 introduces the system model of successive relaying network and defines the received signals at both relays and the intended receiver. Section 2.2 outlines the proposed PLS scheme to improve the secrecy capacity of the system. Section 2.2.1 discusses employing IRI as artificial noise, while Section 2.2.2 illustrates the use of power control to cancel the fading effect of relays-destination channels and Section 2.2.3 demonstrates how the implementation of network coding increases the confidentiality. Section 2.3 formulates the secrecy capacity equations based on the proposed PLS scheme. The performance of this system is then discussed in Section 2.4 in terms of secrecy capacity as a function of Eve's distance from the relays. A summary of the chapter is provided in Section 2.5.

2.1 System Model

Consider a two-path successive relaying system in a wireless network with one sender A (Alice), one receiver B (Bob), two half-duplex relays R_1 and R_2 in the presence of an eavesdropper E as shown in Fig. 2.1, whereas all the transceivers are equipped with single omni-directional antennas, and that the relays are located close to one another, since they are assisting communications from the same sender to the same receiver. In this one-way communication system, A sends signals to R_1 during the *even* time slots (TSs) and to R_2 during the *odd* TSs. While A transmits continuously, R_1 forwards its received signals to B during the *odd* TS, and R_2 forwards its received signals during the *even* TS, using the same spectrum that is utilized by A. It is worth observing that because relays operate in half-duplex mode, the reception by R_1 during the *even* TSs from A is affected by signals from both A and R_2, while in the *odd* TSs, R_1 cannot overhear the signal from A that is destined to R_2.

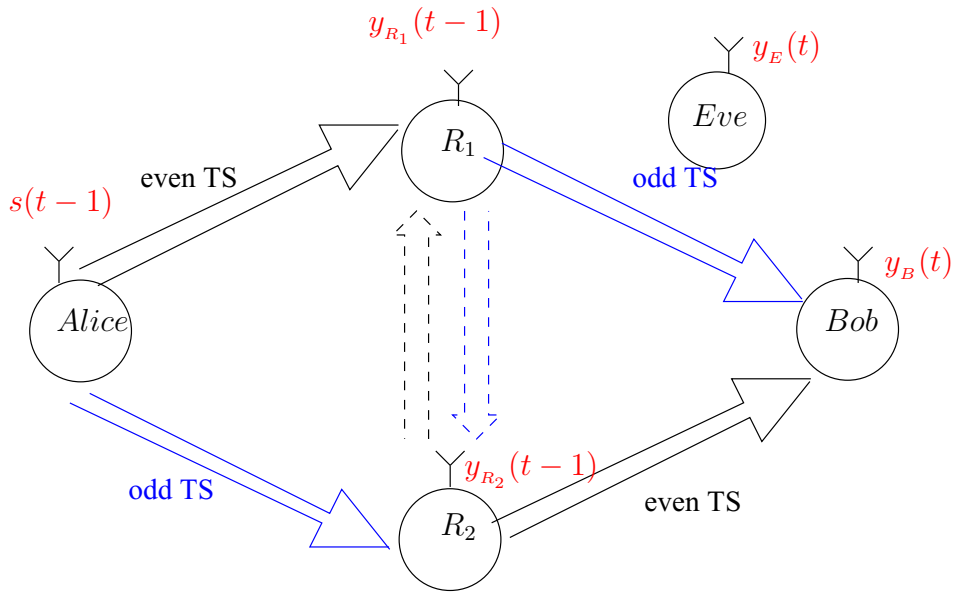


Figure 2.1: The system model: Two-path successive relaying network

Using AF strategy, R_1 transmits in *odd* TSs and R_2 transmits in *even* TSs sending the previously received signals $y_{R_1}(t-1)$ and $y_{R_2}(t-1)$ to B with signal amplification factors g_{R_1} and g_{R_2}. In this chapter, one data stream is transmitted, denoted as $s(t-1)$, and P is the transmit power at A. All wireless links are affected by circular additive white gaussian noise (AWGN) at each node's antenna ($n_{R_i}(t)$, $n_B(t)$ and $n_E(t)$ with the corresponding subscript identifying the terminal) and may exhibit i.i.d. Rayleigh fading. The fading (random) portion of channel gains remain constant during one TS but change independently from one slot to another according to a complex Gaussian distribution ($\mathcal{CN}(0,1)$). The deterministic path loss of signal power as a function of distance determines the average channel conditions which will depend on the inter-distances between different nodes in the system. In the simulation section, we reflect this by working with the power decay as a function of distance d given by $\frac{1}{d^4}$ representing ground wave propagation. The channel gains capturing deterministic signal decay with distance and fading are given as follows:

- h_{AR_i} between A and relays, $i \in \{1,2\}$
- h_{R_iB} between the relays and B

- h_{R_iE} between the relays and E
- h_{RR} between relays

Assume there is no direct link between A and B and no direct link between A and E. Also, the channel gain coefficients are reciprocal (i.e., $h_{R_2R_1} = h_{R_1R_2}$). The corresponding channel gains between different terminals in this system are visualized in Fig. 2.2.

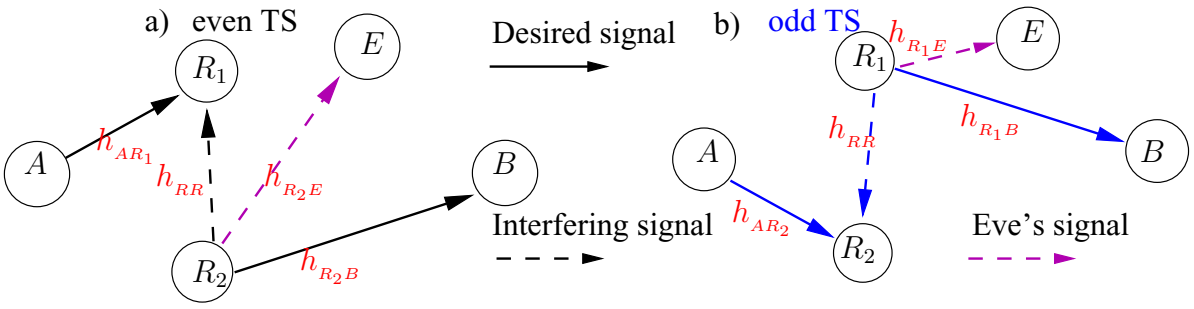


Figure 2.2: The corresponding channel gains with time separation between *even* and *odd* time slots.

During TS = 1, the communication process is initiated, and A is the only node in the network that has signals to transmit. Therefore, the received signal at R_1 during TS = 1 is not accompanied by any interference and is only multiplied (attenuated) by h_{AR_1} and corrupted by the relay's AWGN $n_{R_1}(1)$, which is assumed to have zero mean and unit variance. Hence the received signal at R_1 can be expressed as:

$$y_{R_2}(1) = \sqrt{P}\, h_{AR_2} s(1) + n_{R_2}(1) \tag{2.1}$$

where P stands for transmit power and controls average SNR on a link in the system. During TS = 2, R_2 is responsible for listening to A; however, while A is transmitting signals during TS = 2, R_2 is also transmitting an amplified version of $y_{R_2}(1)$. Therefore, the received signal at R_2 during TS = 2 is not only pure signal from A but also

interference from the transmitted signal by R_1. The received signal at R_2 during TS = 2 can thus be expressed as:

$$y_{R_1}(2) = \sqrt{P}\, h_{AR_1} s(2) + h_{RR} g_{R_2} y_{R_2}(1) + n_{R_1}(2) \tag{2.2}$$

The task of the relays is only to amplify the received signals, whereas dealing with the interference is handled by the receiver B. Thus, the following signal is received at Bob during TS = 2 and TS = 3:

$$y_B(2) = \sqrt{P} h_{R_2 B} g_{R_2} h_{AR_2} s(1) + h_{R_2 B} g_{R_2} n_{R_2}(1) + n_B(2)\ , \tag{2.3}$$

$$y_B(3) = \sqrt{P} h_{R_1 B} g_{R_1} h_{AR_1} s(2) + h_{R_1 B} g_{R_1} h_{RR} g_{R_2} y_{R_2}(1) + h_{R_1 B} g_{R_1} n_{R_1}(2) + n_B(3)\ , \tag{2.4}$$

where $n_B(2)$ is AWGN at Bob in TS 2. Similarly, during TS = 3, R_2 receives signal from A as well as interference from R_1:

$$y_{R_2}(3) = \sqrt{P}\, h_{AR_2} s(3) + h_{RR} g_{R_1} y_{R_1}(2) + n_{R_2}(3) \tag{2.5}$$

and when R_1 forwards this signal to B during TS = 4, it arrives as:

$$y_{R_1}(4) = \sqrt{P}\, h_{AR_1} s(4) + h_{RR} g_{R_2} y_{R_2}(3) + n_{R_1}(4)\ . \tag{2.6}$$

The process continues, and with every TS, R_1 and R_2 exchange the roles of receiving and forwarding signals. Thus (2.2) and (2.5) can be generalized as:

$$y_{R_i}(t-1) = \sqrt{P}\, h_{AR_i} s(t-1) + h_{RR} g_{R_j} y_{R_j}(t-2) + n_{R_i}(t-1) \tag{2.7}$$

where i = 1 and j = 2 if the TS $t-1$ is *even*, and i = 2 and j = 1 if TS $t-1$ is *odd*. Similarly, the received signal at Bob can be expressed in a general form as:

$$y_B(t) = \sqrt{P} h_{R_i B} g_{R_i} h_{AR_i} s(t-1) + h_{R_i B} g_{R_i} h_{RR} g_{R_j} y_{R_j}(t-2) + h_{R_i B} g_{R_i} n_{R_i}(t-1) + n_B(t). \tag{2.8}$$

where i = 1 and j = 2 if the TS t is *odd*, and i = 2 and j = 1 if TS t is *even*.

2.2 Physical Layer Security Scheme

In this work, PLS scheme consists of three components. Namely, IRI as artificial noise, power control, and network coding.

2.2.1 Inter-Relay Interference as Artificial Noise

To enhance the secrecy performance in the system model presented in Section 2.1, we exploit the impact of inevitable IRI at the eavesdropper. The premise for our approach is that in the system model presented, IRI can be fully removed at the intended receiver with possible deterioration in capacity due to AWGN enhancement, while the eavesdropper, in addition to AWGN, is affected by IRI, fading and power decaying.

2.2.2 Power Control

Based on (2.8), the received signal at B is composed of:

1. The desired signal, $s(t-1)$ (shown in green in (2.8))
2. The IRI term (shown in red)
3. Amplified AWGN from the relay
4. AWGN from the desired receiver

To control the received signal levels, we assume the following power control at R_i so that $|h_{R_2B}| \cdot g_{R_2} = 1$ (in *even* TSs) and $|h_{R_1B}| \cdot g_{R_1} = 1$ (in *odd* TSs). We also consider power control at A so that $\sqrt{P} \cdot |h_{AR_i}| = 1$. Using the Finite Impulse Response (FIR) filter at B and assuming knowledge of h_{R_iB}, g_{R_i} and h_{RR}, the auto recursive IRI can be removed (red term in (2.8)). At B, during *even* TS t, this results in the post-processed signal $\hat{y}_B(t)$ given by [7]:

$$\begin{aligned} \hat{y}_B(t) &= s(t-1) + n_{R_2}(t-1) + n_B(t) - \frac{h_{RR}}{h_{R_1B}} n_B(t-1) \\ &= s(t-1) + n_{B,\text{total}}(t) \end{aligned} \tag{2.9}$$

where $n_{B,\text{total}}(t)$ is the total AWGN at B after noise enhancement from IRI removal with variance $Var\big(n_{B,\text{total}}(t)\big) = \sigma^2_{B,\text{total}}$ controlled by SNR at relays and corresponding channel gains.

Without IRI cancellation (due to lack of knowledge of the required CSI from R_i to B), the received signal at E in *even* TSs t has the representation similar to (2.8) with the corresponding change of channel gains in the second hop is given by:

$$\begin{aligned} y_{E}(t) = h_{R_2E} g_{R_2} s(t-1) + h_{R_2E} g_{R_2} h_{RR} g_{R_1} y_{R_1}(t-2) \\ + h_{R_2E} g_{R_2} n_{R_2}(t-1) + n_{E}(t). \end{aligned} \tag{2.10}$$

Similarly, as when analyzing AWGN at B, the term $n_{E,\text{total}}(t) = h_{R_2E} g_{R_2} n_{R_2}(t-1) + n_{E}(t)$ represents the total AWGN at E with variance $\sigma^2_{E,\text{total}}$. It is the second term in (2.10) which represents the IRI (displayed in red) that sets apart the ability to detect $s(t-1)$ at the intended receiver and at the eavesdropper. This is also the case when comparing secrecy of the proposed schemes with single relay transmissions where only the channel gains may protect the legitimate user by being closer to the relays.

2.2.3 Network Coding

In addition to controlling IRI and fading as presented earlier to improve the secrecy capacity by deteriorating the eavesdropper's SINR, network coding can be deployed to take advantage of asymmetry in channel conditions between the relays and Eve. Despite the fact that Bob's capacity may be also reduced because the worst channel condition should be considered due to the mixing of *even* and *odd* messages in bit-level coding (as illustrated in section 1.3), Eve's capacity is reduced further because the distances from E to R_1 and R_2 are not equal for most positions of E. (In our model, the distances between relays and Bob are the same, and if they were not, power control at relays should be adjusted so that Bob receives relay signals at the same power). As a result, when NC is deployed, the eavesdropper's capacity is two times the minimum capacity from the two paths rather than the sum of capacities as it is the case when there is no NC. The reason for this is that in order to reconstruct the original data, information from both links has to be detected reliably. As a result,

it is expected that the secrecy capacity is enhanced.

2.3 Secrecy Capacity

In the system model under study, the total secrecy capacity is the sum of secrecy capacities in *odd* and *even* TSs transmission, while for each TS, the secrecy capacity is the difference between the channel capacities from the relays to the intended receiver B and to the eavesdropper E, respectively, since the operation of two half-duplex relays in successive mode mimics an ideal full-duplex relay, where the sender and receiver are transmitting and receiving all the time [8]. In single data stream signaling, the secrecy capacity in *even* TS transmissions is given by:

$$C_{_{S,R_2B}} = \frac{1}{2}\Big[\log_2\big(1+\frac{P|h_{_{AR_2}}|^2}{\sigma^2_{_{B,\text{total}}}}\big) - \log_2\big(1+\frac{P|h_{_{R_2E}}|^2 g^2_{_{R_2}}|h_{_{AR_2}}|^2}{P|h_{_{R_2E}}|^2 g^2_{_{R_2}}|h_{_{RR}}|^2 g^2_{_{R_2}} + \sigma^2_{_{E,\text{total}}}}\big)\Big]^+. \quad (2.11)$$

The expression for the secrecy capacity in *odd* TS transmissions, $C_{_{S,R_1B}}$, is similar to (2.11) by exchanging R_1 and R_2 subscripts and corresponding changes to get $\sigma^2_{_{B,\text{total}}}$ and $\sigma^2_{_{E,\text{total}}}$. Subsequently, the total secrecy capacity for the two paths is the sum of secrecy capacities of R_1 and R_2 assisted paths as follows:

$$C_{_S}^{Total} = C_{_{S,R_1B}} + C_{_{S,R_2B}} \ . \quad (2.12)$$

When using NC, since we need both coded messages from *even* and *odd* TSs to recover the original data transmitted in these TSs, the capacity for the original data on each link is bounded by the reliable data rate on both paths. In essence, if one link/path to Eve receives faster, the excessive NC data will be useless. Thus, the effective capacity of E is represented as:

$$C_{_E}^{NC} = 2 \cdot \min(C_{_{R_1E}}, C_{_{R_2E}}) \ . \quad (2.13)$$

Then, the total secrecy capacity with NC is given by

$$C_{_S}^{NC} = [C_{_B}^{NC} - C_{_E}^{NC}]^+ \ . \quad (2.14)$$

where C_B^{NC} is Bob's capacity evaluated similarly as in (2.13) when the intended receiver (Bob) has unbalanced links to relays. (Bob's and Eve's capacities for R_2 assisted path are evaluated using first and second terms in (2.11), respectively.)

Finally, it has to be observed that the secrecy capacity expressions derived so far are for a given realization of fading channels and fixed position of nodes in the system under study. In the next section, we present the average (ergodic) secrecy capacity results for numerous realizations of fading channels at different positions of the eavesdropper.

2.4 Performance Evaluation

In this section, MATLAB® simulation results are presented in terms of secrecy capacity performance as a function of Eve's position for our proposed schemes in deterministic and fading environments. The focus on successive relaying is because it significantly enhances the secrecy capacity of the main channel by (i) normalizing the pre-log factor and (ii) keeping Bob's SNR higher than Eve's SINR, even when Eve is closer to the relays than Bob. We evaluate the impact of the proposed PLS scheme on the secrecy capacity performance at any position of Eve and compare it with the performance of the conventional relay system model.

Reference Model

Consider the traditional relaying system where a half-duplex relay aids transmission from Alice to Bob. Assuming that the direct transmission from Alice to Bob is unavailable and the relaying strategy is amplify-and-forward, the secrecy capacity of the conventional scheme is constrained by (i) the pre-log factor ($\frac{1}{2}$) and (ii) Eve's distance from the relay. This means that if Eve is closer to the relay than Bob, Eve's SNR is higher than Bob's SNR. As a result, secrecy capacity is zero. Noting that the relay selection of this scheme is based on selecting the relay which has better channel

conditions with Alice and Bob.

Numerical Results

To evaluate the performance of the successive relaying system and compare it with the reference model, both deterministic and fading channels are analyzed numerically to measure the secrecy capacity. In our simulations, R_1, R_2, and B are in fixed positions and form an equilateral triangle with unity distance from each other, with B on the horizontal axis at coordinates $(\frac{\sqrt{3}}{2}, 0)$ while R_1 and R_2 on the vertical axis at coordinates (0, 0.5) and (0, -0.5), respectively, as shown in Fig. 2.3. In conventional relaying system, B is located on the horizontal axis at coordinates (1, 0) while the relay is located at the origin point. Because we assume that E (similarly as B) is not in the transmission range of A, the position of E is varying in the right-half plane within the square which has a side of 8 (all the distances have been normalized with respect to the transmit power).

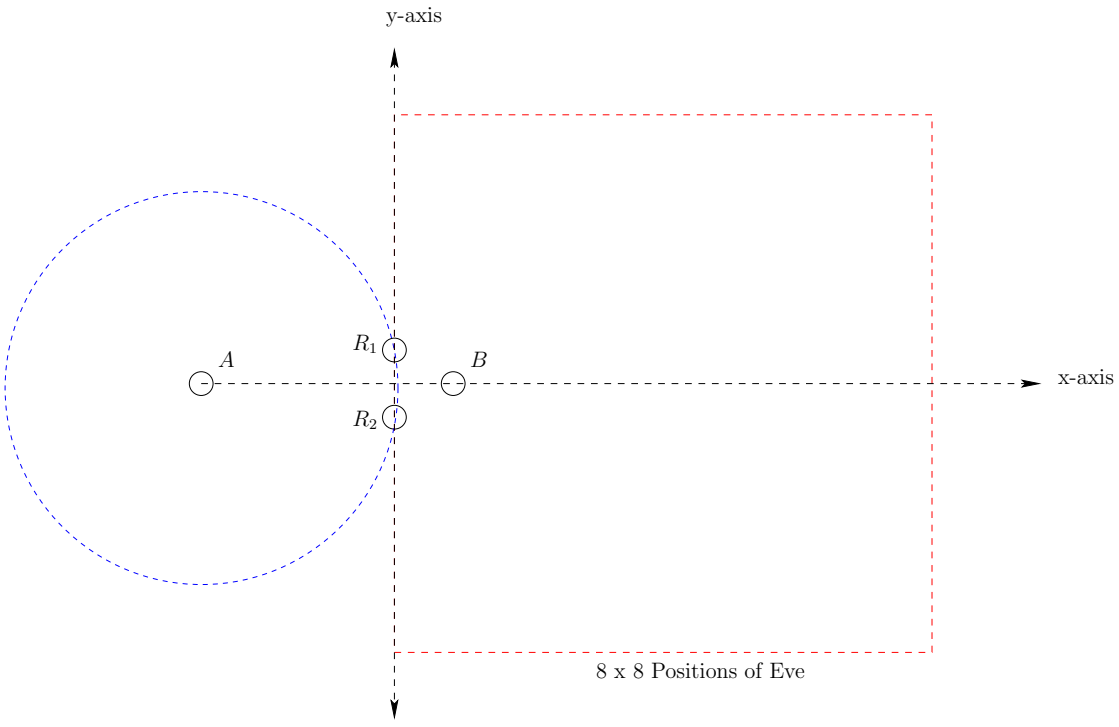


Figure 2.3: X-Y plane for Eve's positions.

In most results presented, the initial average received SNR at B is 10 dB (without noise enhancement). With this, 10^{-5} bit-error rate (BER) can be achieved in practical implementations. Ground wave propagation is considered as power path loss factor (i.e., $\beta = 4$). For fading channels, we present ergodic secrecy capacity evaluated using Monte-Carlo simulations based on averaging link capacities over 10^6 independent channel realizations for a given position of the eavesdropper and the intended receiver. The results are presented as (i) 3D plots in which the x-y plane represents the eavesdropper's positions as shown in Fig. 2.3, and (ii) 2D plots in which a slice from that space along the vertical axis (both relays and the origin) or the horizontal axis (passing through Bob), and the z-axis represents (a) the results of secrecy capacity calculations based on the corresponding formulas derived in Section 2.3 involving distances in the case of the deterministic channel, and (b) the ergodic secrecy capacity when simulating different realizations of fading channels and averaging the corresponding (calculated) secrecy capacities in the case of Rayleigh fading channels.

Figure 2.4 represents 2D slice from secrecy performance of the successive relaying system compared to the conventional half-duplex model in the deterministic environment (path loss and AWGN only). In this figure, the secrecy capacity of two-path relaying (plotted as a black line with plus signs) clearly outperforms the conventional scheme (plotted as a red line with circles) even with the noise enhancement in our system model. Specifically, two-relay system achieves 1.3 bps/Hz in the area where zero secrecy capacity can be achieved by the conventional model. Adding NC component to the PLS scheme in the successive relaying system improves secrecy capacity by up to 5% over the same system without the NC. Also, when E is far from the relays, 30% improvement in the secrecy capacity can be observed using successive relaying system. To have a better view of the system performance, we introduce 3D plots to cover the cube which represents the coverage space of the relays under study. Figure 2.5 visualizes the same performance in 3D plot.

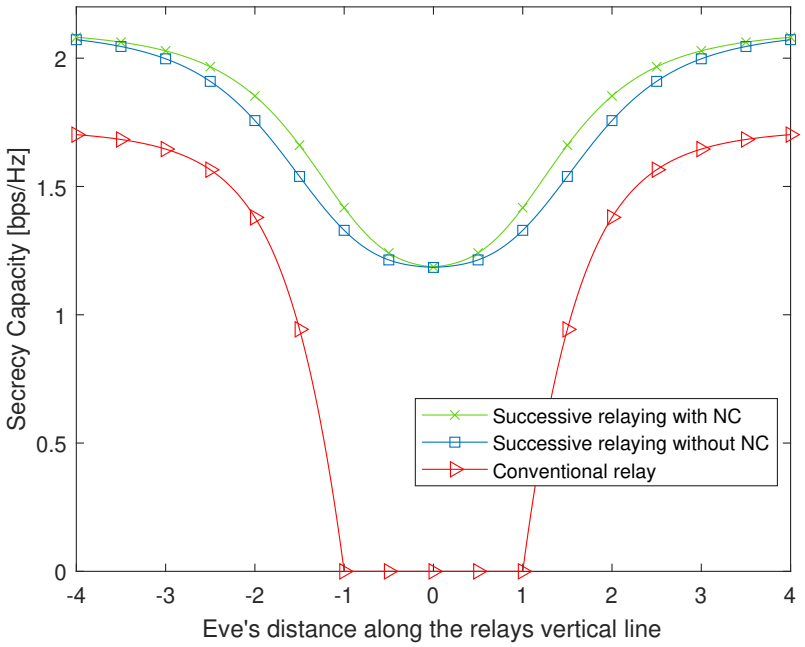


Figure 2.4: Secrecy performance benchmarking for single layer signaling in deterministic environment, represented by a 2D vertical slice.

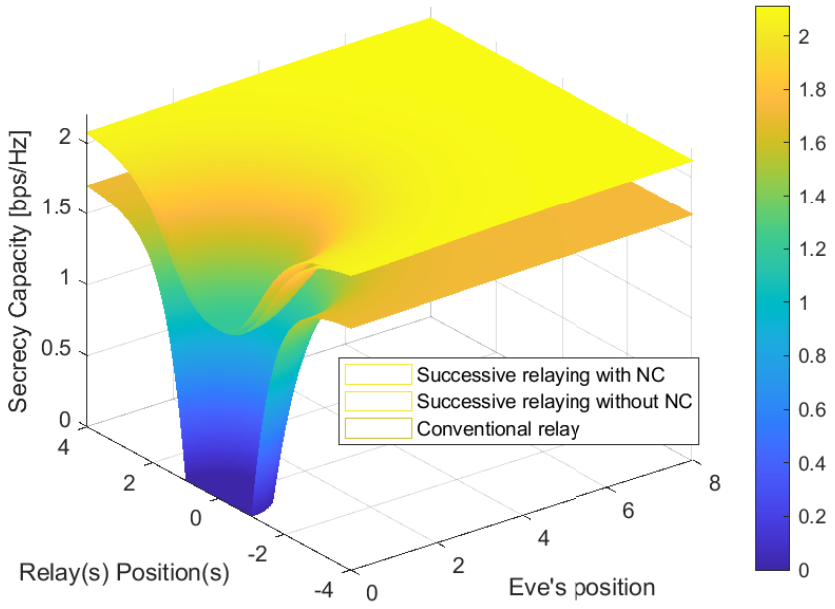


Figure 2.5: Secrecy performance benchmarking for single layer signaling in deterministic environment, represented by a 3D plot.

In Rayleigh fading environment, two-relay system achieves 1.0 bps/Hz in the area where zero secrecy capacity can be achieved by the conventional model. Figure 2.6 visualizes the 2D slice from secrecy capacity performance of the two-relay system compared to the conventional one in a Rayleigh fading environment, where the significant improvement can be observed when E is closer to the relays, while Fig. 2.7 shows the 3D plot for the same performance. In this figure, one can observe the 12% improvement of the secrecy capacity using two-relay system when E is far from the relays.

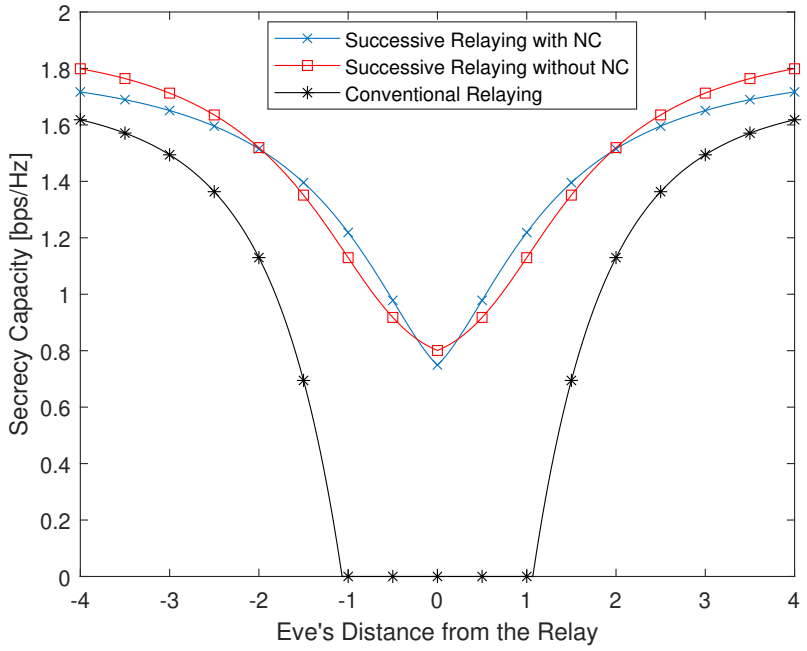


Figure 2.6: Secrecy performance benchmarking for single layer signaling in Rayleigh fading environment, represented by a 2D vertical slice.

It is obvious that the performance in deterministic environment is better than in fading. Figure 2.8 shows the impact of fading on (a) the proposed scheme and (b) the conventional one, respectively.

In addition to 10 dB as average received SNR (i.e., the desired signal power is 10 times more than the noise power), we examined two other values; 7 dB (i.e., the

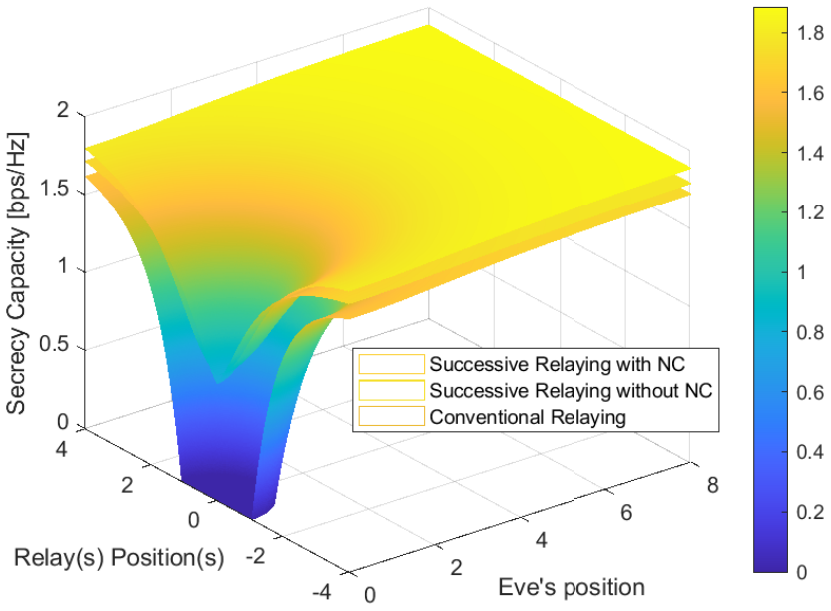
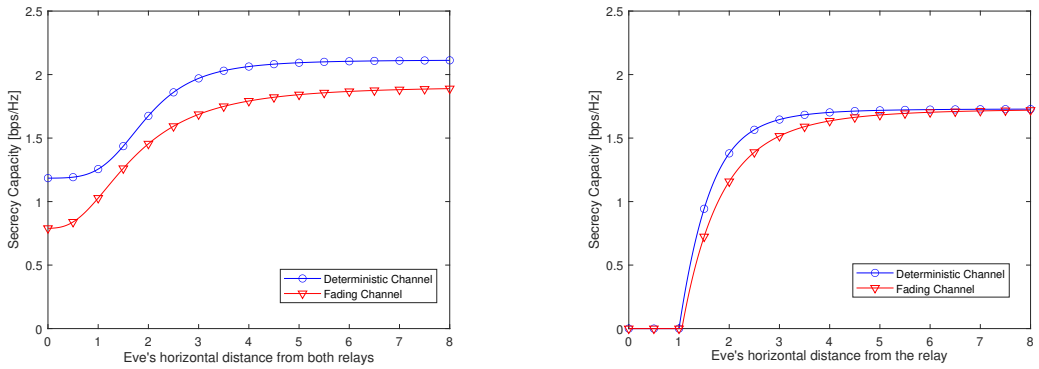


Figure 2.7: Secrecy performance benchmarking for single layer signaling in Rayleigh fading environment, represented by a 3D plot.

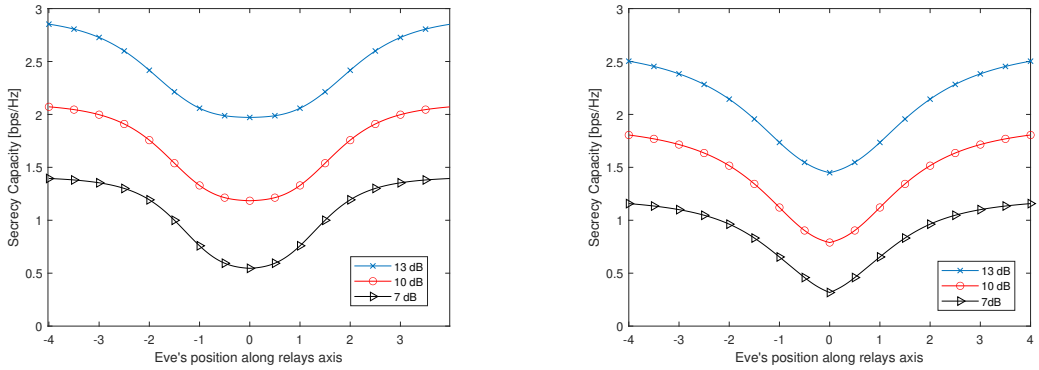


(a) Successive Relaying System (b) Conventional Relaying System

Figure 2.8: Secrecy performance benchmarking in single layer signaling (deterministic vs fading), represented by a 2D horizontal slice.

desired signal power is 5 times more than the noise power), and 13 dB (i.e., the desired signal power is 20 times more than the noise power) to observe its impact on the system performance. It has been observed that the average received SNR is directly proportional with the secrecy performance. Figure 2.9 shows the performance of both relaying systems in deterministic and fading environments while varying the

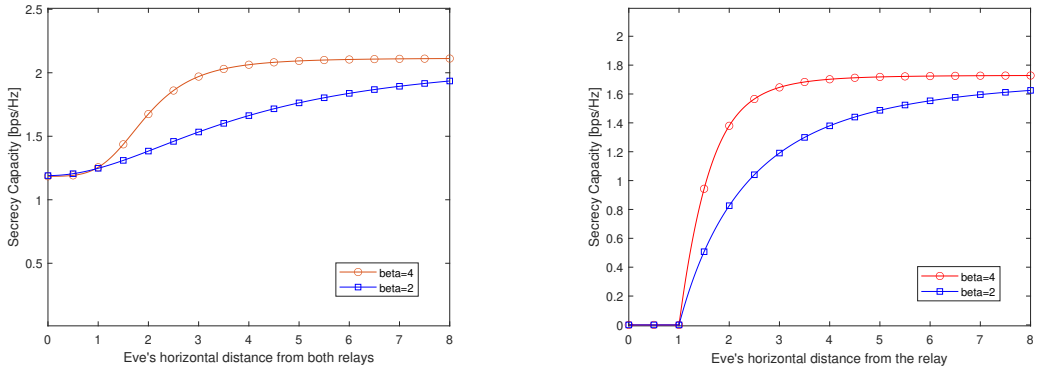
average received SNR. This 2D slice is along relays line (i.e., vertical axis).



(a) Deterministic Channel (b) Fading Channel

Figure 2.9: Secrecy performance in single layer signaling with different average received SNRs, represented by a 2D vertical slice.

These numerical results also examined the effect of the path loss factor in improving the secrecy capacity. Free space is compared to ground wave propagation (power path loss factor = 2 and 4, respectively). It is observed that ground wave propagation improves the secrecy capacity by up to 30% and 50% in two-relays and one-relay system, respectively as shown in Fig. 2.10 for deterministic environment.



(a) Two Relays System (b) One Relay System

Figure 2.10: Power path loss effect on secrecy performance for ground wave propagation (beta=4) and free space (beta=2).

2.5 Summary

In this chapter, we considered two-path successive relaying wireless network in a SISO setting where a pair of half-duplex AF relays mimics the operation of a full duplex relay. In our presented PLS scheme, we exploited the IRI to confuse the eavesdropper while it is mitigated at the intended receiver. In addition, we adapted power control to cancel the fading effect from both relays to the intended receiver and consequently increase the secrecy capacity of the main channel. IRI and power control acted as artificial noise without consuming extra system resources. Network coding is also examined in terms of improving the secrecy capacity of the system model.

In view of the secrecy capacity as a performance metric, the proposed PLS scheme was shown to be superior in successive relaying to the conventional relay system in both deterministic and fading environments even when the eavesdropper is closer to the relays.

Chapter 3

Secrecy Capacity in Successive Relaying with Multi-Layer Transmissions

It is vital in the next generation of wireless systems to have an efficient and secure broadcast for multimedia transmission. However, because of the wide variations in wireless channel conditions among users, as well as the high user mobility in some cases, providing the same QoS to all users in the coverage area poses a significant challenge in the design of any multimedia transmission wireless system.

In traditional broadcast systems, different receiver nodes would experience different SNR depending on the path loss with distance. As a result, the broadcast system throughput is limited by the data rate of the user with worst channel conditions to achieve a desired minimum acceptable image quality. Deploying layered transmission is one of the most successful and efficient solutions for addressing this issue in broadcast wireless networks. Layered transmission is a method of making flexible use of the broadcast spectrum by transmitting multiple data streams on the same radio resources in one signal. The splitting of a data stream into sub-streams of varying importance is common in multimedia applications such as video and audio transmissions. When decoding video at the terminal with different SNRs, different levels of resilience can be obtained by combining hierarchical transmission of video sequences with hierarchical or layered modulations [31].

Superposition coding is a promising approach for sending multiple data streams in broadcast systems in the same signal. The primary goal of superposition coding is to communicate two messages at the same time by encoding them into one signal

with two layers. A "better" receiver of the signal can then recover the messages on both layers, whereas a "worse" receiver can recover the message on the coarse layer and ignore the message on the fine layer [36].

This chapter investigates the PLS aspect of a successive relaying network with superposition coding to determine the theoretical upper limit of the rate at which data can be transmitted confidentially without being leaked to an eavesdropper. When using AF relaying strategy, IRI signals may limit system performance if they are not effectively mitigated. In the same PLS scheme discussed in Section 2.2, IRI is used to provide security by cancelling its effect on the intended receiver and increasing the noise level at the eavesdropper node. Furthermore, the forwarded signal power at the relays is adjusted unique to the relay-destination CSI to normalize the fading effect while increasing the noise level at the eavesdropper. It should be noted that two interference cancellation techniques are used in this chapter: SIC to decode the superimposed signals and IRI cancellation to improve security.

In addition to the impact of IRI on the eavesdropper's signal detection capability, the signals design with multiple quality layers via SC is considered in this chapter to support different secrecy rates for different data streams. This is done with the goal of providing flexible security-level configurations and QoS by allocating power to different layers. The security performance of SC which is a form of power-domain nonorthogonal multiple access (NOMA) is aided, in addition to IRI, by layers of lower power which are decoded last in the SIC detectors.

This chapter is organized as follows; Section 3.1 introduces the layered transmission in successive relaying network and defines the received signals at both relays and the intended receiver. Section 3.2 uses the proposed PLS scheme to determine the secrecy capacity formulas for each data stream. Section 3.3 then evaluates the system's performance in terms of secrecy capacity as a function of Eve's distance from the relays. A summary of the chapter is provided in Section 3.4.

3.1 Power Allocation

Consider the same two-path successive relaying system discussed in section 2.1, where Alice transmits $s(t-1)$ continuously in all TSs and both relays take turns in listening and forwarding. The implementation of the SC by Alice is done by splitting a source message (k bits) into two layers, the base and enhancement layers, with k_1 and k_2 bits in each layer where $k_1 + k_2 = k$, i.e., the QAM symbols from M_1-QAM and M_2-QAM constellations where $M_1 = 2^{k_1}$ and $M_2 = 2^{k_2}$. Assume that $s(t-1)$ represents the two data streams referred to as base and enhancement layers, and they are represented by s_1 and s_2, respectively. These simultaneously transmitted signals with different power levels $P_1 = \alpha_1^2 \cdot P$ and $P_2 = \alpha_2^2 \cdot P$ are combined into $s(t-1)$ as follows:

$$s(t-1) = \sqrt{P} \cdot \Big(\alpha_1 s_1(t-1) + \alpha_2 s_2(t-1) \Big) \tag{3.1}$$

with s_1 and s_2 having 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. The power allocation parameters ($0 < \alpha_i^2 \leq 1$, $i \in \{1, 2\}$) between two layers are such that $\alpha_1^2 + \alpha_2^2 = 1$ and P is the total transmit power at A where $P_1 + P_2 = P$.

Using amplify-and-forward strategy, R_1 and R_2 will amplify the superimposed received signals by g_{R_1} and g_{R_2}, respectively. Assuming that R_2 in *odd* TS $t-1$ is receiving $y_{R_2}(t-1)$ and B in *even* TS t is receiving $y_B(t)$ (i.e., when R_2 is transmitting), and there is no direct link between A and B as visualized in Fig. 3.1, these signals through over-the-air summation can be expressed as:

$$y_{R_2}(t-1) = h_{AR_2} \big(\sqrt{P_1} s_1(t-1) + \sqrt{P_2} s_2(t-1) \big) + h_{RR}\, g_{R_1}\, y_{R_1}(t-2) + n_{R_2}(t-1)\ . \tag{3.2}$$

$$\begin{aligned} y_B(t) = {} & h_{R_2B}\, g_{R_2}\, h_{AR_2} \big(\sqrt{P_1} s_1(t-1) + \sqrt{P_2} s_2(t-1) \big) \\ & + h_{R_2B}\, g_{R_2}\, h_{RR}\, g_{R_1}\, y_{R_1}(t-2) + h_{R_2B}\, g_{R_2}\, n_{R_2}(t-1) + n_B(t)\ . \end{aligned} \tag{3.3}$$

Similar received signal relations as in (3.2) and (3.3) can be derived for *even* TS $t-1$ and *odd* TS t by interchanging the subscripts in R_1 and R_2. This observation is valid

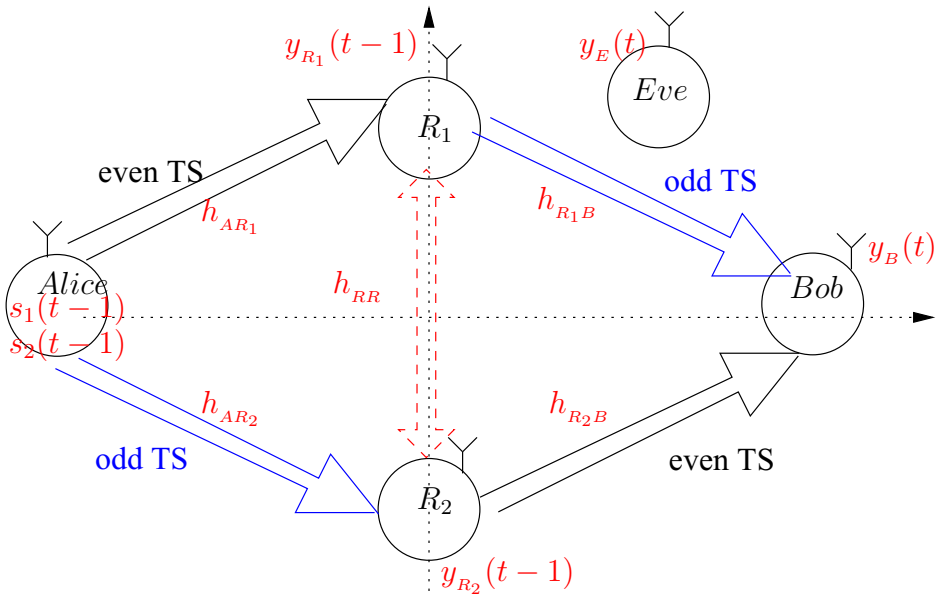


Figure 3.1: Two-path alternate relaying network with layered signaling

for other relations in this chapter, and this is why our initial focus is on *even* TSs t when R_2 is transmitting.

To enhance the secrecy performance in this system model, the following components of PLS scheme discussed in section 2.2 are applied: (a) IRI removal at Bob, and (b) power control unique for R_i-Bob CSI. When $s(t-1)$ is given by (3.1), the received signal at B after IRI removal [7] in *even* TSs is:

$$\hat{y}_B(t) = h_{AR_2}\sqrt{P}\Big(\alpha_1 s_1(t-1) + \alpha_2 s_2(t-1)\Big) + n_{B,\text{total}}(t), \tag{3.4}$$

where $n_{B,\text{total}}(t) = n_{R_2}(t-1) + n_B(t) - \frac{h_{RR}}{h_{R_1B}} n_B(t-1)$ represents the total AWGN at B after noise enhancement from IRI removal with variance $\sigma^2_{B,\text{total}}$ controlled by SNR at relays and corresponding channel gains. On the other hand, without IRI cancellation (due to lack of knowledge of the required CSI from R_i to B), and assuming that there is no direct link between A and E, the received signal at E in *even* TSs t with the corresponding change of channel gains in the second hop is given by:

$$\begin{aligned} y_E(t) = {} & \sqrt{P_1} h_{R_2E} g_{R_2} h_{AR_2}\ s_1(t-1) + \sqrt{P_2} h_{R_2E} g_{R_2} h_{AR_2} s_2(t-1) \\ & + h_{R_2E} g_{R_2} h_{RR} g_{R_1} y_{R_1}(t-2) + n_{E,\text{total}}(t) \end{aligned} \tag{3.5}$$

where the red term represents a non-removable level of IRI at E that deteriorate its SINR and increase the secrecy capacity, and the term $n_{_{E,\text{total}}}(t) = h_{_{R_2E}} g_{_{R_2}} n_{_{R_2}}(t-1) + n_{_E}(t)$ represents the total AWGN at E with variance $\sigma^2_{_{E,\text{total}}}$.

In SC, when decoding data represented by $s_1(t-1)$ and $s_2(t-1)$ at the desired receiver B, assuming $\alpha_1 > \alpha_2$, $s_1(t-1)$ is demodulated first and $s_2(t-1)$ is treated as the interference (this is an additional perturbation on top of enhanced AWGN, fading, and IRI at E). Then, using successive interference cancellation (SIC) [6], after decoding $s_1(t-1)$, the effects of $s_1(t-1)$ is removed from $\hat{y}_{_B}(t)$ and the data represented by $s_2(t-1)$ is demodulated. At B, decoding of $s_2(t-1)$ is only affected by the (black) AWGN term in (3.4). At the eavesdropper, based on (3.5), the detection of both data streams represented by $s_1(t-1)$ and $s_2(t-1)$ follows the same process as at B but is affected by the IRI (in addition to $s_2(t-1)$ and AGWN terms).

3.2 Rate Splitting

Secrecy capacity is the theoretical upper bound of the maximum achievable secrecy rate. In two-layer signaling, the rate splitting concept is used to calculate the capacities in multi-layer signaling. The capacity of the base layer at B in *even* TS transmissions is given by:

$$C^{s_1}_{_{R_2B}} = \frac{1}{2}\log_2\big(1 + \frac{P_1\,|h_{_{AR_2}}|^2}{P_2\,|h_{_{AR_2}}|^2 + \sigma^2_{_{B,\text{total}}}}\big). \tag{3.6}$$

To arrive at (3.6), we observe that when B is decoding the base layer, the enhancement layer $s_2(t)$ is considered an interference with power P_2. Using SIC, B removes the impact of the base layer after decoding it, and then the capacity of the enhancement layer is given by:

$$C^{s_2}_{_{R_2B}} = \frac{1}{2}\log_2\big(1 + \frac{P_2\,|h_{_{AR_2}}|^2}{\sigma^2_{_{B,\text{total}}}}\big)\,. \tag{3.7}$$

The capacities of the base and the enhancement layers at B in *odd* TS transmissions are similar to (3.6) and (3.7) with exchanged R_1 and R_2 subscripts and accounting

for different calculations of $\sigma^2_{B,\text{total}}$. The total capacity at B for the base layer is given by:

$$C_B^{s_1} = C_{R_1B}^{s_1} + C_{R_2B}^{s_1} \tag{3.8}$$

and the total capacity at B for the enhancement layer is similar to (3.8) but with s_2 in superscripts.

When calculating the capacity of the base and the enhancement layers at E in *even* TS transmissions, we need to consider the impact of IRI, and these capacities are given by:

$$C_{R_2E}^{s_1} = \frac{1}{2}\log_2\left(1 + \frac{P_1|h_{R_2E}|^2 g_{R_2}^2 |h_{AR_2}|^2}{P_2|h_{R_2E}|^2 g_{R_2}^2 |h_{AR_2}|^2 + P|h_{R_2E}|^2 g_{R_2}^2 |h_{RR}|^2 g_{R_1}^2 + \sigma^2_{E,\text{total}}}\right) \tag{3.9}$$

$$C_{R_2E}^{s_2} = \frac{1}{2}\log_2(1 + \frac{P_2|h_{R_2E}|^2 g_{R_2}^2 |h_{AR_2}|^2}{P|h_{R_2E}|^2 g_{R_2}^2 |h_{RR}|^2 g_{R_1}^2 + \sigma^2_{E,\text{total}}}) \,. \tag{3.10}$$

The capacities of base and enhancement layers at E in *odd* TS transmissions, $C_{R_1E}^{s_1}$ and $C_{R_1E}^{s_2}$ are calculated as in (3.9) and (3.10) with the corresponding indexing changes in R_1 and R_2. With these, the total capacity at E for the base layer is given by:

$$C_E^{s_1} = C_{R_1E}^{s_1} + C_{R_2E}^{s_1} \tag{3.11}$$

and the secrecy capacity for the base layer is

$$C_S^{s_1} = \left[C_B^{s_1} - C_E^{s_1}\right]^+ . \tag{3.12}$$

The secrecy capacity for the enhancement layer can be evaluated in a similar fashion.

Finally, it has to be observed that the secrecy capacity expressions derived so far are for a given realization of fading channels and fixed position of nodes in the system under study. In the next section, the average (ergodic) secrecy capacity results for numerous realization of fading channels is presented at different positions of the eavesdropper.

3.3 Performance Evaluation

To examine the performance of the proposed scheme, both deterministic and fading channels are analyzed numerically to measure the secrecy capacity. In our simulations, R_1, R_2, and B are in fixed positions and form an equilateral triangle with unity distance from each other, with B on the horizontal axis at coordinates ($\frac{\sqrt{3}}{2}$, 0) while R_1 and R_2 on the vertical axis at coordinates (0, 0.5) and (0, -0.5), respectively, as shown in Fig. 2.3. In conventional relaying system, B is located on the horizontal axis at coordinates (1, 0) while the relay is located at the origin point. Because we assume that E (similarly as B) is not in the transmission range of A, the position of E is varying in the right-half plane within the square which has a side of 8 (all the distances have been normalized with respect to the transmit power). To capture the effects of ground wave propagation, we consider that power path loss factor is 4. With this, 30-50% higher secrecy capacity can be achieved in comparison to free space propagation. Also, in most results presented, the initial average received SNR at B is 10 dB (without noise enhancement). With this, 10^{-5} BER can be achieved in practical implementations. For fading channels, we present ergodic secrecy capacity evaluated using Monte-Carlo simulations based on averaging link capacities over 10^6 independent channel realizations for a given position of the eavesdropper and the intended receiver. When evaluating the performance of superimposed layers, 0.95 of the transmit power is allocated to the base layer s_1 and 0.05 to the enhancement layer s_2. This power allocation provides close to 10^{-12} BER for s_1 and 10^{-5} for s_2 in

practical implementations.

The results are presented as (i) 3D plots in which the x-y plane represents the eavesdropper's positions as shown in Fig. 2.3, and (ii) 2D plots in which a slice from that space along the vertical axis (both relays and the origin) or the horizontal axis (passing through Bob), and the z-axis represents (a) the results of secrecy capacity calculations based on the corresponding formulas derived in Section 3.2 involving distances in the case of the deterministic channel, and (b) the ergodic secrecy capacity when simulating different realizations of fading channels and averaging the corresponding (calculated) secrecy capacities in the case of Rayleigh fading channels.

3.3.1 Numerical Results

Base and enhancement layers are compared to each other in terms of secrecy capacity, and each layer is then benchmarked to the corresponding layer in the conventional single relay system.

In SC scheme, the secrecy performance is dependent on the power allocation for each data layer. Figure 3.2 visualizes a 2D slice for s_1 and s_2 in successive relaying system under deterministic environment (path loss and AWGN only). In this figure, the secrecy capacity of the base layer in successive relaying system clearly outperforms the base layer in conventional relaying system even with noise enhancement in our system model. The same can be said for the enhancement layer. In particular, the base and enhancement layers in successive relaying system achieve 1.1 and 0.2 bps/Hz, respectively, in the area where the conventional relaying system achieves zero secrecy capacity. To gain a better understanding of system performance, a 3D plot is introduced to cover the cube that represents the coverage space of the relays under study. Figure 3.3 visualizes the same performance in 3D plot.

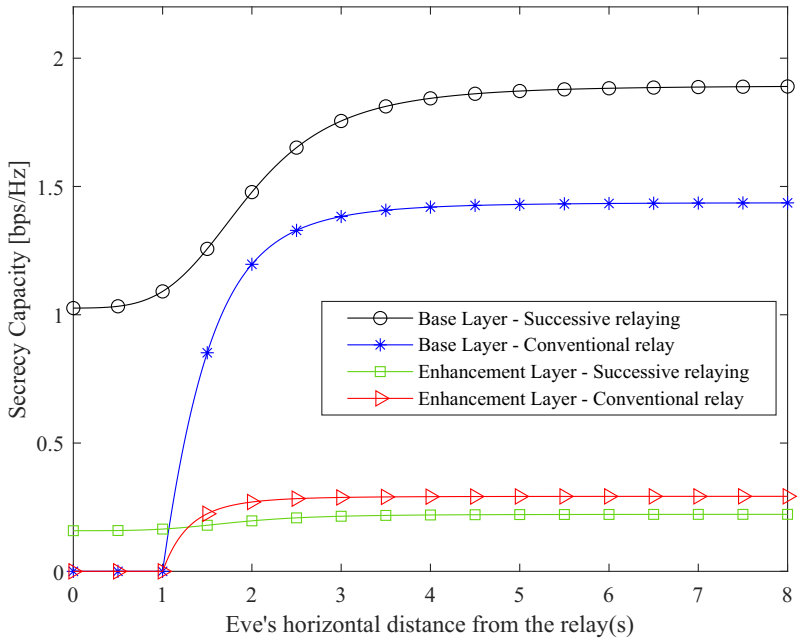


Figure 3.2: Secrecy performance benchmarking for SC scheme in deterministic environment at 10 dB average received SNR, represented by a 2D horizontal slice.

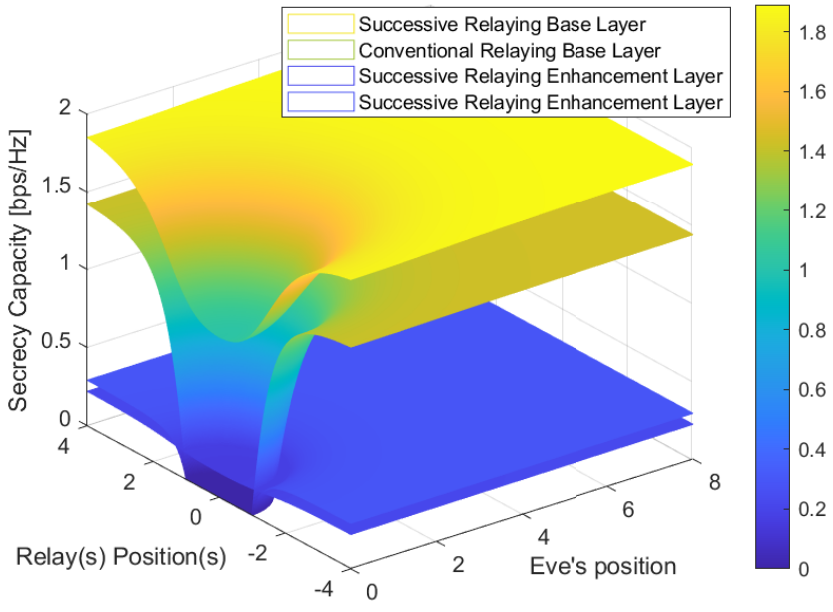


Figure 3.3: Secrecy performance benchmarking for SC scheme in deterministic environment at 10 dB average received SNR, represented by a 3D plot.

In a Rayleigh fading environment, the base and enhancement layers of a successive relaying system achieve 0.7 and 0.1 bps/Hz, respectively in the area where the conventional relaying system achieves zero secrecy capacity. Also, when E is far from the relays, the secrecy capacity of base and enhancement layers in successive relaying system improves by 48% and 27%, respectively, when compared to the conventional system. Figure 3.4 depicts the 2D slice from secrecy capacity performance of the two-relay system versus the conventional one in a Rayleigh fading environment, with a significant improvement when E is closer to the relays. Figure 3.5 shows the 3D plot for the same performance.

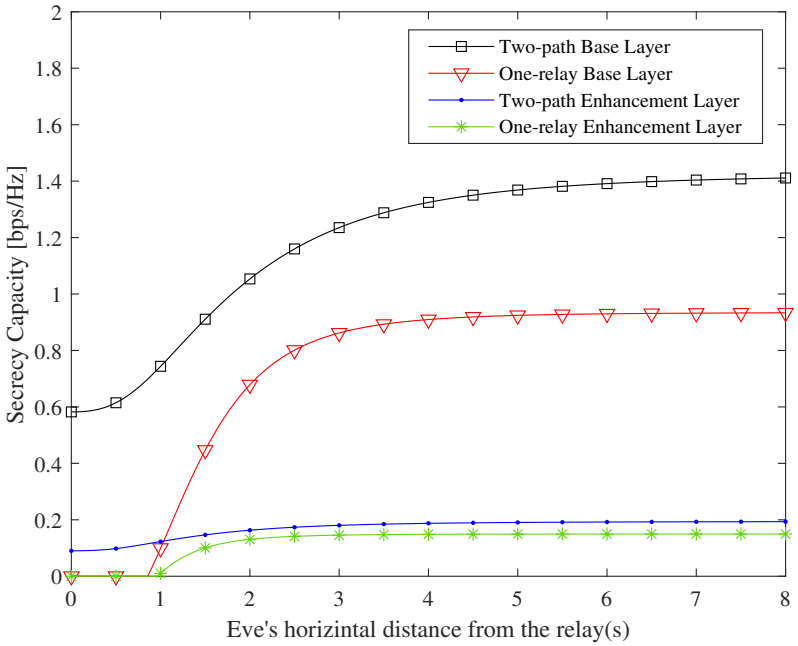


Figure 3.4: Secrecy performance benchmarking for SC scheme in Rayleigh fading environment at 10 dB average received SNR, represented by a 2D horizontal slice.

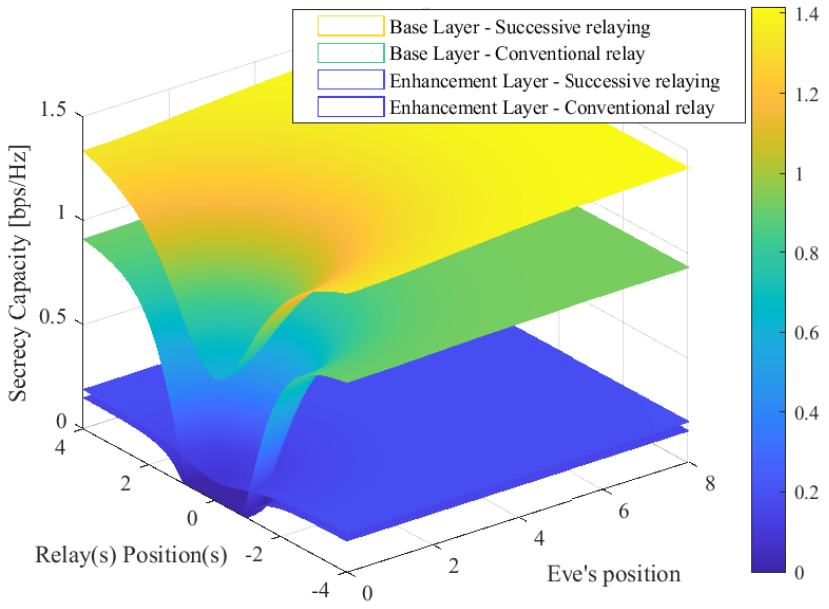


Figure 3.5: Secrecy performance benchmarking for SC scheme in Rayleigh fading environment at 10 dB average received SNR, represented by a 3D plot.

In addition to 10 dB as the average received SNR (i.e., the desired signal power is 10 times greater than the noise power), two other values are evaluated; 7 dB (i.e., the desired signal power is 5 times greater than the noise power), and 13 dB (i.e., the desired signal power is 20 times greater than the noise power) to see how they affected system performance. Figure 3.6 shows the performance of the both relaying systems in deterministic and fading environments, with the average received SNR varied. This 2D slice runs along relays line (i.e., vertical axis). On the other hand, power allocation is the main factor in determining the level of secrecy capacity. Figure 3.7 illustrates the effect of changing the allocated power on the secrecy performance in a deterministic environment.

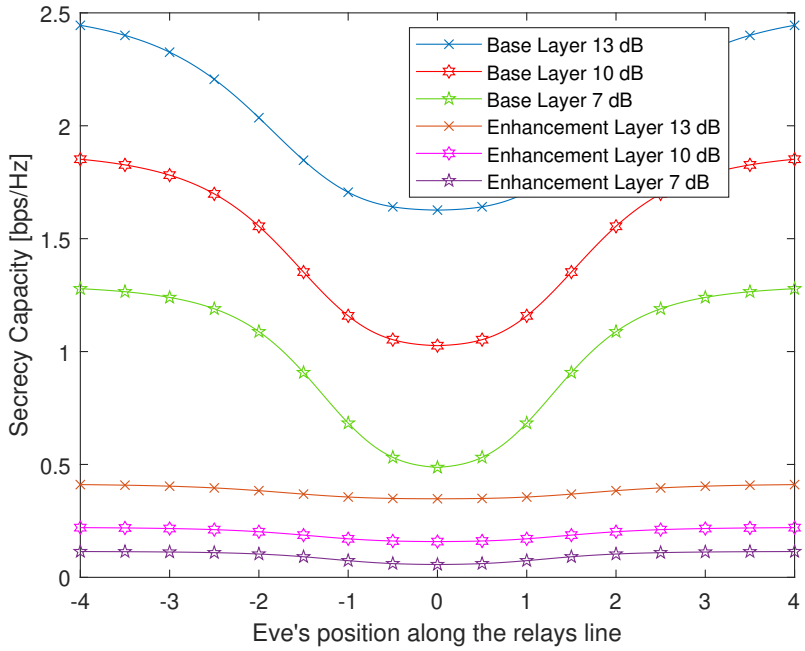


Figure 3.6: Secrecy performance for SC scheme in Rayleigh fading environment with multiple average received SNR, represented by a 2D vertical slice.

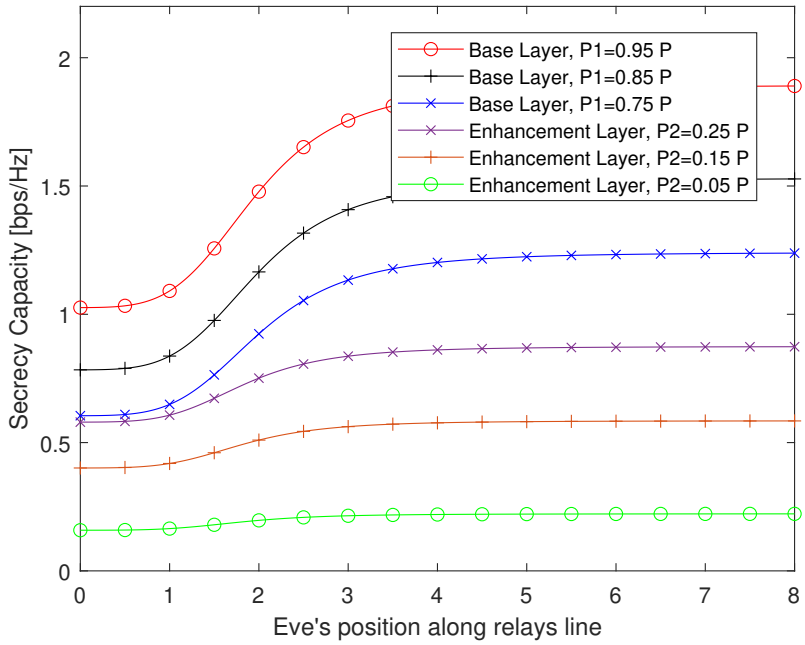


Figure 3.7: Secrecy performance for SC scheme in deterministic environment at 10 dB average received SNR with variable power allocation for the base and enhancement layers, represented by a 2D horizontal slice.

3.3.2 Relative Secrecy Capacity

The percentage of the secrecy capacity over the intended receiver's capacity is known as relative secrecy capacity. Although the base layer of the SC scheme has a higher level of secrecy capacity than the enhancement layer, the opposite is true in terms of relative secrecy capacity. For example, in the fading environment, when Eve's position is fixed at (0.8, 2) coordinates and the ergodic secrecy capacity is measured, the enhancement layer achieves 88% relative secrecy capacity, while the base layer achieves 80%. This result indicates that Eve's position has a smaller impact on the enhancement layer than on the base layer.

3.4 Summary

In this chapter, we looked at successive relaying wireless network with layered transmission via superposition coding in a SISO setting with two half-duplex relays in amplify-and-forward strategy. To improve physical layer security, two techniques were proposed: IRI is used to confuse the eavesdropper while it is mitigated at the desired receiver, and power control is used to cancel the fading effect from both relays to the desired receiver and thus increase the secrecy capacity of the main channel.

The power allocation of each data layer determined the level of secrecy capacity and provided flexible security configuration to different layers using the rate splitting concept. In successive relaying, the proposed PLS scheme clearly outperforms the conventional relaying system, even when the eavesdropper is closer to the relays.

Chapter 4

Conclusions

This chapter provides an overview of the contributions in this thesis and suggestions for future works on this topic. Section 4.1 discusses the contributions of this thesis while Section 4.2 suggests potential future work.

4.1 Thesis Contributions

In this work, we investigated the applicability of the SISO setup in two-path AF relaying system to protect intended receiver's data from being reliably decoded by an eavesdropper even if the channels between the relays and the intended receiver are worse than the channels between the relays and the eavesdropper. The proposed scheme protects data confidentiality under the condition that the channels between the relays and the intended receiver are unknown to the unauthorized user. With this assumption, the intended receiver can remove the IRI while the eavesdropper's channel becomes noisier. This latter effect is similar to AN technique in PLS, in which confidential signals to the legitimate receiver are simultaneously transmitted with AN to eavesdroppers in order to perturb the intercepted signals. The difference here is that the IRI consumes no additional system resources such as power or bandwidth because it is already built into the system's operation. To cancel the IRI by exploiting its structure at any receiver, the knowledge of channel gains between the relays to the legitimate receiver, i.e., CSI, is required. With the relays having access to this information based on the reciprocity assumption, power control tracking changes in signal strength makes channel gain estimation at the eavesdropper impossible. To

characterize the performance limits for secure transmissions in noisy channels, the standard definition for the secrecy capacity is used, which is given by the maximum of (i) difference between the capacity of the main channel and the capacity of the eavesdropper's channel and (ii) zero (actually its average value at given positions of relays, destination, and eavesdropper). Channel fading has a positive impact on secrecy capacity and rate adaptation based on the main channel's CSI, as demonstrated in the thesis.

Another measure that can enhance the secrecy capacity is network coding (NC). In one-way flow, NC is applicable by performing XOR operation on the bit level between each two consecutive packets, after which the coded packet is transmitted. At the receiver, XOR operation is performed between the coded packet and the previous decoded massage. The first packet on the transmitter is XORed with a predefined number or PSNG, and the same is done at the receiver.

In addition to the impact of IRI on the eavesdropper's signal detection capability, the signals design with multiple quality layers via SC is considered in this work to support different secrecy rates for different data streams. This is done with the goal of providing flexible security-level configurations and QoS by allocating power to different sub-streams (layers). The security performance of SC which is a form of power-domain NOMA is aided, in addition to IRI, by layers of lower power which are decoded last in the SIC detectors.

Considering the secrecy capacity as a performance measure, it has been demonstrated that the proposed scheme in two-path successive relaying system outperforms the conventional, one relay, system even when the eavesdropper is closer to the relay(s). Also, we demonstrated that the superposition coding scheme provides different secrecy capacities for different data streams based on the allocated power to each stream.

4.2 Suggested Future Work

In this section some potential future work has been suggested.

1. Multiple Access Channel

In this thesis, we only considered the broadcast channel, where one transmitter can send a signal to multiple receivers. Therefore, there is an opportunity to investigate the multiple access channels, where multiple transmitter send their signals to one receiver, in order to exploit the possibility of improving secrecy capacity.

2. Synchronization of Nodes

In this thesis, one of our general assumptions was that user nodes have the same distance from the relay and all message transmissions are perfectly synchronized. While there are methods and network protocols to achieve synchronous operations, some technologies like OFDM which the symbol rate is very low at each subcarrier can be a solution to this problem. Due to different distances between nodes in real life scenarios, this may impose the challenge because of the variability in the propagation delays of the signals.

3. Imperfect CSI

In this study, we assumed that perfect CSI is instantaneously available to all nodes so that fading channel coefficient can be calculated to use power control. However, in practical applications, CSI is usually estimated at receivers and sent to transmitters which would cause delay and inaccuracy of CSI. Although this problem has been well studied by researchers in other schemes on how to overcome this problem [37]–[39], but it is important to understand the performance limits of the proposed schemes.

4. Generalize Multi-Layer Transmissions

In superposition coding, two data streams were superimposed and investigated in terms of secrecy enhancement; there is an opportunity to explore superimposing more

than two data streams in one signal and allocate the optimal power to each data stream (layer). Based on the nature of the data stream (i.e., audio, video, text, etc), this can provide flexible security-level configurations.

Appendix A

IRI Cancellation in Two-Path Successive Relaying

In two-path successive relaying system, a full interference cancellation algorithm to remove the IRI in a SISO setting is proposed in [7], same assumptions that are stated in Section 2.1 are considered, at TS t, R_1 listens and R_2 transmits.

Using AF strategy, the forwarded signal from R_2 can be represented as:

$$s_{R_2}(t) = g_{R_2} y_{R_2}(t-1), \tag{A.1}$$

where $y_{R_2}(t-1)$ is the received signal at R_2 at TS $t-1$ which is given by:

$$y_{R_2}(t-1) = h_{AR_2} s(t-1) + h_{RR} g_{R_1} y_{R_1}(t-2) + n_{R_2}(t-1). \tag{A.2}$$

The signal received at the destination B is given by:

$$y_B(t) = h_{R_2B} g_{R_2} y_{R_2}(t-1) + n_B(t). \tag{A.3}$$

Substituting (A.2) into (A.3) gives:

$$y_B(t) = h_{R_2B} g_{R_2} h_{AR_2} s(t-1) + h_{R_2B} g_{R_2} h_{RR} s_{R_1}(t-1) + h_{R_2B} g_{R_2} n_{R_2}(t-1) + n_B(t). \tag{A.4}$$

Note that at TS $t-1$, R_1 transmits and R_2 listens, where $s_{R_1}(t-1) = g_{R_1} y_{R_1}(t-2)$ similar to (A.1), and

$$y_B(t-1) = h_{R_1B} s_{R_1}(t-1) + n_B(t-1), \tag{A.5}$$

or we have:

$$s_{R_1}(t-1) = \frac{y_B(t-1) - n_B(t-1)}{h_{R_1B}}. \tag{A.6}$$

Finally substituting (A.6) into (A.4) gives:

$$y_B(t) = h_{R_2B} g_{R_2} h_{AR_2} s(t-1) + \frac{h_{R_2B} g_{R_2} h_{RR}}{h_{R_1B}} y_B(t-1) + n'(t), \tag{A.7}$$

where $n'(t)$ is the noise term which is given by:

$$n'(t) = h_{_{R_2B}} g_{_{R_2}} n_{_{R_2}}(t-1) + n_{_B}(t) - \frac{h_{_{R_2B}} g_{_{R_2}} h_{_{RR}}}{h_{_{R_1B}}} n_{_B}(t-1). \tag{A.8}$$

With the above derivations, the IRI now appears as a single recursive term, i.e., the second term of the right-hand side of (A.7), in the received signal at the destination. Therefore, the IRI can be simply by subtracting $\frac{h_{_{R_2B}} g_{_{R_2}} h_{_{RR}}}{h_{_{R_1B}}} y_{_B}(t-1)$ from (A.7) which is given by:

$$y'_{_B}(t) = h_{_{R_2B}} g_{_{R_2}} h_{_{AR_2}} s(t-1) + n'(t). \tag{A.9}$$

It is clear that (A.9) is IRI free, with only the desired signal (though one TS late) and the noise being present. The transmission data can be easily detected from (A.9).

Bibliography

[1] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, *Signal processing approaches to secure physical layer communications in multi-antenna wireless systems*, ser. Springer Briefs in electrical and computer engineering. Springer, 2013.

[2] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Select. Areas Commun.*, vol. 36, no. 4, pp. 679–695, 2018.

[3] 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.

[4] H.-M. Wang and T.-X. Zheng, *Physical Layer Security in Random Cellular Networks*, 1st ed. Springer, 2016.

[5] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inform. Theory*, vol. 50, no. 12, pp. 3062–3080, 2004.

[6] R. Alsakarnah and J. Ilow, "Superposition coding in alternate DF relaying systems with inter-relay interference cancellation," in *IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2017.

[7] C. Luo, Y. Gong, and F. Zheng, "Full interference cancellation for two-path cooperative communications," in *WCNC*, April 2009, pp. 1–5.

[8] F. Alhumaidi and J. Ilow, "Alternate AF MIMO relaying systems with full inter-relay interference cancellation," in *IEEE 82nd VTC*, 2015.

[9] Qian Yu Liau and Chee Yen Leow, "Physical layer security in two-path successive relaying," in *IEEE 20th International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD)*, 2015.

[10] Y. Zou and J. Zhu, *Physical-Layer Security for Cooperative Relay Networks*. Springer, 2016.

[11] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE 62nd VTC*, vol. 3, 2005, pp. 1906–1910.

[12] A. Nosratinia, T. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 74–80, Oct 2004.

[13] 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.

[14] H. Wicaksana, S. H. Ting, C. K. Ho, W. H. Chin, and Y. L. Guan, "AF two-path half duplex relaying with inter-relay self interference cancellation: diversity analysis and its improvement," *IEEE Trans. Wireless Commun.*, vol. 8, no. 9, pp. 4720–4729, 2009.

[15] K. Park and M. Alouini, "Alternate MIMO relaying with three AF relays using interference alignment," in *IEEE ICC*, 2012.

[16] F. Alhumaidi and J. Ilow, "Transmitter precoding to cancel inter-relay interference in af systems with successive transmissions," in *IEEE CCECE*, 2016.

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

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

[19] T. Rappaport, *Wireless Communications: Principles and Practice*. Prentice Hall PTR, 2001.

[20] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inform. Theory*, vol. 50, no. 12, pp. 3062–3080, 2004.

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

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

[23] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proceedings of the National Academy of Sciences*, vol. 114, no. 1, pp. 19–26, 2017. [Online]. Available: https://www.pnas.org/content/114/1/19

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

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

[26] L. Sun and Q. Du, "A review of physical layer security techniques for Internet of Things: Challenges and solutions," *Entropy*, vol. 20, no. 10, 2018.

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

[28] T. Cover, "Broadcast channels," *IEEE Trans. Inform. Theory*, vol. 18, no. 1, pp. 2–14, 1972.

[29] K. Ramchandran, A. Ortega, K. M. Uz, and M. Vetterli, "Multiresolution broadcast for digital hdtv using joint source/channel coding," *IEEE Journal on Selected Areas in Communications*, vol. 11, no. 1, pp. 6–23, 1993.

[30] M. Schaar and P. Chou, *Multimedia Over IP And Wireless Networks*, 01 2007.

[31] Y. Liu, W. Wang, M. Peng, and S. Zhu, "Optimized layered multicast with superposition coding in cellular systems," *Wireless Communications and Mobile Computing*, vol. 12, no. 13, pp. 1147–1156.

[32] J. A. Cabrera G., M. V. Pedersen, and F. H. Fitzek, "Chapter 9 - network coding," in *Computing in Communication Networks*, F. H. Fitzek, F. Granelli, and P. Seeling, Eds. Academic Press, 2020, pp. 169–195.

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

[34] A. Salem and C. Masouros, "Rate splitting approach under psk signaling using constructive interference precoding technique," in *IEEE WCNC*, 2019.

[35] M. A.-H.-A. Abuyaghi and J. Ilow, "Enhancing Secrecy Capacity in Alternate AF Relaying Networks with Inter-Relay Interference," in *WS19: IEEE ICC 2021 Workshop on 5G and Beyond Wireless Security*, Montreal, Canada, June 2021.

[36] L. Wang, E. Şaşoğlu, B. Bandemer, and Y. Kim, "A comparison of superposition coding schemes," in *IEEE International Symposium on Information Theory*, 2013.

[37] S. Narmatha, R. Jeyanthi, and N. Malmurugan, "Amplify and forward relay network optimization with imperfect CSI," in *2nd ICECS*, 2015, pp. 469–473.

[38] R. Mo, Y. H. Chew, and C. Yuen, "Information rate and relay precoder design for amplify-and-forward MIMO relay networks with imperfect channel state information," *IEEE Trans. Vehicular Technol.*, vol. 61, no. 9, pp. 3958–3968, 2012.

[39] M. Chen, T. C. . Liu, and X. Dong, "Opportunistic multiple relay selection with outdated channel state information," *IEEE Trans. Vehicular Technol.*, vol. 61, no. 3, pp. 1333–1345, 2012.